CRIMINAL ABUSE OF NON-TRADITIONAL PAYMENT METHODS:

A COMPARATIVE ANALYSIS OF THE APPLICATION OF ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING FRAMEWORKS IN THE UNITED KINGDOM, UNITED STATES AND AUSTRALIA

Thesis submitted in accordance with the requirements of the University of Liverpool for the degree of Doctor of Philosophy (Ph.D.).

By

Matthew Robert Shillito

September 2016

THIS PAGE IS INTENTIONALLY BLANK

Contents

Acknowledgements

I am indebted to my primary supervisor, Dr Rob Stokes, were it not for him spotting my potential for doctoral research whilst I was a student on the International Business Law (LL.M) programme, this journey may not have begun. Rob's support and encouragement (as well as his ability to spot the need for a coffee or lunch break) have kept me going through the many ups and downs of this thesis. I will always be grateful to him for giving me this opportunity. I would also like to express my gratitude to my secondary supervisor, Professor Anu Arora, her support has also played a significant part in this thesis coming to fruition.

Alongside my supervision team, I am also very fortunate to have received support from my 'Equity Parents', Professor Debra Morris and Professor Warren Barr. They have played a key role in my development as both a researcher and a lecturer in law. Thanks should also be given to all other Liverpool Law School staff members (past and present) who have fostered an excellent research culture and environment, of which, I am proud to be a part.

It would be impossible to thank all of those who I owe a debt of gratitude in the writing of thesis, but I would also like to thank Dr Stephanie Reynolds and Dr John Fanning for their friendship and support, they have been brilliant role models to follow. I would also like to thank, Brett Crumley, he was an excellent help and sounding board for ideas in the closing stage of this thesis. My gratitude must also be extended to Neil, Jonny, Dan, Ste and Maffus who have kept my spirits high through plenty of beers, pizzas and carveries. I must also express my thanks to Anth and Jason for their yearly visits from Newcastle, the end of this thesis will mark 9 years in Liverpool for me and our friendship is as strong as ever. I have enjoyed many gigs, football matches, drinks and chats with them both, long may it continue.

Finally, and most importantly of all, I would like to thank my family, in particular my Mam, Dad, and Sister. They have shared the trials and tribulations of this thesis more than most. To them I would like to dedicate this thesis.

Matthew Robert Shillito

September 2016, Liverpool.

Acronyms list

ACC – Australian Crime Commission

ACIC – Australian Criminal Intelligence Commission

AFMLS – Asset Forfeiture and Money Laundering Section

AFP – Australian Federal Police

AGD – Attorney General's Department

AIC – Australian Intelligence Community

AML – Anti-Money Laundering

ARA – Assets Recovery Agency

AUSTRAC – Australian Transaction Reports and Analysis Centre

BCCVE – Bureau of Counterterrorism and Countering Violet Extremism

CDD – Customer Due Diligence

CPS – Crown Prosecution Service

CTF – Counter-Terrorist Financing

CTIF – Counter-Terrorism Implementation Task Force

CTR – Currency Transaction Report

CTS – Counter-Terrorism Section

DEA – drug enforcement agency

DFAT – Department of Foreign Affairs and Trade

DOJ – The Department of Justice

DOS – The Department of State

EB – Bureau of Economic and Business Affairs

EU – European Union

FATF – Financial Action Task Force

FBI – Federal Bureau of Investigation

FCA – Financial Conduct Authority

FinCEN – Financial Crimes Enforcement Network

FIU – Financial Intelligence Unit

FSRB – FATF-Style Regional Body

GPML – Global Program against Money Laundering

IMF – International Monetary Fund

IMVTs – Informal Value Transfer Systems

INL – Bureau of International Narcotics and Law Enforcement Affairs

IRS-CI – Internal Revenue Service Criminal Investigation

JMLIT – Joint Money Laundering Intelligence Taskforce

JMLSG – Joint Money Laundering Steering Group

KYC – Know Your Customer

MSB –Money Service Business

NCA – National Crime Agency

NCIS – National Criminal Intelligence Service

NPPS – New Payment Products and Services

NTPMs – Non-Traditional Payment Methods

OFAC – The Office of Foreign Assets Control

OIA – The Office of Intelligence and Analysis

RBA – Risk-Based Approach

SAR – Suspicious Activity Report

SEC – Securities and Exchange Commission

SVCs – Stored Value Cards

TEOAF – Treasury Executive Office for Asset Forfeiture

TFFC – The Office of Terrorist Financing and Financial Crime

TFI – The Office of Terrorism and Financial Intelligence

UK – United Kingdom

UN – United Nations

UNODC – United Nations Office on Drugs and Crime

US – United States of America

Thesis Abstract

The Criminal Abuse of NTPMs for the Purposes of Money Laundering and Terrorist Financing

This doctoral thesis is concerned with the application of the international framework for anti-money laundering and counter-terrorist financing to the threats emerging from the criminal misuse of non-traditional payment methods. The international framework plays a significant role in the development of national responses to money laundering and terrorist financing, it is therefore important to understand how it, and then individual countries have responded to this emerging threat. The thesis will explore three developed economies, with advanced anti-money laundering and counter terrorist financing frameworks, they are: the UK, the US and Australia. From these countries best practices and deficiencies will be identified.

This thesis will examine five NTPMs and outline the money laundering and terrorist financing risks associated with them. It will then Identify and analyse the relevant parts of the international AML and CTF framework, in relation to NTPMs. The analysis that follows will be broken down into the following thematic headings:

1. Global Role and Implementation of the International Framework;
2. Competent Authorities;
3. Application of the Risk-based Approach;
4. Preventive measures;
5. Confiscation of the Proceeds of Crime; and
6. Mutual Legal Assistance.

Following on from this it will assess the compliance of three case study countries with the parts of the international AML and CTF framework that are relevant to NTPMs. The abuse of NTPMs, whilst still an emerging trend, are likely to increase in frequency and evolve in nature,

in the coming years. It is therefore important to know how both the international framework and national responses adapt to these emerging challenges. For these reasons the area is worthy of academic consideration.

Chapter 1 - Introduction

Money Laundering, Terrorist Financing, and the Increasing Prominence of the Abuse of Non-Traditional Payment Methods

"The perception that still endures of money launderers is of a suspicious character turning up at the counter of a bank with a suitcase (probably helpfully labelled 'swag') overflowing with used notes."[1]

1.1. Money Laundering – An Introduction

There is a lack of an authoritative definition of money laundering, principally due to the complexities of the process. One definition that is commonly cited in the literature is Lilley's:

'Laundering is the method by which all proceeds of crime are integrated into the banking systems and business environments of the world… This is the process whereby the identity of dirty money that is the proceeds of crime and the real ownership of these assets is transformed so that the proceeds appear to originate from a legitimate source.'[2]

Where academics have provided further definitions they tend to follow on a similar vein to Lilley. Popa states money laundering is 'the cleaning of dirty money which is a necessity for

[1] Peter Lilley, *Dirty Dealing – The Untold Truth about Global Money Laundering* (3rd edn, Kogan Page, 2006), xii preface.

[2] ibid 6.

any profit generating criminal activity.'[3] Whilst Ryder states: 'money laundering is the illegal process or act by which these individuals or groups attempt to disguise, hide or distance themselves from their illegal activities.'[4] Unger's definition is quite succinct: 'it is the mechanism used to legitimise the profits of criminal activities, so that the criminal can use them without detection.'[5]

Whilst the above definitions of money laundering are helpful in terms of encapsulating the process – giving a short, pithy description of the crime – they do not capture the essence of process itself. It is notable that the Financial Action Task Force (FATF), the international standard setter for anti-money laundering (AML) and counter-terrorist financing (CTF), has avoided giving such a concise definition. Instead, they define money laundering by reference to its constituent parts: aims, process (placement, layering, and integration), typologies, and motivations.[6] The above definitions are captured within the FATF's definition when they note, money laundering is 'the processing of criminal proceeds to disguise their illegal origin'.[7] The approach taken by the FATF has been endorsed by several other bodies such as the IMF and the World Bank.

In terms of the process of laundering, as recognised by the FATF, it can be split into three stages: placement, layering and integration.[8] These stages assist the launderer in their

[3] Camelia Popa, 'Money Laundering using the internet and electronic payments' (2012) 17(8) *Metalurgia International* 219, 219.

[4] Nicholas Ryder, *Money Laundering: An endless cycle* (1st edn, Routledge 2012), 1.

[5] Brigitte Unger, *The scale and impacts of money laundering* (1st edn, Edward Elgar 2007), 21.

[6] Financial Action Task Force, 'Frequently Asked Questions' <http://www.fatf-gafi.org/faq/moneylaundering/> accessed 22 September 2016.

[7] Ibid.

[8] M. Cole, 'Money Laundering' (1993) 8(4) *Journal of International Banking Law*, 129, 129.

attempt to disguise, hide or distance the funds from their illegitimate origin.[9] In their efforts to complete the three stages, money launderers: disguise the source, change the form, or move the money to a place where it is less likely to attract attention.[10] The result is that money laundering has become known as the secret phenomenon.[11] It is only once these stages are complete, that the launder can realise their ill-gotten gains, without fear of them being frozen, seized or confiscated for being the proceeds of crime. In other words, the three stage process breaks the paper trail between the origin of the funds and their later use by the criminal. In order to better understand this, it is necessary to explicate each of the three stages.

The placement stage is the first part of the money laundering process that the criminal goes through in his attempt to make his ill-gotten gains appear legitimate. At this stage, the launderer places the proceeds of the illegal activity into the financial system. This includes but is not limited to: the use of banks, high value goods acquisition, and the acquisition of property and other assets. It is at this stage that the launderer should be the most concerned about their funds. They are at their most vulnerable to detection.[12] A sophisticated method used at this stage by the launderer in an attempt to avoid detection is the process of smurfing[13].

---

[9] Financial Action Task Force, 'Frequently Asked Questions' (n.6).

[10] Ibid.

[11] Unger (n.5).

[12] M. Cole, 'Money Laundering' (1993) 8(4) *Journal of International Banking Law*, 129, 129; and Angela Samantha Maitland Irwin, Kim-Kwang Raymond Choo, and Lin Liu, 'An Analysis of Money Laundering and Terrorist Financing Typologies' (2011) 15(1) Journal of Money Laundering Control 85, 87.

[13] Smurfing is the process of breaking down large cash deposits into a number of smaller deposits in an attempt to evade detection. (See: Előd Takáts, 'A Theory of "crying wolf'': The Economics of Money Laundering Enforcement' (2007) International Monetary Fund Working Paper 07/81, < https://www.imf.org/external/pubs/ft/wp/2007/wp0781.pdf > accessed 22

Once the illegitimate funds have been placed into the system successfully, the launderer needs to begin to lose the trail, this is the layering stage. If the trail is not lost, then the illegitimate source of the funds will be detected. At this stage the funds are transferred or converted numerous times in an attempt to conceal their origins.[14] The more times the funds are transferred or converted the further they get from the original source. If the paper trail still exists, it is this stage where the launderer seeks to lose it, hence the large volume of transactions which take place. It is during this stage that the criminal is likely to use sophisticated, often technologically advanced, methods from moving the funds in order to assist in breaking the paper trail.[15] Traditionally, money launderers have used methods such as offshore limited companies as a means for 'layering' the funds which they are laundering.[16] However, this stage of the process has developed considerably in recent years due to both globalisation and technological advances. These have permitted launderers to complete the layering stage process with less effort.[17] If this stage is fulfilled, following numerous

September 2016). However, if the bank spots such methods in practice it may make a suspicious activity report based on the possibility of smurfing. (B. Unger and F. van Waarden, 'Attempts to Dodge Drowning in Data: Rule- and Risk-Based Anti Money Laundering Policies Compared' (2009), TKI Working Paper 09-19 <http://dspace.library.uu.nl/bitstream/handle/1874/309920/09_19_2.pdf> accessed 22 September 2016). This is dependent on someone spotting the trend.

[14] Kern Alexander, 'The International Anti-Money Laundering Regime: The Role of the Financial Action Task Force' (2001) 4(3) *Journal of Money Laundering Control* 231, 233.

[15] See the FATF Typology Reports for more information on different methods used for layering. Examples available from here: <http://www.fatf-gafi.org/publications/methodsandtrends/?hf=10&b=0&s=desc(fatf_releasedate)> accessed 22 September 2016.

[16] Jonathan Fisher and Jane Bewsey, 'Laundering the Proceeds of Fiscal Crime' (2000) 15(1) J.I.B.L. 11, 19.

[17] See for examples: Financial Action Task Force, *Vulnerabilities of Casinos and Gaming Sector* (March 2009) <http://www.fatf-gafi.org/media/fatf/documents/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf> accessed 22 September 2009; Financial Action Task Force, 'Money

deliberately confusing trails, then the chances of detection are significantly reduced.[18] It is because of these increasingly sophisticated methods, which facilitate the growing cross border element of money laundering, that it is referred to as a 'crime of globalisation.'[19] This global nature of the crime necessitates both the global (which will be seen in chapter 2) and the national (chapters 3, 4, and 5) response.

Once the layering process is complete, the final step for the launderer is to integrate the funds back into the formal financial system. If the first two stages have been efficacious, then the launderer will have lost the paper trail and be able to integrate the funds and enjoy the rewards of their ill-gotten gains, without the risk of detection.

The best chance of success for any AML regime is to catch the funds as early as possible.[20] The further they get through the money laundering process the harder they become to

---

Laundering through Money Remittance and Currency Exchange Providers' (June 2010) <http://www.fatf-gafi.org/media/fatf/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf> accessed 22 September 2016; Financial Action Task Force, *The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing* (October 2013) <http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf> accessed 22 September 2016; Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* (June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 22 September 2016; and Financial Action Task Force, *Emerging Terrorist Financing* Threats (October 2015) <http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf> accessed 22 September 2016.

[18] Joan Wadsley, 'Money Laundering: Professionals as Policemen' (1994) July/August *Conveyancer and Property Lawyer* 275, 277.

[19] Michael Levi, 'Crimes of Globalisation: Some Measurement Issues' in Matti Joutsen, 'New Types of Crime: Proceedings of the International Seminar Held in Connection with HEUNI's Thirtieth Anniversary' (1st edn, European Institute for Crime Prevention and Control, 2012), 107-115.

[20] Cole (n.12).

detect, especially if they get past the layering stage as it is likely the paper trail will have been lost. As will be seen in chapter 2, the international framework has placed a lot of effort into stopping the funds at the placement and layering stages through preventive measures such as customer due diligence (CDD), but also through detection methods like Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs).

In terms of how much money is laundered per year, it is difficult to give a precise total due to the complex and secretive nature of the process.[21] As the amount of money that is laundered each year cannot be qualified absolutely, it is considered to be part of the shadow economy. The FATF has estimated that the annual amount of money laundered is around $590 billion to $1.5 trillion.[22] This estimate has been repeated by institutions such as the FBI;[23] however there have been other estimates. At the lower end of the scale the UN has estimated that it is simply around $500bn a year.[24] Whilst the International Monetary Fund (IMF) estimates that it is in fact 2 to 5 per cent of global GDP.[25] The United Nations Office on Drugs and Crime (UNODC) produced a report in 2009, which placed the figure at $1.6 trillion (or 2.7 per cent of GDP)[26] therefore supporting the IMF estimate. On the basis of such figures it has been

[21] Herbert V. Morais, 'Fighting International Crime and its Financing: The Importance of Following a Coherent Global Strategy Based on the Rule of Law' (2005) 50 *Villanova Law Review* 583, 591.

[22] Financial Action Task Force, 'Frequently Asked Questions' (n.6).

[23] Ibid.

[24] Phyllis Soloman, 'Are Money Launderers All Washed Up in the Western Hemisphere? The OAS Model Regulations' (1994) 17 *Hastings International and Comparative Law Review* 433, 434.

[25] Financial Action Task Force 'Frequently Asked Questions' (n.6).

[26] United Nations Office on Drugs and Crime, 'Illicit Money: How Much is Out There?' <http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html> accessed 22 September 2016.

stated that money laundering is the world's third largest industry.[27] However, despite it being such a significant problem, efforts to counter it have thus far been far from successful. 'Less than 1 per cent of global illicit financial flows are currently being seized and frozen.'[28]

1.2. Terrorist Financing – An Introduction

Terrorist organisations evolve and adapt over time, what does not change is their need to raise, move and use funds.[29] Terrorist financing is not defined in any sort of meaningful way, with all definitions being construed broadly and hindered by a lack of clarity as to what constitutes 'terrorism' itself. The UK Charity Commission has defined terrorist financing as: '*The raising, moving, storing and using of financial resources for the purposes of terrorism.'*[30] The European Commission also provide a similar definition of terrorist financing: *'The provision or collection of funds, by any means, directly or indirectly, with the intention or in the knowledge that they would be used in order to carry out terrorist offences.'*[31] Not only does it encapsulate the donation of finance for terrorist purposes, but also fundraising, and even more broadly the moving and using of property for the purposes of terrorism. It is both

---

[27] Jeffrey Robinson, 'Laundrymen: Inside the World's Third Largest Business' (2nd edn, Pocket Books, 1998), 4.

[28] United Nations Office on Drugs and Crime, *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organised Crimes (Research report)* (October 2011), 5. Available at: <http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf> accessed 22 September 2016.

[29] Financial Action Task Force, *Emerging Terrorist Financing Risks* (October 2015), 5. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf> accessed 22 September 2016.

[30] Charity Commission, *Protecting Charities from Harm: Compliance Toolkit – Chapter 1, Module 1* (2013), 3. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/396183/CT-1-M1.pdf> accessed 22 September 2016.

[31] European Commission, 'Frequently Asked Questions: Anti-Money Laundering' <http://europa.eu/rapid/press-release_MEMO-13-64_en.htm?locale=en> accessed 22 September 2016.

conceptually and practically different to money laundering. The aim of terrorist financing is to channel funds to the end terrorist (or terrorist organisation) with the aim of 'encouraging, planning, assisting or engaging in acts of terrorism.'[32]

Like money laundering, the process of terrorist financing can be split into its constituent parts; the initial stage is the sourcing of resources; that is followed by the distribution and transfer of those funds. To combat terrorist financing the international framework tackles these two areas.[33] Whilst the transfer stage shares many similarities with the money laundering process, and is why this thesis considers both crimes, the rest of this section, in outlining the process of terrorist financing, will demonstrate some significant differences between the two crimes. These differences make tackling terrorist financing at best difficult and at worst virtually impossible.

There is no successful organisation without successful financing,[34] terrorist organisations are no exception to that rule. However, the way in which a terrorist organisation sources its funds are many and varied. Broadly speaking there are seven recognised categories: lone wolf, state sponsored, franchise, bundled support, state sponsoring, shell state, and transnational corporation.[35] It is important, that when considering terrorist funds, that the variety of

[32] Angela Samantha Maitland Irwin, Kim-Kwang Raymond Choo, and Lin Liu, 'An Analysis of Money Laundering and Terrorist Financing Typologies' (2011) 15(1) Journal of Money Laundering Control 85.

[33] Jae-myong Koh, *Suppressing Terrorist Financing and Money Laundering* (1st edn, Springer, 2011), 25.

[34] Ibid, 11.

[35] Ibid, 9.

sources are considered. Indeed, the numerous sources of funding provide an issue for legislators owing to their differing characteristics.[36]

The most worrying and prevalent form of finance for terrorism is self-finance, this is typical of the 'lone wolf' terrorist. It is hard for the counter-measures to spot this level of terrorist financing because the attacks are often small meaning that they need little funding[37], and any funding they do need is often internally generated. Indeed it has been noted that they are often only detected once they have committed an attack.[38]This in itself does not make the current framework futile, although it does further support the theory that anti-money laundering strategies are not always the most effective mechanism for countering terrorist financing. The current system, does mean that, if the funds have been identified as being terrorist funds, then it is possible to trace them back to their source. This is valuable as it can assist in identifying typologies and red-flags for future instances of terrorist financing. The worry is that the funds are not identified as being terrorist funds until after an attack has taken place, meaning that whilst information gained is useful for the prevention of future attacks, the framework itself is not effective in preventing terrorist attacks outright.

In terms of financial power, state-sponsored terrorism is a challenging source of funding and was the traditional method of financing for terrorist groups.[39] Under this category, the

[36] R.E. Bell, 'The Confiscation, Forfeiture and Disruption of Terrorist Finances' (2003) 7(2) *Journal of Money Laundering Control* 105, 107.

[37] Jodi Vittori, *Terrorist Financing and Resourcing* (1st edn, Palgrave Macmillan, 2011), 7.

[38] Beau D. Barnes, 'Confronting the One-Man Wolf Pack: Adapting Law Enforcement and Prosecution Responses to the Threat of Lone Wolf Terrorism' (2012) 92 *Boston University Law Review* 1614, 1615.

[39] See: Ilias Bantekas, 'The International Law of Terrorist Financing' (2003) 97 *American Journal of International Law* 315, 316; and Nimrod Raphaeli, 'Financing of Terrorism: Sources, Methods, and Channels' (2003) 15(4) Terrorism and Political Violence 59.

terrorist group receives all its funding from the state involved, but also gains sanctuary from that state.[40] This is problematic as it means that whilst it is obvious where the terrorist organisation are getting their funds from, it is difficult to prevent them receiving it. The state involved provides a safe haven for the terrorist organisation (or part of it) and the strength of the funding may be considerable given the resources of a whole country. An example of this kind of funding was the Libyan government's central role in the 1986 terrorist attacks against the US service members in a West Berlin disco.[41] This kind of financing was a pressing issue in the 1970s and 1980s,[42] but it is no longer prevalent due to the effect of the international framework's counter measures (outlined in chapter 2). Further, measures such as the US list of States sponsoring terrorism[43] have also helped to reduce the amounts of states involved, whilst terrorists are also no longer reliant on state sponsored terrorism due to the prevalence of other forms of terrorist financing.[44]

Shell state terrorist organisations can be challenging for comparable reasons to state sponsored terrorism, they raise their finance through taking control of an area and exploit it for resourcing[45], again this makes the funds easy to spot but hard to control.

The other main way in which terrorist organisations receive their funding is through mixed sources;[46] this is typical of terrorist groups labelled which can be labelled as 'franchise' or

[40] Vittori (n.37), 7.

[41] Ibid.

[42] Anne C. Richard, *Fighting Terrorist Financing: Transatlantic Cooperation and International Institutions,* (1st edn, Centre for Transatlantic Relations, 2006), 6.

[43] Ibid, 5.

[44] Ibid, 6.

[45] Vittori (n.37), 8.

[46] This is true of franchise terrorist organisations and also of bundled support organisations.

'bundled support'. The fact that the organisation receives its funding from several sources is particularly problematic for the AML/CTF Framework, as whilst it might detect and cut off one form of funding, the organisation will be able to continue its work through funding from one its other revenue sources. Both 'franchise' and 'bundled support' terrorist organisations rely on pleasing their sponsors to maintain their levels of resourcing. With regards to the franchise approach it means that if the major sponsor pulls their support the terrorist organisation will still be able to continue.

One of, if not the most significant, challenges for the AML/ CTF framework in curbing the threat of terrorism comes from the fact that the funds utilised by a terrorist organisation may come from wholly legitimate sources. The funds may appear no different from other funds and further, it is infinitely more challenging to decipher whether funds are to be used for criminal purposes rather than identifying if they derive from such activity. So whilst some instances of terrorist financing will be detected as money laundering, it is likely that many instances will not. This challenge is further compounded by the rise of so called 'cheap-terrorism' meaning that even where the funds are illegitimate the size of the transfer can appear innocuous and mean that it evades detection.

In terms of the transfer and distribution stage of terrorist financing, this involves getting the funds from the source and placing them with the terrorist organisation. This process may involve some of the techniques which are seen at the 'placement' and 'layering' stage of money laundering. Terrorist financers and terrorist organisations may embrace alternative methods of transfer, as found with money launderers, in order to evade detection. Although, as noted above, as the funds may be legitimate or small in value, it is not necessarily of as much use for terrorist financers, as it is for money launderers, to utilise NTPMs. Where NTPMs

are utilised by terrorist financers, Hawala[47] is one of the main mechanisms which is used to avoid detection and transfer money. Schramm and Taube noted that the Hawala system 'is well prepared to elude surveillance and regulation by anti-terrorist groups.'[48]

Whilst as noted above, money is the lifeblood of terrorist organisations, it is more challenging, and less worthwhile to quantify the amount of funds moved for terrorist purposes than money laundering. Any attempted estimates would be hampered for several reasons. First, the funds that are used can often be completely legitimate – in many cases the funds are not tarnished until they have been used for the terrorist purpose. As noted above this makes them difficult to detect, meaning that any attempt to quantify would be reliant on guesswork as to the amount of money which has not been caught. Second, the increasing use of 'cheap-terrorism' means that putting a value on the amount of money advanced for terrorist purposes is not useful. The direct costs of mounting individual attacks have in recent times been low relative to the damage they can yield.[49] Cheap terrorism became possible because modern terrorist organisations tend to adopt a decentralised cell structure, eliminating the need for significant financing to maintain their entire organisations.[50] It means that their financing can take place on a smaller scale and locally. Such modest flows on a local level are difficult to track.[51] When we talk about terrorist financing, it is important to consider the

[47] Hawala is outlined in full below.

[48] Mattias Schramm and Markus Taube, 'Evolution and Institutional Foundation of the Hawala Financial System' (2003) 12(4) *International Review of Financial Analysis* 405, 418.

[49] Financial Action Task Force, *Terrorist Financing* (2008), 7. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf> accessed 22 September 2016.

[50] Koh, (n.33), 10.

[51] Peter Reuter and Edwin M. Truman, *Chasing Dirty Money* (1st edn, Peterson Institute for International Economics, 2005), 142.

result of the crime and not just the commission. Third, the use of underground banking systems[52] and non-traditional payment methods (NTPMs)[53], as with money laundering, further cloud any attempt to quantify the volume of funds advanced to terrorist groups.

Further, whilst quantifying funds advanced for terrorist purposes would be useful, it only tells a rather limited story. Terrorism requires both organisational funds[54] as well as operational funds.[55] A terrorist cell such as Al-Qaida is estimated to need around $30 million a year to sustain its activities.[56] Though it is estimated that only 10% of that is on operational costs, the other 90% goes on organisational costs such as administration and maintenance of the organisation, its camps, and its sleeper cells.[57] Therefore the reason that terrorism can be expensive tends to be linked to the organisational structure of the group. This is arguably the

[52] This phrase has been used to describe informal banking systems that are seen to be secretive and mysterious (see Fletcher N. Baldwin Jr., 'Money Laundering Counter-Measures with Primary Focus on Terrorism and the USA Patriot Act 2001', 2002 6(2) *Journal of Money Laundering Control* 105, 112), or a method of banking that takes place outside the regulated financial services sector (see Nicholas Ryder and Umut Turksen, 'Islamophobia or an Important Weapon? An Analysis of the US Financial War on Terrorism' (2009) 10 *Journal of Banking Regulation* 307, 308).

[53] These will be introduced fully below, in section 1.3.

[54] The costs of maintaining the wider terrorist organisation, its camps, and its sleeper cells.

[55] Operational expenses include salaries of operatives, payments made to the families of martyrs, travel expenses, training of new members, costs associated with forged documents, bribery, weapons acquisition, sustenance, logistics, shared funding, and the direct cost of actual attacks. (See: Financial Action Task Force, 'Terrorist Financing' (2008) available at: <http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf> accessed 22 September 2016). It is estimated that operational costs are a much smaller portion of the costs seen by larger or more traditional hierarchical terrorist groups.

[56] National Commission on Terrorist Attacks on the United States, '9/11 Commission Report' (2004), 170. Available at: <http://govinfo.library.unt.edu/911/report/911Report.pdf> accessed 22 September 2016.

[57] Thomas J. Biersteker and Sue E. Eckert, 'Introduction: The Challenge of Terrorist Financing', In Thomas J. Biersteker and Sue E. Eckert, *Countering the Financing of Terrorism* (1st edn, Routledge, 2008).

hardest type of financing to spot as it does not lead directly to an attack. The direct cost (or operational costs) of the London 7/7 bombings are estimated at just £8,000, the Madrid bombings at $10,000 and the Bali nightclub bombings $50,000.[58] So the significant costs when it comes to terrorist groups are in maintaining a large organisation presence. Small decentralised groups are cheap and effective, and nigh on impossible to detect.

Even where the funds are substantial, it does not follow that they are easier to identify. As seen above the ways in which terrorist groups source their funds are many and varied, meaning many sources can contribute to the funds. It is particularly problematic when mixed funding is used as it is unlikely that all methods will be detected.

1.3. Non-Traditional Payment Methods

It is still fairly typical to assume that funds are transferred via traditional means, indeed there is no getting away from the fact that this is the predominant method. However, that perception has begun to change over the last decade or so, thanks to a mix of regulators, supervisors, law enforcement agencies, and academics shining a light on the increasingly sophisticated methods used by criminals. There is a growing recognition that money launderers and terrorist financers are intelligent individuals, capable of using new, increasingly sophisticated, technologies and payment methods. No longer are launderers and terrorist financers limited to traditional methods such as cheques, payment orders, bank drafts and traveller's cheques.[59] The FATF have underlined the constant challenge of launderers and terrorist financers being one step ahead of regulators and supervisors: '*the*

[58] Financial Action Task Force, *Terrorist Financing* (n.49).

[59] Middle East & North Africa Financial Action Task Force, *Typology Report on "Existing / Emerging Cross Border Payment Methods and their vulnerabilities to ML/TF"* (2007), 2. Available at: <http://www.fiu.gov.om/files/TCBEng.pdf> accessed 22 September 2016.

rapid development, increased functionality, and growing use of new payment products and services (NPPS) globally has created challenges for countries and private sector institutions in ensuring that these products and services are not misused for money laundering and terrorist financing purposes.'[60] It is only logical that as AML and CTF efforts in the formal sector increase the probability of detection, more money will flow through informal sectors where the likelihood of inception are lower. Choo notes: '*Organised crime groups seek out, subvert and exploit . . . appropriate institutional vehicles which receive less regulatory attention*.'[61]

NTPMs, for the purpose of this thesis, encompass a wide assortment of payment methods. Those which will be outlined below, and then used to test the application of the global AML and CTF framework to emerging threats are: informal value transfer systems (IMVTs); wire transfers, stored value cards (SVCs), m-payments and cryptocurrency. It will be seen that whilst there are a number of commonalities between these NTPMs, they also have a number of significant differences – this is what provides the challenge for AML and CTF standard setters and regulators. NTPMs present a volatile and highly responsive threat landscape. It is therefore important that the international AML and CTF Framework is capable of application to these changing threats, and that regulators, supervisors and the private sector appreciate and are able to adjust to these risks. The growing prevalence of NTPMs is highlighted by the vast amount of typology reports and guidance papers the FATF (international standard setter)

[60] Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (June 2013), 3. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 22 September 2016.

[61] Kim-Kwang Raymond Choo, 'New Payment Methods: A Review of 2010 - 2012 FATF Mutual Evaluation Reports' (2013) 36 *Computers and Security* 12, 13.

has dedicated to them over the last decade (2006[62], 2008[63], 2010[64], 2013[65], 2014[66], and 2015[67]).

It is important to note, that as with traditional methods, complete prevention is not possible, the aim of AML and CTF measures in relation NTPMs should be to reduce instances. We are seeing that with increasing prevalence either NTPMs are being used outright, or a mix of NTPMs and traditional payment methods are being used in conjunction. '*The boundaries between the formal and informal value transfer systems are permeable, it puts law enforcers*

[62] Financial Action Task Force, *Report on New Payment Methods* (October 2006). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf> accessed 22 September 2016.

[63] Financial Action Task Force, *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems* (June 2008). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20TF%20Vulnerabilities%20of%20Commercial%20Websites%20and%20Internet%20Payment%20Systems.pdf> accessed 22 September 2016.

[64] Financial Action Task Force, *Money Laundering Using New Payment Methods* (October 2010). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf> accessed 22 September 2016.

[65] Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (n.61); and Financial Action Task Force, *The Role of HAWALA and other Similar Service Providers in Money Laundering and Terrorist Financing* (October 2013). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf> accessed 22 September 2016.

[66] Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CTF Risks* (June 2014). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 22 September 2016.

[67] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (June 2015). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 22 September 2016; and Financial Action Task Force, *Emerging Terrorist Financing Risks* (n.29).

at a disadvantage when money trails in informal systems are not easily investigated.'[68] It is therefore imperative to focus attention on countering the abuse of NTPMs, they need to be treat in the same way we deal with traditional methods, subject to a risk-based approach. NTPMs are used particularly at the layering stage of money laundering, and for the transfer and distribution stage of terrorist financing (though they can be used at other stages of both crimes).

Ryder has observed that '*any financial transaction could involve money laundering since any asset of financial value has potential utility to a launderer*.'[69] This sentiment is particularly relevant in relation to emerging payment technologies, as they offer a launderer or terrorist financer a potentially new transfer process, which, crucially, is unlikely during its infancy to be understood by regulated business, financial intelligence units, or, indeed, governments.[70]

The introduction of these NTPMs, particularly the new payment methods based on internet, wireless devices or private networks is considered to be one of the main global developments in the field of funds transfer and movement.[71] In turn, this globalisation, alongside advances in technology, have been key facilitators in the growth of money laundering and terrorist financing. Of primary concern, is the ease with which these NTPMs further facilitate the transfer of funds across international borders. They challenge the systems stability and safety

[68] Joanna Trautsolt and Jesper Johnson, 'International Anti-Money Laundering Regulation of Alternative Remittance Systems: Why the Current Approach Does Not Work in Developing Countries' (2012) 15(4*) Journal of Money Laundering Control* 407, 408.

[69] Nicholas Ryder*, Financial Crime in the 21st Century* (1st edn, Edward Elgar, 2011), 13.

[70] Robert Stokes, 'Anti-Money Laundering Regulation and Emerging Payment Technologies' (2013) 32 (5) *Banking and Financial Services Policy Report* 1, 1.

[71] Middle East & North Africa Financial Action Task Force, *Typology Report on "Existing / Emerging Cross Border Payment Methods and their vulnerabilities to ML/TF"* (n.60), 2.

and make it potentially more vulnerable to criminal phenomena, including the misuse and abuse of the financial system with the aim of laundering dirty capitals and financing terrorist actions.[72] Where there were once boundaries, there are now none, because of this money laundering and terrorist financing are now truly international in scope and require an international response (this will be examined in chapter 2). In terms of the five case study NTPM's (wire transfers, informal value transfer systems, stored cards, mobile payments and Bitcoin), the biggest factor in their development, has been the advancement of technology, whether that be due to the internet, computers, or chips. Indeed it has been noted that 'an offence that has benefitted most from the internet is money laundering.'[73] These developments have affected the ability of regulators to provide effective AML and CTF frameworks.

Criminals have shown adaptability and opportunism in finding new channels to launder the proceeds of their illegal activities and to finance terrorism. '*As the internet becomes more and more a worldwide phenomenon, commercial websites and internet payment systems are potentially subject to a wide range of risks and vulnerabilities that can be exploited by criminal organisations and terrorist groups.*'[74]

[72] Giorgio Merlonghi, 'Fighting Financial Crime in the Age of Electronic Money: Opportunities and Limitations' (2010) 13(3) *Journal of Money Laundering Control* 202, 202.

[73] Miguel Abel Souto, 'Money Laundering, New Technologies, FATF and Spanish Penal Reform' (2013) 16(3) *Journal of Money Laundering Control* 266, 266.

[74] Financial Action Task Force, *Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems* (June 2008), 1. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20TF%20Vulnerabilities%20of%20Commercial%20Websites%20and%20Internet%20Payment%20Systems.pdf> accessed 22 September 2016.

The globalisation of financial markets, and in particular the liberalisation of cross-border movements and the accompanying domestic deregulation of most financial sectors, has created more opportunities for financial crime to spread through financial systems. With regards to money laundering globalisation means that the layering stage can be achieved by the launderer more easily. For terrorist financing globalisation means that terrorist cells can access their funds at almost any time and anywhere.[75] Due to their scale and reach, economic crimes if left unchecked could have systemic consequences, retarding growth in countries and eroding confidence and support for the global economy.[76] The result of this is that over the last 20 years there has been unprecedented focus by regulators on financial crime and money laundering as sources of financial risk that can potentially undermine the integrity and stability of financial systems. No country is immune and examples can be seen in developed as well as developing countries.[77] The whole process has been termed the 'dark side' of globalisation.[78] It is because of this focus in the last 20 years by regulators, on the financial sector in particular, that the development of NTPM's are seen as crucial to launderers and terrorist financers.

This globalisation has been facilitated in a large part by the advances in technology, these advances have spurred on the development of NTPM's and created new challenges for law

[75] Vittori (n.37), 25.

[76] Sundaresh Menon and Teo Guan Siew, 'Key Challenges in Tackling Economic and Cybercrimes: Creating a Multilateral Platform for International Co-operation' (2012) 15(3) *Journal of Money Laundering Control* 243, 243.

[77] The World Bank, *Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide* (2009), 12. Available at: <http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/CombattingMLandTF.pdf> accessed 22 September 2016.

[78] Peter Reuter and Edwin M. Truman (n.51), 171.

enforcement authorities[79]. Inevitably, criminals recognise this and use technological improvements to advance their craft.[80] They have facilitated the breaking down of borders mentioned above, no longer is there a need to physically cross borders, nor is there a need for the launderer or terrorist financier to get their hands dirty. Money can be moved from one country to another and back again at the click of a button, without any need for physical transportation. Two of the significant advances have been computers and the internet; they play a significant role in the use of NTPM's, particularly where the NTPM is facilitated by an electronic transfer system.[81] The case studies NTPMs which will be looked at in towards the end of this chapter, highlight that the advances in technology which have led to the use of NTPM's '*provide tremendous opportunities for criminals to exploit its interconnectedness, accessibility and anonymity to achieve their illicit objectives, therefore making it harder for the long arm of the law to reach them*.'[82] The reason the above two factors have been so prominent is the fact that launderers and terrorist financiers are always on the lookout for new routes to launder their funds, the prevalent place being those countries which have weak or developing financial systems with inadequate controls. Developed jurisdictions such as the UK or US are likely to have advanced AML and CTF systems which make it more difficult for launderers and terrorist financers to go undetected. The above advances, which have resulted in global markets have meant that launderers and financiers are no longer reliant upon using

[79] Financial Action Task Force, *Money Laundering Using New Payment Methods* (n.65), 12.

[80] Danton Bryans, 'Bitcoin and Money Laundering: Mining for an Effective Solution' (2014) 89 (44) *Indiana Law Journal* 441, 441.

[81] A good example of the development of technology is the use of mobile phones to transfer remittances (m-money); this is an area that could be exploited in the future with regards to money laundering and terrorist financing (for more, see: William Vlcek, 'Global Anti-Money Laundering Standards and Developing Economies: The Regulation of Mobile Money' (2011) 29(4) *Development Policy Review* 415, 416).

[82] Sundaresh Menon and Teo Guan Siew (n.77), 243.

the financial systems in the region which they are domiciled, but that they can access any system in the world, from anywhere in the world.[83] Furthermore they can develop new methods which evade the current detection methods, and which the regulators have a lack of knowledge of, meaning that should they wish, they could transfer funds through countries that are traditionally perceived as having rather robust AML and CTF frameworks.

In the following subsections, we will see that globalisation and advances in technology have offered efficiency gains in terms of transaction speed, finality of payments, security features of technology based payment methods and their lower costs compared to paper payment instruments.[84]

1.3.1. Informal Value Transfer Systems (IMVTs)

IMVTs have for a long time been recognised as playing a major role in the movement of funds for the purposes of money laundering and terrorist financing. The most prominent system of this type, Hawala (or Hundi), predates traditional banking systems and was established in Calcutta in circa 1770.[85] Traditionally, these transactions happen through non-bank financial institutions or other business entities whose primary business activity is not be the transmission of money.[86]

---

[83] Angela Samantha Maitland Irwin, Kim-Kwang Raymond Choo, and Lin Liu, 'An Analysis of Money Laundering and Terrorist Financing Typologies' (2011) 15(1) Journal of Money Laundering Control 85, 87.

[84] Financial Action Task Force, *Money Laundering Using New Payment Methods* (n.65).

[85] Dwijendra Tripathi and Prithi Misra, *Towards a New Frontier: History of the Bank of Baroda*. (1st edn., Manohar Publications, 1985), 6.

[86] Financial Action Task Force, *Report on Money Laundering Typologies 2002 – 2003* (February 2003), 6-7. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2002_2003_ML_Typologies_ENG.pdf> accessed 22 September 2016.

Hawala in its simplest form is 'money transfer without money movement'.[87] The system is based on three main elements: secrecy, performance of the transactions upon verbal instructions and mutual trust among the parties in this system.[88] The remitter[89] visits a local hawaladar (A)[90] who arranges with a hawaladar (B) near the recipient[91], to pay the agreed amount to the recipient. The money which the remitter deposits with the hawaladar (A) does not transfer to the recipient, instead hawaladar (B) pays the recipient the agree amount out of their own funds. A debt then exists between hawaladar (A) and hawaladar (B). The remitter has successfully transferred money to the recipient. There is no record of the transaction, and hawaladar (B) trusts that hawaladar (A) will settle their debt in the future. The two hawaladars tend not to work for the same business, though it is possible that they may do so, generally the relationship between the two is simply based on trust built through family, ethnic, or linguistic ties, as well as business connections.[92]

IMVTs are not intrinsically unscrupulous, several experts have emphasises that '*in the most part IMVT systems provide a service which deals with funds from legitimate sources'*.[93] A key reason for their existence, is the advantages they offer in terms of 'speed, price, accessibility,

---

[87] Financial Crimes Enforcement Network, *The Hawala Alternative Remittance System and its Role in Money Laundering*, 5. Available at: <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/FinCEN-Hawala-rpt.pdf> accessed 22 September 2016.

[88] Middle East & North Africa Financial Action Task Force, *Typology Report on "Existing / Emerging Cross Border Payment Methods and their vulnerabilities to ML/TF"* (n.60), 9.

[89] The person who wishes to send money.

[90] A hawaladar is the broker who facilitates the transfer of money.

[91] The person to whom the money is destined.

[92] Financial Action Task Force, *Report on Money Laundering Typologies 2002 – 2003* (n.86), 7.

[93] Ibid, 10.

and familiarity'.[94] They offer an even more attractive system than wire transfers (discussed in section 1.3.2) in the sense that they only take 1% to 2% commission[95] from the transfer, considerably less than formal wire transfer services like Western Union.[96] Often they are used by remitters simply because they are the only system for getting funds to recipients in remote locations, or those regions that do not have other types of financial services available. Whilst amongst immigrant communities in more developed countries IMVTs are used as a low cost mechanism for the sending of funds back to family in their country of origin.[97] IMVTs have also proven to be of use for Non-profit organisations (NPOs) for similar reasons, allowing them to transfer funds to remote locations or areas which are not adequately served by traditional financial institutions.[98] For NPOs, these are often the areas where their work and resources are needed the most.

Another reasons for the increasing usage of IMVT's is their utility in adapting to difficult circumstances. Unlike the formal financial sector, it is not as susceptible to disturbance in the financial markets. It can withstand 'sudden and dramatic economic, political and social

[94] Jonas Rusten Wang, 'Regulating Hawala: A Comparison of Five National Approaches' (2011) 14(3) *Journal of Money Laundering Control* 210, 210; and see further: Financial Action Task Force, *Report on Money Laundering Typologies 2003 – 2004* (February 2004), 4. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2003_2004_ML_Typologies_ENG.pdf> accessed 22 September.

[95] The Economist (2001), 'Cheap and Trusted: Homing in on Networks of Informal Money Transfers' (2001). Available at: <www.economist.com/node/877145> accessed 22 September 2016.

[96] Panagiotis Liargovas and Spyridon Repousis, 'Underground Banking or Hawala and Greece-Albania Remittance Corridor' (2011) 14(4) *Journal of Money Laundering Control* 313, 314.

[97] Financial Action Task Force, *Report on Money Laundering Typologies 2002 – 2003* (n.87), 7.

[98] Ibid 9.

upheaval as evidenced by their presence in war-ravaged nations such as Afghanistan, Iraq, Kosovo and Somalia.'[99] This is further highlighted by the fact that hawala is seen as 'providing the best, and – this cannot be overemphasised – in many such places the only, means of importing foreign exchange and financing export'[100], where the government has collapsed or social cohesion has unravelled.

In the last decade there have been numerous examples of IMVTs being used for illegal purposes.[101] But, similarly to wire transfers there is a good chance of illegitimate transfers going undetected due to the high number of legitimate and necessary providers who serve a high customer base.[102] The fact that abuse of IMVTs takes place outside the formal financial sector is a significant issue when it comes to detection.[103] Indeed, Hawala has been described as 'an underground banking system, which flies under the radar of modern supervision of financial transactions.'[104] Further, any investigations that do take place require patience,

[99] Rob McCusker, 'Underground Banking: Legitimate Remittance Network or Money Laundering System?' (July 2005) 300 *Trends & Issues in Crime and Criminal Justice* 1, 2. Available at: <http://aic.gov.au/media_library/publications/tandi_pdf/tandi300.pdf> accessed 22 September 2016.

[100] Thomas Viles, 'Hawala, Hysteria and Hegemony' (2008) 11(1) *Journal of Money Laundering Control* 25, 28.

[101] Financial Action Task Force, *Money Laundering & Terrorist Financing Typologies 2004 – 2005* (June 2005), 3. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2004_2005_ML_Typologies_ENG.pdf> accessed 22 September 2016.

[102] Ibid, 33.

[103] Financial Action Task Force, *Report on Money Laundering Typologies 2002 – 2003* (n.87), 8.

[104] Henk van de Bunt, 'The Role of Hawala Bankers in the Transfer of Proceeds from Organized Crime' in Dina Siegel and Hans Nelen, *Organised Crime: Culture, Markets and Policies* (Volume 7, Springer, 2008). Available at: <http://link.springer.com/chapter/10.1007%2F978-0-387-74733-0_9> accessed 22 September 2016.

rapport with witnesses and informants, and good intelligence[105], and therefore the process can be costly in terms of resources.

It has long been noted that Hawala can indeed facilitate the commission, or frustrate the investigation of, various types of serious crimes.[106] There are a number of factors which elucidate the appeal of IMVTs to money launderers and terrorist financers. First, IMVTs seek to avoid the mainstream financial institutions in order to remain undetected by financial monitoring systems or investigative authorities.[107] Second, the system does not require any identification procedures with regards to remitters, and settlements take place intermittently between the remitter's intermediary and his counterpart in the beneficiary's country (the receiving intermediary).[108] Finally, speed has played a key part in making this system attractive to money launderers and terrorists.[109] Funds can be transferred quickly to the least developed regions of the world, where no proper banking services exist, without government

[105] Panagiotis Liargovas and Spyridon Repousis (n.97), 314.

[106] See as examples: Financial Action Task Force, *1998 – 1999 Annual Report* (June 1999). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/1998%201999%20ENG.pdf> accessed 22 September 2016; Financial Action Task Force, *Annual Report 2000 – 2001* (June 2001). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2000%202001%20ENG.pdf> accessed 22 September 2016; and Christine Howlett, 'Investigation and Control of Money Laundering via Alternative Remittance and Underground Banking Systems' (April 2001) Churchill Trust. Available at <https://www.ncjrs.gov/pdffiles1/190720.pdf> accessed 22 September 2016.

[107] Financial Action Task Force, *Report on Money Laundering Typologies 2003 – 2004* (February 2004), 5. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2003_2004_ML_Typologies_ENG.pdf> accessed 22 September 2016.

[108] Middle East & North Africa Financial Action Task Force, *Typology Report on "Existing / Emerging Cross Border Payment Methods and their vulnerabilities to ML/TF"* (n.60), 9.

[109] Financial Action Task Force, *Terrorist Financing* (n.49), 24.

supervision and little or no paper trail.[110] The lack of transparency which is apparent because of this, is a big issue for both regulatory and law enforcement authorities.[111]

The continuing AML and CFT risk associated with IMVTs is due, in a large part, to the different ways in which countries continue to regulate them; some countries require a banking licence for all institutions that transfer money, whilst the others require no regulation at all.[112] Until this issue is addressed IMVTs will continue to cause a significant threat. Where they are regulated, the IMF has noted that this occurs in two different ways; by registration[113] or by licensing[114].[115] As always, any system is better than no system, and the biggest risks emanate from those countries which have no licensing or registration regime.

Despite the fact the IMVT system itself evades the formal financial system, the system can provide a safeguard to some extent. Should IMVT dealers wish to settle their accounts without the hassle of a physical transfer of cash, they have to utilise the formal financial system. In doing so, they leave themselves open to the usual customer due diligence and

---

[110] Panagiotis Liargovas and Spyridon Repousis (n.97), 314.

[111] Financial Action Task Force, *Money Laundering & Terrorist Financing Typologies 2004 – 2005* (n.102), 34.

[112] Ibid 13.

[113] Under a registration regime, the main aim is to encourage remittance service providers to comply with AML/CFT requirements, while setting the threshold for getting authorisation as low as possible. (See: Jonas Rusten Wang, 'Regulating Hawala: A Comparison of Five National Approaches' (2011) 14(3) *Journal of Money Laundering Control* 210, 211).

[114] Licensing regimes, on the other hand, are stricter in the sense that they oblige providers to demonstrate ex ante their ability to comply with regulations through extensive fit-and-proper tests. (See: Jonas Rusten Wang, 'Regulating Hawala: A Comparison of Five National Approaches' (2011) 14(3) *Journal of Money Laundering Control* 210, 211)

[115] International Monetary Fund, *Approaches to a Regulatory Framework for Formal and Informal Remittance Systems: Experiences and Lessons* (2005). Available at: <https://www.imf.org/external/np/pp/eng/2005/021705.pdf> accessed 22 September 2016; and Jonas Rusten Wang, 'Regulating Hawala: A Comparison of Five National Approaches' (2011) 14(3) *Journal of Money Laundering Control* 210, 211.

suspicious activity reporting procedures which may unravel funds that are channelled through IMVTs for the purposes of money laundering and terrorist financing. It is accepted that banks are the predominant mechanism for settling accounts[116], particularly when the sums are large[117], what is uncertain is how likely the gatekeepers to the formal financial system are likely to become suspicious of the settlement activity of IMVT dealers. Indeed, it is important that the formal financial system does not go too far and disproportionately impose AML and CTF measures on IMTV dealers. However, it does seem apparent that the best chance of detecting abuse of IMVTs for the purposes of money laundering or terrorist financing are where the settlement takes place through the formal financial system.[118]

If funds are never settled through the formal financial system by IMVT dealers, then in order for transactions to be traced through underground systems like Hawala, importance needs to be placed on gaining inside information as normal mechanism to counter AML and CFT are not sufficient on their own.[119] Of course this is easier said than done, gaining that kind of information may be difficult due to the fact the system is built around the concept of trust. The best way of doing this, it has been suggested, is to establish informants who operate within the system.[120] Without such developments, the recipient will receive the funds as cash and they will be untraceable at any stage, unless they try to integrate them back into the financial system.

---

[116] Thomas Viles (n.101), 30.

[117] Financial Action Task Force, *Report on Money Laundering Typologies 2002 – 2003* (n.87), 8.

[118] Ibid.

[119] Panagiotis Liargovas and Spyridon Repousis (n.97), 314.

[120] Ibid.

1.3.2. Wire Transfers

Wire transfers were one of the first contemporary forms of NTPMs to emerge, a prominent example of which is Western Union. Similarly to IMVTs transactions, they take place both on a national and international scale,[121] succeeding in further eroding international borders in terms of the transfer of funds. It should be noted from the outset that the majority of funds that go through wire transfers are of legal origin,[122] however the reason for their inclusion in this thesis is that they are capable of being used by launderers and terrorist financers.

The system is very similar to that of IMVTs; it can involve as little as four people (though it is possible to add additional layers to the transfer system): the remitter, the sending agent (A), the distributing agent (B) and the recipient. The transaction begins when the remitter hands over the funds to the sending agent (B). The remitter also specifies the recipient, as well as their location. The funds can be paid in cash, cash equivalent, cheques, and other monetary instruments or in stored value cards.[123] Ordinarily, the remitter will receive a unique reference number to identify the transaction. The remitter then passes this on to the recipient.[124] The funds should be made available to the recipient within 15 minutes.[125] The settlement or clearing of accounts between wire transfer providers does tend to take place through conventional channels; at this stage, as with IMVTs, it is susceptible to detection by financial institutions. The systems used for wire transfers can be considered as both simple and

[121] Financial Action Task Force, *Report on Money Laundering Typologies 2003 – 2004* (n.109), 4.

[122] Financial Action Task Force, *Money Laundering & Terrorist Financing Typologies 2004 – 2005* (n.102), 5-6.

[123] Ibid 6.

[124] Ibid.

[125] Panagiotis Liargovas and Spyridon Repousis (n.97), 320.

complex. They are simple in that the individual components of the system involve operations as basic as receiving cash for a transfer, or communicating information on individual payment orders. But, they can appear to be complex, as they may rely on a series of seemingly unrelated operations at the clearing or settlement phase of the process.[126] Again, as with IMVTs the remitter is not tied into a system in the way they would have to be to use the formal financial system, the agent can undertake transactions on an occasional basis, though they can also be used regularly like formal financial implements.[127]

In countries with large immigrant communities, wire transfers offer a key service in providing them with a means of sending funds to the countries of origin.[128] For other wire transfer users, the systems provide a cost effective and efficient method for transferring money to family or for business reasons.[129] Western Union charges a transfer fee of between £4.90 and £6.90 for most remittances,[130] these charges are lower than the formal financial system but more costly than IMVTs.[131] Wire transfers have also proven useful where there has been political instability, inadequate payment systems, and/or an unstable financial sector and a lack of easily accessible formal financial institutions in remote areas.[132]

---

[126] Financial Action Task Force, *Money Laundering & Terrorist Financing Typologies 2004 – 2005* (n.102), 6.

[127] Middle East & North Africa Financial Action Task Force, *Typology Report on "Existing / Emerging Cross Border Payment Methods and their vulnerabilities to ML/TF"* (n.60), 13.

[128] Financial Action Task Force, *Money Laundering & Terrorist Financing Typologies 2004 – 2005* (n.102), 5.

[129] Ibid.

[130] To find out the latest figures visit: <https://www.westernunion.com/gb/en/send-money/start.html> accessed 22 September 2016.

[131] Samuel Munzele Maimbo and Dailip Ratha, Remittances: Development Impact and Future Prospects (1st edn., World Bank Publications, 2004).

[132] Panagiotis Liargovas and Spyridon Repousis (n.97), 314.

Wire transfers have proved to be popular with money launderers and terrorist financers due to the some of the benefits of the system which were outlined above. 'The increased rapidity and volume of wire transfers, along with the lack of consistent approach in recording key information on such transactions, maintaining records of them and transmitting necessary information with the transactions, serve as an obstacle to traceability by investigative authorities of individual transactions'.[133] Due to the cross-border element of wire transfers each jurisdiction might hold part of the evidence or intelligence impacting on the transaction. Therefore, obtaining an overall view of particular operations from beginning to end is made more difficult.[134] The international community will need to find ways of sharing intelligence on current cases and then allowing joint intelligence-led investigations along wire transfer corridors.[135] The need for a combined international approach to wire transfers cannot be understated. This coupled with the low value of the transfers when compared with the high overall volume of such transactions means that it is easy to hide illegitimate transfers. It is also impossible to establish an average size for terrorist related wire transfers.[136] Wire transfers have a low risk of detection.

Initially, simple wire transfers were sufficient for the launderer and the terrorist financer to evade detection, however as the regulators have become more in touch with how the system is exploited, criminals have had to adapt their techniques. One way of successfully achieving

[133] Financial Action Task Force, *Report on Money Laundering Typologies 2003 – 2004* (n.109), 4.

[134] Financial Action Task Force, *Money Laundering & Terrorist Financing Typologies 2004 – 2005* (n.102), 4.

[135] Ibid, 36.

[136] Financial Action Task Force, *Report on Money Laundering Typologies 2003 – 2004* (n.109), 6.

this is to engage in more complicated wire transfers, involving several transactions in order to disrupt the paper trail and hence avoid detection.[137] A further way that criminals have exploited wire transfers is to channel funds through several different financial instruments so that the wire transfers appear to come from different and seemingly unrelated sources.[138] A particularly complex method which criminals have used is cuckoo smurfing[139].

On the one hand, electronic payment systems provide greater security for transactions by permitting an increased ability to trace individual transactions through electronic records that may be automatically generated, maintained and / or transmitted with the transactions.[140] Transactions that contain full information assist beneficiary financial institutions to identify potentially suspicious transactions. These would require extra diligence and potentially onward reporting to an FIU. When reports on unusual or suspicious wire transfers are received by an FIU, those that contain complete information can be more thoroughly researched and analysed.[141] Complete information is an essential ingredient of detecting and preventing abuse of the wire transfers.[142] This is in an ideal world, unfortunately wire transfer

[137] Ibid, 5.

[138] Ibid.

[139] Cuckoo smurfing is the term used to describe the complex technique, money launderers exploiting wire transfers, use to access their seemingly legitimate funds. In order to access the criminal funds they transfer them through the accounts of unwitting persons, who receive funds or payments from overseas. Whilst the banks have good detection mechanisms for catching this technique they have no means of catching the collector which is why it is still used. (See: Financial Action Task Force, 'Money Laundering and Terrorist Financing Typologies 2004 – 2005 (June 2005), 18. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2004_2005_ML_Typologies_ENG.pdf> accessed 22 September 2016).

[140] Financial Action Task Force, *Report on Money Laundering Typologies 2003 – 2004* (n.109), 4.

[141]Ibid, 7.

[142] Ibid.

can often have information missing from the beginning, or the information does not follow the funds. Differences in requirements for record keeping or transmission of information on the originator of transfers conducted through such businesses may be used to the advantage of the terrorist or other criminals that desire to move funds without being easily detected by authorities.[143] Whatever the underlying reason, the fact that wire transfers sometimes offer the possibility of transmission of funds without strict identification procedures makes them attractive to some customers.[144] These weaknesses have been exposed by using of false identities, 'straw men'[145] or front companies in order to provide clean names and avoid detection,[146] as customer due diligence requirements are not as stringently enforced outside the banking sector.

The level of vulnerability for wire transfers to be misused for terrorist financing differs from that associated with money laundering. In the terrorist financing area, the level of vulnerability may also differ according to whether wire transfer operations are used in providing funds for a specific terrorist action or if such operations are used in transmitting funds that have been collected from legitimate (or illegal) sources to support future terrorist activities. Terrorist financing is difficult to detect particularly where the funds are 'clean' or where illicit, if they are transferred in small quantities. It is important that wire transfer providers screen transactions and customers against relevant terrorist financing related

[143] Ibid, 4.

[144] Financial Action Task Force, *Money Laundering & Terrorist Financing Typologies 2004 – 2005* (n.102), 6.

[145] This is an individual who acts as a front for others (who incur the expense and obtain the benefit of the transaction). Often there is a financial incentive for the individual to undertake the role.

[146] Financial Action Task Force, *Report on Money Laundering Typologies 2003 – 2004* (n.109), 5.

lists.[147] The most successful counter to these transactions is the application of normal AML policies, that is, customer identification, know-your-customer procedures and suspicious transaction reporting.[148]

Wire transfers are still detectable when the funds come back into the financial system. The settlement or clearing accounts of wire transfer providers take place through conventional channels, and for this reason they are susceptible to detection.[149] Any measures that are introduced to detect wire transfers need to be sure not to unnecessarily interrupt legitimate funds or push them underground[150], these will be looked at more in depth in the following chapters. But since settlement of wire transfers tends to involve the use of banks, vigilance by them in applying CDD and SARs can be of use.[151] Of course, as with IMVTs there is the potential for the funds sent via wire transfer to be taken as cash, and in such a case the funds then will be impossible to trace and will miss the secondary checks carried out by the formal financial sector.

1.3.3. Stored Value Cards (SVCs)

Another type of NTPM that has been exploited by terrorists and money launderers is 'stored value cards'. The term prepaid cards and stored value cards are used interchangeably in the cards industry[152], but in the interest of clarity this thesis will refer to them just as stored value

[147] Financial Action Task Force, *Money Laundering & Terrorist Financing Typologies 2004 – 2005* (n.102), 33.

[148] Ibid.

[149] ibid, 34.

[150] Ibid, 3.

[151] Ibid, 35.

[152] The Wolfsberg Group, *Wolfsberg Guidance on Prepaid and Stored Value Cards* (2011), 2. Available at: <http://www.wolfsberg-

cards. Traditionally these cards are offered by businesses from outside the financial sector. They were initially developed as a means for employers to pay their employees efficiently.

SVCs either have a magnetic strip or an electronic chip which allows transactions to be deducted from them. Their function can be best understood as being similar to debit cards.[153] There are two types of systems when it comes to SVCs, either 'open system cards' or 'closed system cards'. Of greatest threat for the purposes of money laundering and terrorist financing are open system cards due to the fact they can be reloaded. Many entities can be involved in the provision of prepaid cards. The roles of these entities vary depending on the business model of the prepaid card product and various roles may be carried out by a single entity or through agents.[154]

They are seen as a desirable method as they are a 'compact and easily transportable method'[155], as well as being; readily available, convenient and affordable.[156] They also have benefits in terms of managing finances as they take away the risk of running into overdrafts.[157] Over the past decade, the cards have been one of the fastest growing segments in consumer

principles.com/pdf/standards/Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14,_2011.pdf> accessed 22 September 2016.

[153] Financial Action Task Force, *Report on New Payment Methods* (n.63), 4.

[154] Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (n.61), 6.

[155] United States Government Accountability Office, *Report to Congressional Requesters, Moving Illegal Proceeds: Challenges Exist in the Federal Government's Effort to Stem Cross-Border Currency Smuggling* (October 2010), 2. Available at: <http://www.gao.gov/new.items/d1173.pdf> accessed 22 September 2016.

[156] Kim-Kwang Raymond Choo, 'Money Laundering Risks of Prepaid Stored Value Cards' (Australian Institute of Criminology No. 363, 2008) 1, 2. Available at: <http://aic.gov.au/media_library/publications/tandi_pdf/tandi363.pdf> accessed 22 September 2016.

[157] Ibid, 2.

finance. They began as a device used to pay for goods and services where the issuer did not need to conduct any analysis on the cardholder's credit standing, or bear the costs for opening and managing a payment account.[158] Cards can be applied for; online, by fax, or over the counter at retailers and check cashing outlets.[159]

However, as with the NTPMs discussed above, SVCs have several traits that make them appealing to money launderers and terrorist financers. In particular, the speed with which funds can be transferred, alongside the anonymity afforded by the method[160], provides a significant risk. Further unloaded inactivated cards can be moved across borders quickly, there is a lack of or at least a difficulty in; providing an audit trail, and compiling an aggregate view of multiple transactions.[161] Open system cards can be mailed to areas with lax money laundering standards and funds can then be withdrawn from ATM's[162], including internationally.[163] Further, where cash or money orders are used to fund the account then there is likely to be no paper trail.[164] It is entirely possibly for a card to be obtained without a

[158] Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (n.61), 5.

[159] Financial Action Task Force, *Report on New Payment Methods* (n.63), 11.

[160] Ibid.

[161] The Wolfsberg Group, *Wolfsberg Guidance on Prepaid and Stored Value Cards* (n.152), 4. Once the cards are out of the country then criminals can convert them into cash. There is also a difficulty in intercepting such cards at national borders, as even if the customs agent sees the prepaid cards, there is no way to know how much value is stored on them.

[162] Kim-Kwang Raymond Choo, 'Money Laundering Risks of Prepaid Stored Value Cards' (n.156), 2.

[163] Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (n.61), 5.

[164] United States Government Accountability Office (n.155), 6.

bank account.[165] Even where it is closed system card with a limit attached to it, more than one card could be purchased without identification.[166]

SVCs have been recognised as being 'almost untraceable instruments'[167], this presents a significant challenge when it comes to AML and CFT due to their reliance on CDD and SARs as counter measures. The cards may be issued at a banking or non-banking institution[168], which poses a difficulty when it comes to countering the risks of money laundering and terrorist financing in the area, especially relating to the non-bank institutions. Detection of SVCs being exploited for the purposes of money laundering or terrorist financing is made more difficult when the SVCs are used to purchase goods[169], which means that the funds never have to come back into the financial system, therefore taking away one of the detection methods. A further risk non-bank institutions pose by providing access to these SVCs, is that in cases where face-to-face verification of cardholder identity are required, evidence of identity may be difficult to verify (e.g. the verification of a foreign passport at a convenience store).[170] On top of this the card may be used by a person other than the purchaser.[171] Without adequate

[165] Financial Action Task Force, *Report on New Payment Methods* (n.63), 11.

[166] American Express sell gift cards with denominations as high as $500 that can be purchased at retailers anonymously (with cash) and without limit (see: Nathan Vardi, 'Cash is King' (Forbes, 7 April 2008), <http://www.forbes.com/forbes/2008/0407/036.html> accessed 22 September 2016).

[167] Gregory Calpakis, executive director of the Association of Certified Anti-Money Laundering Specialists, in: N. Vardi, Cash is King, Forbes (April 7th, 2008)

[168] Middle East & North Africa Financial Action Task Force, *Typology Report on "Existing / Emerging Cross Border Payment Methods and their vulnerabilities to ML/TF"* (n.60), 11-12.

[169] Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (n.61), 5.

[170] Kim-Kwang Raymond Choo (n.156), 4.

[171] Middle East & North Africa Financial Action Task Force, *Typology Report on "Existing / Emerging Cross Border Payment Methods and their vulnerabilities to ML/TF"* (n.60), 14.

cardholder identification the transaction trail alone may be insufficient to help law enforcement trace the cardholder.[172] Indeed, medium-sized non-financial distributors may well have inadequate AML and CFT measures as they do not understand the threat.[173] Their risks are greatest where the card permits greater values to be transmitted[174], or where the system allows for individuals to carry multiple cards simultaneously.[175]

In terms of developments, the cards have stayed quite stagnant technologically; they still rely on magnetic strips or chips.[176] They already meet key objectives with regards to money launderers and terrorist financer's needs in terms of anonymity, speed and ease of access.

Detection of any abuse of SVCs is difficult owing to a number of factors inherent in the SVCSs themselves. First, the institutions involved tend to be small to medium businesses, meaning the burden of compliance with AML and CFT measures is higher for them, notwithstanding the issue of them potentially not understanding the application of AML and CFT measures. Tsingou has noted that 'know your customer and reporting requirements may be less well automated.'[177] Second, some countries have implemented measures that need to be applied to the sale of higher value SVCs, for example FinCEN in the US set a threshold of $2,000 before

---

[172] Financial Action Task Force, *Report on New Payment Methods* (n.63), 11.

[173] Kim-Kwang Raymond Choo (n.156), 3.

[174] Financial Action Task Force, *Report on New Payment Methods* (n.63), 11.

[175] The Wolfsberg Group, *Wolfsberg Guidance on Prepaid and Stored Value Cards* (2011), 10. Available at: <http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14,_2011.pdf> accessed 22 September 2016.

[176] Financial Action Task Force, *Report on New Payment Methods* (n.63), 16.

[177] Eleni Tsingou, 'Global Governance and Transnational Financial Crime: Opportunities and Tensions in the Global Anti-Money Laundering Regime' (2005) Centre for the Study of Globalisation and Regionalisation Working Paper. Available at: <http://wrap.warwick.ac.uk/1959/1/WRAP_Tsingou_wp16105.pdf> accessed 22 September 2016.

stores have to take steps to ensure that SVCs are not being used for money laundering or terrorist financing.[178]

1.3.4. Mobile Payments

In an everyday context, mobile payments refer generally to the use of mobile phones and other wireless communications devices to pay for goods and services.[179] They have expanded rapidly, as access to mobile technology has become more readily available and affordable, their use as a payment method has grown. It was estimated by the FATF that 1.4 billion people will use payments via mobile phones for their financial transactions in 2015.[180] Whilst Future Market Insights have estimated that the volume of mobile payments will reach 106 billion by 2020.[181]

The ability to use mobile technology as an alternative to the formal financial sector has meant that it is used extensively in areas such as Southeast Asia, Africa[182] and some European countries where access to banks is difficult.[183] These countries tend to be those that would

[178] This limit is potentially a problem as there is nothing to stop a launderer or terrorist financer who is aware of this practice from buying a number of cards of smaller value (smurfing), thus evading the measure.

[179] Financial Action Task Force, *Report on New Payment Methods* (n.63), 6.

[180] Ibid 18.

[181] Future Market Insights, 'Mobile Payment Transaction Services Market: Money Transfer & Merchandise Purchase Key Application Segments' (20 July 2015) <http://www.futuremarketinsights.com/press-release/global-mobile-payment-transaction-market> accessed 22 September 2016.

[182] Three quarters of the countries that use mobile money most frequently are in Africa, and mobile banking in some of them has reached extraordinary levels (see: The Economist, 'Mobile Money in Africa: Press 1 for Modernity' (28 April 2012). Available at: <http://www.economist.com/node/21553510> accessed 22 September 2016).

[183] Financial Action Task Force, *Report on New Payment Methods* (n.63), 6. Vicek notes that the possibility to send money instantaneously over the globe in a simple manner represents a significant prospective market for mobile operators, financial services organisations and end users (See: William Vicek, 'Development vs. Terrorism: Money Transfers and EU

be considered to be developing.[184] That is not to rule out their use in developed countries, they are used with increasing regularity there too. It is simply that the area of greatest impact for mobile technology has been developing countries. Mobile payments can encapsulate a number of different processes, but for the purposes of this thesis the focus will be on mobile transfer systems such as M-Pesa.

M-payments provide a fast, safe, and efficient value transfer service, which results in underground services such as hawala becoming less attractive to remitters due to the greater risks involved in its use.[185] They are replacing the use of traditional banks and money service businesses that historically have charged high fees for small transfers.[186] M-Pesa specifically targets those without access to banking services.[187] Over time m-payments have also begun to be used to offer a new option to migrants and 'guest workers' that wish to send part of their wages home to support their families.[188] When mobile payment services are not based

---

Financial Regulations in the UK' (2008) 10(2) *British journal of Politics and International Relations* 286). Basically mobile operators like Vodaphone which operate the M-Pesa service have a competitive advantage in developing countries as they can tap into their existing customer base and billing infrastructure.

[184] Kim-Kwang Raymond Choo, 'New Payment Methods: A review of 2010 - 2012 FATF Mutual Evaluation Reports' (n.62), 15. For more on the use of mobile technology as an alternative to the formal financial sector in developing countries see: Marina Solin and Andrew Zerzan, *Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks*, (GSMA Discussion Paper, January 2010), available at: <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/09/amlfinal35.pdf> accessed 22 September 2016.

[185] US Department of State*, International Narcotics Control Strategy Report: Mobile Payments a Growing Threat* (March 2008). Available at: <http://www.state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm> accessed 22 September 2016.

[186] Ibid.

[187] Kim-Kwang Raymond Choo, 'New Payment Methods: A review of 2010 - 2012 FATF Mutual Evaluation Reports' (n.62), 15.

[188] US Department of State*, International Narcotics Control Strategy Report: Mobile Payments a Growing Threat* (March 2008). Available at:

on an underlying bank or payment card account, the telecom operator typically acts as a payment intermediary to authorise, clear, and settle the payment.[189]

The US Department of State has suggested that new mobile technology potentially provides a 'virtual ATM' to every bearer of a mobile phone[190], a good way to think of how the system works. In order to be able to use the M-Pesa system, the individual concerned needs to first register with an authorised M-Pesa agent by providing a Safaricom mobile number and their identification card, the individual can then deposit money into their account by depositing at a local agent.[191] The system leverages the extensive reach of the mobile networks, so that the mobile remittance service complement existing remittance channels and makes domestic and international low-denomination and high frequency remittances more affordable.[192] The providers, such as Vodafone in the case of M-Pesa, can tap into their customer base and billing structure to invoice payments to their customers and have the potential to acquire banking clients at a relatively low cost.[193]

One of the most obvious money laundering and terrorist financing risks relating to mobile technology arises due to the large amount of money involved in mobile banking and mobile

---

<http://www.state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm> accessed 22 September 2016. See also: William Vicek, 'Development vs. Terrorism: Money Transfers and EU Financial Regulations in the UK' (2008) 10(2) *British journal of Politics and International Relations* 286.

[189] Financial Action Task Force, *Report on New Payment Methods* (n.63), 6.

[190] US Department of State*, International Narcotics Control Strategy Report: Mobile Payments a Growing Threat* (March 2008). Available at: <http://www.state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm> accessed 22 September 2016.

[191] Kim-Kwang Raymond Choo, 'New Payment Methods: A review of 2010 - 2012 FATF Mutual Evaluation Reports' (n.62), 15.

[192] Ibid, 16.

[193] Ibid, 15.

remittance systems[194], meaning that funds linked to money laundering or terrorist financing may go unnoticed. A similar risk that is experienced in the formal financial sector, but unlike the other NTPMs m-payment providers tend to be large enough that they can afford the costs of implementing AML and CTF measures. The risk is further heightened by the ease with which funds can be transferred over the globe instantaneously, in a simple manner.[195] The markets that they are used in tend to be the ones with weak AML and CTF laws and a lack of enforcement, meaning that exploitation of this NTPM may be easier. Contrary to that, it tends to be international companies such as Vodafone that operate this type of payment method, therefore due to the reputational risk associated with being linked to money laundering and terrorist financing, it is likely that they will be keen to have effective AML and CTF measures.

A further risk arises due to the fact that mobile telephone operators engaged in money remittance activities may not be overseen by a country's central bank or other banking regulator but can be subject to AML/CFT measures.[196] The issue will be whether they are getting sufficient support and guidance in their application of AML and CFT measures. On top of this regulation in the area is hard, Kemp has suggested it is 'pervasive and deeply layered'[197] due to the fact there are many overlapping areas which are regulated separately, notably; payments, mobiles, retail and technology.

---

[194] Ibid.

[195] William Vicek, 'Development vs. Terrorism: Money Transfers and EU Financial Regulations in the UK' (2008) 10(2) *British journal of Politics and International Relations* 286. See also: Kim-Kwang Raymond Choo, 'New Payment Methods: A Review of 2010 - 2012 FATF Mutual Evaluation Reports' (n.62), 15.

[196] Financial Action Task Force, *Report on New Payment Methods* (n.63), 6.

[197] Richard Kemp, 'Mobile Payments: Current and Emerging Regulatory and Contracting Issues' (2013) 29 *Computer Law and Security Review* 175, 176.

Again smurfing has been used to the advantage of money launderers and terrorist financers who use NTPMs[198], it has provided them with an evasive technique of breaking up the funds to attempt to shield them from detection.

The detection the misuse of M-Pesa is not quite as straight forward as detection of mobile payments in general. Whereas the traditional form of mobile payments basically consists of the mobile phone facilitating access to an individual's bank account, M-Pesa does not involve the formal financial system thus removing the usual gatekeepers who would be charged with implementing AML and CFT practices. M-Pesa is facilitated by Vodafone, so it is them who are in the best position to implement AML and CFT measures, but they will not have as much experience in dealing with banking practices and the application of AML and CFT measures.

1.3.5. Cryptocurrencies

Bitcoin is the world's first experimental virtual currency (cryptocurrency); managed and transferred via decentralised, pseudonymous, peer-to-peer (P2P) network, over the internet via users running the necessary software.[199] Bitcoin allows users to transfer value without the collection of any personally identifiable information.[200] They were created with the aim of being able to store and transfer value in a simple, quicker and anonymous way,[201] doing so

[198] US Department of State*, International Narcotics Control Strategy Report: Mobile Payments a Growing Threat* (March 2008). Available at: <http://www.state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm> accessed 22 September 2016.

[199] Peter Alldridge*, Money Laundering Law: Forfeiture, Confiscation, Civil Recovery, Criminal Laundering and Taxation of the Proceeds of Crime*, (1st edn, Hart Publishing, 2003).

[200] Bryans (n.81), 441.

[201] Edward Southall and Mark Taylor, 'Bitcoins' (2013) 19(6) C.T.L.R. 177, 178.

without reliance on the heavily regulated traditional financial and credit institutions.[202] Peck has referred to them as being pseudonymous.[203] Bitcoin potentially allows any user, legitimate or criminal, to transfer money at near instantaneous speed at little or no cost, with very low barriers to entry, while remaining virtually anonymous without what could otherwise require a public paper trail.[204] Essentially, Bitcoin and analogous virtual currencies could enable money launderers to move illicit funds faster, cheaper, and more discretely than ever before.[205] Bitcoin is less inflation prone and offers greater anonymity for the transacting parties, but it lacks the reputational security and trust associated with a flat currency backed by the full faith and credit of a sovereign government.[206]

Launderers and terrorist financers can gain access to Bitcoin in two ways: either by mining[207] the Bitcoins themselves, or by purchasing the Bitcoins from a person already in possession of them. The most likely way that a launderer or terrorist financer is going to come into contact with Bitcoins is through purchasing them. In some environments, the crypto-currency

[202] Robert Stokes, 'Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar' (2012) 21(3) *Information & Communications Technology Law* 221, 225.

[203] Morgan E. Peck, 'Bitcoin: The Cryptoanarchists' Answer to Cash', (IEEE Spectrum, June 2012) <http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash> accessed 22 September 2016.

[204] Bryans (n.81), 447.

[205] Ibid.

[206] Ibid, 445.

[207] Bitcoins are mined using special software, all that is required is the computers processing power, so there is no cost attached to them if done in this manner. They can be mined by anyone, anywhere (see: Jacob Aron, 'Future of Money: Virtual Money Gets Real' (New Scientist, 2011) < https://www.newscientist.com/article/mg21028155-600-future-of-money-virtual-cash-gets-real/> accessed 22 September 2016.

operates like currency, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction.[208]

The bitcoins can then be transferred between individuals using the decentralised P2P Bitcoin structure. Bitcoins require two things in order for them to be spent: a Bitcoin address and a private Bitcoin Key. '*A Bitcoin address is a chain of alphanumerical characters which signifies a possibly recipient of a BTC. It can be thought of as an email address to which BTC payments can be sent. Every Bitcoin address has an associated private key which can be regarded as the 'ticket' which allows a user to spent the BTC. It is saved in the digital wallet of the holder.'*[209] The key is an essential ingredient in being able to spend the BTC, without the key to the address the BTCs are lost (permanently).[210]

Again anonymity and speed play a significant role in the appeal of Bitcoin to launderers and terrorist financers. Bitcoin is appealing to the launderer due to the anonymity it affords and the lack of government regulation in place against it.[211] The transactions can be carried out completely behind a computer screen without any face to face transactions, which poses issues relating to CDD.

On top of this, 'the decentralised nature of Bitcoin does pose difficulties, particularly because many of the AML techniques are predicated upon there being a central organisations upon

---

[208] Financial Crimes Enforcement Network, *Application of FinCEN's regulations to Persons Administering, Exchanging, or using Virtual Currencies 1* (2013) <http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf> accessed 22 September 2016.

[209] Robert Stokes, 'Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar' (n.202), 223.

[210] Ibid.

[211] Ibid

which numerous CDD obligations can be imposed'.[212] Without being able to tie an identifiable user to a single Bitcoin address, tracking the injection, layering, and re-entry of laundered funds would be extremely difficult for enforcement entities.[213] Only if one knows the identities associated with each Bitcoin involved in a set of transactions is it possible to meaningfully trace funds through the system.[214] Somehow Bitcoin needs to be held to account, but because of its structure a central regulator is unlikely to work, it was developed to be anonymous. Further even if a regulator could be made, it wouldn't be regulating anything due to the decentralised nature of the currency[215], it doesn't have a bank or any branches.

A final risk lies in the fact that Bitcoin evades the gatekeepers to the financial system as long as the user is happy to keep the value as virtual currency.[216]

There are now numerous emerging crypto-currencies such as Litecoin (which is seen as the silver to Bitcoins gold[217]), Peercoin and Namecoin to name but a few of the more successful

---

[212] Robert Stokes, 'Anti-Money Laundering Regulation and Emerging Payment Technologies' (n.71), 7.

[213] Bryans (n.81), 447.

[214] *United States of America V. Olivia Louise Bolles aka MDPRO* 6:13-mj-1614, 13. <http://www.justice.gov/dea/divisions/mia/2013/mia112113.pdf> accessed 22 September 2016.

[215] Robert Stokes, 'Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar' (n.202).

[216] A good example of Bitcoin's utility to evade detection and be used for illegitimate means can be seen through the case of Silk Road, see: M. Shillito, The Fall of Silk Road isn't the End for Anonymous Marketplaces, Tor or Bitcoin (The Conversation, June 2nd 2015). Available at: < https://theconversation.com/the-fall-of-silk-road-isnt-the-end-for-anonymous-marketplaces-tor-or-bitcoin-42659> accessed 22 September 2016.

[217] Rob Wile, 'What Is Litecoin: Here's What You Need to Know About The Digital Currency Growing Faster Than Bitcoin' (Business Insider, 27 November 2013) <http://www.businessinsider.com/introduction-to-litecoin-2013-11> accessed 22 September 2016.

crypto-currencies. The emergence of these new crypto-currencies is aided by the fact that Bitcoin is an open source code[218]. A significant worry for regulators is whether they can oversee all of these emerging payment technologies in an area that is fast moving.[219]

Where crypto-currencies may cause a real problem for money laundering regulators is where it becomes accepted as a method of payment on a wide scale basis. However, given the limited acceptance of BTC's as payment, it can be suggested that businesses will only accept BTCs due to focus upon the BTC exchange businesses, although the situation would be different if the BTC ever becomes universally accepted.[220] Overstock plans to start accepting them in store, while Virgin Galactic is also accepting them.[221] This could be a problem as it will allow the launderer to spend the crypto-currency straight from their online wallet avoiding the gateway back into the formal financial system which currently acts as the only policing of crypto-currencies like Bitcoin. It will be interesting to see what regulators can do to close this loophole. The first Bitcoin ATM has also been developed.[222]

---

[218] Any developer with the technical knowhow in programming can take the Bitcoin source code and alter it to make a crypto-currency of their own.

[219] M. Shillito and R. Stokes, *Governments want to regulate bitcoin – is that even possible?,* (The Conversation, March 26th 2015). Available at: <https://theconversation.com/governments-want-to-regulate-bitcoin-is-that-even-possible-39266> accessed 22 September 2016.

[220] Robert Stokes, 'Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar' (n.202), 225.

[221] Amit Chowdhry, 'Overstock.com Is Going To Accept Bitcoin in 2014' (Forbes, 21 December 2013) <http://www.forbes.com/sites/amitchowdhry/2013/12/21/overstock-com-is-going-to-accept-bitcoin-in-2014/?utm_campaign=techtwittersf&utm_source=twitter&utm_medium=social> accessed 22 September 2016.

[222] Joseph Gallivan, 'First Bitcoin ATM to Debut in NYC' (New York Post, 12 January 2014) <http://nypost.com/2014/01/12/first-bitcoin-atm-to-debut-in-nyc/> accessed 22 September 2016.

As things stand regulators still have the benefit, that in the most part, users still have to transfer their Bitcoins into real world money, meaning they have to pass a gatekeeper to the financial system who can impose AML obligations. However, if the exceptions above, such as Overstock and Virgin Galactic spread then the problem will become more pressing as individuals will never have to enter the formal financial system and therefore a layer of protection will be removed.

1.4. Common Themes Which Make the use of NTPMs Attractive

Having analysed the five case study NTPMs, there are some parallels that can be drawn, in terms of their respective risk of abuse by launderers and terrorist financers. These similarities, in part, are important in understanding how the international framework for AML and CTF can fight the threats posed by NTPMs. Indeed, whilst some of the NTPMs will have unique components, if we can target some of the broad commonalities between a range of NTPMs then it will make the international framework more responsive. Future proofing is at the forefront of the international frameworks agenda. By assessing the similarities in the way several NTPMs have been exploited, it will allow the thesis to focus on the areas of the international framework that need specific attention to counter future NTPMs.

Before going into the similarities in which the NTPMs have exploited the international AML and CTF framework, it is worth noting a few similarities about the initial development of the NTPMs. It is notable that four of the above mentioned NTPMs; wire transfers, IMVTs, SVCs, and mobile payments all began with legitimate intentions[223] whether that be; allowing

[223] NTPMs have developed as a result of the legitimate need of the market for alternatives to traditional financial services. In some cases, this was driven by the demand for more convenient or safer ways to pay for online purchases; in other cases their development was fostered by a desire to provide access to financial services for those who were excluded from traditional financial services (e.g. those with poor credit ratings, minors, but also

workers in a host state relaying funds to family members in their country of origin, providing a more efficient method of funds transfer, giving access to funds transfer to the unbanked[224], or reducing the costs of transfers[225]. Bitcoin by comparison, is more contentious its aim from the outset was to facilitate quick anonymous transfers.[226] It is therefore debatable as to whether it was always meant to attract more illegitimate transfers, or whether it was simply seeking to safeguard individuals information – an indirect effect of which was that it could assist in facilitating criminal activity. In saying that, Bitcoin is not inherently bad, it is just that it potentially bucks the trend set by the other four NTPMs. It could be the case that launderers and terrorist financers see this as a sign that they could create their own NTPM which has wrongdoing at its core, and obviously attracts legitimate users too, as opposed to them exploiting the vulnerabilities of NTPMs that were set up with legitimate aims. It should further be added that this thesis is not suggesting that Bitcoin was set up with the purpose of facilitating money laundering and terrorist financing, far from it, but because of the lack of integrity at its core, it is open to exploitation and leave the possibility that financers and launderers may seek to exploit the route of using anonymous P2P software in the future.

inhabitants of under-banked regions), and the assumption that NPMs may have a positive effect on national budgets as well as overall national and global economic development. (Financial Action Task Force, *Money Laundering Using New Payment Methods* (n.65), 12).

[224] Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (n.61).

[225] Moving money using cash couriers may be expensive relative to wire transfers (Financial Action Task Force, *Terrorist Financing* (n.49), 24) for instance. Similarly formal financial services may be more expensive than using the Bitcoin system. The Hawala system was generally preferred as it was cheaper than effecting money transfers through the banking system, in addition to the fact that it is a 24-hour service available every day of the year. It was based on trust and did not require the use of many documents (Middle East & North Africa Financial Action Task Force, *Typology Report on "Existing / Emerging Cross Border Payment Methods and their vulnerabilities to ML/TF"* (n.60), 6).

[226] Edward Southall and Mark Taylor (n.201), 178.

However it can be agreed that all 5 of the NTPM are desirable due to their accessibility: especially pre-paid cards and mobile payments as they grant easy access to the payment system by the whole population, including the unbanked.[227] It is just that limits will have to be placed on the NTPMs (some more than others) to ensure they can be used for the good purposes that they were intended to be used for.

Another notable feature is that technological advances are a key facilitator in all of the above NTPMs. The evolution in the management of payment methods has lately undergone rapid progress, which has caused such phenomenon to intertwine with the forceful development of internet communications.[228] The above NTPMs have been facilitated in a variety of different ways by technology whether it is through the development of magnetic strips which enable money to be saved to cards, or the sophisticated use of the internet to facilitate the global transfer of money, at some stage technology has played a role. Due to this development of technology it would seem that the laundering technique or the method used to transfer terrorist funds lays with the ingenuity of launderer or financer themselves. 'Ease of adaptation to new situations and speed the development of new methods' is a fundamental characteristic of money laundering [and terrorist financing].[229] In order to counter this then focus needs to be on knowledge building of NTPMs and understanding the technology – without this then will be no effective response. There is little financial

[227] Financial Action Task Force, *Money Laundering Using New Payment Methods* (n.65), 12.

[228] Guilio Piller and Elvis Zaccariotto, 'Cyber-Laundering: The Union Between New Electronic Payment Systems and Criminal Organisations' (2009) 16(1) *Transition Studies Review* 62.

[229] Isidoro Blanco Cordero, *El Delito de Blaqueo de* Capitals (3rd edn, Thomson Reuters Aranzadi, 2012), in: Miguel Abel Souto 'Money Laundering, New Technologies, FATF and Spanish Penal Reform' (2013) 16(3) *Journal of Money Laundering Control* 266, 268.

intelligence on most forms of NTPMs.[230] The US Department of State have highlighted that with regards to m-payments in particular, law enforcement and intelligence agencies currently have little expertise in the methodologies and technology that are being used[231], this is not isolated to just m-payments, it is true of all NTPMs. Determining either the volume or nature of transactions that use these NTPMs is difficult because few countries appear to be either aware of these payment tools or to be monitoring their use. The Bank for International Settlements (BIS) notes: 'With technology facilitating the breakdown of traditional banking services into multiple components and the addition of analytical tools and other capabilities into traditional banking services, more unlicensed non-bank entities are likely to provide bank-like services via the internet, including those that are extended cross border.'[232]

Another difficulty with NTPMs is that they facilitate cross-border transactions which make the burden of piecing the evidence together harder. It means that there is an increasing reliance on international cooperation and in particular mutual legal assistance to tackle crime.

Arguably, the most important key trend to emerge from the NTPMs discussed above is the concept of anonymity. Anonymity plays a significant role in attracting money launderers and terrorist financers to these new technologies. We have even seen that launderers and financers are willing to take a risk in using methods, such as Bitcoin, which are not very stable

---

[230] US Department of State*, International Narcotics Control Strategy Report: Mobile Payments a Growing Threat* (March 2008). Available at: <http://www.state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm> accessed 22 September 2016.

[231] Ibid.

[232] Financial Action Task Force, *Report on New Payment Methods* (n.63), 19-20.

in terms of price, in order to profit from the anonymity it affords.[233] The development through the use of NTPMs for the purposes of laundering or advancing funds for terrorist purpose has been one of searching for increased anonymity. These NTPMs are better than cash for moving funds for a number of reasons that add to the anonymity: non face-to-face business relationships (which favour the use of straw buyers and false identities), and the absence of credit risk due to the method usually being prepaid discourages service providers from obtaining complete and accurate customer information.[234] Wire transfers did not inherently provide anonymity, due to their being a paper trail, but the model was adapted and used as the basis for IMVTs which did manage to provide a level of anonymity, as they disposed with the paper trail and an individual could be identified on the basis of a number or code that they were given for collecting the cash. SVCs also inherently provide anonymity in that some cards are capable of being bought without any form of identification. Whilst Bitcoin has also provided anonymity, the level of protection afforded by it can be further increased, due to it being an internet currency, by using it alongside other identity maskers like Tor. In order to reduce the anonymity greater emphasis will have to be put on knowledge sharing and CDD being applied to NTPMs.

In terms of their detection, for all five of these NTPMs, at least in the early stages of transactions, there is often a reliance on different gatekeepers to those who usually police

[233] In one day the value of Bitcoin tumbled 21% to $8677.46 (see: Mark Gongloff, 'So, Bitcoin is Crashing' (Huffington Post 12 June 2013). Available at: <http://www.huffingtonpost.com/2013/12/06/bitcoin-crashes_n_4400392.html> accessed 22 September 2016). Its value is based on trust and demand, anything that hits either of these will see its value tumble. Throughout 2013 the exchange rate of Bitcoins was extremely volatile (see: Edward Southall and Mark Taylor (n.201), 178).

[234] Financial Action Task Force, 'Money Laundering through Money Remittance and Currency Exchange Providers' (n.17), 21.

the system. Ultimately, as seen with the above NTPMs they all do need to pass through the formal financial systems (traditional gatekeepers) at some point. Although Bitcoin could become an exception to this rule over the course of its lifetime. The general approach of AML regulation (whether at a global or national level) has focussed upon the use of key professions as de facto policemen, guarding entry points into the financial system and limiting the ability of criminals to transfer value without scrutiny.[235] But again Bitcoin offers a glimmer of a future threat in that if it is successful in becoming accepted as a currency in shops, if the Bitcoin cash machines become more readily available[236], and if there is still no way to regulate it due to it being decentralised then an alternative to the traditional gatekeepers will have to be sought otherwise potential cases of money laundering and terrorist financing will go more easily undetected. An alternative may lay in the banning of Bitcoin, like in Vietnam[237], but that would rest on deciding if its other benefits are sufficient or not to outweigh its detractions.

1.5. Rationale for a Comparative Research and Aims of the Thesis

This thesis utilises comparative law as the basis for further understanding of legal responses to the increasing threat of abuse of NTPMs by money launderers and terrorist financers. There is no universally accepted definition of 'comparative law', however this section will outline the rationale for pursuing this methodology.

---

[235] Joan Wadsley, 'Money Laundering: Professionals as Policemen' (n.18), 288.

[236] Matthew Sparkes, 'UK's First Bitcoin Cash Machine Launches in Shoreditch' (The Telegraph, 7 March 2014). Available at: <http://www.telegraph.co.uk/technology/10682842/UKs-first-Bitcoin-cash-machine-launches-in-Shoreditch.html> accessed 22 September 2016.

[237] The Hindu Times, 'Vietnam Bans Bitcoin' (28 February 2014). Available at: <http://www.thehindu.com/business/vietnam-bans-bitcoin/article5736019.ece> accessed 22 September 2016.

The essential ingredient of this method is that there is a comparison of more than one legal system.[238] These case studies are then 'explicitly contrasted to each other with regard to specific phenomenon or along certain dimension in order to pinpoint otherwise unobservable similarities and differences amongst them…'[239] As Kocka has stated 'often the look into the other country… or the other part of the world affords better understanding of one's own [position].'[240] Azarian takes that further by noting that 'by taking into consideration social actions and events belonging to other contexts, it enables us to see better the implicit and often taken for granted basis of our own practices and phenomena.'[241] Glenn provides us with a useful list of aims of comparative law, it is:

i. An instrument of learning and knowledge;
ii. An instrument of evolutionary and taxonomic science;
iii. A method of contributing to one's own legal system; and
iv. Utilised in the harmonisation of law.[242]

The origins of comparative work go back to the Antiquity, however it now gaining increasing popularity as a method of inquiry, this is highlighted recently by works in the field by

[238] Konrad Zweigert and Hein Kotz, *An Introduction to Comparative Law* (3rd edn., Oxford University Press, 1998), 4.

[239] Reza Azarian, 'Historical Comparison Re-Considered' (2011) 7(8) *Asian Social Science* 35, 35.

[240] Jurgen Kocka, 'The Use of Comparative History' in Ragnar Bjork, *Societies Made up of History: Essays in Historiography, Intellectual History, Professionalizations, Historical Social Theory and Proto-Industrialisation* (1st ed., Akedemitryck AB, Stockholm, 1996), 202.

[241] Reza Azarian, 'Potentials and Limitations of Comparative Method in Social Science' (2011) 1(4) *International Journal of Humanities and Social Science* 113, 115.

[242] H. Patrick Glenn, 'The Aims of Comparative Law, in: J.M.Smits, Elgar Encyclopedia of Comparative Law (1st edn., Cheltenham; Edward Elgar, 2006), 57-65.

Alhosani,[243] Ryder,[244] Pieth & Aiolfi,[245] and Lacey & George.[246] This should not come as any surprise given that anti-money laundering and counter-terrorist financing measures are driven from an international level and countries are assessed periodically against international standards. This makes comparison an increasingly obvious, if not flawless choice.

A key decision when it comes to comparative work is how many case study countries to include and which jurisdictions should be chosen. It is widely accepted that as the number of case studies increase, the level of detail decreases. This is particularly true of a thesis, consisting of a strict word limit. Further, having a limited number of countries was deemed important, so as to avoid deviant or 'outlier' results detracting from the analysis. Few country studies have been referred to by Lijphart as 'the comparative method'[247] and Ragin as 'case-orientated comparative methods'[248]. Therefore, to strike an adequate balance between the utility of findings across jurisdictions and the need to include sufficient detail, the decision was taken to focus on three case study countries: The United Kingdom, United States and

[243] Waleed Alhosani, *Anti-Money Laundering: A Comparative and Critical Analysis of the UK and UAE's Financial Intelligence Units* (1st edn., Palgrave Macmillan, 2016).

[244] Nicholas Ryder, *Money Laundering: An endless cycle* (n.4).

[245] Mark Pieth and Gemma Aiolfi, *A Comparative Guide to Anti-Money Laundering: A Critical Analysis of Systems in Singapore, Switzerland, the UK and the USA* (1st edn., Edward Elgar, 2004).

[246] Kathleen A. Lacey and Barbara Crutchfield George, 'Crackdown on Money Laundering: A Comparative Analysis of the Feasibility and Effectiveness of Domestic and Multilateral Policy Reforms (2003) 23(2) *Northwestern Journal of International Law & Business* 262.

[247] Arend P. Lijphart, 'Comparative Politics and the Comparative Method' (1971) 65(3) *American Political Science Review* 682; and Arend P. Lijphart, 'The Comparable-Case Strategy in Comparative Research' (1975) 8(2) *Comparative Political Studies* 158.

[248] Charles C. Ragin, *The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies* (1st edn., 1987, University of California Press, California), 34-52.

Australia – the specific factors for choosing these are detailed in the next subsection. Indeed, they were chosen mainly as each case study is of interest in their own right, and not merely as a bearer of a set of variables. However, it is worth noting here, the general criteria that played a part in their selection.

The first factor, and an easy one to pass, is that the country case studies had to be actively engaged with the international framework, that is that they engaged with United Nations Conventions in the area and were part of the Financial Action Task Force or one of the FATF-Style Regional Bodies, as it is the data from the FATF assessments that would underpin the analysis in this thesis. Further, if they were countries that played a prominent role in FATF, then they are responsible for the development of the international framework, something that we are looking at, in particular, in this thesis. Second, and a slightly limiting factor, was that the choice was predominantly limited to English speaking countries, as where translations of material are available they either tend to be not up to date, or technicalities may be lost in translation. There also tends to be little translation of material beyond legislation. Thirdly, and finally, it was decided that the country should be considered as an economically developed one, as this should mean they have the resources to finance their laws. By limiting the selection to these criteria and to three countries it meant that problems in terms of comparability and concept stretching were alleviated. Following such a process means that the case studies follow Sartori's view that 'entities to be compared should have both shared and non-shared attributes. They should be at the same time similar and

incomparable.'[249] This owes to the fact the main factor we are looking at in the study is the different approaches taken to meet the same international standards.

There are a few limitations to be aware of in this kind of work. First, owing to the choice of having only a few case studies, the findings cannot be used to derive sweeping generalisations explaining laundering and terrorist financing typologies in countries not studied, their external validity is low. However, this is not the aim of this thesis, and indeed the findings may be used to compare against other countries in future research. Secondly, as this thesis only focuses on a few case studies, these are not random selections, they have been chosen carefully for the purposes of the study.[250] and so whilst some findings may be unexpected, there should be little by way of surprise. It is intuitively obvious, particularly given the nature of this thesis, that there would be little point in comparing countries that are so different that hardly any commonalities can be found. After all, the thesis is dealing with an emerging threat, it is a given that owing to a great number of factors the United States is going to be infinitely better prepared to deal with criminal abuse of NTPMs than Saint Kitts and Nevis for instance. Thirdly, that simply importing rules and solutions from abroad may not work given a difference in backgrounds. Therefore, it is important that whilst differences are observed and noted as potentially being of use, that they are not taken as being a solution in all countries. Fourthly, the thesis to an extent in terms of comparison is limited by the lack of examples of application of the law in practice, so that whilst a particular solution may appear better, there is little by way of evidence to assess its effectiveness. Fifthly, and finally, a

[249] Giovanni Sartori, 'Comparing and Miscomparing' (1991) 3(3) *Journal of Theoretical Politics* 244.

[250] Charles C. Ragin, *The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies* (1st edn., 1987, University of California Press, California), 17.

comparative piece is highly dependent on data, it is not always the case that the same data will be available for all case study countries and that means that any comparison is unlikely to be done in perfect conditions. The data that is available will be dependent on interpretation and that relies on the author understanding the whole set of factors that influenced the data being compiled in the first place which can allow for skewed results.

That said, what cannot be denied, is that despite the few limitations, comparative analysis is an excellent way of assessing the response to a problem and pushing for improvement in the area. The three case study countries as stated above have a number of similarities, as well as their differences but the analysis contained forthwith is kept on track using the thematic approach outlined below.

The aim of this thesis is to assess the implementation of the global AML and CTF framework and its application to NTPMs. It does so by analysing the constituent parts of the international framework, from the international legislative measures of the UN and EU, to the standards which are set by the FATF. In doing so, seven thematic strands have been identified in order to best analyse the framework:

1. International role and implementation of the global AML and CTF framework;
2. Creation of competent authorities;
3. Criminalisation of money laundering and terrorist financing;
4. Adoption and application of the risk-based approach;
5. Counter-measures;
6. Confiscation of the proceeds of crime;
7. Mechanisms for international cooperation / mutual legal assistance.

The thesis then provides a comparative analytical commentary, using these thematic headings to consider how the policy has been implemented into three jurisdictions, and how they have applied it to NTPMs. The three jurisdictions are:

1. United Kingdom;
2. United States; and
3. Australia.

1.6. Why the United Kingdom?

The UK is perceived as a leader in terms of the global AML and CTF effort, it aims to encourage a hostile environment for illicit finances.[251] Its measures on both money laundering and terrorist financing predate the international community. Through the government's 2013 Serious Organised Crime Strategy plans are reaffirmed to restrict the ability of criminals to move, hide, and use the proceeds of crime.[252] Despite that HM Treasury reported that the level of laundered money annually in the UK is around £10bn.[253] Money Laundering is also a key enabler of serious and organised crime, the social and economic cost of which are estimated to be £24 billion a year.[254] Money Laundering is also a key enabler of serious and organised crime, the social and economic cost of which are estimated to be £24 billion a

[251] HM Treasury, 'Digital Currencies: Call for Information' (3rd November 2014) <https://www.gov.uk/government/consultations/call-for-information-anti-money-laundering-supervisory-regime/call-for-information-anti-money-laundering-supervisory-regime> accessed 22 September 2016.

[252] HM Government, *Serious and Organised Crime Strategy* (October 2013), 34. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf> accessed 22 September 2016.

[253] HM Treasury and the Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (October 2015), 3. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf> accessed 22 September 2016.

[254] Ibid.

year.[255] Whilst in terms of terrorism the UK remains a 'severe' threat.[256] Perhaps naturally, due to the size and complexity of the sector and its prominence in determining the UK's GDP, efforts to tackle money laundering and terrorist financing tend to focus on the financial sector. However, it is essential that given their efforts in this sector, that other areas are not overlooked, it must be remembered that criminals will look for the weakest link and seek to undermine that, therefore focus on NTPMs are important. By their own admission the UK has intelligence gaps, particularly in relation to NTPMs.[257] However, by the same token, they have taken a keen interest in understanding NTPMs, recently the UK government engaged in a public consultation for information on cryptocurrencies focussing on both the benefits and threats from their usage.[258] There is good reason for this focus given that the UK drugs market remains significant, and is estimated to be worth nearly £4 billion per annum[259], and a there was a clear UK link in terms of operation and usage of the Silk Road.[260] Therefore

[255] Ibid.

[256] MI5, 'What We Do'. Available at: <https://www.mi5.gov.uk/threat-levels> accessed 22 September 2016.

[257] HM Treasury and the Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (n.238), 5.

[258] HM Treasury, 'Digital Currencies: Call for Information' (n.236).

[259] Hannah Mills, Sara Skodbo, and Peter Blyth, *Understanding Organised Crime: Estimating the Scale and Understanding the Social and Economic Costs* (Home office, October 2013). Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246390/horr73.pdf> accessed 22 September 2016.

[260] See: Shiv Malik and Tom Fox-Brewster, 'Six Britons Arrested Over Silk Road 2.0 Amid Dark-Web Takedown' (The Guardian, 7 November 2014). Available at: <https://www.theguardian.com/technology/2014/nov/07/six-britons-arrested-silk-road-dark-web-takedown-online-drugs> accessed 22 September 2016. The Silk Road was a supposedly anonymous platform for the purchase of narcotics and other illicit items. With the goods being sent out through the postal system. A complex payment system was used; utilising Bitcoin as the payment mechanism and using the ESCROW system as a further filtering mechanism, in an attempt to hide the user's identity. Further, access to the Silk

strengthening the need for the UK to focus on the use of NTPMs. Further, with the introduction, in 2015, of the National Risk Assessment of Money Laundering and Terrorist Financing[261] significant focus has been placed on NTPMs. Finally, it is an interesting time to study the UK with the Conservative government having announced plans for the biggest reforms to money laundering regime in over a decade.[262]

1.7. Why the United States?

The US has long had an aggressive stance towards money laundering and terrorist financing. It is at the forefront of the global fight against financial crime.[263] The US AML policy predates that of the UK and Australia, dating back to the 1960s when the Department of Treasury became concerned about the link between 'illegal activities and offshore bank accounts'.[264] Whilst it also lead the way on CTF globally following 9/11. It is of great interest to see how a country which is so susceptible to financial abuse has adapted to the challenges it faces from the increasing usage of NTPMs. As to the amount of money laundered through the US each

Road was only available to users of the dark web which utilises an intricate server system to mask the identity of the client's IP address.

[261] HM Treasury and the Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (n.238).

[262] HM Treasury and Home Office, 'Biggest reforms to Money Laundering Regime in Over a Decade' (21 April 2016). Available at: <https://www.gov.uk/government/news/biggest-reforms-to-money-laundering-regime-in-over-a-decade> accessed 22 September 2016.

[263] The White House (Office of the Press Secretary), 'Fact Sheet: Obama Administration Announces Steps to Strengthen Financial Transparency, and Combat Money Laundering, Corruption and Tax Evasion' <https://www.whitehouse.gov/the-press-office/2016/05/05/fact-sheet-obama-administration-announces-steps-strengthen-financial> accessed 22 September 2016.

[264] Todd Doyle, 'Cleaning Up Anti-Money Laundering Strategies: Current FATF Tactics Needlessly Violate International Law' (2002) 24 *Houston Journal of International Law* 279, 287.

year, the figures fluctuate wildly, irrespective of which they are all significant sums: the General Accounting Office estimates $100bn[265], another estimate is $300bn[266], and one places it at $500bn[267]. In terms of terrorism, the US is still on alert, the Department of Homeland Security noting in its June 2016 National Terrorism Advisory System Bulletin that 'since issuing the first Bulletin in December 2015, their concerns that violent extremists could be inspired to conduct attacks inside the US have not diminished.'[268] The US has a keen interest in tackling NTPMs, particularly given the fact that terrorists utilised wire transfers to fund the 9/11 attacks.[269] Through its Money Laundering Threat Assessment (MLTA) it has regularly been an early identifier of threats to the financial system from NTPMs. As an example the 2005 MLTA highlighted a concern over the use of stored value cards.[270] It continues to monitor these emerging threats within its National Money Laundering Risk Assessment (NMLRA).[271] Indeed, the US held hearings on Bitcoin in 2013, and became the

---

[265] General Accounting Office, *Money Laundering: Needed Improvements for Reporting Suspicious Transactions Are Planned* (1995), 2. Available at: <http://www.gao.gov/assets/160/155076.pdf> accessed 22 September 2016.

[266] M. Radomyski, 'What Problems Has Money Laundering Posed for the Law Relating to Jurisdiction?' (n.4) 15(1) *Coventry Law Journal* 4, 6.

[267] General Accounting Office (n.251), 1.

[268] US Department of Homeland Security, 'National Terrorism Advisory System Bulletin' (15 June 2016). Available at <https://www.dhs.gov/sites/default/files/ntas/alerts/16_0615_NTAS_bulletin.pdf> accessed 22 September 2016.

[269] John Roth, Douglas Greenburg and Serena Wille, 'Monograph on Terrorist Financing' (Staff Report to the National Commission on Terrorist Attacks Upon the United States), 3. Available at: <http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf> accessed 22 September 2016.

[270] Money Laundering Threat Assessment Working Group, *US Money Laundering Threat Assessment (*December 2005), 20. Available at <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf> accessed 22 September 2016.

[271] See as an example: Department of the Treasury, *National Money Laundering Risk* Assessment (2015). Available at: <https://www.treasury.gov/resource-center/terrorist-

first government agency to issue an announcement related to the technology, highlighting its place as a leader.[272] Aside from financial crime the IRS was also the first tax agency in the world to clarify the treatment of Bitcoin and other digital currencies. So, it is of interest to see if the US lead the way in fighting the abuse of NTPMs for money laundering and terrorist financing, as they do with the general AML and CTF framework.

1.8. Why Australia?

Australia has a mixed history in terms of its AML and CTF compliance. It was once labelled as 'one of the leaders in counter money laundering laws', and some aspects classed as 'ground-breaking'.[273] However, in the FATF's 3rd Mutual Evaluation[274] of Australia's AML and CTF standards it was heavily criticised which resulted in 'both embarrassments for the Australian government and with it international scrutiny of the Australian AML system.'[275] This resulted in Australia being described as 'one of the easiest places to launder money',[276] and as a money

illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf> accessed 22 September 2016.

[272] Timothy B. Lee, This Senate Hearing is a Bitcoin Lovefest (The Washington Post, 18 November 2013) <https://www.washingtonpost.com/news/the-switch/wp/2013/11/18/this-senate-hearing-is-a-bitcoin-lovefest/> accessed 22 September 2016.

[273] Nigel Morris-Cotterill, 'Money Laundering Update' (2006) 34 (March) *Compliance Officer Bulletin* 1, 2.

[274] Financial Action Task Force, Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism, Australia (October 2005). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Australia%20full.pdf> accessed 22 September 2016.

[275] Chris MacNeil, 'Australian Anti-Money Laundering Reform in the International Context' (2007) 22(6) *Journal of International Banking Law and Regulation* 340.

[276] Alexa Rosdol, 'Are OFCs Leading the Fight Against Money Laundering?' (2007) 10(3) *Journal of Money Laundering Control* 337, 337.

laundering jurisdiction of 'primary concern' by the Department of State.[277] But in the recent 4th Mutual Evaluation Report there were signs of improvement, with FATF noting: 'Australia has a strong institutional framework for combatting ML, TF, and proliferation financing. Australia's measures are particularly strong in legal, law enforcement, and operational areas, and targeted financial sanctions, some improvements are needed in the framework for preventative measures and supervision'[278] and 'Australia has a good understanding of most of its main ML risks and coordinates comprehensively to address most of them.'[279]

In terms of the amount of money laundered through Australia varies: the Australian Crime Commission putting the figure between A$2.8bn and A$6.3bn[280], Sathye has placed it as high as A$11.5bn per year[281], whilst Australian Transaction Reports & Analysis Centre (AUSTRAC) puts it at between A$1.0 billion and A$ 4.5 billion, further stating that with some confidence it is around A$3.5 billion.[282] Turning to terrorism, Australia is not at the same threat level as

[277] Department of State, Bureau for International Narcotics and Law Enforcement Affairs, *International Narcotics Control Strategy Report Volume II Money Laundering and Financial Crimes* (March 2010), 223. Available at: <http://www.state.gov/documents/organization/137429.pdf> accessed 22 September 2016.

[278] Financial Action Task Force, Anti-Money Laundering and Counter-Terrorist Financing Measures (April 2015), 7. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 22 September 2016.

[279] Ibid.

[280] Australian Crime Commission, *Organised Crime in Australia 2009* (2010), 9.

[281] Milind Sathye, 'Estimating the Cost of Compliance of AMLCFT for Financial Institutions in Australia' (2008) 15(4) *Journal of Financial Crime* 347, 350.

[282] John Walker Consulting Services, *Estimates of the Extent of Money Laundering in and through Australia* (AUSTRAC, September 1995). Available at: <http://www.criminologyresearchcouncil.gov.au/reports/200304-33.pdf> accessed 22 September 2016.

the UK or US, with its threat level described as 'probable'[283], meaning it is perhaps less likely that terrorist funds would be channelled through the country, though no less important that it is countered. In saying that, Australia is one of the largest markets in the Asia-Pacific region, which makes it very susceptible to illicit financial activities.[284] One of the significant reasons for assessing Australia is that it is one of the few developed countries to have already been assessed, and had the 4th Mutual Evaluation report published, on the basis of its compliance with international standards. As with the UK and US, Australia has shown an interest in NTPMs, recently releasing a discussion paper on GST (Goods and Services Tax) treatment of digital currency, as well as being one of the first to have focussed on the tax element.[285] It is on the verge of introducing money laundering and terrorist financing regulation in the area.[286]

1.9. Conclusion

This chapter has introduced the main areas of this thesis: money laundering, terrorist financing, and NTPMs. In relation to NTPMs it has identified and analysed five prominent case study examples which highlight the challenges that regulators, supervisors and businesses face in dealing with NTPMs. As with any other technique or way to commit a crime, in order to evaluate to which extent the use of the internet and innovative payment instruments can

---

[283] Australian Government, 'Australian National Security' <https://www.nationalsecurity.gov.au/Securityandyourcommunity/Pages/National-Terrorism-Threat-Advisory-System.aspx> accessed 22 September 2016.

[284] Nicholas Ryder, *Money Laundering – An Endless Cycle* (1st edn, Routledge, 2012), 5.

[285] Australian Taxation Office, 'ATO Delivers Guidance on Bitcoin' (QC 42160, 20 August 2014) <https://www.ato.gov.au/Media-centre/Media-releases/ATO-delivers-guidance-on-Bitcoin/> accessed 22 September 2016.

[286] The Australian Government the Treasury, *Australian Government Response to the Senate Economics References Committee Report: Digital Currency* (May 2016) <http://www.treasury.gov.au/~/media/Treasury/Publications%20and%20Media/Publications/2016/Gov%20response%20to%20Digital%20Currency/Downloads/PDF/Government_response_Senate-Committee_Digital-Currency-report-prod.ashx> accessed 22 September 2016.

be convenient for or attractive to someone who is laundering money or financing terrorism, it is important to evaluate the elements of strength and weakness of such instruments and channels.[287] So, for each NTPM it asked:

1. Why the NTPM came about i.e. what was it developed to facilitate?
2. How that NTPM works?
3. What is the money laundering and terrorist financing risks it poses i.e. why have launderers and financers chose to abuse that particular method?
4. How has the NTPM evolved over time to differing counter measures?
5. How can misuse of that NTPM be detected?

Upon completing that, the chapter drew together some of the commonalities, in terms of risks, which will influence how regulators and standard setters attempt to deal with the money laundering and terrorist financing threat of NTPMs.

The rest of this thesis is split into four chapters. The second chapter of the thesis reviews the international AML and CTF framework and in particular its application to NTPMs. This chapter highlights the importance of an international response in terms of the abuse of NTPMs for the purposes of money laundering and terrorist financing, after all a common trend amongst NTPMs is that they are international in scope and break down national borders. The third chapter focusses on the UK, who have long been a leading player in terms of AML and CTF and who have taken a keen role in tackling NTPMs. The next chapter looks at the United States, which has a long history of addressing money laundering and terrorist financing, and which is often seen as a leading voice in terms of AML and CTF. The fifth chapter considers

[287] Merlonghi (n.73), 205.

the response of Australia, which has a mixed history in terms of AML and CTF, but which plays a significant role in improving standards in the Asia-Pacific region. The conclusion of this thesis presents the major findings as well as the future challenges in terms of money launderers and terrorist financers exploiting NTPMs.

Chapter 2 – The International AML and CTF Framework

The Global AML and CTF Framework and its application to Non-Traditional Payment Methods

> "The rapid development, increased functionality, and growing use of new payment products and services (NPPS) globally has created challenges for countries and private sector institutions in ensuring these products and services are not misused for money laundering and terrorist financing purposes… the FATF recognises the innovative use of emerging technologies in this area."[1]

2.1. Introduction

Money laundering and terrorist financing present a substantial threat to both the global financial markets and security systems around the world. Money laundering and terrorist financing do not occur in a vacuum, they typically involve funds and individuals crossing international borders. There is a growing recognition that Non-Traditional Payment Methods (NTPMs) offer the opportunity to criminals to conduct financial crime on a global basis with increasing ease and speed. Rick McDonnell has commented 'those looking to launder illicit

[1] Konrad Zweigert and Hein Kotz, *An introduction to Comparative Law* (3rd edn, Oxford University Press, 2011), 28.

gains or finance terrorism are continually seeking new methods.'[2] Therefore, it is more important than ever that there is an international coordinated response, both for money laundering and terrorist financing generally, and for financial crime through NTPMs. The International Monetary Fund (IMF) have made it clear that the international community regard the fight against money laundering and terrorist financing as a priority.[3] Indeed, this is not a new point, the European Union Council of Ministers stated 'measures adopted solely at a national or even Community level, without taking account of international coordination and cooperation, would have very limited effects.'[4] The goals at the heart of the international effort are: 'protecting the integrity and stability of the international financial system, cutting off the resources available to terrorists, and making it more difficult for those engaged in crime to profit from their criminal activities.'[5] The additional problem with NTPMs is that they continue to emerge and evolve meaning that the line which regulators and standard setters are aiming for is constantly moving. It is for this reason that it is recognised that the international framework needs to be 'appropriate, flexible and future proof.'[6] The Financial

[2] Financial Action Task Force, *Annual Report 2010 – 2011* (June 2011), 7. Available at: < http://www.fatf-gafi.org/media/fatf/documents/reports/FORMATTED%20ANNUAL%20REPORT%20FOR%20PRINTING.pdf> accessed 22 September 2016.

[3] International Monetary Fund, 'Anti-Money Laundering / Combating the Financing of Terrorism – Topics' <http://www.imf.org/external/np/leg/amlcft/eng/aml1.htm> accessed 22 September 2016.

[4] Council Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (the Third Money Laundering Directive), OJ L309 of 25 November 2005, recital 5.

[5] International Monetary Fund, 'Anti-Money Laundering / Combating the Financing of Terrorism – Topics' (n.3).

[6] Financial Action Task Force, *Money Laundering Using New Payment Methods* (October 2010), 66. Available at: <http://www.fatf-

Action Task Force (FATF), the international standard setter for anti-money laundering (AML) and counter-terrorist financing (CTF), builds into its 'soft law' 40 Recommendations a level of flexibility which enables it to adapt to new challenges and emerging threats.

On that basis, this chapter will identify and analyse the international AML and CTF framework as it applies to NTPMs. In particular, it will focus on whether the international framework's response to NTPMs is adequate.

2.2. Rationale for the International Framework

National and regional responses to money laundering and terrorist financing are guided by the international framework for AML and CTF. The international framework has been put in place for a variety of reasons, but there can be no more important reason than to have a global response to a global issue.[7] The phenomenon of globalisation as well as the development of technology[8] has led to money laundering and terrorist financing being increasingly prevalent problems in an era where money can be transferred across the world and back again in seconds. We live in an open and global financial world where funds are highly mobile and new payment tools develop rapidly. With this has come the issue of criminals seeking to abuse these developments, no longer are criminals confined by national

gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf > accessed 22 September 2016.

[7] IMF, 'Compliance with the AML / CFT International Standard: Lessons from a Cross-Country Analysis' (2011) WP/11/177, 11. Available at: <http://www.imf.org/external/pubs/ft/wp/2011/wp11177.pdf> accessed 22 September 2016.

[8] The emergence of high speed international transaction mechanisms such as wire transfers exacerbated the problem, as well as the advent of the internet. They broke down international border in a way that had previously been unimaginable. It meant that money launderers and terrorist financiers could achieve their aims without having to physically move their dirty money, lessening the chance of detection.

borders: they have the world at their fingertips and are seeking to 'penetrate the wider global financial system.'[9] Combatting money laundering and terrorist financing is not just a matter of fighting crime but of preserving the integrity of financial institutions and ultimately the financial system as a whole.[10] It has been argued extensively that domestic factors determine the likelihood of being able to comply with international standards[11], if that is the case then it is clear that less developed countries are inevitably going to be in a weaker position when it comes to implementation and that is why institutions like FATF and in particular the FATF-Style Regional Bodies (FSRB's) are so important due to the support that they offer. Due to this there is the desire to ensure a global minimum standard in relation to AML and CTF, any response is only as strong as its weakest element.[12] It is undesirable that a criminal would be able to target a weaker jurisdiction as a safe haven to launder their illicit gains.[13] An isolated approach would be particularly problematic given that money does not respect international borders, it takes intangible forms and is easily and quickly transferred over long distances, meaning that without some level of cooperation or knowledge sharing it would be almost impossible to trace. There has been concerted cross-border co-operation in thwarting the efforts of both launderers and terrorist financiers alike. In terms of NTPMs specifically, it is

[9] Financial Action Task Force, *FATF Annual Report 2007 – 2008* (June 2008), annex. Available at: <http://www.oecd.org/dataoecd/58/0/41141361.pdf> accessed 22 September 2016.

[10] For the comments of the 1992 FATF president, see Peter Reuter and Edwin M. Truman, *Chasing Dirty Money: The Fight Against Money Laundering* (1st edn, Institute for International Economics, 2004), 129.

[11] IMF, 'Compliance with the AML / CFT International Standard: Lessons from a Cross-Country Analysis' (n.7).

[12] Robert D. Putman, 'Diplomacy and Domestic Politics: The Logic of Two-level Games' (1988) 42(3) *International Organisation* 427.

[13] United Nations Office on Drugs and Crime, 'Money Laundering and the Financing of Terrorism: The United Nations Response', 20. Available at: <http://www.imolin.org/pdf/imolin/UNres03e.pdf> accessed 22 September 2016.

notable of all five of the case studies have the potential to facilitate the international transfer of funds and hence the need for the international community to act. The FATF have noted the need for an international response to the money laundering and terrorist financing threat of NTPMs: 'establishing some form of guidance across all jurisdictions that treat similar products and services consistently according to their function and risk profile is essential to enhance the effectiveness of the international AML/CTF standards.'[14]

2.3. The International Legal Framework

The International AML and CTF framework consists of a variety of different Conventions, Recommendations, and Principles formed by numerous international organisations; two of which, the UN and the FATF, have led the way. Other international organisations such as: The World Bank, the International Monetary Fund, The Egmont Group of Financial Intelligence Units, and the Wolfsberg Group all filter in to this structure, and as such the FATF acts almost like an orchestrator. This lead Zweigert and Kotz to comment that the international law can be viewed as consisting of 'a patchwork of overlap and different animating principles.'[15] As these international standards have been implemented into the national legal frameworks of the vast majority of jurisdictions over the last decade, it highlights an acceptance of them and

[14] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (2015), 4. Available at <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 22 September 2016.

[15] Konrad Zweigert and Hein Kotz (n.1), 28.

their importance to the global response.[16] On a regional level the EU has also played a significant role through its Money Laundering Directives.[17]

As can be seen then from the different forms identified above, the international framework has measures which take effect in different ways. The measures can be described as either 'hard law' or 'soft law' depending on their type and how they are to be implemented into national law. It is beyond the ambit of this thesis to go into detailed debate of the theories behind 'hard law' and 'soft law' instead some guidance will be given as to what amounts to each. 'Hard law' refers to the kind of law that lay persons first think of, 'legally binding obligations that are precise (or can be made precise through adjudication or the issuance or the issuance of detailed regulations) and that delegate authority for interpreting and implementing the law.'[18] Therefore it is clear that both United Nations Treaties and the UN Security Council Resolutions can be classified as 'hard law'. The UN given its position and the measures it can enact is seen as being in the best position to lead both the international efforts against money laundering and terrorist financing.[19] 'Soft law' is altogether more difficult to determine as there is no universally accepted definition. Debate has centred on whether it is: law, quasi law, or not law at all.[20] Again, it is beyond the scope of the thesis to

[16] Indira Carr and Miriam Goldby, 'Recovering the Proceeds of Corruption: UNCAC and Anti-Money Laundering Standards' (2011) 2 *Journal of Business Law* 170, 187.

[17] The EU has produced four Money Laundering Directives, the most recent of which is: Council Directive 2015/849/EC of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [2015] OJ L141/73.

[18] Kenneth W. Abbott and Duncan Snidal, 'Hard and Soft Law in International Governance' (2000) 54(3) *International Organisation* 421, 421.

[19] Hardister, A 'Can We Buy Peace on Earth?: The Price of Freezing Terrorist Assets in a Post-September 11 World' (2003) 28 *North Carolina Journal of International Law and Commercial Regulation* 601, 624.

[20] See for debates: Dinah Shelton, *Commitment and Compliance: The Role of Non-binding Norms in the International Legal System* (1st ed., OUP 2000); Samuel A. Bleicher, 'The Legal

go into these kind of debates but guidance will be given as to what can amount to 'soft law'. Shelton has suggested that 'soft law' refers to: 'an international instrument other than a treaty that contains principles, norms, standards, or other statements of expected behaviour.'[21] In other words, normative provisions contained in non-binding texts.[22] Johnston states that such agreements are in frequent use on the international stage.[23] Further, he notes: their status as 'soft-law' does not necessarily give them less impact than legally binding instruments.[24] Shelton, in support of this, confirms that the use of political pressure can be used to induce others to change their practices.[25] But, she adds: 'generally, however, states cannot demand that others conform to legal norms the latter have not accepted.'[26] They are used over other forms of agreement due to the advantages that they offer, namely: their speed of adoption and because they are viewed as being useful for technical matters that may need rapid or repeated revision.[27] They can often function as an authoritative way to allow

---

Significance of Re-citation of General Assembly Resolutions' [1969] 63 AJIL 444; Hiram E. Chodosh, 'Neither Treaty nor Custom: The Emergence of Declarative International Law' (1991) 26 TEX. INT'L L.J. 87; Rosalyn Higgins, 'The Role of Resolutions of International Organisations in the Process of Creating Norms in the International System', in William .E. Butler, *International Law and the International System* (1st ed., Martinus Nijhoff Publishers 1987); Fredric L. Kirgis Jr., 'Customs on a Sliding Scale' (1987) 81 AJIL 146; and Christopher C. Joyner, U.N. 'General Assembly Resolutions and International Law: Rethinking the Contemporary Dynamics of Norm-Creation' (1981) 11 CAL. W. Int'L L.J. 445.

[21] Dinah Shelton, 'Normative Hierarchy in International Law' [2006] 100 AM. J. Int'l L. 291, 319.

[22] Ibid, 291.

[23] Douglas M. Johnston, *Consent and Commitment in the World Community: The Classification and Analysis of International Instruments (*1st ed., Brill| Nijhoff, 1997).

[24] Ibid.

[25] Dinah Shelton, Normative Hierarchy in International Law (n.21), 319.

[26] Ibid.

[27] Ibid, 322.

treaty parties to resolve ambiguities in a binding text or fill in gaps. From this, the FATF Recommendations can be considered 'soft law'. As noted above, they provide a set of broad principles permit countries to implement them how they see fit. The FATF, because of their status, do not have the power to adopt binding texts. They each bring their own advantages; 'hard law' measures being useful in that they transpose their provisions into national law (Conventions are binding in nature on their signatories), whilst 'soft law' measures are useful as they enforce a principle on an individual jurisdiction but leave it free to that jurisdiction to decide how best to implement it. The aim with the AML and CTF framework is that the two complement each other.

To explain how the two types of law complement each other, the international framework is essentially 'soft law' with 'hard law' elements. As noted above, the FATF orchestrate the AML and CTF framework through its 40 Recommendations, parts of which refer to the relevant 'hard law' measures of the UN, such as the criminalisation of money laundering and terrorist financing. This means that some elements have to be implemented, or there will be sanctions, but for the vast majority of the international framework, countries have freedom as to how to implement. This is useful given that individual countries may have different competing factors which influence their decision.[28] This may be particularly useful in relation to NTPMs

[28] At the heart of the international framework is recognition that independent jurisdictions have diverse legal, administrative, and operational frameworks and different financial systems, and so cannot take identical measures to counter these threats (see: FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, February 2012, 7). An example of this recognition comes from the FATF, whereby their 40 Recommendations set standards which countries should implement by tailoring to their own circumstances. This recognition is important as to try and impose a one-size-fits-all approach to the international framework would merely serve to hinder less developed nations if the framework was too arduous, whereas if the framework was set too low then it would be rendered useless. Therefore, by leaving it up to the individual states

as countries may want to be less restrictive in measures they implement in order to allow the NTPM to flourish. This is possible because of the 'soft law' nature of the 40 Recommendations, and in particular due to the FATF's risk-based approach (RBA) to the Recommendations. Further, despite the FATF Recommendations not being legally binding, Freeman has suggested that they are 'regarded as obligatory' to maintain good relations between states.[29]

2.3.1. Primary Institutions

2.3.1.1. The United Nations

'The UN provides an opportunity for the independent states of the world to discuss global issues which affect them both individually and collectively'.[30] To that end, the UN has long been at the forefront of the international community's efforts to tackle AML and CTF, taking an active role in promoting the harmonisation of countermeasures and the strengthening of international cooperation.[31] The birth of the international effort to tackle money laundering developed initially due to the concerns around the sale of narcotics, with the UN making the proceeds of crime an angle of attack. Therefore the UN's efforts are coordinated by the United Nations Office on Drugs and Crime (UNODC) who have a mandate to ensure that there are no

---

how they implement the aim of the recommendation they can do it in the most effective way for their country.

[29] Michael D. A. Freeman, *Lloyd's Introduction to Jurisprudence* (8th edn, Sweet and Maxwell Limited, 2008), 324.

[30] The United Nations Association – UK, 'What is the United Nations?' <http://www.una.org.uk/content/what-un> accessed 22 September 2016.

[31] United Nations Office on Drugs and Crime, *Money Laundering and the Financing of Terrorism: The United Nations Response*, 3. Available at: <https://www.imolin.org/pdf/imolin/UNres03e.pdf> accessed 22 September 2016.

gaps or loopholes in the international machinery.[32] The UNODC does this through its Global Program against Money Laundering (GPML). Since its introduction the Global Programme has been expanded to cover the proceeds of crime and the financing of terrorism.[33] It assists Governments in confronting criminals who launder the proceeds of crime through the international financial system.[34] The programme has the following aims:

- To assist in the achievement of the objective set up by the General Assembly at its twentieth special session for all States to adopt legislation that gives effect to the universal legal instruments against money laundering and countering the financing of terrorism;
- To equip States with the necessary knowledge, means and expertise to implement national legislation and the provisions contained in the measures for countering money laundering adopted by the General Assembly at its twentieth special session;
- To assist beneficially States in all regions to increase the specialised expertise and skills of criminal justice officials in the investigation and prosecution of complex financial crimes, particularly with regard to the financing of terrorism;
- To enhance international and regional cooperation in combatting the financing of terrorism through information exchange and mutual legal assistance;
- To strengthen the legal, financial and operational capacities of beneficial States to deal effectively with money laundering and the financing of terrorism.[35]

---

[32] Ibid.

[33] United Nations Office on Drugs and Crime, 'Technical Assistance Against Money-Laundering' <https://www.unodc.org/unodc/en/money-laundering/technical-assistance.html> accessed 22 September 2016.

[34] Ibid.

[35] Ibid.

Whilst the UN Convention for the Suppression of the Illicit Traffic in Dangerous Drugs marked the first time the UN focussed on confiscation of the proceeds of crime, the 1988 United Nations Convention against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances (The Vienna Convention) is seen as the breakthrough treaty. It provides 'comprehensive measures against drug trafficking, including provisions against laundering'.[36] It provided that signatories must, 'inter alia, criminalise the laundering of drug proceeds, implement instruments to allow for the determination of jurisdiction over the offence of money laundering, to permit the confiscation of the proceeds of the sale of illegal drugs and/or materials used in their manufacturing, mechanisms to facilitate extradition matters and measures to improve mutual legal assistance.'[37] Png, noted that 'the Vienna Convention represented a fundamental switch in the UN's AML policy away from targeting the manufacturing of illicit narcotic substances towards 'attacking the financial incentives of organised crime and criminal activities.'[38] The Convention was updated and upgraded by the General Assembly in 1998 through its adoption of a plan of action, "Countering Money Laundering" to fine tune and further strengthen the action of international community against the global criminal economy.[39] It was further reviewed in 2009 by a high-level segment of the Commission on Narcotic Drugs, which resulted in Member States adopting the 'Political

[36] United Nations Office on Drugs and Crime, 'United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988' <https://www.unodc.org/unodc/en/treaties/illicit-trafficking.html> accessed 22 September 2016.

[37] Nicholas Ryder, *Money Laundering – An Endless Cycle* (1st edn, Routledge, 2012), 12.

[38] C. Png, 'International Legal Sources I – The United Nations Conventions', in William Blair QC and Richard Brent, *Banks and Financial Crime – The International Law of Tainted Money* (1st edn, Oxford University Press, 2008), 43.

[39] United Nations Office on Drugs and Crime, *Money Laundering and the Financing of Terrorism: The United Nations Response* (n.31), 3.

Declaration and Plan of Action on International Cooperation towards and Integrated and Balanced Strategy to Counter the World Drug Problem'.[40] United Nations Convention against Transnational Organised Crime (the Palermo Convention) in 2000 widened the scope of money laundering to cover the proceeds of all serious crimes and not just drug-related crime.[41]

In 2000, the UN introduced the Convention against Transnational Organised Crime (Palermo Convention) to expand the fight against organised crime. The Palermo Convention, amongst other things: expanded the offence of money laundering to the proceeds of all crimes[42], required signatories to establish regulatory regimes to detect all forms of money laundering, and further promoted international cooperation and exchange of information.[43] The Palermo Convention reflected some of the measures previously introduced by the FATF. The Palermo Convention also obliges States to reinforce requirements for customer identification, record-keeping and the reporting of suspicious transactions. Parties are also advised to set up financial intelligence units to collect, analyse and disseminate information.[44]

[40] United Nations Office on Drugs and Crime, Political Declaration and Plan of Action on International Cooperation Towards an Integrated and Balanced Strategy to Counter the World Drug Problem (High-Level Segment Commission, March 2009), iii. Available at: <https://www.unodc.org/documents/ungass2016/V0984963-English.pdf> accessed 22 September 2016.

[41] United Nations Office on Drugs and Crime, *Money Laundering and the Financing of Terrorism: The United Nations Response* (n.31), 3.

[42] Palermo Convention, Article 6.

[43] Palermo Convention, Article 7 (1) (a) - (b), (3) and (4).

[44] United Nations Office on Drugs and Crime, *Money Laundering and the Financing of Terrorism: The United Nations Response* (n.31), 3.

In 1999 the UN approved its first CTF measure, the Terrorist Financing Convention[45] (CTF Convention). However, the CTF Convention did not come into force until 2002. Only four states (the United Kingdom, Botswana, Sri Lanka and Uzbekistan) ratified it before 9/11.[46] Post-9/11 the number of states that have ratified it stands at 187[47], highlighting the increased political will to counter terrorism.[48] The primary goal of the CTF Convention is to protect the financial system from being misused by a person planning, or engaged in terrorist activities.[49] The CTF Convention requires ratifying states to criminalise terrorism, terrorist organisations and terrorist acts.

Part of the reason for the high number of countries that have ratified the CTF Convention is Security Council Resolution 1373.[50] It required countries to:

- Criminalise the financing of terrorism;
- Freeze any funds related to person involved in acts of terrorism;
- Deny all forms of support for terrorist groups;
- Suppress the provision of safe haven, sustenance or support for terrorists;

[45] This Convention was formerly known as the International Convention for the Suppression of the Financing of Terrorism 1999.

[46] Michael Levi, 'Combatting the Financing of Terrorism: A History and Assessment of the Control of "Threat Finance"' (2010) 50(4) *British Journal Criminology* 650, 652.

[47] For up to date information on the status of the Terrorist Financing Convention, see: <https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-11&chapter=18&clang=_en> accessed 22 September 2016.

[48] Jude McCulloch and Sharon Pickering, 'Supressing the Financing of Terrorism – Proliferating State Crime, Eroding Censure and Extending Neo-Colonialism' (2005) 45 *British Journal of Criminology* 470.

[49] Terrorist Financing Convention 1999, Preamble. Available at: <http://www.un.org/law/cod/finterr.htm> accessed 22 September 2016.

[50] Security Council Resolutions are passed in response to a threat to international peace and security and are binding upon all UN member countries.

- Cooperate with other countries in criminal investigations and sharing information about planned terrorist acts.

Alongside the above the Resolution also called on all States to become parties, as soon as possible, to the relevant international counter-terrorism legal instruments.[51]

Resolution 1373 moreover created the Security Council's Counter Terrorism Committee. Its role is to monitor the implementation of the resolution and monitor the performance of member states in building a global capacity against terrorism. The Council itself is made up of 15 members of the Security Council, and is the UN's leading body to promote collective action against terrorist financing.[52] The CTC has a directory, containing model legislation and other helpful information, for countries seeking help in improving their counter-terrorism infrastructures.[53]

Another Security Council Resolution of significance is 1267, which requires member States to freeze the assets of the Taliban, Osama Bin Laden and Al-Qaeda and entities owned or controlled by them, as designated by the 1267 Committee.

Two other UN initiatives of relevance in terms of CTF is the United Nations Counter-Terrorism Implementation Task Force (CTITF) and the United Nations Global Counter-Terrorism Strategy. CTITF was established by the Secretary-General in 2005 to ensure overall coordination and coherence in the counter-terrorism efforts of the UN system.[54] CTITF is

[51] Security Council Counter-Terrorism Committee, 'About the Counter-Terrorism Committee' <https://www.un.org/sc/ctc/about-us/> accessed 22 September 2016.

[52] Ibid.

[53] Ibid.

[54] United Nations Counter-Terrorism Implementation Task Force, 'Tackling the Financing of Terrorism' (CTITF Working Group Report, October 2009), ii. Available at:

primarily responsible for work on the United Nations Global Counter-Terrorism Strategy. As early as 2009, CTITF had a focus on NTPMs noting that they can 'be instrumental in buoying it by opening new channels through which terrorists can solicit and receive funds'.[55] They note that at the time 'mobile payments, the internet and electronic value cards' are the biggest risk, although 'each carry varying degrees of risk'.[56] As a result of this CTITF recommend that 'authorities should decide at what stage to apply regulation to technologies, keeping in mind that some technological developments become obsolete quickly'.[57] There is a recognition here, as there are by other bodies that regulation of NTPMs is a delicate process, regulators need to know when to intervene and when to allow a technology to flourish or leave it to fail. CTITF also note the need for 'international financial institutions (acting within their mandates), regulators and financial institutions… [to] raise awareness and provide guidance on best practices and discuss new regulatory approaches to mitigate risk'.[58]

It is of relevance to this thesis to note that despite the UN Conventions not directly relating to NTPMs, there are elements of them that are significant to mention. As noted all general measures in terms of AML and CTF apply to NTPMs. One area of particular note is the UN's emphasis on international cooperation. We have already identified in Chapter 1 that NTPMs are a global threat, and as such an internationally coordinated response is imperative. In the Vienna Convention it states: 'The purpose of this Convention is to promote co-operation among the parties so that they may address more effectively the various aspects of illicit

<http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_financing_eng_final.pdf> accessed 22 September 2016.

[55] Ibid, 14.

[56] Ibid.

[57] Ibid, 15.

[58] Ibid.

traffic in narcotic drugs and psychotropic substances having an international dimension'.[59] Further Conventions, such as the Palermo Convention and the CTF Convention have followed a similar path as the Vienna Convention, putting cooperation at the forefront of the efforts whilst extending the number of predicate crimes.[60] Indeed, the objective of the CTF Convention is 'the maintenance of international peace and security and the promotion of good-neighbourliness and friendly relations and cooperation amongst States.'[61] The importance that these Conventions have should not be underestimated, the Vienna Convention has 189 parties to the agreement[62], the Palermo Convention 187 parties[63], and the CTF Convention 187 parties.[64] Thus highlighting that international cooperation underpins the international AML/CTF framework and therefore there is a strong basis with which to begin tackling NTPMs.

[59] UN Convention Against the Illicit Traffic in Narcotic Drugs and Psychotropic Substance 1988, Article 2.

[60] A predicate crime is one which provides the resources for another criminal act, in this case money laundering.

[61] International Convention for the Suppression of the Financing of Terrorism 1999, Preamble.

[62] For information on the status of the Vienna Convention, see: <https://treaties.un.org/doc/Publication/MTDSG/Volume%20I/Chapter%20VI/VI-19.en.pdf> accessed 22 September 2016.

[63] For information on the status of the Palermo Convention, see: <https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en> accessed 22 September 2016.

[64] For up to date information on the status of the International Convention for the Suppression of the Financing of Terrorism 1999, see: <https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-11&chapter=18&clang=_en> accessed 22 September 2016.

2.3.1.2. The Financial Action Task Force

The above UN measures only represent one side of the international AML and CTF framework; the FATF and its 40 Recommendations also play a significant role. Indeed, the FATF has been described as the 'single most important international body in terms of the formulations of anti-money laundering policy'.[65] The FATF was formed in 1989, a year after the UN began its AML programme, by the G7[66] during its summit in Paris. Less than a year later, in April 1990, it issued its first report outlining Forty Recommendations to tackle money laundering.[67]

The FATF is an intergovernmental body and acts as the international standard setter for AML and CTF. It 'sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the financial system'.[68] At present there are over 180 countries in which the Recommendations are implemented and assessed.[69] However, only 34 of those are direct members of the FATF, the rest are members

[65] William C. Gilmore, *Dirty Money – The Evaluation of International Measures to Counter Money Laundering and the Financing of Terrorism* (3rd edn, Council of Europe Publishing, 2004), 89.

[66] The Group of Seven (G7) is an informal bloc of industrialised democracies that meets annually to discuss issues such as global economic governance, international security, and energy policy.

[67] Financial Action Task Force, 'History of the FATF' <http://www.fatf-gafi.org/about/historyofthefatf/> accessed 22 September 2016.

[68] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (February 2012, update June 2016), 7. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 22 September 2016.

[69] See: Financial Action Task Force, 'Members and Observers' <http://www.fatf-gafi.org/pages/aboutus/membersandobservers/> accessed 22 September 2016.

of FATF-Style Regional Bodies (FSRB's).[70] Its mandate operates in eight year cycles and currently runs until the end of December 2020.[71] As long as there is sufficient political will this will continue to be renewed. Typically, its mandate has focussed on the traditional financial sector; however, over time it has expanded to cover money service businesses and other NTPMs. The work of the FATF is funded by the Organisation for Economic Co-operation and Development (OECD).[72] National contributions to the OECD are based on a formula which takes account of the size of each member's economy.[73] The FATF budget for 2015 was €4,060,000.[74]

The FATF Recommendations are intended to play a complimentary role, alongside the UN measures, in the global AML and CTF framework. The FATF aims to ensure that the requirements of the FATF Recommendations are aligned with UN obligations. Thus, countries are able to implement both sets of measures with one legal or regulatory system despite the differences that exist between both sets of requirements.[75] The FATF also Recommendations also complement the UN instruments by covering additional technical issues that are not

[70] Ibid.

[71] Financial Action Task Force, *Financial Action Task Force Mandate 2012-2020* (April 2012), 8. Available at: <http://www.fatf-gafi.org/media/fatf/documents/FINAL%20FATF%20MANDATE%202012-2020.pdf> accessed 22 September 2016.

[72] Organisation for Economic Co-operation and Development, 'Financial Statements of the Organisation for Economic Co-operation and Development as at 31 December 2015' (23 June 2016), 47. Available at: <http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=BC(2016)20&docLanguage=en> accessed 22 September 2016.

[73] Organisation for Economic Co-operation and Development, 'Budget' <http://www.oecd.org/about/budget/> accessed 22 September 2016.

[74] Organisation for Economic Co-operation and Development (n.71).

[75] Financial Action Task Force, 'FATF Recommendations Support United Nations Instruments' < > accessed 22 September 2016.

covered by the UN instruments.[76] The Recommendations themselves provide a set of global AML and CTF standards that members of the FATF and FSRB's should strive to achieve. The CTF framework was affixed to the AML framework through the FATF in 2001, when they expanded their Forty Recommendations to the 40+8 Recommendations, with a ninth added in October 2004.[77] The Nine Special Recommendations focussed on CTF.[78] Following a comprehensive review in 2012, they reverted to just 40 Recommendations which focus on both AML and CTF, rather than separate Recommendations for each crime.[79] Schott has referred to them as 'mandates for action by a country if that country wants to be viewed by the international community as meeting international standards'.[80] They are however, non-binding, and the principles they promote are open to interpretation by states as to how best to implement them into national law. It is the FATF Recommendations that provide the themes for the approach this thesis takes to assessing the international framework and its implementation in relation to NTPMs. Whilst the above UN measures are imperative in the global money laundering and terrorist financing fight, it is the FATF measures that are more tailored to preventing the abuse of NTPMs.

Whilst large parts of the FATF Recommendations are applicable to NTPMs, there are also several specific recommendations that have been developed to specifically deal with the threat of NTPMs and these preventative measures are found under the 'additional measures

[76] Ibid.

[77] Financial Action Task Force, 'History of the FATF' (n.67).

[78] Ibid.

[79] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (n.68).

[80] Paul Allan Schott, *Reference Guide to Anti-Money Laundering and Combatting the Financing of Terrorism* (2nd edn, World Bank / IMF, 2006), III-9.

for specific customers and activities' subsection.[81] They will be outlined in full later in this chapter but identified here, they are:

- Recommendation 14 – Money or value transfer services;
- Recommendation 15 – New technologies;
- Recommendation 16 – Wire transfers.

It is clear from these three Recommendations, that when needed, the FATF will adapt their 40 Recommendations to address new emerging trends where it feels that those trends are not already covered by the guidance. They have recognised this point openly: 'our Recommendations will probably need periodic re-evaluation'.[82] Revisions are intended to 'provide a reinforced response to [current] threats and risks'.[83]

The FATF Recommendations are not sufficient on their own; in order for them to be truly effective they need to be complied with. To ensure this is the case the FATF has developed an assessment process consisting of; self-assessment questionnaires and mutual evaluations. The self-assessment questionnaire is useful as it allows FATF to establish common deficiencies and trends, so that they can determine priorities with regards to any technical assistance it may need to offer. It complements the mutual evaluation process as it provides the necessary preliminary information for the next mutual evaluation of that jurisdiction.[84] The mutual

[81] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (n.67), 14-16.

[82] Financial Action Task Force on Money Laundering: report of 6 February 1990, reproduced in William C. Gilmore, *Dirty Money – The Evaluation of International Measures to Counter Money Laundering and the Financing of Terrorism* (3rd edn, Council of Europe Publishing, 2004), 89.

[83] Financial Action Task Force, *Annual Report 2010 – 2011* (n.2), 7.

[84] Financial Action Task Force, *Review of FATF Anti-Money Laundering Systems and Mutual Evaluation Procedures 1992 – 1999* (February 2001), 1.

evaluation process provides an in depth description and analysis of each country's AML/CFT framework.[85] Importantly each evaluation is completed by a team comprised of 4-6 experts with legal, financial and law enforcement expertise and two members of the FATF Secretariat.[86] The aim of the whole assessment is to ensure the necessary laws, regulations, and other measures of the FATF are fully in force, and being implemented efficiently.[87] This process is not perfect, the FATF President in 2010 (Vlaanderen) stated that the process is often 'resource intensive and sometimes painful.'[88] But on the whole, the FATF through its mutual evaluation process has been 'very successful at ensuring that the standards are well applied by its jurisdictions and has been a model for many other organisations'.[89]

Once the FATF has undertaken its assessments with regards to the progress of its member states, if it finds deficiencies in the course of the assessments then it needs to take appropriate action. The first step that the FATF are likely to take is to send a letter to the non-compliant country or territory (NCCT) explaining their deficiency; this will be followed up by sending a delegation led by the FATF president to ensure deficiencies in the letter are being addressed. In more serious cases the FATF will not stop there they will seek to implement some of the following sanctions; urge financial institutions worldwide to scrutinise business relations and transactions with person, companies, and financial institutions domiciles in the

[85] Financial Action Task Force, 20 years of the FATF Recommendations 1990 – 2010 (June 2010), 6. Available at: <http://www.cbr.ru/today/anti_legalisation/fatf/20_years.pdf> accessed 22 September 2016.

[86] Financial Action Task Force, *Annual Report 2009 – 2010* (July 2010), 19. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2009%202010%20ENG.pdf> accessed 22 September 2016.

[87] Financial Action Task Force, *Annual Report 2010 – 2011* (n.2), 11.

[88] FATF President (Vlaanderen) on 'The Challenge of Compliance with the FATF Standards' 3rd June 2010.

[89] Financial Action Task Force, *Annual Report 2010 – 2011* (n.2), 5.

relevant country from the FATF membership.[90] The FATF also maintains the NCCT list on its website, the list provides a convenient record of all countries who are having problems meeting the FATF standards. The aim is that the list will invoke peer pressure on countries to comply with the 40 Recommendations.[91] FATF's efforts in identifying NCCT have been reinforced by consistent calls from the G20 to continue this successful work. The G20 has also called on the FATF to regularly update its public list on non-cooperative jurisdictions and jurisdictions with strategic deficiencies.[92]

The FATF also produces regular typology reports which review and report on money laundering and terrorist financing trends. In recent times these have focussed heavily on NTPMs: Hawala[93], Money Remittance and Currency Exchange Providers[94], Commercial

[90] Financial Action Task Force, Annual Report 1995 – 1996 (June 1996). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/1995%201996%20ENG.pdf> accessed 22 September 2016.

[91] Financial Action Task Force, 20 years of the FATF Recommendations 1990 – 2010 (n.84), 7.

[92] Financial Action Task Force, 'G20 Support for FATF's Work on Fighting Money Laundering and Terrorist Financing' <http://www.fatf-gafi.org/documents/documents/g20-communique-july-2013.html> accessed 22 September 2016.

[93] Financial Action Task Force, The Role of Hawala and other Similar Service Providers in Money Laundering and Terrorist Financing (October 2013). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf> accessed 22 September 2016.

[94] Financial Action Task Force, Money Laundering Through Money Remittance and Currency Exchange Providers (June 2010). Available at: <http://www.fatf-gafi.org/media/fatf/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf> accessed 22 September 2016; and Financial Action Task Force, *Guidance for a Risk-Based Approach Money or Value Transfer Services* (February 2016). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf> accessed 22 September 2016.

Websites and Internet Payment Systems[95], New Payment Methods[96], and Virtual Currencies[97]. This highlights the increasing focus being placed on NTPMs and the increasing threat they pose.

2.3.1.3 The European Union

The European Union has taken an active role in the development of international AML measures since their inception. In particular, they were involved with the United Nations 1988 Convention and the 1990 Council of Europe money laundering Convention. Its own efforts to tackle money laundering began in the 1970s when the European Council's European Committee on Crime Problems created a Select Committee to investigate the illegal transfer of the proceeds of crime between member states.[98] Further, the EU, through the European Commission, is one of only two regional organisations to be a full member of the FATF.[99] It

[95] Financial Action Task Force, *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems* (June 2008). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20TF%20Vulnerabilities%20of%20Commercial%20Websites%20and%20Internet%20Payment%20Systems.pdf> accessed 22 September 2016.

[96] Financial Action Task Force, *Report on New Payment Methods* (October 2006). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf> accessed 22 September 2016; and Financial Action Task Force, *Money Laundering Using New Payment Methods* (n.6), 66; and Financial Action Task Force, *FATF Report: Emerging Terrorist Financing Risks* (October 2015). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf> accessed 22 September 2016.

[97] Financial Action Task Force, *Virtual Currencies – Key Definitions and Potential AML/CTF Risks* (June 2014). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 22 September 2016.

[98] Nicholas Ryder, *Money Laundering – An Endless Cycle* (n.37), 12.

[99] Financial Action Task Force, 'FATF Members and Observers' <http://www.fatf-gafi.org/about/membersandobservers/> accessed 22 September 2016.

should also be noted that alongside this 'European Community Member States (all of the 'old' 15) have participated in the FATF either from its commencement or shortly afterwards, taking an active role in the development of the 40 Recommendations.[100] The European Commission also has observer status on the Committee of Experts on the evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL).[101] EU rules in this area are largely based on international standards adopted by the FATF; they are tailored to the EU's needs and complemented by national rules.[102] Alongside this there are a number of EU-wide cooperation initiatives, of particular relevance is the 'Expert Group on Money Laundering and Terrorist Financing (EGMLTF)'. The group meets regularly to share views and help the Commission define policy and draft new legislation. From the minutes of its meetings, it is clear that they take an interest in NTPMs.[103] The European Parliament have also issued briefing notes on NTPMs outlining their development and risks associated with their usage.[104] Interestingly the EU has also financially supported projects outside of the Union such as

[100] Valsamis Mitsilegas, Bill Gilmore, 'The Eu legislative framework against money laundering and terrorist financing: a critical analysis in the light of evolving global standards (2007) 56(1) International & Comparative Law Quarterly 119, 119.

[101] European Commission, 'Financial Crime' <http://ec.europa.eu/justice/civil/financial-crime/index_en.htm> accessed 22 September 2016.

[102] Ibid.

[103] For example, in the minutes of the EGMLTF meeting of 13 June 2014, there is extensive discussion of the threat emerging from virtual currencies. It also highlights the importance of information gathering by other bodies such as the European Banking Authority (EBA). European Commission, 'Register of Commission Expert Groups and Other Similar Entities: Expert Group on Money Laundering and Terrorist Financing (E02914)' (11 May 2015) <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2914&Lang=EN> accessed 22 September 2016.

[104] See as an example: European Parliamentary Research Group, 'Virtual Currencies: Challenges following their introduction' (PE 579.110, March 2016) <http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/579110/EPRS_BRI(2016)579110_EN.pdf> accessed 22 September 2016.

GAFISUDs (Financial Action Task Force of South America)[105] New Payment Methods report[106], showing a recognition that NTPMs need to be tackled on a global scale and highlighting the EU's global influence in fighting financial crime.

To date, the EU has implemented four Money Laundering Directives which banks and payment institutions fall under the scope of[107]: the First Anti-Money Laundering Directive[108], the Second Anti-Money Laundering Directive[109], the Third Anti-Money Laundering Directive[110], and the Fourth Anti-Money Laundering Directive[111] which all EU member states must be compliant with by 26th June 2017. It is worthy of note that the Third Directive was the first to extend the scope of the EU's AML regime to countering the financing of terrorism,

[105] Note that GAFISUD is now known as GAFILAT (Financial Action Task Force of Latin America.

[106] GAFISUD, 'Guide on New Payment Methods: Prepaid Cards, Mobile Payment and Internet Payment Services' (June 2013) <http://www.cocaineroute.eu/wp-content/uploads/2014/08/GUIDE-ON-NEW-PAYMENT-METHODS2.pdf> accessed 22 September 2016.

[107] European Commission, 'Fact Sheet: Questions and Answers: Anti-money Laundering Directive' (5 July 2016) <http://europa.eu/rapid/press-release_MEMO-16-2381_en.htm> accessed 22 September 2016.

[108] Council Directive 91/308/EEC of 10 June 1991 on Prevention of the Use of the Financial System for the Purpose of Money Laundering OJ L166/77.

[109] Council Directive 2001/97/EC of 4 December 2001 amending Council Direction 91/308/EEC on Prevention of the Use of the Financial System for the Purpose of Money Laundering – Commission Declaration OJ L344/76.

[110] Council Directive 2005/60/EC of 26 October 2005 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering and Terrorist Financing OJ L309/15.

[111] Council Directive (EU) 2015/849 of 20 May 2015 on the Prevention of the Use of The Financial System for the Purposes of Money Laundering or Terrorist Financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC OJ L141/73.

as well as adopting an 'all-crime' approach to money laundering.[112] Broadly speaking, the implementation of new Directives mirrors developments in the international framework (particularly those made by the FATF). It should also be noted that the 2006 Funds Transfer Regulation, which compliments the Third Directive, is being repealed by the new Wire Transfer Regulations 2 (WTR2) which is on the same implementation time scale as the Fourth AML Directive. All NTPMs fall within the remit of the Money Laundering Directives by virtue of them being payment methods utilised provided by institutions.

In relation to the Fourth Directive, there are a number of amendments proposed in the Commission's Action Plan which will tighten member states approach to NTPMs. The aim is to put these measures into place during 2016. The EUs focus on NTPMs is highlighted by the comments of First Vice-President Frans Timmermans: "In the coming months the Commission will update and develop EU rules and tools through well-designed measures to tackle emerging threats…".[113] First, in relation to virtual currencies (such Bitcoin) the updated Fourth Directive will contain a measure bringing virtual currency exchange platforms under the scope of the Directive to ensure the application of customer due diligence controls when exchanging virtual currency for fiat currency, in an effort to end the anonymity associated with such exchanges.[114] Further in relation to stored value cards they plan to lower the thresholds for identification and widen customer verification requirements.[115] These measures are being

[112] J. Fisher, 'Recent development in the fight against money laundering' (2002) 17(3) Journal of International Banking Law 67, 67.

[113] First Vice-President Frans Timmermans, 'European Commission – Press Release: Commission Presents Action Plan to Strengthen the Fight Against Terrorist Financing' (2 February 2016) <http://europa.eu/rapid/press-release_IP-16-202_en.htm> accessed 22 September 2016.

[114] Ibid.

[115] Ibid.

introduced to "improve the oversight of many financial means used by terrorists, from cash and cultural artefacts to virtual currencies and anonymous pre-paid cards, while avoiding unnecessary obstacles to the functioning of payments and financial markets for ordinary, law-abiding citizens."[116]

2.3.2. Secondary institutions

2.3.2.1. International Monetary Fund and the World Bank

Despite being two completely separate bodies, both organisations have identical goals with regards to AML and CTF, and thus work jointly in all of their efforts to achieve these goals.[117] Their engagement in the international AML/CFT effort dates back to early 2001[118] when they responded to calls from the international community to expand their work to AML and CTF. In conjunction with this the two Boards of Executive Directors of the World Bank and the IMF met, and recognised that money laundering is a problem of global concern that affects major financial markets and smaller ones.[119] Following 9/11 they increased their involvement in AML and CTF, recognising the FATF 40 Recommendations as the relevant international standards.

The IMF and the World Bank have set up a mechanism to co-ordinate the provision of technical assistance to countries to strengthen their economic, financial and legal systems

[116] Ibid, Vice-President Valdis Dombrovskis (in charge of the Euro and Social Dialogue).

[117] Paul Allan Schott, *Reference Guide to Anti-Money Laundering and Combatting the Financing of Terrorism* (2nd edn., World Bank / IMF, Washington DC, 2006), X-2.

[118] IMF, 'The IMF and the Fight Against Money Laundering and the Financing of Terrorism' (March 2016) <http://www.imf.org/external/np/exr/facts/aml.htm> accessed 22 September 2016.

[119] Paul Allan Schott, *Reference Guide to Anti-Money Laundering and Combatting the Financing of Terrorism* (2nd edn., World Bank / IMF, Washington DC, 2006), X-2.

with regards to money laundering and terrorist financing. The IMF has over thirty dedicated AML / CFT experts coming from diverse national and professional backgrounds,[120] thus giving them quite a wide scope for providing assistance and spotting new trends and themes. It was however stressed from the outset that the IMF's involvement in AML and CFT should be confined to its areas of competence.[121] The cooperation that it offers is based around the best practices and international standards derived from the Vienna Convention, the Terrorist Financing Convention, relevant Security Council Resolutions and the FATF 40+9 Recommendations.[122] Since 2009 most of this technical assistance has been financed via the Topical Trust Fund.[123] The primary objective of technical assistance provided by the World Bank and the IMF is to assist countries in the implementation of the full AML/CTF standard. Technical assistance includes:

- Designing institutional frameworks;
- Legislative drafting and the provision of legal advice;
- Enhancing financial supervisory regimes;

[120] IMF, 'Ongoing IMF Research Projects on Anti-Money Laundering / Combating the Financing of Terrorism: An Overview' (April 2007) <http://www.imf.org/external/np/leg/amlcft/eng/orpaml.htm> accessed 22 September 2016.

[121] N. Kyriakos-Saad, C-A. PNG, and J-F. Thony, 'Recent Developments in International Monetary Fund Involvement in Money Laundering and Combating the Financing of Terrorism Matters' <http://www.imf.org/external/np/leg/amlcft/eng/pdf/cdmfl_v4.pdf> accessed 22 September 2016.

[122] IMF, Anti-Money Laundering / Combating the Financing of Terrorism: Technical Assistance on AML / CFT <http://www.imf.org/external/np/leg/amlcft/eng/aml3.htm> accessed 22 September 2016.

[123] Topical Trust Fund, 'Anti-Money Laundering / Combating the Financing of Terrorism' (April 2009) <http://www.imf.org/external/np/otm/2009/anti-money.pdf> accessed 22 September 2016.

- Building capacity of financial intelligence units and other agencies.[124]

The Regional Policy Global Dialogue on AML/CTF series is one example of the technical assistance offered by the World Bank and the IMF, it provides the opportunity for countries to participate in a videoconference alongside staff of the IMF and World Bank, FSRB's, regional development banks and other international organisations to discuss and exchange information.[125] The purpose of the conference is to discuss and exchange information which is of interest to countries within a region. Whilst there is only some evidence to suggest that it is currently the case[126], these conferences would represent an appropriate forum for countries to discuss best practices in relation to NTPMs. Given that the FSRBs attend and as such there will be stronger and weaker countries within a region, then feedback would be able to be given on how the stronger countries have tackled the money laundering and terrorist financing threat of NTPMs.

The IMF and World Bank also assist the FATF in the mutual evaluation of member states. In 2002, the Bank, IMF and FATF worked in closely to establish a common methodology for assessing compliance with the 40 Recommendations. The methodology was agreed and

---

[124] IMF, 'Anti-Money Laundering and Combating the Financing of Terrorism: Observations from the Work Program and Implications Going Forward – Supplementary Information' (August 2005) 18 <https://www.imf.org/external/np/pp/eng/2005/083105s.pdf> accessed 22 September 2016.

[125] Paul Allan Schott, *Reference Guide to Anti-Money Laundering and Combatting the Financing of Terrorism* (2nd edn., World Bank / IMF, Washington DC, 2006), X-3.

[126] IMF, 'Anti-Money Laundering and Combating the Financing of Terrorism: Regional Videoconference: Central and West Africa Region—BCEAO (Banque Centrale des Etats de l'Afrique de L'Ouest), BEAC (Banque des Etats de l'Afrique Centrale), angola, Cape Verde, Democratic Republic of Congo, and Rwanda' (2003) <http://documents.worldbank.org/curated/en/879731468781780843/pdf/271850Anti1mon1entral010West0Africa.pdf> accessed 22 September 2016.

endorsed by the FATF at its October 2002 Plenary meeting.[127] This has been periodically updated over time to reflect updates to the FATF 40 Recommendations. It is available online so that countries are aware of what they are being assessed against.[128] This methodology ensures consistency in assessment, given that different individuals conduct assessments in different jurisdictions. The FATF, IMF and World Bank all recognised each other's Mutual Evaluation reports. Where the IMF undertake the mutual evaluation process of a jurisdiction they coincide it with their Financial Sector Assessment Program (FSAP) and the Offshore Financial Centres Assessment (OFC) which already incorporate elements of the FATF mutual evaluation procedure as part of their assessment. The result is that the workload for the AML/CFT assessments is shared between the FATF, the FSRB's, the IMF, and the World Bank[129], which results in efficiency gains in terms of time and money. Assessments are conducted roughly every seven years.

Further, the research that the IMF undertakes with regards to money laundering and terrorist financing contribute to the understanding of the area and as such are complimentary to the work of other organisations such as FATF. The research done by the IMF also serves to integrate the AML and CFT issues into the larger financial sector and macroeconomic agenda

---

[127] Financial Action Task Force, 'Financial Action Task Force on Money Laundering: Annual Report 2001–2002' (June 2002), 2. Available at <http://www.fatf-gafi.org/media/fatf/documents/reports/2001%202002%20ENG.pdf> accessed 22 September 2016.

[128] Financial Action Task Force, 'Methodology: For Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems' (February 2013). Available at <http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf> accessed 22 September 2016.

[129] N. Kyriakos-Saad, C-A. PNG, and J-F. Thony, 'Recent Developments in International Monetary Fund Involvement in Money Laundering and Combating the Financing of Terrorism Matters' 7 <http://www.imf.org/external/np/leg/amlcft/eng/pdf/cdmfl_v4.pdf>

of the fund.[130] It therefore broadens the scope beyond that of FATF by integrating AML and CFT threat with general financial practices and threats. The IMF has produced research papers and discussion notes on NTPMs.[131] Whilst, these do not focus solely on AML and CTF threats, such risks are considered within the wider discussion of the NTPM.

2.3.2.2. Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision (Basel Committee) was formed in 1974 by the central bank governors of the Group of 10 (G-10) Countries.[132] Countries are represented by their central back or their prudential regulation authority (where it is not the central bank). It has a more limited role than other international organisations discussed in this chapter. It does not have an overarching AML and CTF remit but it does involve itself in certain aspects of the international framework. 'The Basel Committee has no formal international authority or force of law; instead it articulates broad supervisory standards and guidelines and recommends statements of best practices on a wide range of bank supervisory issues'.[133]

---

[130] IMF, 'Ongoing IMF Research Projects on Anti-Money Laundering / Combating the Financing of Terrorism: An Overview' (April 2007) <http://www.imf.org/external/np/leg/amlcft/eng/orpaml.htm> accessed 22 September 2016.

[131] As examples see: Tanai Khiaonarong, 'IMF Working Paper: Oversight Issues in Mobile Payments' (WP/41/123, July 2014) <https://www.imf.org/external/pubs/ft/wp/2014/wp14123.pdf> accessed 22 September 2016 and Dong He, Karl Habermeier, Ross Leckow, et al, 'IMF Staff Discussion Note: Virtual Currencies and Beyond: Initial considerations' (SDN/16/03, January 2016) <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> accessed 22 September 2016.

[132] Note there are actually 11 members of the G-10: Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom and the United States.

[133] Paul Allan Schott, *Reference Guide to Anti-Money Laundering and Combatting the Financing of Terrorism* (2nd edn., World Bank / IMF, Washington DC, 2006), III-9.

In 1988, the Basel Committee issued its Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (Statement on Prevention).[134] It encompasses four main principles:

- Proper customer identification;
- High ethical standards and compliance with laws;
- Cooperation with law enforcement authorities; and
- Policies and procedures to adhere to the statement.

It has done further work in the area; in 1997, it introduced its Core Principles for Effective Banking Supervision (amended in 2006)[135] under which principle 15 (new principle 18) focuses on money laundering and in particular Know Your Customer (KYC) rules and how they should be implemented. These principles are supplemented by the 'Core Principles Methodology' which was also amended in 2006 to reflect the changes to the Core Principles, changing from 11 essential criteria and 5 additional criteria to 12 +1. In 1999 it added additional criteria to the 1997 principles; these stress the importance of compliance with the FATF recommendations so adding further weight to the BCBS influence on AML and CFT, whilst showing its support for the work of FATF in the area. To this end it has continued to support the work of FATF and worked together with FATF on amending the FATF Recommendations in 2003.

[134] BCBS, 'Prevention of Criminal Use of the Banking system for the Purpose of Money-Laundering' (December 1988) <http://www.bis.org/publ/bcbsc137.pdf> accessed 22 September 2016.

[135] Op. Cit n.1

Also it worked on a paper on Customer Due Diligence in Banks in 2001[136], which again had implications on the global AML framework, suggesting improvements for deficiencies in KYC procedures globally. As well as on 'Consolidated know Your Customer (KYC) Risk Management'[137] which worked further on KYC with regards to risk in the banking sector.

Whilst these measures are aimed at banks, the Basel Committee is of importance to this thesis for two reasons. First, often NTPMs will filter back into the formal financial system at some point and so it is important that the banking sector has high AML and CTF standards. Second, a lot of the standards it promotes and works on, with the international community will also be applicable to NTPMs, and so there may be some transferable knowledge from the Basel Committees work in relation to banks.

2.3.2.3. FATF-Style Regional Bodies

The FATF-Style Regional Bodies are seen by the FATF as being a way to influence global efforts and ensure the successful implementation of the FATF Recommendations in all areas of the world.[138] They are based on the FATF and have AML and CTF as their sole objectives. It has been noted that they are 'crucial for the long term viability of FATF's mandate'.[139] Their main task is ensuring the implementation of the FATF Recommendations amongst their regional

[136] BCBS, 'Customer Due Diligence for Banks' (2001) <http://www.bis.org/publ/bcbs85.htm> accessed 22 September 2016.

[137] BCBS, 'Consolidated know your Customer (KYC) Risk Management' (2004) <http://www.bis.org/publ/bcbs110.pdf> accessed 22 September 2016.

[138] Keesoony, Selina, 'International anti-money laws: the problems with enforcement' (2016) 19(2) Journal of Money Laundering Control, 130-147 at 133.

[139] FATF President Paul Vlaanderen (12th APG Annual Meeting), 'The essential role of the FATF style Regional Bodies (FSRBs) in the fight against money laundering and terrorist financing' (2009) <http://www.fatf-gafi.org/document/39/0,3746,en_32250379_32236879_43268455_1_1_1_1,00.html> accessed 22 September 2016.

membership.[140] In pursuance of this goal, they also give guidance to their members on how to improve their compliance, particularly to those countries with lower capacity.[141] They also assist the FATF in the mutual evaluation process, in the FATF year 2010-2011 the FSRB's undertook 22 mutual evaluations.[142]

There are currently nine FSRBs[143],taking into account their membership the FATF standards now reach over 180 countries, thus any initiatives that the FATF implement with regards to NTPMs are going to have a wide application. Membership is open to any country or jurisdiction within the given geographic region that is willing to abide by the rules and objectives of the organisation. 14 FATF members are also members of FSRB's[144], the identity of those 14 members can fluctuate depending on which two FATF member states are acting as representatives in MONEYVAL (the European FSRB), FATF members operate a two year rotating membership of MONEYVAL.

---

[140] Financial Action Task Force, *Annual Report 2007 – 2008* (June 2008), i. Available at: < http://www.fatf-gafi.org/media/fatf/documents/reports/2007-2008%20ENG.pdf> accessed 22 September 2016.

[141] Ibid.

[142] Financial Action Task Force, *Annual Report 2010 – 2011* (June 2011), 13. Available at: < http://www.fatf-gafi.org/media/fatf/documents/reports/FORMATTED%20ANNUAL%20REPORT%20FOR%20PRINTING.pdf> accessed 22 September 2016.

[143] They are: the Asia/Pacific Group on Money Laundering (APG; the Caribbean Financial Action Task Force (CFATF); Eurasian Group (EAG); Eastern & Southern African Anti-Money Laundering Group (ESAAMLG); Central Africa Anti-Money laundering Group (CABAC); Latin America Anti-Money Laundering Group (GAFILAT); Western Africa Money Laundering Group (GIABA); Middle East and North Africa Financial Action Task Force (MENAFATF); and Council of Europe Anti-Money Laundering Group (MONEYVAL).

[144] Financial Action Task Force, *Annual Report 2010 – 2011* (June 2011), 13. Available at: < http://www.fatf-gafi.org/media/fatf/documents/reports/FORMATTED%20ANNUAL%20REPORT%20FOR%20PRINTING.pdf> accessed 22 September 2016.

The FSRB's have 'associate member' status of the FATF.[145] The 'associate' member status grants FSRB's a number of rights; access for FSRB delegations to all FATF meetings, access for FSRB member jurisdictions to FATF working group meetings, access for FSRB member jurisdictions to FATF Plenary meetings, access to FATF documents, input on FATF discussions and decisions, assistance from FATF, right to participate in FATF mutual evaluations, FATF to further enhance joint exercises.[146] This increased status was the result of work by the FATF in the early 2000's to grow the level of cooperation between the FSRB's and FATF.[147]

The FSRB's are actively involved in a number of projects with the FATF that cover NTPMs. In 2010, MONEYVAL produced a joint report with FATF on money remittance providers, outlining the money laundering and terrorist financing risk.[148] MONEYVAL has also produced an extensive report on cybercrime covering a number of the NTPMs covered in this thesis.[149] There is further evidence of FSRB's focussing on NTPM's with the Asia/Pacific Group and the Eurasian Group holding a joint typologies and capacity building workshop with two days

---

[145] Financial Action Task Force, *Annual Report 2004 – 2005* (June 2005), Foreword. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2004%202005%20ENG.pdf> accessed 22 September 2016.

[146] Financial Action Task Force, *Annual Report 2009 – 2010* (July 2010), Foreword. Available at: < http://www.fatf-gafi.org/media/fatf/documents/reports/2009%202010%20ENG.pdf> accessed 22 September 2016.

[147] Financial Action Task Force, *Annual Report 2004 – 2005* (June 2005), Foreword. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2004%202005%20ENG.pdf> accessed 22 September 2016.

[148] Financial Action Task Force, 'Money Laundering through Money Remittance and Currency Exchange Providers' (June 2010) <http://www.coe.int/t/dghl/monitoring/moneyval/Activities/RepTyp_MSBs_en.pdf> accessed 22 September 2016.

[149] Moneyval, 'Research Report: Criminal Money Flows on the Internet: Methods, Trends and Multi-Stakeholder Counteraction' (March 2012) <http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)6_Reptyp_flows_en.pdf> accessed 22 September 2016.

dedicated to understanding virtual currencies.[150] As noted earlier in this thesis, GAFILAT and the European Union have also worked together to produce a report on NTPMs.[151] So it is clear from these examples[152] that there is a concerted effort by the FATF and its FSRBs to develop their members understanding of NTPMs.

2.3.2.4. The Egmont Group

The Egmont Group provides an international forum to promote and discuss the findings of the individual Financial Intelligence Units (FIU's). It leverages the capabilities of its membership to exchange information to fight money laundering, terrorism financing and other major crimes.[153] It was established in 1995 following the successful meeting of a group of FIU's, so far it has 151 members[154] and it meets on an informal basis. Essentially its role is to orchestrate the individual FIU's, which under the FATF Recommendations are obligatory for member states.

To be a member of the Egmont Group a country's FIU must meet their definition: *"a central, national agency responsible for receiving, (and as permitted, requesting), analysing and*

---

[150] APG, '2013 APG/EAG Joint Typologies and Capacity Building Workshop, 23–27 September, Ulaanbaatar, Mongolia' (September 2013) <http://www.apgml.org/events/details.aspx?e=309020bb-b42b-4ebf-8249-b2c7d3016bea> accessed 22 September 2016.

[151] GAFISUD, 'Guide on New Payment Methods: Prepaid Cards, Mobile Payment and Internet Payment Services' (June 2013) <http://www.cocaineroute.eu/wp-content/uploads/2014/08/GUIDE-ON-NEW-PAYMENT-METHODS2.pdf> accessed 22 September 2016.

[152] Note that this paragraph is not intended to provide an exhaustive list of the NTPM activities of FSRBs.

[153] Egmont Group, 'Summary Strategic Plan 2014-2017' (2014), 1 *<www.egmontgroup.org/library/download/355> accessed 22 September 2016.*

[154] Egmont Group, 'Annual Report 2014-2015' (2015). Available at <http://www.egmontgroup.org/library/annual-reports> accessed 22 September 2016.

disseminating to the competent authorities, disclosures of financial information: (i) Concerning suspected proceeds of crime and potential financing of terrorism, or (ii) Required by national legislation or regulation, in order to combat money laundering and terrorism financing."[155] A member must also commit to act in accordance with the Egmont Group's Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases.[156]

Given its role, the Egmont Group is key in the fight against abuse of NTPMs. In their strategic plan for 2014-2017 they identify virtual currencies and cybercrime as areas which need to be considered and responded to.[157] As will be seen below the suspicious activity reporting regime still applies to NTPMs and as such each country's FIU will receive reports about NTPMs. It is up to them to disseminate these reports amongst FIU's so that all FIU's can build technical capabilities in relation to NTPMs. In 2014-2015, the Egmont Group's Training Working Group coordinated and delivered seven training sessions and two operational executive training sessions on topics of operational relevance to FIUs.[158] One of these focussed on New Payment Methods[159] providing FIU's with the necessary training to deal with suspicious activity reports (SARs) relating to NTPMs. Further the Europe I Region of the

[155] Egmont Group, 'Interpretive Note Concerning the Egmont Definition of a Financial Intelligence' (2004) *<www.egmontgroup.org/library/download/8> accessed 22 September 2016.*

[156] Egmont Group, 'Statement of Purpose' <http://www.egmontgroup.org/statement_of_purpose> accessed 22 September 2016.

[157] The Egmont Group, 'Strategic Plan 2014-2017' (May 2015), 2 and 14.

[158] Egmont Group of Financial Intelligence Unites, Annual Report 2014-2015 (2015), 16. Available from: <http://www.egmontgroup.org/library/annual-reports> accessed 22 September 2016.

[159] Ibid.

Egmont Group has identified NTPMs as providing a problem for FIU's[160], and so attention will be focussed on improving this during 2015-2016.

2.3.2.5. The Wolfsberg Group

The Wolfsberg Group was founded in 2000 by a group of 12 banks[161], its role in the global AML and CFT framework has proven to be particularly successful, despite having no power in relation to the creation of legal frameworks. However, what it has done very well is to provide a vehicle for the constituent banks to voice their concerns. The Wolfsberg Group are the only international AML/CFT initiative which is run by the private sector, so it is giving a new perspective on the international AML/CTF framework.

The Wolfsberg Group has been able to achieve its aims of giving a voice to the private sector in a number of ways but mainly through the Wolfsberg Principles[162]. These were first published in 2000 and were most recently amended in 2014[163]. The Principles are supplemented by numerous guidelines. In the last decade the Wolfsberg Group have released statements on; the suppression of terrorist financing and numerous AML areas. The success

[160] Ibid, 32.

[161] Wolfsberg Group, 'Global Banks: Global Standards' 2012 <http://www.wolfsberg-principles.com/> accessed 22 September 2016.

[162] Wolfsberg Group, 'The Wolfsberg Global Anti-Money Laundering Guidelines for Private Banking' (2002) <http://www.wolfsberg-principles.com/pdf/Wolfsberg_AML_Guidelines_for_PB_(2002).pdf> accessed 22 September 2016.

[163] Wolfsberg Group, 'Wolfsberg Anti-Money Laundering Principles for Correspondent Banking' (2014) <http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg-Correspondent-Banking-Principles-2014.pdf> accessed 22 September 2016.

of these principles is primarily down to the coverage of its members which make up more that 60% of the world market in private banking.[164]

The success of the Wolfsberg Group's work has seen them play an active role in the development of the 40 Recommendations, in both 2003 and 2012. The Group has been appreciative of this and described it as "a testament to the progress made in effective engagement between the public and private sectors in recent years . . . which provide a unique opportunity to enhance the efficiency of the AML/CFT efforts as envisaged by the FATF standards."[165]

The Wolfsberg Group have also been active in relation to NTPMs. In 2011 it released guidance on Prepaid and Stored Value Cards noting that it is the 'most widely used of the New Payment Methods'.[166] The paper notes that whilst 'there is a widely held perception that all Prepaid and Stored Value Card arrangements represent a high risk of money laundering' that the Wolfsberg Group does not believe that view to be useful: 'there is a broad spectrum of risk for Card Arrangements, and . . . a generalised view of risk cannot be taken'.[167] It further noted the need for the adoption of a risk based-approach to stored value cards.[168]

---

[164] M.Pieth and G. Aiolfi, 'The Private Sector Becomes Active: The Wolfsberg Process' (2003) 10(4) J.F.C. 359, 362.

[165] Wolfsberg Group, 'Comment letter on the FATF consultation process', (6th January 2011), 1 <http://www.wolfsberg-principles.com/pdf/Wolfsberg_Group_Comment_Letter_on_FATF_Consultation_Paper_Jan-6th-2011_unsigned.pdf> accessed 22 September 2016.

[166] Wolfsberg Group, 'Wolfsberg Guidance on Prepaid and Stored Value Cards' (2011) 1 <http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14,_2011.pdf> accessed 22 September 2016.

[167] Ibid, 14.

[168] Ibid.

In 2014, the Wolfsberg Group also issue guidance on mobile and internet payment systems.[169] It notes that the growing use of NTPMs has resulted in 'greater complexity for regulators, and for financial institutions, in relation to assessing corresponding risk and the application of, and responsibility for, AML controls, particularly if the transactions flow through one or more jurisdictions and involve multiple service providers'.[170] It provides its opinions on the role of 'non-bank service providers (NBSPs)' noting that:

- NBSPs involved in money transmission should be subject to AML regulation / oversight;
- Unregulated NBSPs should be considered high risk;
- Financial Institutions need to consider their regulatory / reputation position of dealing with unregulated NBSPs if money transmission is involved; and
- Increased harmonisations of mobile, internet, and prepaid terminology is desirable to aid discussion and guidelines.[171]

These guidelines on NTPMs are useful, and the Wolfsberg Group clarifies that when considering these mobile payment providers they should not be considered to 'represent an automatic high risk of money laundering'.[172]

[169] Wolfsberg Group, 'Wolfsberg Guidance on Mobile and Internet Payment Services (MIPS)' (2014) <http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg-Group-MIPS-Paper-2014.pdf> accessed 22 September 2016.

[170] Ibid, 1–2.

[171] Ibid, 14.

[172] Ibid.

2.4. The Risk-Based Approach to Anti-Money Laundering and Counter-Terrorist Financing

The risk-based approach (RBA) is an integral part of the international response to money laundering and terrorist financing. The FATF states that the risk-based approach is preferred over the rule-based approach for a few reasons:

- A more efficient allocation of resources;
- It prioritises risk; and
- It minimises the burden for low-risk customers.[173]

The risk-based approach is outlined under Recommendation 1 of the 40 Recommendations; it can be split into two clear parts. First, '*countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively.*' This is more of a preparatory stage, identifying and assessing the risk; the next stage is the one which is of great importance. The framework then states '*based on that assessment, countries should apply a risk based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified*.' This is a beneficial step as it allows countries to adopt greater measures in areas of higher risk, and reduced measures where the risks are lower. Indeed the interpretative note to Recommendation 1 notes that '*by adopting a RBA, competent authorities, financial institutions and DNFBPs should be able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified, and would*

[173] Financial Action Task Force, 'FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion' (Report, February 2013) 29 <https://perma.cc/RN8Y-98Q9> accessed 22 September 2016.

enable them to make decisions on how to allocate their own resources in the most effective way.'[174] It is going to be of use with regards to NTPM's as it means that when a new emerging NTPM arises, as it poses a risk, countries should be taking measures to counter the threat. So in many ways Recommendation 1 alongside Recommendation 15 mean that NTPM's, even if they are not explicitly provided for in the international framework itself, should be being addressed by countries. It is worth noting that under the FATF methodology for assessing compliance with the 40 Recommendations there are a few key pieces of information when it comes to compliance with Recommendation 1. Countries are required to keep their risk assessments up to date.[175] Thus meaning any new money laundering and terrorist financing risks, including those posed by NTPM's, should be picked up by relevant countries in complying with the international framework. Based on this '*countries should apply a RBA to allocating resources and implementing measures to prevent or mitigate money laundering or terrorist financing*.'[176] So there is an onus on countries to have applied resources to areas which may themselves be under resourced in order to help them comply with AML and CFT requirements. Further worthy of note is that '*countries may only permit financial institutions… to take simplified measures to manage and mitigate risks, if lower risks have been identified, and criteria 1.9 to 1.11 are met. Simplified measures should not be permitted whenever there*

[174] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (February 2012, update June 2016), Interpretive Notes, 31. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 22 September 2016.

[175] Financial Action Task Force, 'Methodology: For Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems' (February 2013) 1.3. Available at <http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf> accessed 22 September 2016.

[176] Ibid.

is a suspicion of money laundering and terrorist financing.' So the circumstances where lower measures can be implemented are rare, and it seems unlikely that a NTPM when scrutinised would not present money laundering and terrorist financing risks. The RBA allows countries to mitigate financial exclusion, which represents a money laundering and terrorist financing risk and an impediment to achieving effective implementation of the FATF Recommendations.[177]

To assist countries in applying the RBA to NTPMs, the FATF has produced guidance papers, notably in relation to: prepaid cards, mobile payments and internet based payment services[178] and virtual currencies[179]. These should be read and applied, in conjunction with the FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment.[180] Factors which may indicate a high level of risk in relation to NTPMs include:

- The extent to which it can be used globally for making payments or transferring funds;[181]

[177] FATF, Guidance for a risk-based approach: Prepaid Cards, Mobile Payments and Internet-based payment services (June 2013), 27. Available at: < http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 22 September 2016.

[178] Ibid.

[179] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (n.14).

[180] Financial Action Task Force, 'National Money Laundering and Terrorist Financing Risk Assessment' (February 2013). Available at: <http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf> accessed 22 September 2016.

[181] FATF, 'Guidance for a risk-based approach: Prepaid Cards, Mobile Payments and Internet-based payment services' (June 2013), 15. Available at: < http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 11/07/2016; and Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (n.14), 9.

- Its re-usability;[182]
- The ability to be used by a large number of counterparties in a wide geographical area;[183] and
- The ability to be funded anonymously in a non-[184]face-to-face transaction (particularly where cash is the payment method used).[185]

Finally, the FATF notes that all measures introduced to mitigate the risk of abuse of NTPMs should be proportionate to the risk.[186]

2.5. The Criminalisation of Money Laundering and Terrorist Financing

Criminalisation is the foundation of the international approach to AML and CTF upon which everything else rests. The international standard setter for AML and CTF, the FATF, states that in its 40 Recommendations: '*Countries should criminalise money laundering on the basis of the* Vienna Convention*[187] and the* Palermo Convention.*[188] Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of*

[182] FATF, Guidance for a risk-based approach: Prepaid Cards, Mobile Payments and Internet-based payment services (June 2013), 14. Available at: < http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 11/07/2016.

[183] Ibid, 16.

[184] Ibid, 20.

[185] Ibid, 16.

[186] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (n.14), 12.

[187] UN Convention Against Illicit Traffic in Narcotics Drugs and Psychotropic Substances, 1988 <http://www.unodc.org/pdf/convention_1988_en.pdf> accessed 22 September 2016.

[188] UN Convention Against Transitional Organized Crime and the Protocols Thereto, 2004 <http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf> accessed 22 September 2016.

predicate offences.'[189] Whilst with regards to terrorist financing it states that: '*Countries should criminalise terrorist financing on the basis of the* Terrorist Financing Convention[190], *and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.'*[191]

This is an effective method employed by the FATF: first, the UN already has put in place the framework relating to AML and CTF. If the FATF also had a framework for AML and CTF then it would either simply duplicate the UN framework, or would have differences (which would cause issues relating to knowing which to implement, or render one ineffective). Secondly, as the FATF 40 Recommendations are soft law measures they are not legally binding. As the FATF's sole purpose is the prevention of money laundering and terrorist financing then it makes sense that they would refer its members to a hard law measure (of which the vast majority would already be members). This approach by the FATF also adds to the cohesiveness of the international framework. Thirdly, it would substantially increase the length of the 40 Recommendations by including money laundering and terrorist financing

[189] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (February 2012, update June 2016), Recommendation 3. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 22 September 2016.

[190] International Convention for the suppression of the Financing of Terrorism, 1999 <http://www.un.org/law/cod/finterr.htm> accessed 22 September 2016.

[191] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (February 2012, update June 2016), Recommendation 5. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 22 September 2016.

legislation under Recommendations 3 and 5. The 40 Recommendations are meant to be read as a guidance list of how a country should implement an effective AML and CTF framework.

As noted earlier in the chapter, the Vienna Convention was solely focussed on drug related money laundering; this distinction was removed by the Palermo Convention which widened the ambit of the crime to an all-crime money laundering offence. Article 7 of the Palermo convention is particularly important as it lays out criteria noting what jurisdictions should be doing with regards to AML.

Article 2(1) of the International Convention for the Suppression of Terrorist Financing provides clearly the approach which the UN wants individual jurisdictions to take when implementing CTF into national law:

> '*Any person commits an offence within the meaning of this convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out: (a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or (b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other persons not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing an act*.'

The UN has purposely construed the offence widely so as to make sure terrorist funds can be caught by the offence. Given the potential effects of TF the desire to have such a wide ranging set of offences so as to discourage people from assisting in the laundering of funds for the purposes of terrorist financing is obvious. If the seriousness of the crime is considered, then

it is obvious why it would be desirable to have such a wide ranging set of offences so as to discourage people from assisting in the laundering of funds for the purpose of terrorist financing. Article 2(3) further provides that it will not be a defence if the terrorist act did not actually occur. This highlights that the offence looks at the conduct and not the result of the crime.

Due to the nature of terrorist financing it is important that an international response to a terrorist act can be implemented immediately. The UN provides the vehicle for the international framework to do this, through its Security Council. Any Security Council Resolutions are instantaneously binding upon its members without the need for signatories. In the immediate aftermath of 9/11 the Security Council released Resolution 1373.[192] The Resolution 1373 comprises four key areas relating to countering terrorism, however for the purposes of this thesis it is the section on the suppression of the financing of terrorism that is important. In order to suppress terrorist financing, the Resolution imposes numerous obligations relating to cutting off the funds to terrorist, promoting the exchange of information and the denial of safe havens. Resolution 1373 made the cutting off of funds to terrorists an angle of attack.[193]

The UN also compliments other elements of the international framework with the United National Global Counter-Terrorism Strategy, it incorporate a dual strategy; Resolution

[192] The need to implement such a resolution highlights that the

[193] The Resolution also recognised that a failure to act would have a knock on effect in other areas such as; transnational organised crime, illicit drugs, money laundering, illegal arms trafficking, and illegal movement of nuclear, chemical, biological and other potentially deadly materials (for more see paragraph 4 of the Resolution). The UN had an interest in preventing these areas of crime as well so it makes sense to prevent money laundering and terrorist financing which could contribute to the growth of these other crimes.

60/288[194] and a plan of action.[195] This proved to be a significant step for both the UN and the global framework as a whole.

The international regulation will filter down to all of the case study countries so it needs to be set out. The next section will lay out the requirements and sanctions that the international framework puts into place which the case study countries have to implement.

In applying AML/CFT preventive measures to NTPMs, countries should consider which entities fall within the scope of the FATF Recommendations. In defining financial institutions, the FATF provides a list of financial activities or operations in the glossary to be covered for AML/CFT purposes.[196]

Providers of NTPMs fall within the definition of financial institution by conducting money or value transfer services, or by issuing and managing a means of payment, and therefore should be subject to AML/CFT preventive measures as required by the FATF Recommendations.[197] FATF's guidance does however permit countries to exempt activities that amount to a financial institution under the Interpretative Note to Recommendation 1, from the relevant preventative measures, in two situations:

---

[194] UN General Assembly Resolution 60/288, The United Nations Global Counter-Terrorism Strategy <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/504/88/PDF/N0550488.pdf?OpenElement> accessed 22 September 2016.

[195] UN, 'UN Global Counter-Terrorism Strategy' Plan of Action <https://www.un.org/counterterrorism/ctitf/en/un-global-counter-terrorism-strategy#plan> accessed 22 September 2016.

[196] Financial Action Task Force, Guidance for a risk-based approach: Prepaid Cards, Mobile Payments and Internet-based payment services (June 2013), 12. Available at: < http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 22 September 2016.

[197] Ibid.

1. Where there is a proven low risk of money laundering and terrorist financing[198]; or
2. When a financial activity (other than the transferring or money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is a low risk of money laundering and terrorist financing.[199]

It is unlikely given the fact that NTPMs have high risks potential, and are a mechanism for the transfer of money or value, that they would fall under either of these exemptions. Wire transfers and informal value transfer systems cannot benefit from the exemption due to financial activity being conducted on an occasional or very limited basis.[200]

One issue for countries will be determining which entity (or entities) in the provision of NTPMs should be responsible for the implementation of preventive measures and the application of such measures at the national level.[201] We have seen that AML and CTF measures cannot be implemented directly on digital currencies due to their decentralised nature. The FATF has helpfully recommended that the solution in this case is for countries to regulate digital currency exchanges, where the digital currency is transferred into fiat

[198] This occurs in strictly limited and justified circumstances; and it is related to a particular type of financial institution or activity, or Designated Non-Financial Business or Person.

[199] Financial Action Task Force, Guidance for a risk-based approach: Prepaid Cards, Mobile Payments and Internet-based payment services (June 2013), 13. Available at: < http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 22 September 2016.

[200] Recommendation 10 states that financial institutions should be required to undertake CDD measures when carrying out occasional transactions that are wire transfers.

[201] FATF, Guidance for a risk-based approach: Prepaid Cards, Mobile Payments and Internet-based payment services (June 2013), 12-13. Available at: < http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 22 September 2016.

currency.[202] They also suggest that in the alternate, digital currency activities may be prohibited in line with a countries other interests such as consumer protection, safety and soundness, and monetary policy.[203] If countries consider prohibition then they should take into account whether it would simply act to drive their usage underground and whether it would increase the risk globally.[204] Where prohibition is the step that is taken then countries still require outreach, education and enforcement actions.[205]

2.6. Preventive Measures

The international framework introduces a number of countermeasures when it comes to tackling money laundering and terrorist financing. They come from a range of places but mainly the FATF Recommendations. Article 7 of the UN Convention against Transnational Organised Crime provides that each signatory should implement a far-reaching AML regime for banks, other financial institutions and other groups that are vulnerable to money laundering. This should include requirements for customer identification, record keeping and the reporting of suspicious transactions.[206] Providers of NPPS fall within the definition of financial institution by conducting money or value transfer services, or by issuing and managing a means of payment, and therefore should be subject to AML/CFT preventive

[202] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (n.14), 9.

[203] Ibid.

[204] Ibid.

[205] Ibid.

[206] UN Convention against Transnational Organised Crime, art. 7(1)(a).

measures as required by the FATF Recommendations.[207] It is the aim of this subsection to introduce the different countermeasures and discuss their usefulness when it comes to NTPM's.

2.6.1. Customer Due Diligence

One of the main measures advocated by the international framework to counter money laundering and terrorist financing is the application of customer due diligence (CDD). CDD is an imperative measure when it comes to countering money laundering and terrorist financing, anonymous accounts and transactions are an inherent risk to the security of any country. The FATF has worked closely with the BCBS and the Wolfsberg Group in developing its CDD measures.[208] One of the major findings of chapter one was that anonymity is a key motivator in the use of NTPMs by launderers and terrorist financers, therefore it is important that CDD is applied to build up a history on the transactions and allow regulators to trace the funds back to the criminal. CDD address this as it seeks to maintain the paper trail by ensuring the institution keeps information about all its customers in case of financial crime, so that the perpetrator can be traced. The process is quite rightly a rigorous one in order to protect the

[207] Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (June 2013), 12. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 22 September 2016.

[208] As examples see: Wolfsberg Group, 'Comment letter on the FATF consultation process', (6th January 2011), 1. Available at: <http://www.wolfsberg-principles.com/pdf/Wolfsberg_Group_Comment_Letter_on_FATF_Consultation_Paper_Jan-6th-2011_unsigned.pdf> accessed 22 September 2016; and Financial Action Task Force, Guidance for a Risk-Based Approach: The Banking Sector (October 2014). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf> accessed 22 September 2016.

financial system, and provides little scope for when an institution would be able to avoid applying CDD.

Recommendation 10[209] of the FATF 40 Recommendations lays out the approach of the international framework with regards to CDD. Recommendation 10 provides that: 'financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.' Further it states the situations when CDD should be undertaken: 'when undertaking business relations, carrying out occasional transactions, there is suspicion of money laundering or terrorist financing, or the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data'.[210] The FATF notes in relation to NTPMs that: 'CDD is an effective measure to mitigate money laundering and terrorist financing risk' and further that 'under the RBA, the extent to which NTPM providers should take measures to identify and verify their customers identity will vary depending on the level of risk posed by the product.'[211] As a minimum the transaction record of a payment

[209] This Recommendation was heavily influenced by the early work of the Basel Committee on Banking Supervision (BCBS) particularly through its seminal paper in 1988: 'Prevention of the Criminal use of the Banking System for the Purpose of Money Laundering'(see: BCBS, Prevention of Criminal use of the Banking System for the purpose of Money-Laundering' (1988) <http://www.bis.org/publ/bcbsc137.pdf> accessed 22 September 2016), of which proper customer identification was one of four key principles (J-M. Koh, 'Suppressing Terrorist Financing and Money Laundering', (Springer, 2006; Berlin, Germany), 144).

[210] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (February 2012, update June 2016), Recommendation 10 (i-iv). Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 22 September 2016.

[211] Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (June 2013), 21. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 22 September 2016.

or funds transfer should include information identifying the parties to the transaction, any account(s) involved, the nature and date of the transaction, and the amount transferred.[212]

Whilst the above is straight forward in relation to the majority of NTPMs, a particular difficulty has arisen in relation to cryptocurrencies such as Bitcoin. Due to the decentralised structures they can adopt, the traditional approach of the financial institution / controlling institution implementing CDD measures cannot be relied upon. The FATF recommend that digital currency exchanges[213] are therefore responsible for implementing CDD measures.[214] It is suggested that CDD measures should be applied by digital currency exchanges when establishing business relations or when carrying out occasional transactions, using 'reliable, independent source documents, data or information.'[215] It is also noted by the FATF digital currency exchanges may carry out occasional wire transfers covered by Recommendation 16 and its Interpretive Note.[216]

Under the FATF Recommendations 'financial institutions' have freedom to adopt simplified CDD measures, or enhanced CDD measures depending on their assessment of the risk. For NTPM providers that establish business relations, a 'simplified set of CDD measures may be basic and minimal' but they must respond to the key CDD components.[217] But, NTPMs should

---

[212] Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (June 2013), 24. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 22 September 2016.

[213] Businesses which is responsible for exchanging digital currency for fiat currency.

[214] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (n.14), 12.

[215] Ibid.

[216] Ibid.

[217] Ibid.

also ensure that it has procedures in place to conduct enhanced CDD measures where high money laundering and terrorist financing risk is identified.[218] The greater the functionality of the NTPM, the more likely the need for enhanced CDD, particularly where the NTPM allows an individual to gain access without a face-to-face transaction.

2.6.2. Reporting Requirements

The FATF has stated that irrespective of the level of CDD employed, transaction monitoring and suspicious activity reporting is essential for all NTPMs.[219] They further note, that 'its importance is even greater, however, where obtaining reliability information on the customer may be difficult.'[220] FATF Recommendation 20 provides for the reporting of suspicious transactions, 'if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit.'[221] To assist in the detection of suspicious activity, NTPM providers should 'consider putting in place transaction monitoring systems which can detect suspicious activity based on money laundering and terrorism financing typologies and indicators.'[222]

---

[218] Ibid, 13.

[219] Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (June 2013), 22. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 22 September 2016.

[220] Ibid.

[221] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (February 2012, update June 2016), Recommendation 20. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 22 September 2016.

[222] Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (June 2013), 25. Available at:

In order to incentivise the reporting of suspicions Recommendation 21[223] provides that 'financial institutions, their directors, officers and employees should be protected against any criminal or civil penalty for breach of any restriction on disclosure of information, as long as the information is in good faith, and based on a suspicion.' Under the same Recommendation it is an offence to 'tip-off' a client or customer that a suspicious activity report (SAR) has been filed. These SAR's are sent to and collated by the Financial Intelligence Unit (FIU) in each country, they are then inputted into a database which can be accessed by all members of the Egmont Group.

Again, whilst traditional methods of suspicious activity reporting and transaction monitoring can be applied to the majority of NTPMs, digital currency provide a challenge for regulators. Whilst theoretically the public nature of transaction information available on the blockchain facilitates transaction reporting, due to the level of anonymity afforded by digital currencies, the blockchain's usefulness in for monitoring and identifying suspicious activity is hindered.[224]

2.6.4. Specific NTMP Measures

2.6.4.1. CDD in Relation to New Technologies

Recommendation 15 on CDD in relation to 'new technologies' is one of the most important in relation to NTPMs. It provides that 'Countries and financial institutions should identify and

<http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 22 September 2016.

[223] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (February 2012, update June 2016), Recommendation 21. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 22 September 2016.

[224] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (n.14), 11-13.

assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products.'[225] The type and extent of measures introduced under this Recommendation should be proportionate to the level of risk associated with the new payment product or service. An issue with this Recommendation is its wide application and the lack of Interpretative Note. Further, the guidance in the 'FATF Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems' simply rephrases the Recommendation itself.[226] Recently, given the advances in relation to cryptocurrencies and other NTPMs the FATF has provided some further assistance through Guidance Papers.[227] In assessing the risks of NTPMs, countries should consider the FATF Guidance for National Money Laundering and Terrorist Financing Risk Assessment[228], the FATF also notes that this should be combined with considering the Interpretive Note to Recommendation 10 on CDD.

---

[225] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (February 2012, update June 2016), 17. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 22 September 2016.

[226] Financial Action Task Force, 'Methodology: For Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems' (February 2013). Available at <http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf> accessed 22 September 2016.

[227] As examples see: Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (June 2013). Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 22 September 2016; and Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (n.14), 11-13.

[228] Financial Action Task Force, FATF Guidance: National Money Laundering and Terrorist Financing Risk Assessment (February 2013). Available at: <http://www.fatf-

A list of risk-factors that countries should consider when assessing NTPMs includes:

- Non-face-to-face relationships and anonymity;
- Geographical reach;
- Methods by which they are funded;
- If the NTPM is linked to cash;
- Segmentation of services; and
- Use of the risk matrix.[229]

The FATF clarified in its 2015 Guidance Paper on virtual currencies that national requirements in relation to Recommendation 15 should also apply to virtual currency payment products and services (VCCPS), this includes digital currency exchanges that transfer cryptocurrency for fiat currency.[230] It further notes that national authorities are expected to enforce the obligation, and financial institutions . . . should be proactive in fulfilling the expectations set forth in Recommendation 15.[231]

2.6.4.2. Wire Transfers

Recommendation 16 on Wire Transfers provides that '*countries should ensure that financial institutions include required and accurate originator information, and require beneficiary information, on wire transfers and related messages, and that the information remains with*

gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf> accessed 22 September 2016.

[229] Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (June 2013), 19-20. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 22 September 2016.

[230] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (n.14), 10.

[231] Ibid, 14.

the wire transfer or related message throughout the payment chain.' So basically modifying the customer due diligence requirements found under Recommendation 10 to be applicable to wire transfers. By ensuring that such information is required and that it follows the transaction then it means in suspected cases of money laundering or terrorist financing the funds can be traced back to the guilty party. It further provides that as with normal transactions '*countries should ensure that… financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out under UN Security Council Resolutions 1267 and 1373*.' This ensures that terrorists and launderers will not escape the ambit of 1267 and 1373 simply by using wire transfers. In terms of guidance upon the application of Recommendation 16, the FATF Methodology[232] is quite comprehensive in this area. It provides a de minimis limit of USD/EUR 1,000 for the application of Recommendation 16[233], unless a country imposes a lower limit itself[234]. This requirement ensures that the burden is not too great on the financial institution in terms of customer due diligence. It also provides that Recommendation 11 of the FATF 40 Recommendations, on record keeping, applies to wire transfers and is imposed the ordering financial institution.[235] It is worth noting that the FATF in their 'Guidance for a Risk Based Approach' have stated that '*prepaid cards that offer person-to person transfers have a functionality that is similar to wire transfers and should therefore be subject to*

[232] Financial Action Task Force, 'Methodology: For Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems' (February 2013). Available at <http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf> accessed 22 September 2016.

[233] Ibid 16.1.

[234] Ibid 16.3.

[235] Ibid 16.7.

Recommendation 16.'[236] So whereby a prepaid card is used to effect a transfer of funds between persons, similar to that of a wire transfer then Recommendation 16 applies. Where prepaid cards are used to purchase goods and services then the ordinary AML and CTF measures apply. Further in relation to virtual currencies, the FATF has clarified that Recommendation 16 also applied to them as 'usually, convertible virtual currency transactions will involve a wire transfer'.[237] Therefore virtual currency transfers should also have originator and beneficiary information.

2.6.4.3. Money or Value Transfer Services

Where NTPMs fall within the definition of Money or Value Transfer Services (MVTS)[238] under the Glossary to the FATF Recommendations then Recommendation 14 is applicable to them. It deals with the significant issue of MVTS not being licensed or registered. It states that '*countries should take measures to ensure that natural or legal person that provide money or value are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations Countries*

[236] Financial Action Task Force, 'Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services' (June 2013), 31. Available at <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 22 September 2016.

[237] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (n.14), 12.

[238] Money or value transfer services (MVTS) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions may include any new payment methods (Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (n.67), 123).

should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.'[239] It also provides that '*any natural or legal person working as an agent should be licensed or registered… or the MVTS should maintain a list of all its agents accessible by the competent authority.'*[240] Therefore it ensures that branches and franchises do not escape the framework. The FATF Methodology provides that it is the MVTS themselves which should be monitoring AML/CFT compliance[241], meaning that liability is on the MVTS to ensure compliance. Further under the FATF Methodology for Recommendation 16 it states that MVTS providers should 'be required to comply with all of the relevant provisions of Recommendation 16.'[242] This widens the application of Recommendation 16 and ensures that the considerable overlap between MVTS and wire transfers is comprehensively covered.

In relation to MVTS providers that offer cross-border services, countries should 'make it clear in both law and guidance that the jurisdictional licensing and/or registration criteria that applies to bricks-and-mortar MVTS also applies to these MVTS, even if the service provided is headquartered offshore.'[243] FATF has clarified that 'the registration / licensing requirements

---

[239] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (February 2012, update June 2016), 17. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 22 September 2016.

[240] Ibid.

[241] Financial Action Task Force, 'Methodology: For Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems' (February 2013) 14.3. Available at <http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf> accessed 22 September 2016.

[242] Ibid, 16.16.

[243] Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (June 2013), 30. Available at:

of Recommendation 14 also apply to domestic entities providing convertible virtual currency exchange services between virtual currency and fiat currencies.'[244]

2.7. Confiscation of the Proceeds of Crime

Confiscation of the proceeds of crime is at the heart of the action taken by the international community to counter AML and CTF. Arnone and Borlini state: 'a comprehensive legal answer to the serious threat of organised crime ought to include not only the repression of single offences, but also tracing, freezing and confiscation of the financial resources used by the organisations to survive and proliferate.'[245] Under Recommendation 4 of the FATF 40 Recommendations it is stated that: '*Countries should adopt measures similar to those set forth in the Vienna Convention, the Palermo Convention, and the Terrorist Financing Convention, including legislative measures, to allow competent authorities to freeze or seize and confiscate.'*

It was the Vienna Convention which initially recognised the importance of 'tracing, freezing and confiscating the proceeds of crime' but only with regards to drug related money laundering. Under Article 5 (1) (a) of the 1988 UN Convention confiscation of the proceeds of drug crime, or property to the value thereof. Whilst Article 5(2) makes it compulsory for the competent authorities in the necessary jurisdiction to 'identify, trace, and freeze or seize proceeds, property instrumentalities or any other things referred to in paragraph one of this

<http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 22 September 2016

[244] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (n.14), 10.

[245] M. Arnone and l. Borlini, 'International anti-money laundering programmes: empirical assessment and issues in criminal regulation' (2010) 13(3) J.M.L.C. 226, 230.

article, for the purpose of eventual confiscation.' The Palermo Convention widened the scope of the offence of money laundering so that tracing, freezing and seizing the proceeds could be done in relation to all crime money laundering. The Convention for the Suppression of Terrorist Financing, introduced the same measures for tracking funds advanced for the purposes of terrorism.

The definitions for 'freezing, seizing and confiscation' were initially laid out in the Vienna Convention and subsequently referred to in future Conventions. Article 1(l) of the Vienna Convention states that: "freezing or seizure means temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or a competent authority.[246]" Confiscation is defined in Article 1(f) as 'the permanent deprivation of property by order of a court or other competent authority.' These measures give members of the UN and members of FATF considerable powers to deal with the proceeds of crime or the resources of crime in order to prevent them reaching their end user. They are equally of use for both money laundering and terrorist financing.

It is appropriate that these measures are implemented on an international level as they are needed on a global scale, the confiscation, freezing and seizing offences are heavily reliant on the work done by the relevant bodies on customer identification, and so the KYC principles and frameworks discussed above that are laid out by the international framework have a direct effect on the potential success of the confiscation, freezing and seizing offences. If the

[246] UN, UN Convention against the illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988, <http://www.unodc.org/pdf/convention_1988_en.pdf> accessed 22 September 2016.

launderer or the financier cannot be identified, then there is no prospect of recovering the assets of the crime or preventing of the use of funds for a future crime.

The freezing, seizing and confiscation of funds is still of importance when it comes to countering NTPMs, the only question is how useful they actually prove to be. That will depend upon how much success the launderer or terrorist financer has in evading suspicion. But just because NTPMs may be more effective in channelling the funds to their end goal, does not mean that we should not have freezing, seizing and confiscation measures in place. The freezing of funds when it comes to NTPMs is just as important as with any other form of money laundering or terrorist financing. However, there is a lack of guidance on an international level as to how confiscation should take place when it involves NTPMs, particularly with something like cryptocurrencies where they utilise a new currency.

2.8. Cooperation and Mutual Legal Assistance

Cooperation and mutual legal assistance play a critical role in the international AML and CTF framework. Their importance is arguably heightened when considering money laundering and terrorist financing through NTPMs, as most NTPMs have a significant cross border element to them. In order to tackle the abuse of NTPMs there is a need for good communication and cooperation as the proceeds of crime can easily and quickly transfer from one country to another. The main mechanisms for international cooperation are found in FATF Recommendations 36-40.[247] This section will outline the mechanisms which facilitate an effective, coordinated response to the threat of money laundering and terrorist financing.

[247] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (n.67), 27.

Recommendation 36 prescribes in particular that countries take steps to become party to and implement fully: 'the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999.'[248]

Recommendation 37 focusses on Mutual Legal Assistance. Prost has defined Mutual Legal Assistance as a 'process by which states seek and provide assistance in gathering evidence for use in criminal cases or in the restraint and confiscation of the proceeds of crime'.[249] The Vienna Convention provides that signatories should provide 'the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to criminal offences.'[250] Prost has called this Convention 'the most important instrument for the advancement of mutual legal assistance.'[251] Some measures in the Vienna Convention were amended by the Palermo Convention. Article 18 of the Palermo Convention emphasises the importance of mutual legal assistance, 'State Parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences covered by this Convention.'[252]

FATF Recommendation 37 provides the international standard for mutual legal assistance 'countries should rapidly, constructively and effectively provide the widest possible range of

[248] Ibid.

[249] Kimberly Prost, 'No Hiding Place – How Justice Need Not be Blinded by Borders', in Steven David Brown, *Combating International Crime: The Longer Arm of the Law* (1 edn, Routledge Cavendish, 2008), 142.

[250] Article 7(1).

[251] Kimberly Prost, 'No Hiding Place – How Justice Need Not be Blinded by Borders', in Steven David Brown, *Combating International Crime: The Longer Arm of the Law* (1 edn, Routledge Cavendish, 2008), 143.

[252] Article 18.

mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions and related proceedings.'[253] The addition of mutual legal assistance in relation to predicate offences was added in 2012[254], and as such the UK and US are yet to be assessed against this increased standard. The FATF have clarified that Recommendation 38, on the freezing and confiscation of funds, extends to countries helping to identify, freeze, seize and confiscate proceeds and instrumentalities of crime which may take the form of virtual currency.[255] Further, the Recommendation provides that 'countries should have an adequate legal bases for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation.'[256] It is noted that in particular, countries should:

- Not restrict the provision of mutual legal assistance;
- Ensure that mutual legal assistance requests are dealt with in a timely manner, through an established body. To monitor this, countries should set up a case management system;
- Not use 'Fiscal matters' as an exemption to the provision of mutual legal assistance;
- Not use financial sector confidentiality and secrecy laws to override the obligation to provide mutual legal assistance;

[253] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (n.67), 27.

[254] Gary W. Sutton, 'The New FATF Standards' (2013) 4(1) Geo. Mason J. Int'l Com. Law 68, 129.

[255] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (n.14), 11.

[256] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (n.67), 27.

- Maintain the confidentiality of mutual legal assistance requests.[257]

Prost has further noted that: 'mutual legal assistance can be rendered directly between competent authorities in two states, often justice ministers. This is one of the features of mutual assistance which makes it an effective and efficient mechanism of co-operation.'[258] It is also worthy of note, that alongside the FATF standards on mutual legal assistance, the UN General Assembly have advanced a Model Treaty on Mutual Assistance. Prost notes that this provides an excellent guide for nations wishing to develop mutual legal assistance treaties.[259]

The EU as a regional body has also been active in the area, introducing a number of initiatives. Its members signed a Protocol to the Convention on Mutual Assistance in Criminal Matters.[260] In June 2003, the EU and the US also concluded a mutual legal assistance agreement.[261] The agreement increases the possibilities to exchange financial information between EU member states and the US in the context of criminal investigations.[262]

[257] Ibid.

[258] Kimberly Prost, 'No Hiding Place – How Justice Need Not be Blinded by Borders', in Steven David Brown, Combating International Crime: The Longer Arm of the Law (1 edn, Routledge Cavendish, 2008), 142.

[259] Ibid, 144.

[260] 1959 Council of Europe Convention on Mutual Legal Assistance in Criminal Matters.

[261] Council of Europe, EU/US Agreements on Extradition and on Mutual Legal Assistance (14826/09, 23 October 2009) <https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/110727.pdf> accessed 22 September 2016.

[262] Ibid, 2.

Recommendation 39 on Extradition is also worthy of note, the FATF has noted that countries must have effective extradition assistance in the context of virtual currency related crimes.[263] In particular countries should:

- Ensure money laundering and terrorist financing are extraditable offences;
- Ensure that they have clear and efficient processes for the timely execution of extradition requests, including prioritisation where appropriate;
- No place unreasonable or unduly restrictive conditions on the execution of requests; and
- Ensure they have an adequate legal framework for extradition.[264]

So whilst, the mutual legal assistance provisions are not tailored to NTPMs in the same way that other provisions are, they are still incredibly important to preventing the abuse of NTPMs for the purposes of money laundering and terrorist financing. Given the global reach of NTPMs it is imperative that countries have sufficient mutual legal assistance provisions in place.

2.9. Conclusion

This chapter has sought to outline the international response to the threat of money laundering and terrorist financing through NTPMs. It was identified in chapter 1 that there was a need for a global response to an international issue. FATF Recognised this stating 'the FATF still has a major job to do with setting standards, given the increasingly sophisticated

[263] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (n.14), 12.

[264] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (n.67), 29.

system.'[265] NTPMs do not respect international boundaries and as such countries are likely to be dealing with either transactions that have crossed international borders or transactions within their jurisdiction but where the NTPM operator is based outside their dominion. Ad hoc responses by independent jurisdictions would therefore lead to significant weaknesses AML/CTF framework and a huge inconsistency in approach. This would likely be more exaggerated in terms of NTPMs, particularly in relation to less developed countries who would lack the resources and know how to be first responders. Indeed, even developed countries may have different priorities and goals meaning that they would not have sufficient focus on NTPMs. Launders and terrorist financers are already known to target the weakest links of the global AML and CTF framework and therefore it's is important to set minimum standards to avoid this. As will be seen below, the international framework informs national jurisdictions of newly emerging NTPMS and their risk factors, provides standards to follow in terms of countering the abuse of NTPMs by launderers and terrorist financers, and facilitates the exchange of best practices between countries.

Whilst it is clear there are many international bodies with a focus on AML and CTF, what is less clear is how many of them are involved in efforts to tackle the abuse of NTPMs. It is obviously apparent the role that the FATF play in that they have produced a number of guidance papers on applying the risk-based approach to NTPMs, within which they identify how their 40 Recommendation apply to specific NTPMs. They also produce typology reports with the function of understanding and spreading knowledge in relation to NTPMs. Regionally we have also seen the EU and the FSRBs follow paths to the FATF. In terms of the other international organisations, they tend to have contribute to AML and CTF broadly, with the

[265] Financial Action Task Force, *FATF Annual Report 2007 – 2008* (n.9), 21.

FATF being left to tailor the approach to NTPMs. What has been particularly impressive to see is the ability of the FATF to update its 40 Recommendations inside assessment periods to reflect new threats.

Obviously, the international framework is only as effective as the desire of the constituents to implement it. For this reason, the rest of the thesis will look at three case study countries: the UK, US and Australia. It will consider their implementation of the international AML/CTF framework and how they have adapted to the threat of NTPMs, using the headings established in this chapter.

Chapter 3 – The United Kingdom

The United Kingdom's implementation of the international AML and CTF framework to tackle abuse of NTPMs

> "Law enforcement agencies have identified a common methodology whereby criminals are moving the proceeds of crime through a variety of channels and then onto a combination of new payment products in order to disguise and move criminally derived funds. Law enforcement agencies have identified, in a limited number of cases, criminals using large franchised money service businesses to purchase digital currencies from exchangers. This method, law enforcement agencies believe, has been developed to avoid the retail banking sector."[1]

3.1. Introduction

The third chapter of this thesis analyses and critically considers how the UK, in implementing the global anti-money laundering and counter-terrorist financing framework (identified in

[1] HM Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (October 2015), 87. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf> accessed 22 September 2016.

chapter 2), has dealt with the growing threat of criminals utilising non-traditional payment methods.

The UK has a longstanding history in efforts to counter money laundering and terrorist financing, often their measures have predated those of the international community, which makes it an interesting case study in terms of how it has adapted to new challenges. It aims to encourage a hostile environment for illicit finances.[2] Its AML and CTF framework encapsulates the legislative measures of the United Nations (UN) and the European Union (EU), as well as the Recommendations of the Financial Action Task Force (FATF). The governments' objectives are to deter, detect and disrupt money laundering and terrorist financing.[3] Any efforts to meet this must include tackling NTPMs, failure to do so would undermine the objective. In their 2007 Third Mutual Evaluation Report, the FATF stated that the United Kingdom has 'a comprehensive legal structure to combat money laundering and terrorist financing.'[4] There have been a number of developments in NTPMs since 2007, particularly with mobile payments and cryptocurrencies, despite this their compliance with the international framework should give them a firm basis which enables them to respond to

[2] HM Treasury, 'Call for Information: Anti-Money Laundering Supervisory Regime' (Updated 21 April 2016) <https://www.gov.uk/government/consultations/call-for-information-anti-money-laundering-supervisory-regime/call-for-information-anti-money-laundering-supervisory-regime> accessed 22 September 2016.

[3] HM Treasury, '*Anti-Money Laundering and Counter Terrorist Finance Supervision Report 2010-11'* (November 2011) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204350/amlctf_supervision_report_201011.pdf> accessed 22 September 2016.

[4] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (June 2007), 15. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20UK%20FULL.pdf> accessed 22 September 2016.

new challenges and threats. The UK wishes to foster an environment where legitimate actors flourish, and a hostile environment for illicit of innovative payment methods.[5]

The UK's anti-money laundering and counter financing of terrorism regime has a clear aim: to ensure that the UK financial system is a hostile environment for illicit finances, while minimising the burden on legitimate businesses and reducing the overall burden of regulation.[6] 'Our aim is a regime hostile to illicit finance and to terrorists, but which allows ordinary law-abiding citizens to freely access financial services'.[7] The government is firmly committed to 'tackling the scourge of money laundering and terrorist financing, which undermines the integrity of financial institutions and markets, and enables serious and organised crime, grand corruption, and terrorism'.[8]

In terms of actual instances of money laundering and terrorist financing in the UK, calculating this falls under the same pitfalls as laid out in the in chapter 1 when discussing the extent of money laundering and terrorist financing globally. Various bodies have given estimates on the extent of laundering each year in the UK; the Financial Services Authority estimate between

[5] HM Treasury, Digital Currencies: Response to the Call for Information (March 2015), 19. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 22 September 2016.

[6] HM Treasury, Anti-Money Laundering and Counter Terrorist Finance Supervision Report 2014 – 2015 (May 2016). Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/525355/anti-money-laundering-counter-terrorist-report-2014-15.pdf> accessed 22 September 2016.

[7] Ibid, foreword.

[8] Ibid.

£23bn and £57bn[9]; whilst HM Treasury suggest the figure is closer to £10bn[10]; and New Statesman put the figure at £48bn.[11] The National Crime Agency, an institution that should be well placed to give an estimate, stated that the amount of money laundered was unknown.[12] It is certain that the increasing use of NTPMs will in some, albeit rather small way, play a part in this uncertainty. However they did recognise that the scale of laundering is a 'strategic threat to the UK's economy and reputation'.[13] It is doubtful that any of the estimates take into account the use of NTPMs, and because of when the FSA and HM Treasury predictions were made, they would not have taken into account mobile payments or cryptocurrencies being used as a means for criminals to launder funds. Most likely, criminal funds moved by NTPMs form part of the UK's shadow economy and were not contemplated as part of these estimates. Whilst in terms of terrorism the UK remains a 'severe' threat.[14] Perhaps naturally, due to the size and complexity of the sector and its prominence in determining the UK's GDP, efforts to tackle money laundering and terrorist financing tend to

[9] Financial Services Authority, 'What is financial crime?' <www.fsa.gov.uk/pages/About/What/financial_crime/money_laundering/faqs/index.shtml > accessed 22 September 2016.

[10] HM Treasury, 'The Financial Challenge to Crime and Terrorism' (February 2007) <http://webarchive.nationalarchives.gov.uk/+/http:/www.hm-treasury.gov.uk/d/financialchallenge_crime_280207.pdf> accessed 8 August 2013.

[11] James Nickerson, 'I took a "kleptocracy tour" around London and discovered the corruption capital' (7 March 2016, New Statesman) <http://www.newstatesman.com/politics/economy/2016/03/i-took-kleptocracy-tour-around-london-and-discovered-corruption-capital> accessed 22 September 2016.

[12] National Crime Agency, 'National Strategic Assessment of Serious and Organised Crime 2015' (23rd June 2015) <http://www.nationalcrimeagency.gov.uk/publications/560-national-strategic-assessment-of-serious-and-organised-crime-2015/file> accessed 22 September 2016.

[13] Ibid.

[14] MI5, 'Threat Levels' <https://www.mi5.gov.uk/threat-levels> accessed 22 September 2016.

focus on the financial sector. However, it is essential that given their efforts in this sector, that other areas are not overlooked, it must be remembered that criminals will look for the weakest link and seek to undermine that, therefore focus on NTPMs are important. By their own admission the UK has intelligence gaps, particularly in relation to NTPMs.[15]

The most common way for criminals to move their funds in the UK is through the banking sector as it has one of the largest commercial banking sectors in the world. In 2005 there was £1,231bn worth of deposits held in UK banks[16] providing camouflage for the movement of illicit funds. However, the move towards alternative methods of laundering has been recognised. In the 3rd FATF Mutual Evaluation they noted the use of money and value transmission agents and wire transfers.[17] The Financial Conduct Authority recognised the risk of criminals abusing mobile payments.[18] HM Treasury acknowledged the threat to the UK of launderers utilising digital currencies, such as bitcoin, to move their funds.[19] Whilst the NTPMs discussed in this thesis are utilised to differing degrees what is clear is that they are all recognised as causing a threat. An important question to be answered in this chapter is how the UK's AML and CTF framework is addressing this risk.

---

[15] HM Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (n.1), 5.

[16] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 263.

[17] Ibid.

[18] Financial Conduct Authority, 'Thematic review: Mobile banking and payments' (September 2014) <https://www.fca.org.uk/static/documents/thematic-reviews/tr14-15.pdf> accessed 22 September 2016.

[19] HM Treasury, Digital Currencies: Response to the Call for Information (n.5).

In terms of AML and CTF strategy, HM Treasury takes the lead, in 2016 it published the 'action plan for anti-money laundering and counter-terrorist finance' in what it called "the most significant change to our anti-money laundering and counter-terrorist financing regime in over a decade."[20] The main legislative provisions are the Proceeds of Crime Act 2002, The Money Laundering Regulations 2007, and the Terrorism Act 2000 (as amended by the Anti-Terrorism, Crime and Security Act 2001; the Terrorism Act 2006; the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment Regulations 2007, and the Serious Crime Act 2015)). The next part of this chapter will assess the UK's implementation of the international AML and CTF framework, and in particular the parts of relevance to NTPMs.

3.2. Global Role and Implementation of the International AML/CTF Framework

This section will outline both the significant role that the UK plays in the international framework, as well as highlighting the international AML and CTF measures that it has implemented.

[20] Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance* (April 2016). Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517992/6-2118-Action_Plan_for_Anti-Money_Laundering__web_.pdf> accessed 22 September 2016.

The UN was introduced in Chapter 2[21], the UK has a long connection with the UN; in 1945 it was one of 51 states to sign the UN Charter, becoming a founding member.[22] In terms of AML and CTF, it has ratified the following UN Conventions:

- Vienna Convention (December 1990 and ratified June 1991);
- Palermo Convention (signed December 2000 and ratified in February 2006);
- International Convention for the Suppression of the Financing of Terrorism (signed January 2000 and ratified March 2001).

Alongside the above Conventions the provisions of S/RES/1267(1999) and S/RES/1373(2001) are also in effect in the UK owing to its membership of the UN.

Unlike the US and Australia, the UK as a member of the European Union is obliged to implement the AML and CTF measures introduced by the EU. As noted in Chapter 2[23], EU rules on AML and CTF are largely based on the international standards adopted by the FATF but tailored to the EU's needs and complemented by national rules. The following EU measures impact the UK AML and CTF framework:

- Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime 1990 (Ratified September 1990);

[21] See section 2.3.1.1. for an explanation of the role of the UN in the international AML & CTF Framework.

[22] United Nations Association – UK, 'What is the United Nations' <http://www.una.org.uk/content/what-un> accessed 22 September 2016.

[23] See section 2.3.1.3. for full explanation of the role of the EU in the international AML & CTF Framework.

- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism 2005 (Warsaw Convention) (signed 29/09/2014 and ratified 27/04/2015)[24];
- The First Money Laundering Directive (published 1991 and implemented 1993);
- The Second Money Laundering Directive (published 2001 and implemented 2003);
- The Third Money Laundering Directive (published 2005 and implemented 2007);
- The Wire Transfer Regulations[25];
- The Fourth Money Laundering Directive (published 2015 and likely implemented in early 2017).
- Wire Transfer Regulations 2[26].

As can be seen then, the UK has been active in implementing the UN and EU measures relating to money laundering and terrorist financing. The only measure that has caused an issue is the Warsaw Convention which took the UK nine years to sign and a decade to ratify. The reason put forward for the delay was that there 'had been "quite a knotty policy issue" over Article 47, which allows the postponement of transactions at the request of a foreign financial

[24] The UK received heavy criticism for its failure to implement this Convention in a timely manner, not least from the House of Lords who stated that 'we doubt there was ever any good reason for the delay in the signature of the Warsaw Convention by the United Kingdom . . .' and further 'the failure to sign and ratify the Warsaw Convention sends out a negative message about current United Kingdom commitment to the prevention and control of money laundering and the financing of terrorism.' (For more on this see: HL Paper 132-I, Chapter 2. Available at: <http://www.publications.parliament.uk/pa/ld200809/ldselect/ldeucom/132/13202.htm> accessed 22 September 2016).

[25] EC Regulation No 1781/2006 of 15 November 2006.

[26] Regulation (EU) 2015/847 of 20 May 2015.

intelligence unit.'[27] Despite this the House of Lords questioned whether the reason was sufficient and why it would take a further 18 months to implement.[28] Curiously it took a further 5 years to sign the Convention from the date of the House of Lords paper. The UK works closely with the European Commission to ensure that cross-European legislation is strong enough to prevent the use of the financial system for money laundering.[29] To that end the have published a response to the 'European Commission's report on the application of the Directive on the prevention of money laundering and terrorist financing'[30] and have helped shape proposals for the Fourth Money Laundering Directive.[31] As noted in Chapter 2 the Fourth Money Laundering Directive will contribute significantly to the UK's response to the threat of abuse of NTPMs, however it should be noted that as with other areas, the UK tends to respond prior to EU measures and go beyond the EU's minimum standard. Indeed the UK for instance has taken a proactive stance on digital currencies[32], the EU measures for which will only come into place in 2017.

[27] Stephen Webb in: HL Paper 132-I, Chapter 2. Available at: <http://www.publications.parliament.uk/pa/ld200809/ldselect/ldeucom/132/13205.htm#a22> accessed 22 September 2016.

[28] HL Paper (n.23).

[29] HM Treasury, *Policy Paper: Preventing Money Laundering* (June 2013). Available at: <https://www.gov.uk/government/publications/preventing-money-laundering/preventing-money-laundering> accessed 22 September 2016.

[30] HM Treasury, Report to the European Parliament and to the Council on the Application of the Directive 2005/60/EC on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing (June 2012). Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200634/fin_response_ec_report_application_directive_on_prevention_of_money_laundering_terrorist_financing.pdf> accessed 22 September 2016.

[31] HM Treasury, *Policy Paper: Preventing Money Laundering* (n.29).

[32] HM Treasury, Digital Currencies: Response to the Call for Information (n.5).

Of course implementation of the legislative instruments only tells one side of the UK's role in the international framework, there are also international standards and best practices to be taken into account.

The most important of these is the FATF. The UK was one of the original 16 members of the FATF and has chaired the organisation on two occasions; once in 1993[33] and again in 2007[34]. HM Treasury has noted that 'the UK played an instrumental role in its [the FATF] development'.[35] The UK 'continues to play a leading role in the development of global standards; the identification of new risks and typologies; the production of guidance and best practice, incorporating a risk-based approach; and the assessment of countries compliance with those standards.'[36] As well as this, the UK is a Cooperating and Supporting Nation to Caribbean FATF (CFATF) and Eastern and South African Anti-Money Laundering Group (ESAAMLG), and attends the Middle East North Africa FATF (MENAFATF) and MONEYVAL as an observer.[37] As well as being a key figure in the FATF's work, the FATF 'is central to the UK's international objectives'[38] in relation to its money laundering and terrorist financing strategy. The UK has performed strongly in the FATF's Mutual Evaluation programme, in its 2007 Third

[33] Financial Action Task Force, Annual Report 1993-1994 (June 1994). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/1993%201994%20ENG.pdf>

[34] Financial Action Task Force, Annual Report 2007-2008 (June 2008). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2007-2008%20ENG.pdf> accessed 22 September 2016.

[35] HM Treasury, *Policy Paper: Preventing Money Laundering* (n.29).

[36] HM Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (n.1), 13.

[37] Ibid.

[38] HM Treasury, 'Appointment of the UK President of the Financial Action Task Force'. Available at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/534959/hmt_advisory_notice_june_2016.pdf> accessed 22 September 2016.

Mutual Evaluation Report the FATF assessed the UK as being fully compliant with 19 of the 40 Recommendations, largely compliant on nine, partially compliant on nine and non-compliant on three Recommendations.[39] In terms of the Nine Special Recommendations on terrorist financing the UK was assessed as compliant on five, largely compliant on three, and partially compliant on one.[40] Importantly in relation to NTPMs it was rated as compliant with the Recommendation on 'new technologies & non face-to-face business', largely compliant with the Recommendation on 'money/value transfer services', and partially compliant with the Recommendation on 'wire transfers'.[41] So whilst overall the UK's implementation of the FATF's standards is good, there is room for improvement, particularly in relation to NTPMs. Overall, the FATF stated that the 'UK has a comprehensive legal structure to combat money laundering and terrorist financing. The money laundering offence is broad, fully covering the elements of the Vienna and Palermo Conventions, and the number of prosecutions and convictions is increasing.'[42]

Further to the above, the UK is also a member of various other international organisations. The UK FIU was a founding member of the Egmont Group and was granted full membership in June 1995. When the National Crime Agency (NCA) took over from the Serious Organised Crime Agency (SOCA) in October 2013 it has to complete a formal application to the Egmont

[39] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 283-287.

[40] Ibid, 287-288.

[41] Ibid, 283-288.

[42] Ibid 4.

Group in order to gain recognition.[43] The UK is also a member of the Basel Committee on Banking Supervision.

3.3. Competent Authorities

The UK has designated a number of competent authorities to the fight against money laundering and terrorist financing. In order to smooth the functioning of those regulating the area, there is a memorandum of understanding in place which is reviewed annually.[44]

3.3.1. Primary Authorities

3.1.1.1. HM Treasury

HM Treasury is government's economic and finance ministry with primary responsibility for setting the UK's economic policy. It works towards achieving strong and sustainable economic growth.[45] Under that ambit, it is the UK's leading AML and CTF authority. It has joint overall co-ordination of the UK AML/CTF policy alongside the Home Office[46]. It is also responsible for the implementation of the EU Money Laundering Directives and the Wire Transfer Directives, as well as the UN's financial sanctions obligations. HM Treasury also leads the UK delegation

[43] Ibid 85.

[44] FCA, 'Payment Systems Regulator Limited: Annual Report and Accounts 2015/2016' (HC 386, 12 July 2016) 30 <https://www.psr.org.uk/sites/default/files/media/PDF/PSR-annual-report-2015-2016.pdf> accessed 22 September 2016.

[45] HM Treasury, 'About Us', available at: <https://www.gov.uk/government/organisations/hm-treasury/about> accessed 22 September 2016.

[46] The role of the Home Office is introduced below in section 3.1.1.2.

to the FATF, as well as representing the UK at a variety of other international settings or conferences concerning AML & CTF.[47]

The pertinence of HM Treasury in relation to AML and CTF is highlighted by the fact that it was responsible, alongside the Home Office, for producing the UK's first National Risk Assessment (NRA) of Money Laundering and Terrorist Financing[48]. The aim of the assessment is to 'identify, understand and assess the money laundering and terrorist financing risks faced by the UK.'[49] It states that whilst the 'assessment should not be relied upon in isolation, the improved understanding it provides should assist the government, law enforcement agencies, supervisors and the private sector in targeting their resources at the areas of highest risk, ensuring that the UK's approach to preventing financial crime is risk-based and proportionate.'[50] It is clear from this then that HM Treasury plays a significant role in the UK's AML and CTF Framework. It is also clear that its role places a strong emphasis on NTPMs, the assessment focusses on emerging threats and recognises that knowledge of NTPMs 'is mixed'[51]. Based on the NRA, the HM Treasury and the Home Office have produced the risk-based Anti-Money Laundering Action Plan[52]. The Action Plan represents the most significant change to the UK's anti-money laundering and terrorist financing regime in over a decade[53],

[47] Financial Action Task Force, Third Mutual Evaluation Report Anti-Money Laundering and Combatting the Financing of Terrorism: The United Kingdom of Great Britain and Northern Ireland (n.35), 24.

[48] HM Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (n.1).

[49] Ibid, 3.

[50] Ibid, 4.

[51] Ibid, 5.

[52] Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance* (n.20).

[53] Ibid, 3.

replacing the 2004 Money Laundering Strategy.[54] The changes that it proposes will all be in place in time for the FATF's next on-site visit planned for February / March 2018.[55] The four priority areas identified are:

- A stronger partnership with the private sector;
- Enhancing the law enforcement response;
- Improving the effectiveness of the supervisory regime; and
- Increasing international reach.[56]

Under this Action Plan, HM Treasury has significant responsibilities in terms of ensuring that the action points are followed through, notably relating to: a stronger partnership with the private sector (running risk awareness programmes), improving the effectiveness of the supervisory regime, and developing a new approach to cross-border information sharing (in partnership with the Home Office).[57]

HM Treasury has taken a leading role in reducing the knowledge gap on digital currencies. In 2014 it launched a call for information[58] on the benefits and risks associated with the increasing usage of digital currencies, such as Bitcoin. In its 'response to the call for

---

[54] HM Treasury, *Anti-Money Laundering Strategy* (2004) available at: <http://webarchive.nationalarchives.gov.uk/+/http:/www.hm-treasury.gov.uk/media/D57/97/D579755E-BCDC-D4B3-19632628BD485787.pdf> accessed 22 September 2016.

[55] Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance* (n.20), 5-6.

[56] Ibid, 30.

[57] Ibid, 5-6.

[58] The original call for information can be found here: HM Treasury, 'Digital Currencies: Call for Information' (November 2014) available at: <https://www.gov.uk/government/consultations/digital-currencies-call-for-information> accessed 22 September 2016.

information', as well as highlighting the knowledge gained from responses, HM Treasury also outlines plans to bring digital currency exchange firms under the anti-money laundering regulatory umbrella, 'as it is at the point where users "cash in" and "cash out" of digital currency networks that money laundering and terrorist finance risk is highest.'[59]

3.1.1.2. Home Office

The Home Office works in conjunction with HM Treasury in co-ordinating the UK AML/CTF policy. It plays a fundamental role in the security and economic prosperity of the United Kingdom.[60] Two of its five priorities are to 'prevent terrorism' and 'cut crime'.[61] In terms of the AML and CTF regime, the Home Office takes responsibility for the asset recover scheme and the mutual legal assistance regime.

As noted above, the Home Office co-lead the development of the UK's 'Action Plan for AML and CTF' with HM Treasury. Under this Action Plan the Home Office has significant responsibilities in terms of ensuring that the action points are followed through, notably relating to: improving relations with the private sector (including reforming the suspicious activity reports (SARs) regime), enhancing the response of law enforcement; and increasing

[59] Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance* (n.20), 19.

[60] Home Office, 'About Us', available at: <https://www.gov.uk/government/organisations/home-office/about> accessed 22 September 2016.

[61] Ibid.

the UK's international reach (in relation to information sharing).[62] The Home Office also co-authored the UK's National Risk Assessment.[63]

Further, the Home Office, alongside the British Bankers' Association and the NCA, chairs the Serious and Organised Crime Financial Sector Forum.[64] That Forum established the Joint Money Laundering Intelligence Taskforce (JMLIT).[65]

3.1.1.3. Foreign and Commonwealth Office

The Foreign and Commonwealth Office has a very limited role in relation to money laundering and terrorist financing and it is restricted to the implementation of international Treaties and Conventions.[66]

3.3.2. Secondary Authorities

The secondary authorities supplement the work of the primary authorities. As can be seen from the National Risk Assessment and the Action Plan, the secondary authorities are delegated tasks and responsibility by the Home Office and HM Treasury.

3.3.2.1. The Financial Conduct Authority

The Financial Conduct Authority (FCA) is the supervisor for the financial sector. It was established in 2013 by the Financial Services Act 2012 which gave the Bank of England responsibility for protecting and enhancing financial stability, bringing together macro and

---

[62] Home Office and HM Treasury, Action Plan for Anti-Money Laundering and Counter-Terrorist Finance (n.20), 15-6.

[63] HM Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (n.1).

[64] Home Office and HM Treasury, Action Plan for Anti-Money Laundering and Counter-Terrorist Finance (n.20), 10.

[65] The JMLIT will be introduced below in section 3.3.3.1.

[66] Nicholas Ryder, *Money Laundering – An Endless Cycle?* (1st edn, Routledge, 2011), 80.

micro prudential regulation.[67] As part of this, the Financial Services Authority (FSA) was abolished and in its place a strengthened regulatory architecture was created within the Bank of England, consisting of the Financial Policy Committee, the Prudential Regulation Authority, and the FCA. The new structure was a response to the perceived failings of the FSA during the last financial crisis. In terms of its relevance to tackling financial crime, Teasdale suggests that the FCA was 'the recipient of an already developed enforcement strategy.'[68] The FCA has taken on all of the FSA's responsibilities relating to financial crime, including the role of supervisor under the Regulations. It works closely with the Prudential Regulation Authority (PRA) on these issues.[69]

Under the Financial Services Act 2012, the FCA when discharging its general functions must take action to minimise the risk of a business being used for a purpose connected with financial crime. The FCA requires all authorised firms to have systems and controls in place to mitigate the risk that they might be used to commit financial crime.[70] The FCA expects firms to do this on a risk-based basis noting that there is no 'one size fits all' approach.[71] Financial crime is given an intentionally wide definition under the Financial Services Act 2012; it

---

[67] HM Treasury, Financial Services Bill receives Royal Assent, available at: <https://www.gov.uk/government/news/financial-services-bill-receives-royal-assent> accessed 22 September 2016.

[68]Sara Teasdale, 'FSA to FCA; Recent Trends in UK Financial Conduct Regulation' (2011) 26(12) J.I.B.L.R. 583, 586.

[69] HM Treasury, 'Research and Analysis: Anti-Money Laundering and Counter Terrorist Finance Supervision Report' (Updated 26 May 2016) <https://www.gov.uk/government/publications/anti-money-laundering-and-counter-terrorist-finance-supervision-reports/anti-money-laundering-and-counter-terrorist-finance-supervision-report-2012-13> accessed 22 September 2016.

[70] Financial Conduct Authority, 'Financial Crime', available at: <https://www.fca.org.uk/firms/financial-crime> accessed 22 September 2016.

[71] Ibid.

includes any offence involving: fraud or dishonesty[72]; misconduct in, or misuse of information relating to, a financial market[73]; handling of the proceeds of crime[74]; or the financing of terrorism[75]. As is clear from the FCA's website, it follows a similar approach to the FSA, in that it focuses on the systems and controls that firms have in place, stating 'by using effective systems and controls, your firm can detect, prevent and deter financial crime.'[76] Part X Chapter 1 of the FSMA 2000 defines the FCAs rule-making powers and states it has the power to 'make rules in relation to the prevention and detection of money laundering.'[77] Further guidance on this can be found in the FCA Handbook under the SYSC Senior Management Arrangements, Systems and Controls section.[78]

In terms of knowledge building, the FCA has extensive powers to investigate financial crime. The powers to gather information are outlined in s.165 – 177 of the FSMA 2000, in particular the powers granted to the FCA include: to require information[79]; to appoint investigators[80]; to assist overseas regulators[81]; and to grant additional powers to investigators[82].

[72] Financial Services Act 2012, s.1H(3)(a)

[73] Ibid, s.1H(3)(b)

[74] Ibid, s.1H(3)(c)

[75] Ibid, s.1H(3)(d)

[76] Financial Conduct Authority, 'Financial Crime' (n.70).

[77] Financial Services and Markets Act 2000, s. 146.

[78] Financial Conduct Authority, 'FCA Handbook', available at: <https://www.handbook.fca.org.uk/handbook/SYSC/> accessed 22 September 2016.

[79] Financial Services and Markets Act 2000, s.165 and s.165A, B, and C.

[80] Ibid, s.167 and 168.

[81] Ibid, s.169 and 169A.

[82] Ibid, s.172.

Where the FCA has sufficient knowledge to advance a case then they can also advance a case in their own right[83], but must comply with any conditions or restrictions to that power laid down in writing by HM Treasury.[84] Should the FCA feel the need to then they can also impose two other punishments: financial penalties[85]; or suspend permission to carry out regulated activities[86]. These punishments are particularly useful deterrents to smaller NTPM providers who are still establishing themselves. As we will see NTPM providers have to be registered and thus suspending permission to carry out activities would remove their ability to legally operate in the sector.

Where the FCA is conducting an investigation which crosses international borders then it may seek assistance from abroad, similarly an international supervisor may request assistance from the FCA. The Financial Services Act 2012 updates s.354 of the Financial Services and Markets Act 2000, it gives the FCA must takes such steps as it considers appropriate to cooperate with others who either have similar functions to themselves or who will assist in the prevention or detection of financial crime.[87] As has already been noted, the cross border movement of funds for money laundering and terrorist financing is becoming ever more common, therefore it is imperative that the UK has sufficient mechanisms for cooperation and sharing information between organisations domestically and internationally. The thesis has also already highlighted how this will be a significant factor in countering the abuse of NTPMs given their tendency to facilitate cross-border transactions.

[83] Ibid, s.401(2)(a).

[84] Ibid, s.401(5).

[85] Ibid, s.206.

[86] Ibid, s.206A.

[87] Ibid, s.354A.

The FCA has demonstrated significant interest in NTPMs. They launched Project Innovate to foster innovation in financial services.[88] One of the noteworthy differences between the FCA and the FSA is that they have an objective to promote competition.[89] It is unusual amongst financial regulators for having such a mandate.[90] This involves promoting effective competition in the interests of consumers in the markets for regulated financial services[91], or services provided by a recognised investment exchange in carrying on regulated activities[92]. It has been noted, that: 'Innovation can benefit consumers, whether by reducing hassle, reducing costs or improving products. So we want to ensure that regulation unblocks these benefits rather than blocks them.'[93] There are two main strands to the work of Innovation Hub. The first strand is giving direct support to innovators. The second is considering how to adapt the regulatory regime to foster innovation.[94] The FCA wants to be aware when innovation is stymied by regulatory barriers, so that it can ensure that its frameworks remain fit for purpose in an evolving world.[95] It is clear then that part of the FCA's strategy is to allowing emerging technology and payment methods to flourish, this includes newly

[88] FCA, 'Innovation: The Regulatory Opportunity' (October 2014, updated November 2014) <https://www.fca.org.uk/news/innovation-the-regulatory-opportunity> accessed 22 September 2016.

[89] Financial Services Act 2012, s.1B(3)(c).

[90] FCA, 'Disruptive Innovation in Financial Markets' (October 2015) <https://www.fca.org.uk/news/speeches/disruptive-innovation-financial-markets> accessed 22 September 2016.

[91] Financial Services Act 2012, s.1E(1)(a).

[92] Ibid, s.1E(1)(b).

[93] Speech by Martin Wheatley, Chief Executive of the FCA, available at: <https://www.fca.org.uk/news/speeches/innovation-regulatory-opportunity> accessed 22 September 2016.

[94] FCA, 'Innovation: The Regulatory Opportunity' (n.88).

[95] FCA, 'Disruptive Innovation in Financial Markets' (n.90).

emerging NTPMs. Project Innovate is still in its infancy but there is promise that it will serve to foster the development of NTPMs and allow them to flourish.

3.3.2.2. The National Crime Agency

The National Crime Agency (NCA) became operational in October 2013[96], three years after it was first announced by the coalition government. It replaced the Serious Organised Crime Agency (SOCA)[97] and was created to be a powerful and effective crime-fighting agency.[98]

The NCA leads the UK law enforcement fight against serious and organised crime. Its job is to 'disrupt and bring to justice those serious and organised criminals who present the highest risk to the UK.'[99] It provides leadership in a number of areas through its organised crime, border policing, economic crime and CEOP commands.[100] The Economic Crime Command leads the national response to economic crime, which includes money laundering.[101] In terms of tackling money laundering it aims to do so by:

[96] National Crime Agency, 'National Crime Agency Goes Live', available at: <http://www.nationalcrimeagency.gov.uk/news/193-nca-launch-article> accessed 22 September 2016.

[97] The Home Office, The National Crime Agency: A Plan for the Creation of a National Crime Fighting Capability, London: Home Office, 2011.

[98] National Crime Agency, 'NCA Annual Plan 2015/2016 (2015), 4. Available at: <http://www.nationalcrimeagency.gov.uk/publications/541-nca-annual-plan-2015-16-v1-0/file> accessed 22 September 2016.

[99] National Crime Agency, 'About Us', available at: <http://www.nationalcrimeagency.gov.uk/about-us> accessed 22 September 2016.

[100] National Crime Agency, 'What We Do', available at: <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do> accessed 22 September 2016.

[101] HM Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (n.1), 5.

- Leading a multi-agency action to understand and combat national and international-scale money laundering;
- Working with law enforcement, regulators, banks and professional bodies to disrupt criminal access to professional skills (e.g. solicitors, accountants); and
- Increasing the impact of the NCA's operational capabilities in financial investigation, civil recovery and taxation.[102]

The NCA administers the asset recovery provisions found in the Proceeds of Crime Act 2002. The NCA's priority in this area is to deny criminals their assets by every lawful means necessary, its focus on the disruptive value of taking assets away.[103] The dedicated Asset Confiscation Enforcement team was set up in the NCA's Economic Crime Command in January 2014 to provide national coordination of activity across the agency and with partners in tackling unenforced confiscation orders and prioritising the orders of the most serious criminals.[104] In its first year of operation the NCA recovered over £22 million of criminal assets.[105]

It also acts as the UK's Financial Intelligence Unit (FIU). Whilst the FIU is a part of the NCA's Economic Crime Command, it is operationally independent of the NCA which means that it

[102] National Crime Agency, 'What We Do: Economic Crime Command', available at: <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime> accessed 22 September 2016.

[103] HM Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (n.1), 25.

[104] NCA, 'National Crime Agency: Annual Report and Accounts' (HC 35, 13 July 2015) 30 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/444184/NCA_Annual_Report_2014-15__web_.pdf> accessed 22 September 2016.

[105] National Crime Agency, 'NCA Annual Plan 2015/2016 (n.98), 6.

has the authority and capacity to operate autonomously.[106] It is a fully functioning member of the Egmont Group of Financial Intelligence Units. The NCA, in its role as an FIU, gathers, analyses and disseminates criminal intelligence from suspicious activity reports (SARs).[107] Once strategic and tactical intelligence is derived from the SARs, they are then available to all law enforcement agencies for investigation, except for those in some risk sensitive categories.[108] It should be noted here that the NCA is leading a reform of the SARs regime ahead of the next FATF mutual evaluation.[109] When the FIU was housed in SOCA, the FATF commented that it 'substantially meets the criteria of Recommendation 26 and appears to be a generally effective FIU'[110]; it will be interesting to see how the FATF views the new FIU in its next assessment of the UK.

In an effort to improve the UK's international outreach in terms of AML and CTF, the NCA will create International Liaison Officer posts.[111] This will assist in cases where there is the cross border transfer of funds, particularly prevalent through NTPMs. In order to get the most from this outreach the NCA will liaise with international groups such as the G20 and the FATF.[112]

---

[106] HM Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (n.1), 25.

[107] Ibid.

[108] Ibid.

[109] Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance* (n.20), 31.

[110] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 4.

[111] Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance* (n.20), 27.

[112] Ibid.

Finally, in terms of the NTPMs the NCA's position as an all-encompassing crime agency sees a real benefit. The NTPM's, particularly those such as mobile payment methods and virtual currencies are vulnerable to cybercrime which is another area of focus for the NCA. This means that they are in a good position to understand the threats that face NTPMs, as well as to gather information about abuse of NTPMs.

3.3.2.3. HMRC

HMRC is designated as a 'supervisory authority' under the Money Laundering Regulations 2007. It is responsible for Money Service Businesses (MSBs) which may encompass bitcoin exchanges and payment processors in the future given the UK's plan to make them subject to AML provisions.[113] MSBs are the main exception to FCA authorisation and supervision in the UK.[114]

3.3.3. Tertiary authorities

3.3.3.1. Joint Money Laundering Intelligence Taskforce (JMLIT)

The JMLIT was established under the Serious and Organised Crime Financial Sector Forum, chaired by the Home Office, the British Bankers' Association and the NCA.[115] JMLIT is led by the NCA with the rest of its membership comprising representatives of the financial sector, City of London Police, the FCA, HMRC and the Home Office.[116] The pilot was launched with the overarching objective of 'providing an environment in which the financial sector and

[113] Consultation paper.

[114] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 12.

[115] Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance* (n.20), 15.

[116] Ibid.

government can exchange and analyse information and intelligence to detect, prevent and disrupt money laundering and wider economic crime threats against the UK.'[117] There was a firm belief prior to its introduction that the time had come for the government and private sector bodies to fight financial crime together. The pilot completed in April 2016 and the UK has formally committed to transitioning the JMLIT from a pilot to permanent programme.[118] The NCA is now working with overseas law enforcement agencies to help inform the development of similar partnerships.[119]

3.3.3.2. British Bankers' Association

The British Bankers association is the leading trade association for the UK banking sector with 200 member banks headquartered in over 50 countries with operations in 180 jurisdictions worldwide.[120] It has produced AML guidelines for banks which are published on their behalf by the Joint Money Laundering Steering Group. In terms of its role with regards to NTPMs, the British Bankers' Association keeps it members up to date with developments[121], alerts

[117] National Crime Agency, 'JMLIT Executive Summary of FTI Report', available at: <http://www.nationalcrimeagency.gov.uk/publications/708-jmlit-executive-summary-of-fti-report/file> accessed 22 September 2016.

[118] National Crime Agency, 'Joint Money Laundering Intelligence Taskforce', available at: <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit> accessed 22 September 2016.

[119] Ibid.

[120] British Bankers Association, 'About Us', available at: <https://www.bba.org.uk/about-us/> accessed 22 September 2016.

[121] As an example see: British Bankers' Association, 'Divorcing Blockchain from Bitcoin', available at: <https://www.bba.org.uk/news/insight/divorcing-blockchain-from-bitcoin/#.V8y5DfkrKUk> accessed 22 September 2016.

them to risks[122], and notes general information on them[123]. Therefore they assist banks in keeping current and inform their policy in relation to NTPMs.

3.3.3.3. Joint Money Laundering Steering Group (JMLSG)

The JMLSG consists of the leading UK Trade Associations in the Financial Services Industry. Its primary aim is to encourage and share good practice in AML and to give practical assistance in interpreting the UK Money Laundering Regulations 2007.[124] It achieves this through issuing detailed Guidance Notes which are amended to dovetail with the introduction of new Money Laundering Regulations. The JMLSG currently gives guidance to electronic money issuers which would include certain 'stored value card' providers.

3.4. Application of a Risk-Based Approach to AML and CTF

The risk-based approach (RBA), advocated by the FATF 40 Recommendations, forms an integral part of the UK's AML and CTF regime.[125] The UK adopted the RBA in 2003 a year before the FATF introduced it. It is currently found in the Money Laundering Regulations (MLR) 2007, which was implemented as a result of the EU's Third Money Laundering Directive.[126] In October 2012, the MLR 2007 were updated, following a thorough review and

---

[122] As an example see: British Bankers' Association, 'BBA Brief – 4 February 2016', available at: <https://www.bba.org.uk/news/bba-brief/bba-brief-4-february-2016/#.V8y6l_krKUk> accessed 22 September 2016.

[123] Ibid.

[124] Joint Money Laundering Steering Group, 'Welcome to the Joint Money Laundering Steering Group Website', available at: <http://www.jmlsg.org.uk/> accessed 22 September 2016.

[125] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 29.

[126] Directive 2005/60/EC on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing.

consultation by the government, the amendments reduced regulatory burden and resulted in a supervisory regime that was 'more robust, effective and proportionate.'[127] In having its RBA in the MLR 2007, the UK is different to the US and Australia in that they both have theirs in primary legislation. Despite this, it is a vocal supporter of the RBA and advocates its use in the development of international standards by the FATF, at EU level and within the UK.[128] Indeed, 'a key part of the UK's financial crime strategy is to entrench the risk-based approach.'[129] Ryder has commented that, the UK has taken the most proactive approach towards utilising the RBA.[130]

The RBA requires all relevant persons to establish and maintain appropriate and risk-sensitive policies to enable them to comply with the various requirements of the MLR 2007'. The MLR 2007 provide: 'a relevant person must establish and maintain appropriate and risk-sensitive policies and procedures relating to: (a) customer due diligence measures and ongoing monitoring; (b) reporting; (c) record-keeping; (d) internal control; (e) risk assessment and management; and (f) the monitoring and management of compliance with, and the internal communication of, such policies and procedures'.[131]

[127] HM Treasury, 'Research and Analysis: Anti-Money Laundering and Counter Terrorist Finance Supervision Report' (n.69).

[128] HM Treasury, *Anti-Money Laundering and Counter Terrorist Finance Supervision Report 2010-11*, (n.3), 5.

[129] Explanatory memorandum for the Money Laundering Regulations 2007 <http://www.legislation.gov.ac.uk/uksi/2007/2157/memorandum/contents>, 3.

[130] Nicholas Ryder, *Money Laundering – An Endless Cycle?* (n.66), 78.

[131] Regulation 20(1).

The consequence of the RBA is that the detail of implementation is in the hands of industry and therefore tailored to fit the needs of the people who it impacts upon.[132] HM Treasury has been critical of the application of the RBA in the UK, noting that whilst supervisors demonstrate a good knowledge of the RBA, there is still development needed in terms of implementing a fully risk-based approach.[133] As things stand, HM Treasury suggests that there is inconsistency between supervisors in the identification and assessment of risk, whilst further the level of risk-modelling varies drastically.[134]

The FCA note that firms which embrace the RBA will focus their AML resources on the areas which will have the biggest impact, leading to a reduction in money laundering and terrorist financing.[135] Firms are assisted in implementing the RBA by a number of different instruments. The JMLSG industry written guidance gives practical assistance to firms in assessing and mitigating their money laundering risk and putting in place an effective and efficient AML control environment.[136] On top of this, in 2015 the FCA published a guide[137] which was designed to help firms adopt a 'more effective, risk-based and outcomes-focussed

---

[132] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 111.

[133] HM Treasury, Anti-Money Laundering and Counter Terrorist Finance Supervision Report 2014 – 2015 (n.6), 17.

[134] Ibid.

[135] FCA, 'Money Laundering and Terrorist Financing' (August 2015, updated June 2016) <https://www.the-fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing> accessed 22 September 2016.

[136] FSA, 'Review of Firms' Implementation of a Risk-Based Approach to Anti-Money Laundering (AML)' (March 2008) <http://www.fca.org.uk/static/documents/fsa-aml-implementation-review.pdf> accessed 22 September 2016.

[137] FCA, Financial Crime: a guide for firms (April 2015). Available at: <https://www.handbook.fca.org.uk/handbook/document/FC1_FCA_20150427.pdf> accessed 12/07/2016.

approach to mitigating financial crime risk.'[138] The FCA are clear that whilst this contains good and poor practice, that it is not prescriptive and that firms can achieve the aims of the RBA using their own methods.[139]

HM Treasury have highlighted the importance of the RBA in relation to NTPMs noting that 'Key to an effective RBA to supervision is having a methodology that is dynamic and responsive to emerging threats.'[140] There is a safeguard for NTPMs in that the government is clear that AML and CTF obligations should be carried out in an intelligent way that ensures that businesses can grow and not be weighed down by red tape.[141] So, NTPMs should not be unduly burdened by AML and CTF measures, they should be given some freedom to develop. Indeed, the UK wants to encourage and promote the use of innovative payment methods to increase competition in financial services.[142] The FCA have also noted that to effectively implement the RBA, skilled and well informed staff are needed[143], it is questionable whether NTPM providers have such staff. Actual published guidance on how the UK's RBA applies to NTPMs is thin at best.

---

[138] Ibid, 5.

[139] FSA, 'Review of Firms' Implementation of a Risk-Based Approach to Anti-Money Laundering (AML)' (n.136).

[140] HM Treasury, Anti-Money Laundering and Counter Terrorist Finance Supervision Report 2014 – 2015 (n.6), 17.

[141] Ibid, Foreword.

[142] HM Treasury, Digital Currencies: Response to the Call for Information (n.5), 19.

[143] FCA, 'The FCA's Risk Based Approach to AML Supervision' (CNBV Workshop on AML and CFT, Mexico City, 8-9 September) <http://www.cnbv.gob.mx/PrevencionDeLavadoDeDinero/Documents/Presentation%20for%20Mexico%20City%20workshop%20FINAL%2020150901.pdf> accessed 22 September 2016.

3.5. Criminalisation of Money Laundering and Terrorist Financing

3.5.1. Money Laundering

The UK's primary money laundering legislation is all contained in the Proceeds of Crime Act (POCA) 2002, Part VII. In the FATF's 3rd Mutual Evaluation of the UK, they rated it as 'compliant' with the provisions on the criminalisation of money laundering.[144] The UK approach is broad and fully compliant with the relevant parts of the Vienna Convention and the Palermo Convention.[145] HM Treasury states 'the Proceeds of Crime Act applies international standards in a way that delivers one of the world's most powerful tools against money laundering.'[146] It takes an all-crimes approach, they do not have a finite list of crimes that constitute predicate offences.

The UK anti-money laundering regime does not seek directly to prevent crime; rather, it seeks to prevent criminals from enjoying the use of the proceeds of their crime.[147] The UK's primary offences are contained in s.327-329 of POCA, they are: concealing, disguising, converting, transferring or removing criminal property from the jurisdiction;[148] entering into or becoming concerned in an arrangement knowing or suspecting it to facilitate the acquisition, retention,

---

[144] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 40.

[145] Ibid, 4.

[146] HM Treasury, *Anti-Money Laundering Strategy*, (London: HM Treasury, 2004).

[147] Slaughter and May, 'An Introduction to the UK Anti-Money Laundering Regime' (March 2008) <https://www.slaughterandmay.com/media/559043/an_introduction_to_the_uk_anti_-_money_laundering_regime.pdf> accessed 22 September 2016.

[148] Proceeds of Crime Act 2002, s.327.

use and control of criminal property on behalf of another person;[149] and acquiring, using or possessing criminal property.[150] A person guilty of one of these offences is liable on conviction on indictment to a maximum terms of 14 years, or to a fine, or to both.[151] Statistics provided to the FATF by the UK authorities indicate that the average terms of imprisonment for 2003 and 2004 are 49.5 and 30.6 months respectively.[152]

These above offences can be committed by anyone, and apply to NTPMs as criminal property includes: money, all forms of property, or things in action and other intangible or incorporeal property.[153] In applying the offences it is immaterial who carried out the criminal conduct and who benefitted from it.[154] It is a defence to all three substantive offences for a person in the regulated sector to make a disclosure to the National Crime Agency about their knowledge or suspicion of money laundering.[155]

In addition, the UK also has offences of failing to report, contained in s.330-332 of POCA. These apply where a person has knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering, where the information came to him in the course of business in the regulated sector.[156] It is stated that any business

[149] Proceeds of Crime Act 2002, s.328.

[150] Proceeds of Crime Act 2002, s.329.

[151] Proceeds of Crime Act 2002, s.334.

[152] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 35.

[153] Proceeds of Crime Act 2002, s.340(9).

[154] Proceeds of Crime Act 2002, s.340(4).

[155] Proceeds of Crime Act 2002, s.338.

[156] Proceeds of Crime Act 2002, s.330-332.

which accepts deposits can be classed as being in the 'regulated sector'.[157] All the NTPMs looked at in this thesis accept sums of money being paid into them, they either store it or transfer it for the customer. Alongside failing to report, it is also an offence, under POCA to tip off a client that you have made a report.[158] The maximum penalty on conviction on indictment for failing to disclose, or for tipping off, is five years imprisonment and an unlimited fine.[159]

In comparison to Australia's approach of having 19 separate offences of money laundering the UK approach is more concise and efficient. Indeed the FATF has noted that POCA has had a 'significant and positive impact on the UK's ability to restrain, confiscate and recover proceeds of crime.'[160]

3.5.2. Terrorist Financing

The terrorist financing offences are contained in the Terrorism Act 2000. The UK has long criminalised terrorist financing, beginning with the Prevention of Terrorism (Temporary Provisions) Act 1989, which was introduced due to the threat posed by Northern Ireland.[161] The difference in approach to money laundering is summarised well by Alexander 'traditional money laundering, covered by POCA. . . concerns property which is derived from crime and efforts to combat it therefore focus on origin. With terrorist funding, however, the focus is

[157] Proceeds of Crime Act 2002, Schedule 9, Part 1.

[158] Proceeds of Crime Act 2002, s.333(A).

[159] Proceeds of Crime Act 2002, s.334.

[160] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 4.

[161] It is worthy of note that this Act was generally seen as weak and no convictions were made under it.

not on where the property has come from but where it is destined: its ultimate purpose.'[162] The 2000 Act defines terrorist property as (a) money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation); (b) proceeds of the commission of acts of terrorism; and (c) proceeds of acts carried out for the purposes of terrorism.[163] The Act describes property broadly, and 'money or other property' is wide enough to encompass all NTPMs. The Terrorism Act 2000 creates five main offences relating to terrorist financing. Section 15 makes it a criminal offence for a person to solicit[164], receive[165], or provide[166] money or property on behalf of terrorists if they intend (or have reasonable cause to suspect) that such money may be used for terrorism.[167] Section 16 surrounds 'use and possession', a person commits an offence if they use money or other property for terrorist purposes.[168] The person commits the offence if they possess money or other property[169], and they intend (or have reasonable cause to suspect) that it will be used for terrorism.[170] Funding arrangements are covered under section 17, a person commits an offence under this section if they 'enter into or become concerned in an arrangement in which money or property is made available to another'[171] and the person intends (or has reasonable

[162] R. Alexander, *Insider Dealing and Money Laundering in the EU: Law and Regulation* (1st edn, Ashgate, 2007), 173.

[163] Terrorism Act 2000, s.14(1).

[164] Terrorism Act 2000, s.15(1).

[165] Terrorism Act 2000, s.15(2).

[166] Terrorism Act 2000, s.15(3).

[167] Terrorism Act 2000, s.15(1), (2) and (3).

[168] Terrorism Act 2000, s.16(1).

[169] Terrorism Act 2000, s.16(2)(a).

[170] Terrorism Act 2000, s.16(2)(b).

[171] Terrorism Act 2000, s.17(1)(a).

cause to suspect) that it will be used for terrorism.[172] Section 18, covers 'terrorist money laundering', and it is breach if a person 'enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property'[173] by concealment,[174] removal from the jurisdiction,[175] by transfer to nominees,[176] or in any other way.[177] Anyone found guilty of an offence under any of the above sections shall be liable on conviction on indictment to imprisonment not exceeding 14 years, an unlimited fine, or both.[178] As with the money laundering offences under POCA, the Terrorism Act 2000 also has an offence of 'failure to disclose', this places a duty to report where a person believes or suspects that there has been an offence under sections 15 - 18.[179] The Act makes it a criminal offence for people who conduct business in the regulated sector and do not report their knowledge or suspicion.[180] Similarly to POCA, there is also a defence if a person discloses any knowledge or suspicion of terrorist activity to the National Crime Agency.[181] It is worthy of note that for the purposes of these offence, the burden is to prove beyond a

[172] Terrorism Act 2000, s.17(1)(b).

[173] Terrorism Act 2000, s.18(1).

[174] Terrorism Act 2000, s.18(1)(a).

[175] Terrorism Act 2000, s.18(1)(b).

[176] Terrorism Act 2000, s.18(1)(c).

[177] Terrorism Act 2000, s.18(1)(d).

[178] Terrorism Act 2000, s.22(1)(a).

[179] Terrorism Act 2000, s.19(1)(a).

[180] Terrorism Act 2000, s.21 A.

[181] Terrorism Act 2000, s.20.

reasonable doubt that the property is terrorist property,[182] this can cause a challenge for the prosecution.

3.6. Preventive Measures

Ryder notes that the UK, were one of the first EU members to incorporate preventative measures in relation to money laundering.[183] The current measures in relation to preventative measures are contained in the Proceeds of Crime Act 2002, and the Money Laundering Regulations 2007.

3.6.1. Customer Due Diligence

The purpose of the Money Laundering Regulations 2007 is to 'impose standards of behaviour governing 'know your client' regulation in relation to customers.' All measures found under the Money Laundering Regulations 2007 apply to 'financial institutions' which is construed widely enough to cover money service businesses of which the NTPMs tend to fall into. The UK's measures in relation to know your customer / customer due diligence can be found in Part 2 of the Money Laundering Regulations. As part of the risk-based approach to AML and CTF they provide for enhanced due diligence and simplified due diligence.[184] Alongside this it is important that financial institutions monitor the customer throughout the business

[182] R. E. Bell, 'The Confiscation, Forfeiture and Disruption of Terrorist Finances' (2003) 7(2) *Journal of Money Laundering Control* 105, 113.

[183] Nicholas Ryder, *Money Laundering – An Endless Cycle?* (n.66), 91.

[184] Money Laundering Regulations 2007, Regulation 13.

relationship.[185] Under Part 3, it is a requirement that financial institutions keep a record of this information.[186]

3.6.2. Suspicious Activity Reports

Suspicious activity reports (SARs) are a key part of the UK's preventive measures strategy. The UK Financial Intelligence Unit (UKFIU), sits within the Economic Crime Command of the NCA. It is an offence, under the Proceeds of Crime Act 2002, to fail to disclose suspicion to the NCA.[187] It is the role of the UKFIU to receive the suspicious activity filed in pursuance of the above obligation. The UKFIU is a member of the Egmont Group which enables it to seek financial intelligence from other members in order to support NCA operations and projects.

An area of contention with the UK system surrounds the use of the term 'suspicion' as a trigger for submitting an SAR. The problem arises because it is a vague concept based on a subjective state of mind, as Feldman observes 'suspicion is a far less assured state of mind than either knowledge or belief.'[188] Case law such as Da Silva;[189] K Ltd v National Westminster Bank Plc;[190] and Shah v HSBC Private Bank Ltd[191] have debated the merits of this test and the conclusion they come to, perhaps unhelpfully is that suspicion is a 'possibility, which is more than fanciful, that the relevant facts exist'[192] and that a 'vague feeling of unease would not

[185] Money Laundering Regulations 2007, Regulation 8.

[186] Money Laundering Regulations 2007, Regulation 19.

[187] Proceeds of Crime Act 2002, s.330 - s.332.

[188] *Criminal Confiscation Orders: The New Law* (1988), para.3.09

[189] [2006] EWCA Crim 1654.

[190] [2006] EWCA Civ 1039.

[191] [2012] EWHC 1283.

[192] Longmore LJ, in K Ltd v National Westminster Bank Plc [2006] EWCA Civ 1039.

suffice.'[193] Brown and Evans have opined that 'in most cases, the statement by those making an SAR that they have a suspicion will be enough.'[194] However Shah, did cloud the area when Longmore LJ suggested that he 'cannot see why, rather than submit to summary judgement dismissing the claim, Mr Shah cannot require the bank to prove its case that it had the relevant suspicion.'[195] So in once sense the threshold is low, however the views of Longmore LJ in Shah would seem to indicate that an individual or firm should have to justify their suspicion. If this seems like a difficult test to apply for banks, it can only be more difficult for NTPM providers who may have a lack of resources and therefore staff may be stretched, particularly in smaller businesses.

The SARs regime is becoming unmanageable, KPMG noted that the number of SARs submitted, between 1995 and 2002, increased from 5,000 to 60,000.[196] By 2010 that had grown to 240,582 SARs.[197] The most recent figure released for 2014/15 indicate that this has grown again to 381,882 reports.[198] The number is not sustainable and the growth in the number of SARs is perhaps indicative of individuals being unsure what to report.

---

[193] Longmore LJ, in Da Silva [2006] EWCA Crim 1654.

[194] G. Brown and T. Evans, 'The Impact: The Breadth and Depth of the Anti-Money Laundering Provisions Requiring Reporting of Suspicious Activities' (2008) 23(5) *Journal of International Banking Law and Regulation* 274, 275.

[195] Shah v HSBC Private Bank Ltd [2010] EWCA Civ 31.

[196] KPMG, *Money Laundering: Review of the Reporting System* (KPMG, 2003), 14.

[197] Serious Organised Crime Agency, *The Suspicious Activity Reports Regime Annual Report 2010* (2010), 4. Available at: <http://www.octf.gov.uk/OCTF/media/OCTF/images/publications/SARS%20Annual%20Report/SARs-Annual-Report-2010.pdf?ext=.pdf> accessed 22 September 2016.

[198] National Crime Agency, Suspicious Activity Reports Annual Report 2015 (2016), 13. Available at: <http://www.nationalcrimeagency.gov.uk/publications/677-sars-annual-report-2015/file> accessed 22 September 2016.

The UK has also recently begun, what the NCA describe as a 'sustained and potentially radical period of change' in the operation of the SARs regime.[199] They note that the 4th EU Anti-Money laundering Directive and developments with the FATF Recommendations enforce the need for change.[200] More on these changes is available in the 'Action Plan', but it is of relevance to note that it indicates that the SARs regime is to be refocused on entities that pose the highest risks, rather than on individual transactions.[201]

3.6.3 Specific NTPM Measures

3.6.3.1. New Technologies

The last time that the UK was assessed for compliance with the Recommendation on 'new technologies', was in the 2007 FATF 3rd Mutual Evaluation of the United Kingdom. At that time, it was still 'Recommendation 8' rather than 'Recommendation 15'.

The Money Laundering Regulations 2007 require financial institutions[202] to have in place effective systems and controls to mitigate the money laundering and terrorist financing risks faced by their business.[203] This is supported by the FCA handbook, which states that 'a firm should ensure that the systems and controls include . . . appropriate measures to ensure that money laundering risk is taken into account in its day-to-day operation, including in relation to:

---

[199] Ibid, 3.

[200] Ibid.

[201] Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance* (n.20), 13.

[202] Money Laundering Regulations 2007, Regulation 3(1)(b).

[203] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 128.

(a) The development of new products;

(b) The taking-on of new customers; and

(c) Changes in its business profile.'[204]

An important measure in relation to NTPMs is Regulation 14(2) of the Money Laundering Regulations 2007 which recognises the increased risks where 'the customer has not been physically present for identification purposes' and therefore provides for enhanced due diligence to take place in such scenarios. It was recognised in Chapter 1 that a number of NTPMs appeal to launderers and terrorist financers due to the fact that they facilitate non-face-to-face transactions. The JMLSG have also provided guidance on avoiding the risks associated with non-face-to-face transactions.[205] Alongside JMLSG guidance, HMRC have also provided their own guidance requiring money service businesses to examine copies of original documents when carrying out CDD.[206]

Whilst this 3rd Mutual Evaluation Report is useful in terms of laying out the UK's measures in the area, and noting that it was rated as 'compliant'[207] with the Recommendation at the time, it would be fair to state that the UK was not assessed on the basis of the kind of challenges we now face from NTPMs. What can be noted is that the measures under the Money Laundering Regulations 2007 appear broad enough to cover the threat of most emerging NTPMs, provided they come under the scope of FCA regulation. With regards to Bitcoin, it

[204] Financial Conduct Authority Handbook, SYSC 3.2.6G G (4).

[205] For more, see: Joint Money Laundering Steering Group, Prevention of Money Laundering / Combatting Terrorist Financing (2014 Revised Version), Part I 5.5.10 – 5.5.17. Available at: <http://www.jmlsg.org.uk/download/9803> accessed 22 September 2016.

[206] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 125.

[207] Ibid.

would of course be dependent on digital currency exchanges being brought under the scope of AML and CTF regulation[208], as due to Bitcoin's decentralised system there is no one entity to apply these measures to.

3.6.3.2. Wire Transfers

The UK's wire transfer provisions are governed by EU law, at the time of the last FATF assessment of the UK that was the Wire Transfer Regulation 1[209], and the UK was rated as being 'partly compliant' with the FATF Recommendation.[210] The UK was criticised for the fact that the Wire Transfer Regulation 1 was not in compliance with the FATF Recommendation, that the sanctions regime was not effective or dissuasive, and the FATF questioned the effectiveness of measures found in the EU requirements.[211] The Regulation is 'widely drawn and intended to cover all types of funds transfer falling within its definition as made "by electronic means", other than those specifically exempted wholly or partly by the Regulation.'[212] So applying to electronically based NTPMs. It is notable that the new Wire Transfer Regulation (revised)[213] when it comes into force from 26 June 2017, will contain a more comprehensive guide to the means which are exempted.

[208] HM Treasury, Digital Currencies: Response to the Call for Information (n.5), 19.

[209] Regulation (EC) No. 1781/2006.

[210] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 138.

[211] Ibid.

[212] Joint Money Laundering Steering Group, Prevention of Money laundering and Combating Terrorist Financing, Guidance for the UK Financial Sector Part III: Specialist Guidance (December 2011, 2011 Review Edition), 5. Available at: <http://www.jmlsg.org.uk/download/7323> accessed 22 September 2016.

[213] Regulation (EU) 2015/847.

3.6.3.3. Money or Value Transfer Services

The UK was judged as being 'largely compliant' with the money or value transfer Recommendation.[214] Money or Value Transfer service providers in the UK are known as money service businesses and are supervised by the HMRC.[215] The FATF noted that the sector is large and that HMRC would benefit from increased resources as well as its powers of sanction.[216] A money service business is a business which 'acts as a bureau de change'; or 'transmits money, or any representation of money, in any way (although just collecting and delivering money as a 'cash courier' is not transmitting money'; or cashes cheques that are payable to customers.[217] Money service businesses need to register with HMRC[218], similar to the US and Australian systems. To operate as a money service business in the UK, it is also required that the company passes the 'fit and proper' test.[219] The other concerns of the FATF that prevented the UK from being considered fully 'compliant' focussed around inadequate sanctions to be used against directors and senior managers; and some concern around the extent of customer identification undertaken.[220]

[214] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 202.

[215] Ibid, 201.

[216] Ibid.

[217] HM Revenue & Customs, 'Money Laundering Regulations: Money Service Business Registration' <https://www.gov.uk/guidance/money-laundering-regulations-money-service-business-registration> accessed 22 September 2016.

[218] Money Laundering Regulations 2007, Regulation 26.

[219] Money Laundering Regulations 2007, Regulation 28.

[220] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 202.

3.7 Confiscation of the Proceeds of Crime

The UK has a long and established history in terms of forfeiting and confiscating the proceeds of crime. These measures are seen as important parts of the UK's quest to substantially reduce the level of serious and organised crime, including money laundering and terrorist financing. In the FATF's last Mutual Evaluation of the UK, they found them to be 'compliant' with their Recommendation on confiscation of the proceeds of crime.[221] Through the Proceeds of Crime Act (POCA) 2002 they have successfully ratified the Vienna, Palermo and Corruption Conventions as well as the relevant provisions of UN Security Council Resolutions 1267 and 1373.

Despite the above, Ryder has noted that the 'UK response to the confiscation of the proceeds of crime could still be regarded as in its infancy and is subject to a great deal of uncertainty.'[222] Whilst Fisher adds that 'It is an open secret that the restraint and confiscation regime in Part 2 of the POCA 2002 has failed to meet its declared objective of separating serious and organised criminals from the benefits of their crimes.'[223] It should be noted however, that whilst praise for the current position is not high, it has been noted that 'since the publication of Hodgson Committee in 1984, the UK's approach towards the confiscation of the proceeds of crime has improved considerably.'[224]

---

[221] Ibid, 63.

[222] Nicholas Ryder, *Money Laundering – An Endless Cycle?* (n.66), 101.

[223] Jonathan Fisher QC, 'Part 1 of the Serious Crime Act 2015: strengthening the Restraint and Confiscation Regime' (2015) 10 Criminal Law Review 754,754.

[224] Nicholas Ryder, 'To Confiscate or Not to Confiscate? A Comparative Analysis of the Confiscation of the Proceeds of Crime Legislation in the United States of America and the United Kingdom' (n.215), 770.

The UK's main asset recovery provisions are found in the POCA 2002, which was amended by the Serious Crime Act 2015 in a bid to 'strengthen the operation of the asset recovery process by closing loopholes in the Proceeds of Crime Act 2002.'[225] The main body responsible for asset recovery is the National Crime Agency, who took over from the Serious Organised Crime Agency in May 2013, due to changes brought about by the Crime and Courts Act 2013.

The NCA has four confiscation measures under POCA, they are:

- Criminal confiscation;[226]
- Civil recovery;[227]
- Taxation;[228] and
- Seizure and forfeiture of cash.[229]

The first measure open to the NCA under POCA is criminal confiscation. Once the defendant has been convicted per s.6 of POCA, the criminal confiscation regime requires the NCA to prove two questions. First, whether the defendant has a criminal lifestyle.[230] Second, whether or not the defendant has profited from the illegal behaviour.[231] In relation to the first question, a defendant is considered to have a criminal lifestyle if one of the three following conditions are met: (1) it is a 'lifestyle offence' as specified in Schedule 2 of POCA; (2) it is part of a 'course of criminal conduct'[232]; and (3) it is an offence committed over a period of at least

[225] Introductory Note to the Serious Crime Act 2015.

[226] Proceeds of Crime Act 2002, Part 2.

[227] Proceeds of Crime Act 2002, Part 5, Chapter 2.

[228] Proceeds of Crime Act 2002, Part 6.

[229] Proceeds of Crime Act 2002, Part 5, Chapter 3.

[230] Proceeds of Crime Act 2002, s.6(4)(a).

[231] Proceeds of Crime Act 2002, s.6(4)(b).

[232] Proceeds of Crime Act 2002, s.75(2)(b).

six months and the defendant has benefitted from it.[233] Alldridge notes that the quantification of benefit for the purposes of making confiscation orders is now in a 'serious mess' and it is 'riddled with inconsistency.'[234] Once these questions have been addressed then the courts will decide upon the 'recoverable amount'[235] and grant the confiscation order that compels the defendant to pay. As part of an effort to improve the efficacy of the confiscation regime and drastically increase the collection rate, Part 1 of the Serious Crime Act 2015 introduced a number of measures to POCA. One measure worthy of particular note is that the time to pay a confiscation order in s.11 of POCA has been reduced from six months to three months[236], halving the time to pay before interest starts to accrue and the potential for a magistrate to enforce a default sentence.[237]

The second measure open to the NCA under POCA is civil recovery. Civil recovery is typically utilised by the NCA where criminal recovery is unavailable due to lack of a prosecution.[238] The NCA cannot initiate proceedings of their own accord, but they are permitted to do so where cases are passed to it when there is insufficient evidence to pursue a criminal confiscation, or where the Crown Prosecution Service decided not to pursue the case: due to the public interest criteria; where confiscation proceedings are unsuccessful due to procedural

[233] Proceeds of Crime Act 2002, s.75(2)(c).

[234] Peter Alldridge, 'Proceeds of Crime Law Since 2003 – Two Key Areas' (2014) 3 *Criminal Law Review* 171, 188.

[235] For more on the 'recoverable amount', see: Proceeds of Crime Act 2002, s.7.

[236] Serious Crime Act 2015, s.5(3)(b).

[237] Stephen Gentle, Cherie Spinks, and Tim Harris, 'Legislative Comment, Proceeds of Crime Act 2002: Update' (2016) 139 (Sep) Compliance Officer Bulletin 1, 6.

[238] Proceeds of Crime Act 2002, s.240.

mistakes; and where the defendant has died or is abroad.[239] It has been noted that the NCA are more likely to go down the civil recovery route rather than the 'onerous' criminal route.[240] They can bring action against anyone who they believe to hold recoverable property[241], in order to do so some of the following must be present:

- Recoverable property has been identified and has an estimated value of at least £10,000;[242]
- Recoverable property has been acquired in the last 12 years;
- Recoverable property includes property other than cash, cheques and the like; and
- There is evidence proven to civil standards of criminal conduct.[243]

The NCA simply has to show on the balance of probabilities that there is some evidence of criminal activity.[244] Ryder has noted that the civil burden of proof has proven to be extremely controversial and identifies the case of Gale and another v Serious Organised Crime Agency[245] as a good example of this.[246] However, Alldridge has noted that despite the misgivings of

[239] Angela V. M. Leong, 'Assets Recovery under the Proceeds of Crime Act 2002: the UK Experience', in Simon N. M. Young, Civil Forfeiture of Criminal Property: Legal Measures for Targeting the Proceeds of Crime (1st edn, Edward Elar, 2009).

[240] Stephen Gentle, Cherie Spinks, and Tim Harris, 'Legislative Comment, Proceeds of Crime Act 2002: Update' (n.237), 13.

[241] Proceeds of Crime Act 2002, s.243(1).

[242] Proceeds of Crime Act 2002, s.287.

[243] Nicholas Ryder, 'To Confiscate or Not to Confiscate? A Comparative Analysis of the Confiscation of the Proceeds of Crime Legislation in the United States of America and the United Kingdom' (n.215), 789.

[244] Proceeds of Crime Act, s.241.

[245] [2011] UKSC 49.

[246] Nicholas Ryder, 'To Confiscate or Not to Confiscate? A Comparative Analysis of the Confiscation of the Proceeds of Crime Legislation in the United States of America and the United Kingdom' (n.215), 790.

some, and in comparison to the criminal recovery route, the civil procedure has operated fairly successfully.[247]

The third measure open to the NCA under Part 6 of POCA is taxation. It enables the NCA, to act in the position of HM Revenue & Customs and tax any income where the respondent is unable to verify the legitimacy of its source.[248] The NCA has to prove that it has 'reasonable grounds to suspect' that funds are taxable or come from criminal conduct.[249] The general functions that the NCA can use are income tax,[250] capital gains tax,[251] corporation tax,[252] national insurance contributions,[253] statutory sick pay,[254] statutory maternity pay,[255] statutory paternity pay,[256] statutory adoption [257] pay and student loans.[258] Cory has criticised this measure noting that the noting that the amount of assets recovered by this mechanism is relatively insignificant when compared to the approximated profits produced by criminal enterprises.[259]

[247] Peter Alldridge, 'Proceeds of Crime Law Since 2003 – Two Key Areas' (n.234), 188.

[248] Proceeds of Crime Act 2002, s.317.

[249] Proceeds of Crime Act 2002, s. 317(1)(a) and (b).

[250] Proceeds of Crime Act 2002, s. 323(1)(a).

[251] Proceeds of Crime Act 2002, s. 323(1)(b).

[252] Proceeds of Crime Act 2002, s. 323(1)(c).

[253] Proceeds of Crime Act 2002, s. 323(1)(d).

[254] Proceeds of Crime Act 2002, s. 323(1)(e).

[255] Proceeds of Crime Act 2002, s. 323(1)(f).

[256] Proceeds of Crime Act 2002, s. 323(1)(g).

[257] Proceeds of Crime Act 2002, s. 323(1)(h).

[258] Proceeds of Crime Act 2002, s. 323(1)(i).

[259] Richard Cory 'Taxing the Proceeds of Crime' (2007) 4 *British Tax Review* 356, 356.

The fourth and final measure open to the NCA is in relation to the 'seizure and forfeiture of cash' under Part 5 Chapter 3 of POCA. It permits law enforcement agents to seize any cash if they have reasonable grounds for suspecting that it is (a) recoverable property, or (b) intended by any person for use in unlawful conduct.[260] An office may also seize any cash, part of which he reasonable grounds for suspecting to be (a) recoverable property, or (b) intended by any person for use in unlawful conduct, if it is not practicable to seize only that part.[261]

The assets that the National Crime Agency (NCA) recover are used to provide for the state and also for any victims of the crime.[262] It is worth of note that any success, attributable to the act, has been achieved despite the remarkable instability in the lead enforcement agency of the Act's provisions.[263] Since POCA's inception there have been three enforcement agencies: the Asset Recovery Agency, the Serious Organised Crime Agency and the NCA. But, the creation and transfer of powers between agencies is perhaps the best evidence of the perceived failures of those agencies to obtain the quantity of criminal assets expected.[264] It is hard to resist the conclusions of Padfield, that 'it was obvious since before the enactment of POCA that the enforcement of confiscation orders would be a nightmare' and that 'enforcement bodies would target less sophisticated criminals if their priority was simply to collect money.'[265] The issue of confiscation is not a number regime, criminals utilise

[260] Proceeds of Crime Act 2002, s.294(1).

[261] Proceeds of Crime Act 2002, s.294(2).

[262] Stephen Gentle, Cherie Spinks, and Tim Harris, 'Legislative Comment, Proceeds of Crime Act 2002: Update' (n.237), 1.

[263] Ibid.

[264] Ibid.

[265] Nicola Padfield, 'Depriving Criminals of the Proceeds of Their Crimes (2016) 10 *Criminal Law Review 695*, 696.

increasingly sophisticated methods that are more and more difficult to detect and therefore confiscate the funds. However, the fact that only '26p in every £100 of criminal proceeds were confiscated'[266] is a statistic not to be ignored.

The UK regime also includes the forfeiture of terrorist cash, under the Terrorism Act 2000 all a criminal has to do is be found guilty of a terrorist financing offence.[267] This includes fund raising,[268] use and possession,[269] funding arrangements [270] or money laundering.[271] If one of these is present, then the court will grant a forfeiture order of 'money or other property in the possession or under the control of a convicted person and which, at the time he intended should be used, or had reasonable cause to suspect might be used for the purposes of terrorism or he knew or had reasonable cause to suspect would or might have been used for the purposes of terrorism.'[272] These forfeiture provisions cover the seizure of terrorist cash anywhere in the UK.[273]

As noted in other chapters, this section is a broader, general AML and CTF section. It does not matter which NTPM mechanisms the criminal uses to transfer funds as most of them result in cash. One area which has proven difficult is with regard to cryptocurrency, Greater

[266] Comptroller and Auditor General, "Confiscation Orders" HC738 Session 2013-2014, 17 December 2013.

[267] See Anti-terrorism, Crime and Security Act 2001, Schedule 1, para 1(a) and (b).

[268] Terrorism Act 2000, s. 15.

[269] Terrorism Act 2000, s. 16.

[270] Terrorism Act 2000, s. 17.

[271] Terrorism Act 2000, s. 18.

[272] Terrorism Act 2000, schedule 4.

[273] Anti-terrorism, Crime and Security Act 2001, schedule 1.

Manchester Police have had difficulty in confiscating bitcoin due to lack of evidence.[274] The UK Government has indicated, as part of their next step following a call for information in relation to digital currencies, that they are still looking at how to confiscate digital currency funds where transactions are for criminal purposes.[275]

3.8. Mutual Legal Assistance

Chapter 2 highlighted that cooperation and mutual legal assistance are integral parts of the international effort to counter the abuse of NTPMs by launderers and terrorist financers, a globalised crime cannot be solved with a localised approach. The FATF has noted that the UK's mutual legal assistance framework is 'generally seen as being adequate.'[276] It would be fair to say that the UK's mutual legal assistance regime has come a long way since the FATF's mutual evaluation report in 2006. As a signatory of the Vienna, Palermo, CTF, and Merida Conventions, the UK has a strong foundation from which to build in terms of international cooperation.

It has been noted that the 'Mutual Legal Assistance system is time consuming and complex but provides an essential function for the recovery of UK criminal proceeds laundered overseas.'[277] The Home Office adding 'the UK is committed to assisting investigative,

[274] For more information on this, see: <http://n8prp.org.uk/research/n8-prp-small-grants/> accessed 22 September 2016.

[275] HM Treasury, Digital Currencies: Response to the Call for Information (n.5), 4.

[276] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 263.

[277] HM Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (n.1), 87.

prosecuting and judicial authorities in combatting international crime and is able to provide a wide range of mutual legal assistance.[278]

The UK's mutual legal assistance provisions are contained in three statutes; the Criminal Justice (International Co-operation) Act 1990; the Criminal Justice and Public Order Act 1994; and the Crime (International Co-operation) Act 2003. In particular, the 1990 Act has been labelled as a 'vital weapon in the armoury of those who investigate and prosecute international financial crime and is frequently utilised by the prosecuting authorities in the United Kingdom.'[279]

Requests are made to the UK for mutual legal assistance through a formal Letter of Request.[280]

The Home Office acts as the UK Central Authority for mutual legal assistance requests.[281] They will seek to respond to a request within three days where possible, however it is noted that this may not always be possible.[282] If a request is urgent then the Home Office will try to deal with it as soon as possible.[283] The Serious Fraud Office's Proceeds of Crime Division deals with incoming requests for mutual legal assistance involving asset freezing and the enforcement

---

[278] Home Office, *Requests for Mutual Legal Assistance in Criminal Matters: Guidelines for Authorities Outside of the United Kingdom* (12th Edition, 2015), 4. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415038/MLA_Guidelines_2015.pdf> accessed 22 September 2016.

[279] Jonathan Fisher, 'Reducing International Financial Crime – Plus ça Change . . .' (2001) 16(3) *Journal of International Banking Law* 67, 67.

[280] Home Office, *Requests for Mutual Legal Assistance in Criminal Matters: Guidelines for Authorities Outside of the United Kingdom* (n.278), 4.

[281] Ibid.

[282] Ibid.

[283] Ibid, 14.

of overseas confiscation orders.[284] Whilst the Crown Prosecution Service obtains restraint orders and enforces overseas confiscation orders on behalf of overseas jurisdictions pursuant to requests for Mutual Legal Assistance (MLA).[285] A key strategy of the Crown Prosecution Service has been the 'identification and targeting of priority countries where UK efforts can have the most impact.'[286]

The UK has an extensive number of agreements for mutual legal assistance,[287] and like the US, is able to 'share confiscated or forfeited assets with other jurisdictions, and internally is able to use funds confiscated to incentivise law enforcement and prosecutions agencies in their work.'[288] It has been noted that 'although the [UK's] process might be slow and cumbersome, there is no doubt that there is an increased willingness and indeed an increased level of sophistication among prosecuting authorities in dealing with overseas jurisdictions and no defendant should believe that assets are outside the UK will remain so.'[289]

3.9. Conclusion

The chapter has highlighted the leading role that the UK plays in tackling money laundering and terrorist financing, indeed its aim is to create a hostile environment for illicit finances,

[284] HM Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (n.1), 26.

[285] Ibid, 27.

[286] Ibid.

[287] For more, see: <https://mlat.info/country-profile/united-kingdom> accessed 22 September 2016.

[288] Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (n.4), 263.

[289] Stephen Gentle, Cherie Spinks, and Tim Harris, 'Legislative Comment, Proceeds of Crime Act 2002: Update' (n.237), 6-7.

and its efforts have often predated the international community, this made it an obvious choice as a case study country. Further, the amount of illicit funds that pass through the UK each year, coupled with the fact it is a target jurisdiction for launderers and terrorist financers mean that it has had to develop a robust AML and CTF Framework, because of this criminals are likely to use more surreptitious payment methods in an effort to avoid detection.

It has been highlighted that whilst NTPMs are not as much of a threat to US as traditional forms of money laundering and terrorist financing, their threat is not insignificant either. The UK has a number of competent authorities who are tasked with dealing with AML and CTF. These competent authorities have also become concerned with NTPMs. HM Treasury has a key role to play in countering the threat of launderers and terrorist financers abusing NTPMs, in performing its National Risk Assessment, they are responsible for identifying emerging threats to the UK economy. They have also played an important role in reducing the knowledge gap in relation to digital currencies such as bitcoin by running a call for information, and publishing a follow up report. This gives an insight into the threats that emanate from the use of digital currencies and the UK's potential response to them. HM Treasury should be commended for their approach of utilising the knowledge base of the private sector, academics and other individuals to inform their policy on an emerging area of legal interest. It is also worthy of note that the FCA have an objective to promote competition, something that its predecessor, the Financial Services Authority, never had to do. This competition objective means that the FCA has an interest in NTPMs, and from an AML and CTF perspective needs to make sure that they are sound. Further, through its Innovation Hub it wants to ensure that innovation is not being stifled by regulatory barriers, an important consideration in relation to NTPMs. Finally, in relation to the National Crime Agency,

cybercrime is a key area of their work and digital currencies and mobile payments link into this.

In relation to the criminalisation of money laundering and terrorist financing, it would be fair to describe the UK's approach as comprehensive, it has implemented the measures found in the Vienna, Palermo and Terrorist Financing Conventions and so its standards in relation to criminalisation should not come as a surprise. The main provisions relating to criminalisation are found in the Proceeds of Crime Act 2002 and the Terrorism Act 2000. The use of NTPMs does not make an impact on criminalisation as the offences are construed broadly to be committed through any payment method. Turning to the preventive measures, whilst the FATF Mutual Evaluation Assessment of the UK is useful in terms of understand the level they are operating at, it should be noted that it was completed in 2006 under a different assessment framework and as such the compliance ratings are not so useful anymore. The UK should be commended for being one of the first EU countries to incorporate preventive measures in relation to money laundering. The main preventive measures are located in the Proceeds of Crime Act 2002 and the Money Laundering Regulations 2007. It is imperative given the amount of money laundered through the UK annually, its location in the world, and its reputation that it has strong preventive measures. All measures found under the Money Laundering Regulations 2007 apply to 'financial institutions' which is construed widely enough to cover money service businesses of which the NTPMs are categorised under. It should be noted that HM Treasury have indicated the digital currency exchanges will be classified under this heading too. In relation to customer due diligence the Money Laundering Regulations 2007 cover both enhanced and simplified diligence the application of which are dependent on the risk-based approach. The UK's suspicious activity reporting regime has the same draw backs experienced worldwide, defensive reporting leading to vast amounts of

reports, and compliance costs impacting on financial institutions. However, the UK are seeking to address this through the HM Treasury and Home Office 'Action Plan' for the improvement of the AML regime. Its changes in relation to the SARs regime have been labelled as sustained and potentially radical with it being refocussed on entities that pose the highest risks, rather than on individual transactions. It remains to be seen how successful this approach will be and in particular whether it will lead to SARs being missed because an entity was not consider to be risky. The UK has also implemented measures specific to NTPMs. With regards to wire transfers (or 'electronic transfers') they have for a long time required a plethora of information surrounding the transaction. In relation to money or value transfer services, the UK earmarks them all as money service businesses, which mean that they are reporting entities for the purposes of AML and CTF. They are also required to register with HMRC, this helps to keep a record of all providers and weed out illegitimate providers. Failure to register results in a penalty. The final specific measure relating to NTPMs is in relation to new technologies. The UK has measures in place to ensure that providers consider the risks or new technologies and services. The FCA Handbook require that firms have systems and controls that include appropriate measures to ensure that money laundering risk is considered in relation to new products. The US should be praised overall for its preventive measures, they have adopted a strong approach however an area of concern is with regards to the reporting regime, although they are not alone in this area.

The UK sees the confiscation of the proceeds of crime as a crucial mechanism in their quest to substantially reduce the level of organised and serious crime. There are four main methods of confiscation open to the NCA: criminal confiscation, civil recovery, taxation and the seizure and forfeiture of cash. The US has performed well in this area in relation to compliance with international standards, which has led academics to praise the overall regime, despite the

misgivings about the burden of proof in the civil mechanism. The UK is a prime example of the difficulties posed by digital currencies in relation to the confiscation regime. Greater Manchester Police have had difficulty in confiscating bitcoin due to lack of evidence and inability to access the bitcoin wallet. The UK government have indicated they are still considering how to apply confiscation methods to digital currencies.

The importance of mutual legal assistance in relation to NTPMs should not be underestimated, the UK through the Home Office was noted as having an adequate scheme. However, it is fair to say that the UK regime has come some way since the 2006 mutual evaluation report. The Home Office has indicated the importance to the UK of a strong mutual legal assistance to regime. The UK has an extensive number of mutual legal assistance treaties and like shares the confiscated proceeds with any jurisdiction which assists in an investigation. In an effort to improve the UK's international outreach in terms of AML and CTF, the NCA will create International Liaison Officer posts. This will assist in cases where there is the cross border transfer of funds, particularly prevalent through NTPMs.

So then, whilst it is clear that traditional methods pose by far and away the biggest threat to the UK in terms of monetary value it cannot be argued that NTPMs do not pose a significant risk. The UK has tailored its AML and CTF framework to NTPMs well.

Chapter 4 – The United States

The United States' implementation of the international AML and CTF framework to tackle abuse of NTPMs

> "The potential for anonymity in financial transactions underlies most of the vulnerabilities in this risk assessment. There is always a concern regarding the potential exploitation of any new product or technology as a vehicle for money laundering. US law enforcement and regulatory agencies are monitoring trends in new payment methods such as virtual currencies."[1]

4.1. Introduction

The fourth chapter of this thesis studies and examines how the US, in implementing the global anti-money laundering and counter-terrorist financing framework (identified in chapter 2), has dealt with the risks associated with the growing criminal misuse of non-traditional payment methods.

[1] Department of the Treasury, National Money Laundering Risk Assessment (2015), 93. Available at: <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf> accessed 22 September 2016.

The United States AML and CTF framework has even earlier origins than the UK and Australian systems, it was introduced and then evolved in response to narcotics-trafficking, it is this long evolving history that makes it a fascinating case study in terms of how it adapts to fresh challenges. The US AML and CTF framework, despite predating the legislative measures prescribed by the UN and recommended by the Financial Action Task Force, has implemented them into its regime. The US, like the UK and Australia, plays a leading role in developing the FATF Recommendations and as such it is imperative that they are seen to be implementing the measures. The United States is committed to 'identifying, disrupting, and dismantling money laundering and terrorist financing' and achieves this by 'aggressively pursuing financial investigations.'[2] There have been a number of developments in NTPMs since 2007, particularly with mobile payments and cryptocurrencies, despite this their compliance with the international framework should give them a firm basis which enables them to respond to new challenges and threats.

As with the UK and Australia, there are difficulties in calculating the extent of money laundering and funds being moved for terrorist purposes in the US. There are a number of estimates of what that figure may be: the General Accounting Office has given an estimate of $500bn[3]; Radomyski suggested around $300bn[4]; whilst Reuter and Truman suggest that the

[2] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (June 2006), 14. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20US%20full.pdf> accessed 22 September 2016.

[3] General Accounting Office, 'Money Laundering: Extent of Money Laundering through Credit Cards is Unknown' (Washington, DC: General Accounting Office, 2002), 1. Available at: <http://www.gao.gov/assets/240/235231.pdf> accessed 22 September 2016.

[4] M. Radomyski, 'What problems has money laundering posed for the law relating to jurisdiction?' (2010) 15(1) *Coventry Law Journal* 4, 6.

figure was between $650bn and $800bn in 1995.[5] Most recently, the Department of the Treasury, whilst noting that 'it is difficult to estimate with any accuracy how much money is laundered in the United States', has put the figure at $300bn.[6] The range of figures available show the uncertainty surrounding the amount of illicit funds being moved around the US system. In 2005, it was recognised that 'the volume of dirty money circulating through the United States is undeniably vast and criminals are enjoying new advantages with globalisation and the advent of new financial services such as stored value cards and online payment systems'[7], it is clear that a decade on this is still the case.[8] So, as with the UK and Australia, it is certain that the increasing use of NTPMs will in some, albeit comparatively small way, play a part in this uncertainty. What we do know is that whatever the amount of money laundered it does pose a threat to the integrity of their financial system, however because of their greater size it will not affect them to the same extent as the two other case study countries. Similarly to the UK and Australia statistics, it is unlikely that any of the estimates take into account the use of NTPMs, and because of when the General Accounting Office and Reuter and Truman predictions were made, they would not have taken into account mobile

[5] Peter Reuter and Edwin M. Truman, 'Chasing Dirty Money' (2004), Washington, DC; Peterson Institute for International Economics), 13.

[6] Department of the Treasury, National Money Laundering Risk Assessment (n.1).

[7] Money Laundering Threat Assessment Working Group, U.S. Money Laundering Threat Assessment (December 2005) available at: <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf> accessed 22/06/2016.

[8] For examples of the continuing threat of emerging technologies see: Department of Treasury, 'National Money Laundering Risk Assessment' (2015) available at <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf> accessed 22 September 2016; Department of Treasury, 'National Terrorist Financing Risk Assessment' (2015) available at <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf> accessed 22 September 2016.

payments or cryptocurrencies being used as a means for criminals to launder funds. Even the estimation by Department of Treasury is only in contemplation of laundering through the banking sector as well as more traditional money service businesses.[9] In terms of terrorism, the US is still on alert, the Department of Homeland Security noting in its June 2016 National Terrorism Advisory System Bulletin that "since issuing the first Bulletin in December 2015, their concerns that violent extremists could be inspired to conduct attacks inside the US have not diminished."[10]

As with the UK and Australia, it is most common that criminals seek to transfer their funds through the banking sector. A key reason for this is that deposits in US banks are currently at a record high of $10.9 trillion[11], providing extensive cover for illicit transfers. For that reason, the US gives the highest priority to keeping the core financial system secure.[12] However, money service businesses (MSBs), including informal value transfer systems (IMVTs), are consistently identified as the third-most utilised money laundering method in the US, behind the formal financial sector and cash businesses.[13] For that reason MSBs also receive priority within the AML/CFT strategy.[14]

---

[9] Department of the Treasury, National Money Laundering Risk Assessment (n.1).

[10] US Department of Homeland Security, 'National Terrorism Advisory System: Bulletin' (June 2016) <https://www.dhs.gov/sites/default/files/ntas/alerts/16_0615_NTAS_bulletin.pdf> accessed 22 September 2016.

[11] Forbes, Q2 2015 US Banking Review: Total Deposits, September 1st 2015 available at <www.forbes.com/sites/greatspeculations/2015/9/01/q2-2015-u-s-banking-review-total-deposits/#4e2f6dcf1e7d> accessed 22 September 2016.

[12] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2).

[13] Ibid, 15.

[14] Ibid.

The US AML and CTF strategy is led by three bodies; the Department of Treasury, the Justice Department and the Department of State, each of which are supported by subsidiary offices or secondary competent authorities. Ryder, stresses that there are too many bodies seeking to lead the fight in the US.[15] However, FATF suggests that the system appears to be working effectively.[16] The main legislative provisions are the Bank Secrecy Act 1970 (as amended by The Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act 2001), the US PATRIOT Act, and the Money Laundering Control Act 1986. The next part of this chapter will assess the US's implementation of the international AML and CTF framework, and in particular the parts of relevance to NTPMs.

4.2. Global Role and Implementation of the International AML/CTF Framework

This section will outline both the significant role that the US plays in the international framework, as well as highlighting the international AML and CTF measures that it has implemented.

The UN was introduced in Chapter 2[17], the US like the UK and Australia, has a long connection with the UN; in 1945 it was one of 51 states to sign the UN Charter, becoming a founding member.[18] The US Mission to the UN (USUN) is responsible for carrying out the nation's

[15] Nicholas Ryder, *Money Laundering – An Endless Cycle?* (1st edn, Routledge, 2012), 47.

[16] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 17-18.

[17] See section 2.3.1.1. for an explanation of the role of the UN in the international AML & CTF Framework.

[18] United Nations Association-UK, 'What is the United Nations?' <http://www.una.org.uk/content/what-un> accessed 22 September 2006.

participation in the world body.[19] In terms of AML and CTF, it has ratified the following UN Conventions:

- Vienna Convention (ratified February 1990);
- Palermo Convention (signed December 2000 and ratified in November 2005);
- International Convention for the Suppression of the Financing of Terrorism (signed January 2000[20] and ratified in 2002).

Alongside the above Conventions the provisions of S/RES/1267(1999) and S/RES/1373(2001) are also in effect in the US owing to its membership of the UN. The US's close links to the UN's counter-terrorist financing objectives can be highlighted by the fact that the US Secretary to the Treasury chaired a special meeting of the UN Security Council on combatting ISIL finance and all forms of terrorist financing.[21]

Of course implementation of the legislative instruments only tells one side of the US's role in the international framework, there are also international standards and best practices to be considered.

The most important set of standards come from the FATF. The US, like the UK and Australia, is a founding member of the FATF and has chaired the organisation once in 1995[22]. Financial

[19] United States Mission to the United Nations, 'About' <http://usun.state.gov/about> accessed 22 September 2016.

[20] The United States signed the Convention on the 10th January 2000, the first day possible to sign the Convention.

[21] Department of the Treasury, 'Joint Treasury and US Mission to the United Nations Fact Sheet: UN Security Council Meeting of Finance on Countering the Financing of Terrorism', available at: <https://www.treasury.gov/press-center/press-releases/Pages/jl0307.aspx> accessed 22 September 2016.

[22] Financial Action Task Force, *Annual Report 1995-1996* (June 1996). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/1995%201996%20ENG.pdf> accessed 22 September 2016.

Crimes Enforcement Network (FinCEN) acted as the US's delegate to the FATF between 1994 and 1998[23], but since then the role has been taken by the US Department of the Treasury.[24] The Department of the Treasury has noted that their Office of Terrorist Financing and Financial Crime (TFFC), alongside other inter-agency counterparts, has been a 'driving force behind the global propagation of strong anti-money laundering standards via the FATF.'[25] As many international terrorist groups pose a direct threat to the US homeland and US national security interests abroad, the United States has a vested interest in disrupting their financial activity even if it never actually reaches the US financial system.[26] One of the ways it achieves this is through its support in the development of 'strong international AML/CTF standards and working towards robust implementation of them through the FATF and the UN as well as other bodies.'[27] As well as this, the US is a Co-operating and Supporting Nation to the Caribbean FATF (CFATF), a member of the Asia / Pacific Group, and observer to Eastern and South African Anti-Money Laundering Group (ESAAMLG), Financial Action Task Force of Latin America (GAFILAT), and observer to the Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL).[28] Indeed it has been noted that the US play a key

[23] Financial Crimes Enforcement Network, 'The Financial Action Task Force' <https://www.fincen.gov/international/fatf/> accessed 22 September 2016.

[24] Financial Action Task Force, 'United States' available at: <http://www.fatf-gafi.org/countries/#United States> accessed 22 September 2016.

[25] Money Laundering Threat Assessment Working Group, U.S. Money Laundering Threat Assessment (n.7), ii.

[26] Department of Treasury, 'National Terrorist Financing Risk Assessment' (2015) 23. Available at <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf> accessed 22 September 2016.

[27] Ibid.

[28] Financial Action Task Force, 'United States' (n.24).

role in the FATF[29], and the US has worked extensively with foreign officials to promote the implementation of AML and CTF policies.[30]

The US is similar to the UK in terms to compliance with the FATF Recommendations, performing strongly in its 2006 Third Mutual Evaluation Report. The US was assessed as being fully compliant with 12 of the 40 Recommendations, largely compliant with 22, partially compliant with 2, and non-compliant with 4. In terms of the Nine Special Recommendations it is compliant with 3, and largely compliant with 6. Of particular note is that it was rated as largely compliant with the Recommendation on 'new technologies & non face-to-face business', largely compliant with the Recommendation on 'money/value transfer services', and largely compliant with the Recommendation on 'wire transfers'.[31] So, it is clear that at the time of the last FATF assessment, the US was for the most part meeting the international standards for NTPMs. Overall, the FATF stated that the 'US has a strong culture of AML/CTF compliance in financial institutions and non-financial businesses.'[32] They further note that 'money service businesses, including informal value transfer systems, serve as an alternative to banks for many individuals in the US' and for that reason they 'also receive high priority within the AML/CTF strategy.'[33]

---

[29] Ellen S. Podgor, 'Money Laundering and Legal Globalisation: Where Does the United States Stand on This Issue?' 5(1) Washington University Global Studies Law Review 151, 156.

[30] As examples of the US shaping FATF policy see: Richard K. Gordon, 'On the Use and Abuse of Standards for Law: Global Governance and Offshore Financial Centres' (2010) 88 N.C. L. Rev. 501, 565-566; and Ben Hayes, 'Counter-Terrorism, "Policy Laundering", and the FATF: Legalising Surveillance, Regulating Civil Society' (2012) April INT'L J. Not-For-Profit L. 5, 7.

[31] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 283-288.

[32] Ibid.

[33] Ibid, 15.

Alongside the above, and as with the UK and Australia, the US is also a member of various other international organisations. The US FIU, FinCEN, headed a meeting of core financial intelligence units (FIUs) in 1995 which led to the creation of the Egmont Group of Financial Intelligence Units.[34] The US is also a member of the Basel Committee on Banking Supervision.

4.3. Competent Authorities

As with the UK and Australia, the US has entrusted a number of competent authorities to the fight against money laundering and terrorist financing. Primarily, that responsibility lies between three authorities; the Department of Treasury, the Justice Department and the Department of State. There are a number of secondary competent authorities or subsidiary offices that facilitate the work of these primary competent authorities. Several external agencies play a role in the anti-money laundering enforcement in the US, including: the Federal Bureau of Investigation (FBI), the Drug Enforcement Agency (DEA) and the Securities and Exchange Commission (SEC). Ryder has stated that it could be argued that the US 'has too many agencies attempting to tackle money laundering'[35], however he also notes that 'this appears to be of little concern to the FATF'[36] who concluded that 'the US has designated law enforcement authorities that have responsibility for ensuring that money laundering offences

[34] United States General Accounting Office, 'Money Laundering: FinCEN's Law Enforcement Support, Regulatory, and International Roles' (Statement of Norman J. Rabkin, Director, Administration of Justice Issues, General Government Division), (April 1998), Appendix III page 19.

[35] Nicholas Ryder, *Money Laundering – An Endless Cycle?* (n.15), 47.

[36] Ibid.

are properly investigated. These authorities have adequate powers, are producing good results and seem to be working effectively.'[37]

4.3.1. Department of the Treasury

The Department of the Treasury (Treasury) is the administrator of US AML [and CTF policy].[38] It performs a critical and extensive role in enhancing national security through the implementation of economic sanctions against foreign threats to the US, by identifying and targeting the financial support networks of national security threats, and by improving the safeguards of the US financial systems. In terms of CTF it aims to make access to 'the US financial system more difficult and risky for terrorists and their facilitators.'[39] Whilst with regards to AML it is 'fully dedicated to combatting all aspects of money laundering at home and abroad.'[40] The PATRIOT Act 2001 gave the Treasury broad rule-making and enforcement powers. The Treasury has a number of subsidiary offices which develop AML and CTF policy and strategy, these will be introduced below.

4.3.1.1. The Office of Terrorism and Financial Intelligence (TFI)

The Office of Terrorism and Financial Intelligence (TFI) is the subsidiary office responsible for marshalling the Treasury's intelligence and enforcement functions, it has the twin aims of 'safeguarding the financial system against illicit use and combatting rogue nations, terrorist

---

[37] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 72.

[38] L. Low, H. Tilen, and K. Adendschein, 'Country report: the US anti-money laundering system', in M. Pieth and G. Aiolfi (eds), *A comparative guide to Anti-money Laundering: A critical analysis of systems in Singapore, the Uk and USA* (Cheltenham: Edward Elgar, 2004), 346.

[39] Department of Treasury, 'National Terrorist Financing Risk Assessment' (n.26), 2.

[40] Department of Treasury, 'Resource Center' <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/Money-Laundering.aspx> accessed 22 September 2016.

facilitators, weapons of mass destruction proliferators, money launderers, drug kingpins, and other national security threats.'[41] TFI 'develops and implements US government strategies to combat terrorist financing domestically and internationally, develops and implements the National Money Laundering Strategy[42], as well as other policies and programs to fight financial crimes.'[43] In 2015, it produced the National Money Laundering Risk Assessment[44], and the National Terrorist Financing Risk Assessment[45].

4.3.1.2. The Office of Terrorist Financing and Financial Crime (TFFC)

The Office of Terrorist Financing and Financial Crime (TFFC) acts as the policy development and outreach office for the TFI. TFFC's remit is broad, working across all elements of the national security community as well as with the private sector and foreign governments to 'identify and address the threats presented by all forms of illicit finance to the international financial system.'[46] In order to fulfil this aim, the TFFC develops 'initiatives and strategies to deploy the full range of financial authorities to combat money laundering, terrorist financing

[41] Department of Treasury, 'About: Terrorism and Financial Intelligence'<https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx> accessed 22 September 2016.

[42] Department of Treasury, '2007 National Money Laundering Strategy' (2007) <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/nmls.pdf> accessed 22 September 2016.

[43] Department of Treasury, 'About: Terrorism and Financial Intelligence'<https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx> accessed 22 September 2016.

[44] Department of the Treasury, National Money Laundering Risk Assessment (n.1), 93.

[45] Department of Treasury, 'National Terrorist Financing Risk Assessment' (n.26).

[46] Department of Treasury, 'About: Terrorism and Financial Intelligence: Terrorist Financing and Financial Crimes' <https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorist-Financing-and-Financial-Crimes.aspx> accessed 22 September 2016.

. . . both at home and abroad.'[47] These focus on initiatives to increase transparency of the international financial system, and also threat-specific strategies and initiatives to apply and implement targeted financial measures to the full range of security threats.[48] The TFFC also represents the US at relevant international bodies, including heading the US delegation to the FATF and FATF-Style Regional Bodies (FSRBs).[49]

4.3.1.3. The Office of Intelligence and Analysis (OIA)

The Treasury's Office of Intelligence and Analysis (OIA) advances national security and protects financial integrity by informing Treasury decisions with timely, relevant, and accurate intelligence and analysis.[50] The OIA was established by the Intelligence Authorization Act 2004.[51] It is responsible, under the Act, for receiving, examining and distributing foreign intelligence and foreign counter-intelligence information related to the areas of competence of the Department of Treasury. OIA officers inform the formulation of Treasury policy and the execution of Treasury's regulatory and enforcement authorities, most notably by providing all-source intelligence analysis which targets and supports Treasury actions taken under the USA PATRIOT Act.[52] FATF states that its priorities include 'identifying and attacking the

[47] Ibid.

[48] Ibid.

[49] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2).

[50] Department of Treasury, 'About: Terrorism and Financial Intelligence: Office of Intelligence and Analysis (OIA)' <https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Intelligence-Analysis.aspx> accessed 22 September 2016.

[51] Pub. L. No. 108–177, §314, 1117 Stat. 2599, 2610.

[52] Department of Treasury, 'Strategic Direction Fiscal Years 2012-2015', 3 <https://www.treasury.gov/about/organizational-structure/offices/Documents/Strategic%20Direction%2008-13-12.pdf> accessed 22 September 2016.

financial infrastructure of terrorist groups; identifying and addressing vulnerabilities that may be exploited by terrorists and criminals in domestic and international financial systems; and promoting stronger relationships with Treasury's partners in the US and around the world.'[53]

4.3.1.4. Financial Crimes Enforcement Network (FinCEN)

The Financial Crimes Enforcement Network (FinCEN) acts as both the US Financial Intelligence Unit (FIU) and the federal government's primary AML/CTF regulator. It is a bureau in the Treasury[54], and was created in 1990. FinCEN's aim is to 'safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.'[55] To achieve that aim, FinCEN has two strategic goals; the first, to 'safeguard the financial system from evolving money laundering and national security threats'; and the second, to 'maximise sharing of financial intelligence between FinCEN and its domestic and foreign partners in government and private industry.'[56] The expansion of FinCEN's role to cover terrorist financing came through the USA PATRIOT Act 2001, as well as becoming part of the Treasury's Office of Terrorism and Financial Intelligence.[57]

---

[53] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 16.

[54] Financial Crimes Enforcement Network, 'Strategic Plan 2014-2018', 3 <https://www.fincen.gov/sites/default/files/shared/Strategic_Plan_2014-2018_508.pdf> accessed 22 September 2016.

[55] FinCEN, 'Mission' <https://www.fincen.gov/about/mission> accessed 22 September 2016.

[56] For a full outline of these strategic goals, see: Financial Crimes Enforcement Network, 'Strategic Plan 2014-2018', 3 <https://www.fincen.gov/sites/default/files/shared/Strategic_Plan_2014-2018_508.pdf> accessed 22 September 2016.

[57] Department of the Treasury, 'Role of Treasury' <https://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/to180-01.aspx>. Treasury Order 180–1 dated 26 September 2002.

FinCEN has a number of statutory areas of responsibility:

- Enforcing compliance with the Bank Secrecy Act 1970 through enforcement action in its role as AML/CTF civil regulator across a variety of financial industries;
- Receipt of millions of financial reports each year and maintaining a database of over 170 million reports;
- Analysing and disseminating intelligence from those reports to federal, state, and local law enforcement, federal and state regulators, foreign FIUs, and industry;
- Maintaining a network of sharing with FIUs in more than 140 partner countries.[58]

NTPM providers are caught under the umbrella of FinCEN's areas of responsibility owing to the Bank Secrecy Act 1970 which covers a wide range of financial institutions, including: depository institutions; money service businesses; casinos; insurance companies; institutions in the securities and futures sector; dealers in precious metals, stones and jewels; non-bank residential mortgage lenders and originators; and providers and sellers of prepaid access.[59] Therefore under the Bank Secrecy Act 1970, FinCEN's role in administering the reporting obligations of the Bank Secrecy Act 1970 are also applicable to NTPM providers. Given the kind of global challenge presented by NTPMs, FinCEN's role in collating currency transaction reports and suspicious activity reports are imperative to the fight against the misuse of NTPMs for the purposes of money laundering and terrorist financing.

Further, as noted above, one of FinCEN's strategic goals is to safeguard the financial system from evolving money laundering and national security threats. They note that the moving of

[58] Financial Crimes Enforcement Network, 'Strategic Plan 2014-2018', 3 - 4 <https://www.fincen.gov/sites/default/files/shared/Strategic_Plan_2014-2018_508.pdf> accessed 22 September 2016.

[59] Ibid, 4.

illicit funds is done 'using a variety of means and methods, many of which are rooted in a lack of transparency, such as the use of . . . anonymous payment systems. . .'[60] They note that they aim to prevent through three key objectives:

- Adoption of strong AML/CTF regulatory safeguards;
- Employing targeted financial measures against priority threats; and
- Use research, analysis, and advanced analytics to identify and explain priority threats to the financial system.[61]

FinCEN also supports the Department of the Treasury's efforts to promote the adoption of international standards involving AML and CTF.[62] Indeed, FinCEN is committed to the expansion of FIUs around the world.[63] They have assisted other countries to create FIU's and supported the FATF.[64]

4.3.1.5. The Office of Foreign Assets Control (OFAC)

The Office of Foreign Assets Control (OFAC) is another subsidiary of the Treasury. OFAC 'administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorist, international

[60] Ibid, 6.

[61] Ibid, 6 - 8.

[62] Financial Crimes Enforcement Network, 'The Financial Action Task Force' <https://www.fincen.gov/international/fatf/> accessed 22 September 2016.

[63] United States General Accounting Office, 'Money Laundering: FinCEN's Law Enforcement Support, Regulatory, and International Roles' (n.34), Appendix III page 19.

[64] C. Jackson, 'Combating the new generation of money laundering: regulations and agencies in the battle of compliance, avoidance, and prosecution in a post-September 11 world', Journal of High Technology Law, 2004, 3, 139–71, at 139.

narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the US.'[65] OFAC power derives from the President's wartime and national emergency powers, as well as from authority granted by specific legislation to impose controls on transactions and assets subject to US jurisdiction.[66] OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries.[67] OFAC also lists individuals, groups and entities that are designated under programs that are not country specific.[68]

4.3.1.6. Treasury Executive Office for Asset Forfeiture (TEOAF)

The Treasury Executive Office for Asset Forfeiture (TEOAF) was created in 1992 to manage the Treasury Forfeiture Fund (TFF). The TFF is the receipt account for deposit of non-tax forfeitures made pursuant to laws enforced or administered by itself or participating Department of Homeland Security agencies.[69] The agencies involved are: the Internal Revenue Service Criminal Investigations Division (IRS-CI), US Immigration and Customs

[65] Department of Treasury, 'About: Terrorism and Financial Intelligence: Office of Foreign Assets Control (OFAC)' <https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx> accessed 22 September 2016.

[66] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 16.

[67] Department of Treasury, 'Office of Foreign Assets Control: Specially Designated Nationals and Blocked Persons List' (September 2016) <https://www.treasury.gov/ofac/downloads/sdnlist.pdf> accessed 22 September 2016.

[68] Department of Treasury, 'Resource Center: Consolidated Sanctions List Data Files' (September 2016) <https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/consolidated.aspx> accessed 22 September 2016.

[69] Department of Treasury, 'About: Terrorism and Financial Intelligence: Treasury Executive Office for Asset Forfeiture' <https://www.treasury.gov/about/organizational-structure/offices/Pages/The-Executive-Office-for-Asset-Forfeiture.aspx> accessed 22 September 2016.

Enforcement (ICE), US Customs and Border Protection, US Secret Service, and US Coast Guard.[70]

4.3.2. Department of Justice (DOJ)

The Department of Justice (DOJ) is the principal entity responsible for overseeing the investigation and prosecution of money laundering and terrorist financing offences at a federal level.[71] The DOJ, through the Drug Enforcement Administration (DEA) 'seeks to deny safe havens to criminal organisations involved in drug trafficking, drug-related terrorist activities , and money laundering, thus depriving drug trafficking organisations of their illicit profits.'[72] The DOJ also manages the US assets forfeiture provisions which aim to tackle the issue of criminals making a profit from their illegal activity. The agencies and offices of the DOJ that are involved in the tackling of AML and CTF are introduced below.

4.3.2.1. Asset Forfeiture and Money Laundering Section (AFMLS)

The Asset Forfeiture and Money Laundering Section (AFMLS) lead the DOJ's asset forfeiture and AML enforcement efforts.[73] The AFMLS takes the following roles:

- Prosecutes and coordinates complex, sensitive, multi-district, and international money laundering and asset forfeiture investigations;
- Provides legal and policy assistance and training to federal, state, and local prosecutors and law enforcement personnel, as well as to foreign governments;

---

[70] Ibid.

[71] F Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 17.

[72] D. Hopton, *Money Laundering: A Concise Guide for All Businesses* (Farnham: Gower, 2009), pp. 19–20.

[73] Department of Justice, 'Asset Forfeiture and Money Laundering Section (AFMLS)' <https://www.justice.gov/criminal-afmls> accessed 22 September 2016.

- Assisting policy makers by developing and reviewing legislative, regulatory, and policy initiatives; and
- Managing the DOJ's Asset Forfeiture Program, including distributing forfeited funds and properties to appropriate domestic and foreign law enforcement agencies and to community groups within the United States, as well as adjudicating petitions for remission or mitigation of forfeited assets.[74]

These different functions of the AFMLS are designated to different units. There are five unites: the Forfeiture Unit, the International Unit, the Money Laundering and Bank Integrity Unit, the Policy and Training Unit, and the Programme Operations Unit.[75]

As noted above, the AFMLS holds responsibility for the coordination, direction, and general oversight of the Asset Forfeiture Programme.[76] The programme encompasses the seizure and forfeiture of assets that represent the proceeds of, or were used to facilitate federal crimes.[77] The primary goal of the Programme is to employ asset forfeiture powers in a manner that enhances public safety and security.[78]

[74] Ibid.

[75] Ibid.

[76] Department of Justice, 'Participants and Roles' <https://www.justice.gov/afp/participants-and-roles> accessed 22 September 2016.

[77] Department of Justice, 'Asset Forfeiture Program' <https://www.justice.gov/afp> accessed 22 September 2016.

[78] Ibid.

4.3.2.2. Counter-terrorism Section (CTS)

The Counter-terrorism Section (CTS) designs, implements, and supports law enforcement efforts, legislative initiatives, policies and strategies aimed at combatting terrorism.[79] It seeks to assist through the investigation and prosecution of individuals involved in terrorism anywhere in the world that could have an impact on significant US interests and persons.[80] Some of its main roles are:

- Investigating and prosecuting terrorism and terrorist financing cases (nationally and internationally);
- Participating in the systematic collection and analysis of data and information relating to the investigation and prosecution of terrorism cases;
- Coordinating with US government agencies (such as the Treasury and State Departments, the FBI, intelligence agencies and the Department of Homeland Security) to facilitate prevention of terrorist activity through daily detection and analysis and support to the field;
- Formulating legislative initiatives and DOJ policies and guidelines relating to terrorism;
- Conducting training conferences, seminars and lectures on terrorism-related topics;
- Participating in the foreign terrorist organisation designation process with the Departments of State and Treasury and other DOJ components; and

[79] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 17.

[80] Department of Justice, 'Counterterrorism Section' <https://www.justice.gov/nsd/counterterrorism-section> accessed 22 September 2016.

- Sharing information and trouble-shooting issues with international prosecutors, agents and investigating magistrates to assist in addressing international threat information and litigation initiatives.[81]

4.3.2.3. Office of International Affairs

The Office of International Affairs plays a significant role in DOJ policy in the areas of extradition and mutual legal assistance.[82]

4.3.3. Department of State (DOS)

The Department of State (DOS) mission is to 'shape and sustain a peaceful, prosperous, just and democratic world and foster conditions for stability and progress for the benefit of the American people and people everywhere.'[83] As part of this mission, the DOS conducts a wide variety of regional and bilateral initiatives relating to money laundering and terrorist financing.[84] DOS is the lead authority in relation to mutual legal assistance.[85] It also represents the US government at several multilateral institutions, including amongst other the FATF,

[81] Ibid.

[82] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 18.

[83] Department of State, '2015 Agency Financial Report: Advancing America's Interests through Global Leadership and Diplomacy' (16 November 2015) 7 <http://www.state.gov/documents/organization/249770.pdf> accessed 22 September 2016.

[84] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 18.

[85] General Accounting Office, 'Money Laundering: Extent of Money Laundering through Credit Cards Is Unknown' (n.3), 46.

FSRBs and the UN 1267 Sanctions and Counter-Terrorism Committees.[86] In fulfilling its AML and CTF functions, it liaises with the Treasury and DOJ.

The DOS, through its Terrorist Financing Working Group (TFWG) has set up the New Payment Methods Ad Hoc Working Group (NPMWG), which is concerned with virtual currencies and emerging payment systems. The NPMWG highlights the growing concern NTPMs and the fact that the DOS has an eye on the risk of their abuse for money laundering and terrorist financing.

4.3.3.1. Bureau of Economic and Business Affairs (EB)

The Bureau of Economic and Business Affairs (EB) pursues Economic Diplomacy for the US, 'making our nation and our people more prosperous and secure.'[87] The EB's main role in terms of financial crime is in preventing terrorist states the benefits of trade with the US and to deny access to the global financial system.[88] It does so through its Counter Threat Finance and Sanctions division.

4.3.3.2. Bureau of International Narcotics and Law Enforcement Affairs (INL)

The Bureau of International Narcotics and Law Enforcement Affairs (INL) has primary responsibility for issues dealing with money laundering and financial crimes.[89] Its main relevance to the thesis is through the International Narcotics Control Strategy Report (INCSR)

---

[86] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 18.

[87] Department of State, 'Bureau of Economic and Business Affairs' <http://www.state.gov/e/eb/> accessed 22 September 2016.

[88] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 18.

[89] Ibid, 18.

which it publishes annually.[90] As per the its obligations under the Foreign Assistance Act of 1961[91], the INCSR includes a volume on money laundering and terrorist financing. As part of the report, it does consider how countries are implementing measures to tackle the abuse of NTPMs, in particular virtual currencies, mobile payments, and wire transfers.[92] The INL combats crime by helping over 90 foreign governments build effective law enforcement institutions that counter transnational crime.[93] The INL also provides a coordinating function on intelligence relating to money laundering and other financial crimes, and meets regularly with intelligence agencies to monitor worldwide trends and developments.[94]

4.3.3.3. Bureau of Counterterrorism and Countering Violent Extremism (BCCVE)

The Bureau of Counterterrorism and Countering Violent Extremism (BCCVE) leads the Department of State in the whole-of-government effort to counter-terrorism abroad and to secure the US against foreign terrorist threats.[95] The BCCVE took over from the Office of the Coordinator for Counter Terrorism in 2012. Working alongside US Government agencies, other DOS bureaus and National Security Staff, the BCCVE develops and implements

[90] The most recent report in 2016 marked the 32nd annual report prepared pursuant to the FAA.

[91] As amended by the "FAA," 22 U.S.C. § 2291.

[92] Department of State, Bureau for International Narcotics and Law Enforcement Affairs, 'International Narcotics Control Strategy Report – Volume II: Money Laundering and Financial Crimes' (March 2016) <http://www.state.gov/documents/organization/253983.pdf> accessed 22 September 2016.

[93] <http://www.state.gov/j/inl/> accessed 22 September 2016.

[94] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 18-19.

[95] Department of State, 'Who We Are' <http://www.state.gov/j/ct/about/> accessed 22 September 2016.

counterterrorism strategies, policies, and operations.[96] The BCCVE also provides an 'on-call' capability to respond to terrorist incidents worldwide.[97]

4.3.4. Law Enforcement Agencies

Alongside the above Government agencies there are also a number of US law enforcement agencies which play a role in AML and CTF, these will be introduced below.

4.3.4.1. Drug Enforcement Administration (DEA)

The Drug Enforcement Administration's (DEA) primary area of concern is investigations of drug trafficking, but through this it has an interest in financial crime. The DEA was created by President Nixon to establish single unified command to combat "an all-out global was on the drug menace."[98] In fulfilling its mission it is responsible for the 'seizure and forfeiture of assets derived from, traceable to, or intended to be used for illicit drug trafficking.'[99] The DEA realises that it cannot successfully target the whole $100 billion spent annually on drugs in the US, so it has identified and targeted those illegal proceeds that flow back to sources of supply as the top priority of its financial enforcement program.[100] By targeting the money, the DEA aims to identify cases as well as disrupt and dismantle the financial infrastructure of drug trafficking organisations.[101] In 2012, the DEA also took over the functions of the National Drug

[96] Department of State, 'Mission' <http://www.state.gov/j/ct/about/mission/index.htm> accessed 22 September 2016.

[97] Ibid.

[98] Department of State, 'DEA History' <https://www.dea.gov/about/history.shtml> accessed 22 September 2016.

[99] Department of State, 'DEA Mission Statement' <https://www.dea.gov/about/mission.shtml> accessed 22 September 2016.

[100] Department of State, 'DEA: Money Laundering' <https://www.dea.gov/ops/money.shtml> accessed 22 September 2016.

[101] Ibid.

Intelligence Center (NDIC), principally its Document and Media Exploitation (DOMEX) branch and its strategic analysis functions.

Indeed, the DEA has identified that NTMPs are a major money laundering typology in relation to the movement of drug proceeds; 'emerging payment methods to include cryptocurrencies and online payment systems to facilitate internet-based drug sales.'[102] To counter these threats the DEA works nationally and internationally with law enforcement and financial industry counterparts to identify, target, and ultimately prosecute the command and control elements of international sources of drug supply.[103]

4.3.4.2. Federal Bureau of Investigation (FBI)

The Federal Bureau of Investigation (FBI) is an intelligence-driven and threat-focussed national security organisation with both intelligence and law enforcement responsibilities.[104] It was formed in 1908 when Attorney General Bonaparte ordered the special agent force to report to Chief Examiner Stanley W. Finch.[105] It became known as the FBI in 1935.[106] Ironically, even at its outset in 1908, technological revolution was at the heart of the work it undertook.[107] It is the primary US agency responsible for investigating financial crime,

[102] Ibid.

[103] Ibid.

[104] FBI, Department of Justice, 'FBI: About' <https://www.fbi.gov/about> accessed 22 September 2016.

[105] FBI, Department of Justice, 'FBI: History: Timeline' <https://www.fbi.gov/history/timeline> accessed 22 September 2016.

[106] Ibid.

[107] FBI, Department of Justice, 'FBI: A Brief History' <https://www.fbi.gov/history/brief-history> accessed 22 September 2016.

including money laundering and financial crime.[108] The FBI's involvement in AML is through its restored Money Laundering Unit.[109] It promotes the investigation and prosecution of money laundering across all of its investigations.[110] Whilst in terms of CTF, the Terrorist Financing Operations Section (TFOS) coordinates efforts to track and shut down terrorist financing and to exploit financial information in an effort to identify previously unknown terrorist cells and to recognise potential activity / planning.[111]

The FBI has taken a keen interest in NTPM, most recently through its Virtual Currency Emerging Threats Working Group (VCET) which it founded in 2012. The VCET comprises individuals from the Justice Department (in particular from the AFMLS and the Computer Crime and Intellectual Property section), the FBI, the DEA, and multiple US Attorney's Offices.[112] The FBI have also prepared a report on Bitcoin intended for use within the law enforcement community, however it has been leaked publically.[113]

---

[108] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 19.

[109] FBI, Department of Justice, 'FBI Revamps Money Laundering Investigations' (March 2016) <https://www.fbi.gov/audio-repository/news-podcasts-thisweek-fbi-revamps-money-laundering-investigations.mp3/view> accessed 22 September 2016.

[110] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 19.

[111] FBI, Department of Justice, 'Terrorism' <https://www.fbi.gov/investigate/terrorism> accessed 22 September 2016.

[112] J. Anthony Malone, *Bitcoin and other virtual currencies for the 21st Century* (1st edn, Create Space Independent 2014).

[113] FBI, Department of Justice, 'Intelligence Assessment: (U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity' (24 April 2012) <https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf> accessed 22 September 2016.

4.3.4.3. Internal Revenue Service Criminal Investigation (IRS-CI)

The Internal Revenue Service Criminal Investigation (IRS-CI) enforces money laundering, terrorist financing and criminal tax statutes.[114]

4.4. Application of a Risk-Based Approach to AML and CTF

The US Government prioritises its AML/CFT domestic and international initiatives based on perceived systemic vulnerabilities and the relative risk to US interests.[115] The US was one of the first countries to move back to a risk-based AML regulation, doing so by 1996.[116] Former Director of FinCEN, William J. Fox stated that they 'strongly believe that compliance must be risk-based in order to fairly and effectively regulate the panorama of industries represented under the Bank Secrecy Act 1970 umbrella.'[117] Another former Director of FinCEN, James H. Freis, reaffirmed their position stating that 'we are committed to a risk-based approach to effectively and efficiently implement Bank Secrecy Act requirements. . . across all of the diverse industries we regulate.'[118]

---

[114] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 19.

[115] Ibid, 15.

[116] Bridgitte Unger and Frans van Waarden, 'How to Dodge Drowning in Data? Rule –and Risk – based Anti-Money Laundering Policies Compared' (2009) 5(2) *Review of Law and Economics* 953, 957.

[117] Financial Crime Enforcement Network, 'William J Fox, Director, Financial Crime Enforcement Network: Women in Housing and Finance' (25 February 2004) <https://www.fincen.gov/news/speeches/william-j-fox-director-financial-crimes-enforcement-network-1> accessed 22 September 2016.

[118] Financial Crimes Enforcement Network, Prepared remarks of James H. Freis, Jr, Kewellers Vigilance Committee AML Seminar, 10 March 2008. Available at: <https://www.fincen.gov/news/speeches/prepared-remarks-james-h-freis-jr-director-financial-crimes-enforcement-network-3> accessed 22 September 2016.

It is clear that what suits one business or organisation, would not suit another. For this reason perhaps, the RBA is 'widely supported by the financial industry, although some smaller institutions have expressed a preference to have greater certainty on some of their obligations.'[119] FinCEN recognised prior to the FATF making the risk-based approach one of its standards that it was a good method to adopt, and in 2004 stated that they have 'significant responsibilities in a risk-based system. They must have made every effort to fully explain their regulations and provide well thought-out guidance and expert assistance. This guidance must be both formal and informal and should be delivered through a myriad of technologies.'[120] The Department of the Treasury, through its National Money Laundering Threat Assessment, has also confirmed the application of the RBA to NTPMs stating that 'nonbank providers of prepaid access are required to develop, implement, and maintain a risk-based AML program. . .'[121] Despite this, guidance to NTPM providers regarding the risk-based approach is scarce. But they did recognise that giving such guidance and information is not easy.[122]

The US's RBA is clearly illustrated through the regulatory approach adopted by FinCEN in relation to the Bank Secrecy Act 1970 and the USA PATRIOT Act 2001.[123] Indeed, the US adopts a RBA to the extent that it is not overridden by the prescriptive requirements under

[119] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 94.

[120] Financial Crime Enforcement Network, 'William J Fox, Director, Financial Crime Enforcement Network: Women in Housing and Finance' (n.117).

[121] Department of the Treasury, National Money Laundering Risk Assessment (n.72).

[122] Financial Crime Enforcement Network, 'William J Fox, Director, Financial Crime Enforcement Network: Women in Housing and Finance' (n.117).

[123] Nicholas Ryder, *Money Laundering – An Endless Cycle?* (n.15), 45.

the USA PATRIOT Act.[124] This is supplemented by the Bank Secrecy Act / Anti-Money Laundering (BSA/AML) Examination Manual, the manual 'reflects the ongoing commitment of the Federal and State banking agencies to provide current and consistent guidance on risk-based policies.'[125] However, some smaller businesses have stated that a more prescriptive approach would be beneficial in some instances.[126] This is likely to be the case for some of the smaller NTPM providers too. It can be resource intensive for smaller firms to assess the risk of all customers and sectors, and then apply AML and CTF measures to them depending on that risk. FinCEN's Associate Director for Enforcement, Thomas Ott has commented that in the majority of FinCEN's enforcement actions, the financial institution will have failed to 'establish and implement policies and procedures that were appropriately risk-based and reasonably designed to assure and monitor compliance with the Bank Secrecy Act 1970.'[127] So it is clear that the risk-based approach is not easy to get right.

[124] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 94.

[125] Financial Crimes Enforcement Network, Annual Report 2010 (2010), 31. Available at: <https://www.fincen.gov/sites/default/files/shared/annual_report_fy2010.pdf> accessed 22 September 2016.

[126] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 94.

[127] Financial Crimes Enforcement Network, 'Prepared Remarks of FinCEN Associate Director for Enforcement Thomas Ott, delivered at the National Title 31 Suspicious Activity and Risk Assessment Conference and Expo' (17 August 2016). Available at: <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-associate-director-enforcement-thomas-ott-delivered-national> accessed 22 September 2016.

4.5. Criminalisation of Money Laundering and Terrorist Financing

4.5.1. Money Laundering

The origins of the US AML policy date back to the 1960's when they became 'increasingly concerned by the use of offshore bank accounts by Americans engaged in illegal activity',[128] the concern was particularly in relation to drug related crime. However it was not until the Money Laundering Control Act 1986 that the US became the first country to criminalised money laundering as an independent crime.[129] Indeed the US police predates international measures.[130] Sultzer has outlined the rationale for introducing the money laundering offence, 'laundering was criminalised because of the nature of non-compliance with the reporting provisions of the Bank Secrecy Act 1970, the use of structure payments to avid the financial reporting thresholds and the acceleration of the drug trade and large amounts of money associated with it.'[131] Ryder has supported this, noting that it was the inherent weakness of the BSA that finally led to the criminalisation of money laundering.[132] 'It was not until the implementation of the Money laundering and Financial Crimes Act 1998 which required the issuance of an annual National Money Laundering Strategy that the US had a codified AML Policy.'[133] The premise behind the US prosecution of money laundering is that if the

[128] T. Doyle, 'Cleaning Up Anti-Money Laundering Strategies: Current FATF Tactics Needlessly Violate International Law' (2002) 24 *Houston Journal of International Law* 279, 282.

[129] D. Hopton, *Money Laundering: A Concise Guide for All Businesses* (1st edn, Gower, 2009), 33; and Steven Mark Levy, *Federal Money Laundering Regulation: Banking Corporate and Securities Compliance* (1st edn, Aspen Publishers, 2003), 3.

[130] Micheal Levi and Peter Reuter, 'Money Laundering' (2006) 34 *Crime and Justice* 289, 296.

[131] S. Sultzer, 'Money Laundering: The Scope of the Problem and Attempts to Combat It' (1995) 63 Tennessee Law Review 143, 158.

[132] Nicholas Ryder, *Financial Crime in the 21st Century* (1st edn, Edward Elgar, 2011), 20.

[133] Ibid.

government traces a criminal's proceeds from illegal activities, it will discourage criminals from engaging in such activities by cutting off the criminals illicit gains.[134] However, the US policy now targets the proceeds of a range of criminal offences including: weapons, human trafficking, fraud, political corruption, and the financing of terrorism[135]

The first offence under the Money Laundering Control Act breaks down into three parts relating to domestic money laundering,[136] international money laundering,[137] and the use of sting agencies to expose illegal activities.[138] In regards to international money laundering the individual must 'know' that the proceeds derive from a specified illegal activity.[139] For international money laundering the individual must know that the funds represent the proceeds of some form of unlawful activity.[140] The penalty for these three offences is a civil sanction of no more than either the value of the 'property funds, or monetary instruments involved in the transaction'[141] or $10,000.[142]

With the majority of NTPMs they will be caught under the definition of monetary instruments as they utilise the 'coin or currency of the United States or of any other country'.[143] It will be

---

[134] United States General Accounting Office, 'Money Laundering: Needed Improvements for Reporting Suspicious Transactions are Planned' (1995) (Report to the Ranking Minority Member)

[135] Mark A. Provost, 'Money Laundering' (2009) 46(1) *American Criminal Law Review* 837, 838.

[136] 18 USC § 1956(a)(1)(2006).

[137] 18 USC § 1956(a)(2)(2006).

[138] 18 USC § 1956(a)(3).

[139] 18 USC § 1956(a)(2)(B)(i).

[140] 18 USC § 1956(a)(B)(i).

[141] 18 USC § 1956(b)(1)(A).

[142] 18 USC § 1956(b)(1)(B).

[143] 18 USC § 1956(c)(4).

interesting to see whether Bitcoin could be caught under this provision as it is not a currency of any country. Further Bitcoin cannot be classed as a financial institution for the purposes of the Act.[144]

Chung suggests that legislation in the US has proven to be an effective way of curbing money laundering.[145] Sultzer expands on this noting that there was only one conviction in 1987 but by 1993, 857 defendants were convicted.[146] Whilst the FATF note that as of 2005, 1,075 people have convictions.[147]

4.5.2. Terrorist Financing

The first law to criminalise terrorist financing was the Suppression of the Financing of Terrorism Convention Implementation Act 2002, which implemented the International Convention for the Suppression of the Financing of Terrorism. Under the Act it is a criminal offence 'to collect or provide funds to support terrorist activities (or to conceal such fundraising efforts), regardless of whether the offense was committed in the US or the accused was a US citizen.'[148]

There are four terrorist financing offences under federal law:

[144] 18 USC § 1956(b)(6).

[145] Sam Chung, 'Criminalizing Money Laundering as a Method and Means of Curbing Corruption, Organised Crime and Capital Flight in Russia' (1999) 8(3) *Pacific Rim Law & Policy Journal Association* 617, 625.

[146] S. Sultzer, 'Money Laundering: The Scope of the Problem and Attempts to Combat It' (n.131), 177.

[147] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 37.

[148] 18 USC § 2339C.

1. Providing material support for commission of certain offences;[149]
2. Providing material support or resources to a foreign terrorist organisation;[150]
3. Proving or collecting terrorist funds;[151] and
4. Concealing or disguising either material support to terrorist organisations or funds to be used for terrorist acts.[152]

The FATF has stated that the US CTF measures are 'very difficult legislation to follow and in some aspects unnecessarily complicated.[153] Whilst Ryder states, 'the impact of its provisions must be questioned, as al-Qaeda continues to inspire and finance terrorist attacks, a point illustrated by the failed car bomb in New York in May 2010.'[154] As with the US AML provisions it is unlikely that the current provisions cover Bitcoin, although Bitcoin exchanges would be covered under the definition of a financial institution by means of being a currency exchange.[155] The other NTPMs would be as they simply transfer or store fiat currency.

4.6. Preventive Measures

Ryder has identified the US as being the first country to implement some of the key preventive measure that are now synonymous with AML and CTF, 'the US was the first to require reporting entities to file currency transaction reports and suspicious activity reports.'[156] The

[149] 18 USC § 2339A(a).

[150] 18 USC § 2339B(a).

[151] 18 USC § 2339C(a).

[152] 18 USC § 2339C(c)

[153] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 39.

[154] Nicholas Ryder, *Money Laundering – An Endless Cycle?* (n.15), 77.

[155] 31 USC § 5312(a)(2)(j).

[156] Nicholas Ryder, *Money Laundering – An Endless Cycle?* (n.15), 59-60.

current measures in relation to preventative measures are contained in the Bank Secrecy Act 1970. For the purposes of the provisions, 'financial institution' covers 'a currency exchange'[157] and a 'licenced sender of money or any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions.'[158] This would seem to cover all NTPMs, including virtual currency exchanges. It is an obligation that financial institutions have an anti-money laundering program which includes 'the development of internal policies, procedures and controls; the designation of a compliance officer; an ongoing employee training programme; and an independent audit function to test programs.'[159]

4.6.1. Customer Due Diligence

Under the Bank Secrecy Act, financial institutions are required to verify the identity of their customer when the open an account.[160] It is a requirement that financial institutions 'establish appropriate, specific, and, where necessary, enhanced, due diligence policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering through those accounts.'[161] As with the other case study countries, the US, in line with its risk-

[157] 31 USC § 5318(a)(2)(J).

[158] 31 USC § 5318(a)(2)(R).

[159] 31 USC § 5318(h).

[160] 31 USC § 5318.

[161] 31 USC § 5318(i)(1).

based approach to AML and CTF has provision for enhanced[162] and simplified due diligence.[163] It is a requirement that financial institutions keep such records for a period of five years.[164]

4.6.2. Reporting Requirements

The first mechanism that the US utilise is Currency Transaction Reports (CTRs), these require a financial institution to make a report of transactions in excess of $10,000.[165] Under that, they have defined a transaction as being a deposit, withdrawal, exchange or transfer of money.[166] This acts to create a paper trail of high value transactions. But, Benning has stated that while they 'produced a large quantity of reports, they produced little useful information.'[167]

The second measure that the US use are suspicious activity reports, these were introduced by the Anti-Money Laundering Act 1992.[168] Suspicious activity reports are a central part of the US's preventative measures strategy. The US Financial Intelligence Unit, FinCEN is responsible for the collection of these reports. FinCEN is the founder member of the Egmont Group, and its membership enables it seek financial intelligence from other members in order to support their operations and projects. FinCEN have introduced 'Interactive SAR Stats', an

---

[162] 31 USC § 5318(i)(2)(B).

[163] 31 USC § 5318(i)(3).

[164] Federal Financial Institutions Examination Council, 'Bank Secrecy Act, Anti-Money Laundering and Office of Foreign Assets Control' <https://www.ffiec.gov/bsa_aml_infobase/documents/FDIC_DOCs/BSA_Manual.pdf> accessed 22 September 2016.

[165] 31 USC § 5313 and 31 CFR § 103.22(b)(1).

[166] 31 CFR §103.28.

[167] Joseph F. Benning, 'Following Dirty Money: Does Bank Reporting of Suspicious Activity Pose a Threat to Drug Dealers?' (2002) 13(4) *Criminal Justice Policy Review* 337, 337-338.

[168] Annunzio–Wylie Anti-Money Laundering Act §1517.

application which enables users to search Bank Secrecy Act data for aggregated counts of defined suspicious activities, sector by sector, or in combination, as they choose, and the data is updated monthly so users can access the most up to date information as quickly as possible.[169]

As with the UK and Australia, the term 'suspicion' causes problems for those responsible for reporting. A transaction should be reported where the financial institution 'knows, suspects, or has reason to suspect it involves or is an attempt to disguise proceeds from illegal activity; is designed to evade the requirements of the Bank Secrecy Act; or it appears to have no business or apparent lawful purpose.[170] If this seems like a difficult test to apply for banks, it can only be more difficult for NTPM providers who may have a lack of resources and therefore staff may be stretched, particularly in smaller businesses. Due to this, the FATF report that FinCEN will receive around 14 million reports on an annual basis which means that it is 'not able to perform a comprehensive analysis of each SAR, but instead devotes its analytical resources to those SARs considered most valuable to law enforcement.'[171] The usefulness of this strategy can be questioned in terms of NTPMs, as it is likely given the usage of smaller NTPMs that any individual would not attempt to move large sums through them due to the risk of detection. Indeed, a wire transfer linked to 9/11 was the subject of a currency transaction report by was never picked up by FinCEN.

---

[169] Financial Crimes Enforcement Network, *SAR Stats Technical Bulletin* (October 2015), 1. Available at: <https://www.fincen.gov/sites/default/files/sar_report/SAR_Stats_2_FINAL.pdf> accessed 22 September 2016.

[170] 31 CFR § 103.21(a)(2) (1995).

[171] D. Alford, 'Anti-Money Laundering regulations: A Burden on Financial Institutions' (2004) 19 *Carolina Journal of International Law and Commercial Regulation* 437, 466.

FinCEN usefully have a section on the kind of reports made by MSBs, they state that the majority of SARs filed by MSBs relate to 'crowdfunding transactions.'[172] They noted a substantial increase in the amount of SARs from MSBs.[173] However, they also note that MSB's in more than 100,000 instances provided insufficient information in the SAR.[174] Again, this highlights that NTPM providers may struggle in terms of compliance, more so than traditional reporting entities. This should not be surprising given the differences in size and structure.

4.6.3 Specific NTPM Measures

4.6.3.1. New Technologies

As with the UK, the last time that the US was assessed for compliance with the Recommendation on 'new technologies', was in the FATF's Third Round of Mutual Evaluations.[175] At that time, it was still 'Recommendation 8' rather than 'Recommendation 15' and the US was rated as being 'largely compliant'.[176]

The main criticism by the FATF and the reason that it was rated as 'largely compliant' and not 'compliant' was that the US failed to implement measures for money service businesses (including money remitters and foreign exchange providers) to have policies and procedures in place to address the risks associated with non-face-to-face transactions.[177] The US focussed

[172] Financial Crimes Enforcement Network, *SAR Stats Technical Bulletin* (October 2015), 9. Available at: <https://www.fincen.gov/sites/default/files/sar_report/SAR_Stats_2_FINAL.pdf> accessed 22 September 2016.

[173] Ibid, 20.

[174] Ibid, 20.

[175] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2).

[176] Ibid, 121.

[177] Ibid, 120.

primarily on the risks associated with new technology in the banking sector. However, it was noted that FinCEN was working with law enforcement to better understand the risks posed by various types of stored value cards and internet payment products in order to amend their rules.[178] The US did indeed act upon this, introducing measures in relation to non-bank MSB's. FinCEN issued interpretative guidance in April 2005[179], just before the FATF's on-site visit for the Third Mutual Evaluation Report. It clarified that money service businesses, which include money transmitters and providers of prepaid access, are subject to the full range of Bank Secrecy Act regulatory requirements. Though it should be noted that prepaid providers will not be considered to be money services businesses in some limited situations, contained in the Code of Federal Regulations.[180] FinCEN has noted that, money service businesses AML and CTF measures should be dependent on the perceived level of risk of the technology, and its own size and sophistication.[181] They have also found that virtual currencies exchanges should be considered to be a money service business, specifically a money transmitter, for the purposes of the application of Bank Secrecy Act obligations.[182]

---

[178] Ibid.

[179] Financial Crimes Enforcement Network, Interagency Interpretive Guidance on Providing Banking Services to Money Service Businesses Operating in the United States (April 2005) <https://www.fincen.gov/resources/statutes-regulations/guidance/interagency-interpretive-guidance-providing-banking> accessed 22 September 2016.

[180] 31 CFR § 1010.100.

[181] Financial Crimes Enforcement Network, Interagency Interpretive Guidance on Providing Banking Services to Money Service Businesses Operating in the United States (n.179).

[182] Department of the Treasury Financial Crimes Enforcement Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (FIN-2013-G001), 1. Available at: <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> accessed 22 September 2016.

4.6.3.2. Wire Transfers

The US similarly to the UK was rated as being largely compliant with the FATF Recommendation on wire transfers.[183] Wire transfers have been monitored in the US since the introduction of the recordkeeping requirements and the "Travel Rule", these require financial institutions in the US to include originator information in all wire transfers greater than or equal to $3,000, apart some exempted transactions.[184] The FATF criticised the US for this limit, suggesting that it should be $1,000.[185] Despite this, the US have maintained the $3,000 limit.

In terms of record keeping, the wire transfer provider should retain the following information:

- The name and address of the transmitter;[186]
- The amount;[187]
- The execution date;[188]
- Any payment instructions received from the transmitter with the transmittal order;[189]
- The identity of the recipients financial institution;[190]

[183] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism: United States of America* (n.2), 135.

[184] 31 CFR 1010.410 (e).

[185] 31 CFR 1010.410 (e).

[186] 31 CFR § 1010.410 (e)(1)(A).

[187] 31 CFR § 1010.410 (e)(1)(B).

[188] 31 CFR § 1010.410 (e)(1)(C).

[189] 31 CFR § 1010.410 (e)(1)(D).

[190] 31 CFR § 1010.410 (e)(1)(E).

- As many of the following as possible: (1) the name and address of the recipient;[191] (2) the account number of the recipient;[192] (3) Any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.[193]

4.6.3.3. Money or Value Transfer Services

The US was rated as being 'largely compliant' with the money or value transfer Recommendation.[194] Money or Value Transfer service providers in the US are known as money service businesses and are supervised by the Securities and Exchange Commission.[195] Money Service Businesses are subject to the full range of Bank Secrecy Act regulatory controls, including the AML provisions.[196] Under the existing BSA regulations, MSBs are defined to include five types of financial service providers: (1) currency dealers or exchangers; (2) check cashers; (3) issuers of traveller's checks, money orders or stored value; and (5) money transmitters.[197] In terms of NTPMs the majority will fall under the definition of a money transmitter. The US Code defines a money transmitting business as 'any business which provides check cashing, currency exchange, or money transmitting or remittance services, or issues or redeems money orders, travelers' checks, and other similar instruments or any other person who engages as a business in the transmission of funds, including any

[191] 31 CFR § 1010.410 (e)(1)(E)(1).

[192] 31 CFR § 1010.410 (e)(1)(E)(2).

[193] 31 CFR § 1010.410 (e)(1)(E)(3).

[194] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism, United States of America* (n.2), 198.

[195] Ibid, 190.

[196] 31 CFR 103.125.

[197] Money Laundering Threat Assessment Working Group, US Money Laundering Threat Assessment (December 2015), 7. Available at: <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf> accessed 22 September 2016.

person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system.'[198] It is a requirement, as in the UK and Australia, that anyone who operates a money transmission business registers them.[199] Giving false or incomplete information when registering is considered as a failure to comply with the requirements to register.[200] When registering the business must provide:

- The name and location of the business;[201]
- The name and address of each person who – (a) owns or controls the business; (b) is a director or officer of the business; or (c) otherwise participates in the conduct of the affairs of the business;[202]
- The name and address of any depository institution at which the business maintains a transaction account;[203]
- An estimate of the volume of business in the coming year;[204] and
- Such information as the Secretary of the Treasury may require.[205]

[198] 31 USC § 5330(d)(1)(A).

[199] 31 USC § 5330.

[200] 31 USC § 5330(a)(4).

[201] 31 USC § 5330(b)(1).

[202] 31 USC § 5330(b)(2).

[203] 31 USC § 5330(b)(3).

[204] 31 USC § 5330(b)(4).

[205] 31 USC § 5330(b)(5).

Worryingly, the Treasury have stated that 'outside of the major firms [money service businesses] rates of registration have remained low.'[206] It has been suggested that the reason for this is because of 'language, culture, cost, and training issues.'[207] The Organised Crime Drug Enforcement Task Force have reported a 5% increase in money service business-related cases, with the total of money laundering cases growing from 11%-16%.[208]

4.7. Confiscation of the Proceeds of Crime

As with the UK and Australia, tackling the proceeds of crime is a central tenet of the US AML and CTF framework.[209] The measures that will be introduced below are important parts of the US's mission reduce the amount of laundering and terrorist financing activity which takes place in or through the US, as well as globally. In the FATF's last Mutual Evaluation of the US in 2006, they rated them as 'largely compliant' with the Recommendation on the confiscation of the proceeds of crime.[210] They were similarly rated as 'largely compliant' with the Recommendation on freezing and seizing terrorist funds.[211] It is notable that these compliance levels are lower than both the UK and Australia. The US have successfully ratified the Vienna, Palermo and Corruption Conventions as well as the relevant provisions of UN Security Council Resolutions 1267 and 1373.

---

[206] Money Laundering Threat Assessment Working Group, US Money Laundering Threat Assessment (n.197), 8.

[207] Ibid.

[208] ibid.

[209] Stefan D. Cassella, 'An Overview of Asset Forfeiture in the United States', in Simon N. M. Young, *Civil Forfeiture of Criminal Property: Legal Measures for Targeting the Proceeds of Crime* (1st edn, Edward Elgar, 2009), 24.

[210] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism, United States of America* (n.2), 51.

[211] Ibid, 59.

The US's main asset recovery mechanisms are found under Title 18, Chapter 46 of the US Code. Unlike the UK and Australia, the US does not have just one body overseeing its asset recovery programme. In the US, it is primarily administrated by the Department of Treasury through its Treasury Executive Office for Asset Forfeiture who manage the Treasury Forfeiture Fund[212]; and the Department of Justice who manages the Asset Forfeiture Program.[213] The Asset Forfeiture Program plays a 'critical role in disrupting and dismantling illegal enterprises, depriving criminals of the proceeds of illegal activity, deterring crime, and restoring property to victims.'[214] There are also a number of other agencies involved in the US Asset Forfeiture Program such as; the United States Postal Inspection Service, the Food and Drug Administration, the United States Department of Agriculture, Office of the Inspector General, the Department of State, Bureau of Diplomatic Security and the Defence Criminal Investigative Service.[215] The Comprehensive Crime and Control Act 1984 provides that the proceeds of forfeiture action should all be placed in a 'special forfeiture fund' that is jointly held at the Department of Justice and the Department of Treasury.[216]

---

[212] For more information on the Treasury Forfeiture Program, see: Department of the Treasury, 'About' available at: <https://www.treasury.gov/about/organizational-structure/offices/Pages/The-Executive-Office-for-Asset-Forfeiture.aspx> accessed 22 September 2016.

[213] For more information on the Asset Forfeiture Program, see: Department of Justice, 'Asset Forfeiture Program' available at: <https://www.justice.gov/afp> accessed 22 September 2016.

[214] Department of Justice, National Asset Forfeiture Strategic Plan 2008 – 2012 (2012), 5. Available at: <https://www.justice.gov/sites/default/files/criminal-afmls/legacy/2014/11/07/strategicplan.pdf> accessed 22 September 2016.

[215] Nicholas Ryder, 'To Confiscate or Not to Confiscate? A Comparative Analysis of the Confiscation of the Proceeds of Crime Legislation in the United States of America and the United Kingdom' (2013) 8 *Journal of Business Law* 767, 782.

[216] Barclay Thomas Johnson, 'Restoring Civility – The Civil Asset Forfeiture Reform Act of 2000: Baby Steps Towards a More Civilized Civil Forfeiture System' (2002) *35 Indiana Law Review* 1045, 1049-1050.

Title 18, Chapter 46 of the US Code has two measures for asset forfeiture, the third is found under Title 19, they are:

- Criminal forfeiture;[217]
- Civil forfeiture;[218]
- Administrative forfeiture.[219]

The first measure open to US law enforcement agencies under the Criminal Code is criminal forfeiture. Once the defendant is convicted of: laundering of the proceeds of unlawful activity;[220] or engaging in monetary transactions in property derived from specified unlawful activity;[221] or being an unlicensed money transmitting business,[222] then they are obliged to forfeit any property involved in the offence.[223] So, in the US a forfeiture order is handed out in conjunction with a conviction under one of the three offences outlined above. On top of this, a defendant may be ordered to pay a financial penalty, recompense the victim and to disgorge the proceeds of crime or the property utilised in the commission of the criminal offence.[224] Cassella adds that these powers are 'a powerful law enforcement tool that is

[217] 18 USC. § 982.

[218] 18 USC. § 981.

[219] 19 USC. § 1607.

[220] 18 USC. § 1956.

[221] 18 USC. § 1957.

[222] 18 USC. § 1960.

[223] 18 USC. § 982(a)(1).

[224] Stefan D. Cassella, 'The Case for Civil Recovery: Why in Rem Proceedings are an Essential Tool for Recovering the Proceeds of Crime' (2008) 11(1*) Journal of Money Laundering Control* 8, 9.

rapidly becoming a fixture in federal criminal practice.'[225] Whilst he also notes that in relation to money laundering the forfeiture provision are particularly stringent and apply to all the property involved in the commission of the offence.[226]

The second measure open to US law enforcement agencies under the Criminal Code is civil forfeiture. Where the criminal route is not available, or is perceived as too difficult a route to go down in terms of the evidential burden then US law enforcement agencies may use the civil forfeiture regime. This is a non-conviction based route and the action is taken 'in rem' against the property rather than against any individual person. The property that can be forfeited under the order is that involved in a transaction or attempted transaction in violation of the following offences: laundering of the proceeds of unlawful activity;[227] or engaging in monetary transactions in property derived from specified unlawful activity;[228] or being an unlicensed money transmitting business.[229] The Supreme Court in *United States v Various Items of Personal Property* clarified that in rem 'is the property which is proceeded against and, by resort to a legal fiction, held guilty and condemned through it were conscious instead of inanimate and insentient.'[230] As with the UK and Australian regimes, the civil forfeiture route only requires the prosecution to show on the balance of probabilities that the

[225] Stefan D. Cassella, 'Criminal Forfeiture Procedure: An Analysis of Developments in the Law Regarding the Inclusion of a Forfeiture Judgement in the Sentence Imposed in a Criminal Case' (2004) 32 American Journal of Criminal Law 55, 102.

[226] Stefan D. Cassella, 'An Overview of Asset Forfeiture in the United States', in Simon N. M. Young, *Civil Forfeiture of Criminal Property: Legal Measures for Targeting the Proceeds of Crime* (1st edn, Edward Elgar, 2009), 35.

[227] 18 USC. § 1956.

[228] 18 USC. § 1957.

[229] 18 USC. § 1960.

[230] 82 US 577, 581.

funds or property was linked to a crime. As a result of this, Moores has referred to the civil regime as being an 'easy way to deprive criminals of the fruits of their labour.'[231] Johnson adds further that this is simply a method to boost government coffers,[232] a view he takes from the courts who viewed it as a way to boost income by prosecuting minor offences.[233] Whilst it has been cautioned that 'improperly used, forfeiture could become more like a roulette wheel employed to raise revenue from innocent but hapless owners whose property is unforeseeably misused, or a tool wielded to punish those who associate with criminals, than a component of the justice system.'[234] Nelson, whilst seeing that the forfeiture regime has a place in the US asset recovery framework 'civil drug forfeiture is an important weapon in the war on drugs' did note that due to 'the broad language of the Forfeiture Statute, coupled with the zealousness of the drug war, erodes important constitutional safeguards.'[235]

The third route, administrative forfeiture, is found under Title 19 of the Criminal Code.[236] Like the administrative forfeiture this is an in rem action. However, in comparison to the both the criminal and civil forfeiture regimes, it is not a 'judicial matter requiring the commencement

[231] Eric Moores, 'Restoring the Civil Asset Forfeiture Reform Act' (2009) 51 *Arizona Law Review* 777, 779.

[232] Barclay Thomas Johnson, 'Restoring Civility – The Civil Asset Forfeiture Reform Act of 2000: Baby Steps Towards a More Civilized Civil Forfeiture System' (n.216), 1069.

[233] See: Rucker v Davis 237 F.3d 1113, 1125 (9th Cir.) (en banc), reversed, Dep't of Housing and Urban Development v. Rucker, 122 S. Ct. 1230 (2002).

[234] Justice Thomas in: Bennis v. Michigan, 516 U.S. 442, 456 (1996) (Thomas, J., concurring).

[235] S. Nelson, 'The Supreme Court Takes a Weapon from the Drug War Arsenal: New Defences to Civil Drug Forfeiture' (1994) 26 *Saint Mary's Law Journal* 157, 159.

[236] 19 USC. § 1607.

of a formal action in a federal court.'[237] The operation of the administrative forfeiture regime is limited to:

- Property valued at less than $500,000;[238]
- Property where its importation is illegal;[239]
- Where the property is used mechanism to move illegal substances;[240] and
- Where it is a coin or currency of any description.[241]

The US implements its obligations relating to terrorist financial sanctions under both UNSCR 1267 and 1373 through Executive Order 13224.[242] Executive Order 13224 prohibits 'any U.S. person or entity from transacting or dealing with individuals and entities owned or controlled by, acting for or on behalf of, financially, technologically, or materially assisting or supporting, or otherwise associated with, persons listed in the Executive Order or subsequently designated by the Secretaries of the Treasury and State under the terms of the Executive Order.'[243] Further, the USA PATRIOT Act permits the federal government and law enforcement agencies to seize and forfeit the assets of terrorists.[244] The criminal forfeiture regime can be applied to all proceeds lined to the following crimes: providing material support

---

[237] Stefan D. Cassella, 'An Overview of Asset Forfeiture in the United States', in Simon N. M. Young, *Civil Forfeiture of Criminal Property: Legal Measures for Targeting the Proceeds of Crime* (1st edn, Edward Elgar, 2009), 36.

[238] 19 USC. § 1607(a)(1).

[239] 19 USC. § 1607(a)(2).

[240] 19 USC. § 1607(a)(3).

[241] 19 USC. § 1607(a)(4).

[242] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism, United States of America* (n.2), 51-52.

[243] Ibid, 52.

[244] Stefan D. Casella, 'Forfeiture of Terrorist Assets under the USA PATRIOT Act of 2001' (2002) 34 *Law and Policy in International Business* 7, 7.

to terrorists;[245] providing material support or resources to designated foreign terrorist organisations;[246] providing or collecting funds for the financing of terrorism.[247] Whilst the civil forfeiture regime can be applied to: terrorist activities;[248] and collecting or providing of funds for the financing of terrorism.[249]

As noted with regards to the other case study countries, in terms of NTPMs generally these forfeiture procedures are straight forward to apply in the sense that the funds tend to remain in fiat currency. Where the NTPMs provide a problem is at the detection stage. However, cryptocurrencies do provide a problem for the confiscation of the proceeds of crime. The US have first-hand experience of confiscating bitcoin, through the FBI's action against the Silk Road. When they took down[250] the Silk Road they seized circa 30,000 bitcoins worth around $6 million at the time.[251] They later seized another 144,000 bitcoins worth at least $28.5 million.[252] The wallet[253] that the FBI moved the funds to after confiscating can be viewed publically.[254] The US then adopted the policy that Australia would also later adopt, of

[245] 18 USC. § 2339A.

[246] 18 USC. § 2339B.

[247] 18 USC. § 2339C.

[248] 18 USC. § 981(a)(1)(g).

[249] 18 USC. § 981(a)(1)(h).

[250] The FBI infiltrated the Silk Road, and closed down the site.

[251] Andy Greenberg, 'FBI Says It's Seized $28.5 Million in Bitcoins from Ross Ulbricht, Alleged Owner of Silk Road' (Forbes, 25 October 2013) <http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/#3f56f1161440> accessed 22 September 2016.

[252] Ibid.

[253] See chapter 1 for an explanation of bitcoin wallets.

[254] To see the total amount of bitcoins transferred and the final balance reflecting the fact they were auctioned off, visit:

auctioning[255] off the bitcoin so that they receive fiat currency and place that in the asset forfeiture fund.

4.8. Cooperation and Mutual Legal Assistance

As highlighted in chapter 2, cooperation and mutual legal assistance are the cornerstones of the international effort to counter the abuse of NTPMs by launderers and terrorist financers, a globalised crime cannot be solved with a localised approach. The FATF has noted that the US's mutual legal assistance framework is 'comprehensive and robust.'[256]

The Department of State is the lead US authority in relation to mutual legal assistance,[257] as evidenced by the fact that it signs off on the agreements.[258] The OIA is a subdivision of the Department of Justice is a key player in the Department of Justice's policy towards extradition and mutual legal assistance. The OIA serves as the United States Central Authority with respect to all requests for information and evidence received from and made to foreign

<https://blockchain.info/address/1FfmbHfnpaZjKFvyi1okTjJJusN455paPH> accessed 22 September 2016.

[255] Nate Raymond, 'U.S. Auctions Some 30,000 Bitcoins from Silk Road Raid' (Reuters, 27 June 2014) <http://www.reuters.com/article/us-bitcoin-auction-idUSKBN0F22LG20140628> accessed 22 September 2016.

[256] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism, United States of America* (n.2), 260.

[257] General Accounting Office, *Money Laundering: Extent of Money Laundering Through Credit Cards is Unknown* (General Accounting Office, 2002), 46. <http://www.gao.gov/assets/240/235231.pdf> accessed 22 September 2016.

[258] As an example see: Mutual Legal Assistance Agreement Between the United States of America and the European Union (June 2003) <http://www.state.gov/documents/organization/180815.pdf> accessed 22 September 2016.

authorities under Mutual Legal Assistance Treaties[259] and multilateral conventions regarding assistance in criminal cases.'[260] The also assist the Department of State in negotiating and implementing treaties.[261] Further, as a signatory of the Vienna, Palermo, CTF, and Merida Conventions, the US can 'provide wide measures of mutual legal assistance to foreign authorities for criminal investigations, prosecutions and related proceeds for offences covered by these Conventions.'[262]

The Department of Justice has noted that 'extradition and mutual legal assistance requests are critical tools for law enforcement and prosecutors in bringing criminals, including terrorists, to justice.'[263] They further add that they will 'work with foreign partners to effectively use our network of bilateral extradition treaties, mutual legal assistance treaties, multilateral conventions and other international agreements and networks.'[264]

Where the United States confiscate property, and they have had the assistance of any foreign government, then they are authorised to share the forfeited property.[265] From 1989 to 2013, the international asset sharing program administered by the Department of Justice shared

[259] The current Mutual Legal Assistance Treaties can be found here: <https://mlat.info/country-profile/united-states> accessed 22 September 2016.

[260] Department of Justice, 'Office of International Affairs' <https://www.justice.gov/criminal-oia> accessed 22 September 2016.

[261] Ibid.

[262] Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism, United States of America* (n.2), 260.

[263] Department of Justice, *Strategic Plan, Fiscal Years 2014-2018* (2014), 15. Available at: <https://www.justice.gov/sites/default/files/jmd/legacy/2014/02/28/doj-fy-2014-2018-strategic-plan.pdf> accessed 22 September 2016.

[264] Ibid.

[265] 18 USC § 981(i)(1).

$248,869,984 with 43 countries.[266] The US have used this approach to 'aggressively pursue' cooperation in relation to investigations narcotics trafficking and money laundering, offering the possibility of sharing in forfeited assets.[267]

4.9. Conclusion

The United States is one of the pre-eminent jurisdictions in relation to AML and CTF, it is prides itself in being a global leader and in shaping the international framework. The US's AML regime evolved as a response to drug-trafficking and its CTF regime began in the late 1990's. Despite its legislative measures pre-dating the international effort it has sought to ensure consistency with what is being advocated on an international level. It adopts an aggressive stance towards money laundering and terrorist financing, and it is this that marks it out as an interesting case study in relation to NTPMs. Further, the US has the most illicit funds pass through its system each year, it is undeniable that as their general AML and CTF framework became stronger, criminals have sought and used more covert payment methods to avoid detection.

It has been highlighted that whilst NTPMs are not as much of a threat to US as traditional forms of money laundering and terrorist financing, their threat is not insignificant either. The US has a plethora of competent authorities, which has led academics to criticise that there is too much overlap in the US systems. The US competent authorities output in relation to NTPMs is not as transparent as that of the UK and Australia, which is not to say that they are

[266] Department of State, '2014 INCSR: Treaties, Agreements, and Asset Sharing' <http://www.state.gov/j/inl/rls/nrcrpt/2014/vol2/222469.htm> accessed 22 September 2016.

[267] Ibid.

not doing anything in relation to NTPMs, just that they are not broadcasting it in the same way. However they do have a number of bodies concerning themselves with it. In saying that, there are a number of items published by the US that are either directly related to NTPMs or refer to them. The Office of Terrorism and Financial Intelligence produced National Risk Assessments in 2015 on both money laundering and terrorist financing. The Treasury have also produced a guidance paper on Hawala, highlighting how it can affect the US. These both highlight the threats to the US of NTPMs, in particular they make reference to the risks of stored value cards, wire transfers and digital currencies. FinCEN given its role as the US FIU and its regulatory powers has direct interaction with NTPMs owing to provisions of the Bank Secrecy Act and the PATRIOT Act. Given their role is to protect the financial system, from emerging money laundering and terrorist financing threats and the fact that NTPMs tend to need banking facilities, it is useful that FinCEN have the dual role (as FIU and regulator) that enables them to be directly involved in relation to NTPMs. An excellent initiative by the Department of State, through its Terrorist Financing Working Group was the setting up of the New Payment Methods Ad Hoc Working Group which concerns itself with digital currencies such as bitcoin as well as other new emerging NTPMs, this allows the Department of State to have a good stream of knowledge in relation to emerging money laundering and terrorist financing threats. Finally, the US law enforcement agencies have also been involved in investigations relating to NTPMs, this allows them to develop their knowledge of the area.

In relation to the criminalisation of money laundering and terrorist financing, the US approach is comprehensive, as would be expected of it given its reputation. The US has implemented the measures found in the Vienna, Palermo and Terrorism Financing Convention. The use of NTPMs does not make an impact on criminalisation as the offences are construed broadly to be committed through any payment method. Turning to the preventive measures, whilst the

FATF Mutual Evaluation Assessment of the US is useful in terms of understand the level they are operating at, it should be noted that it was completed in 2006 under a different assessment framework and as such the compliance ratings are not so useful anymore. The US was the first country to implement some of the key preventive measures that are now synonymous with AML and CTF. The main preventive measures are located in the Bank Secrecy Act 1970 and the US PATRIOT Act. It is imperative given the amount of money laundered through the US annually, its location in the world, and its reputation that it has strong preventive measures. Indeed, at the last FATF evaluation of the country they were assessed highly in this regard. NTPMs are covered owing to the definition of 'financial institution' employed by the Bank Secrecy Act which includes 'financial institution' and 'currency exchanges', as well as 'licensed sender's of money or any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions.' This also has enough scope to cover virtual currency exchanges. In relation to customer due diligence, the US provides for both enhanced and simplified measures, dependant on the risk-based approach this permits NTPMs, and banks providing financial facilities to NTPMs to tailor their compliance measures. The US operates a suspicious activity report regime, this suffers the same sort of problems that all systems across the world face in relation to defensive reporting and compliance costs. These undoubtedly can and will have a knock on effect to NTPM providers in the fact that reports about the abuse of NTPMs may go unnoticed due to the US strategy of devoting analytical resources to those SARs that are considered most valuable to law enforcement. The US has also implemented measures specific to NTPMs. With regards to wire transfers (or 'electronic transfers') they have for a long time required a plethora of information surrounding the

transaction. However, they have also, rightly been criticised for the lack the implementation of a $3,000 threshold for this. This potentially leaves a whole host of transactions without an adequate paper trail and leaves a gap that criminals may seek to exploit. In relation to money or value transfer services, the US earmarks them all as money service businesses, which mean that they are reporting entities for the purposes of AML and CTF. They are also required to register with FinCEN, this helps to keep a record of all providers and weed out illegitimate providers. Failure to register results in a penalty. The final specific measure relating to NTPMs is in relation to new technologies. The US has measures in place to ensure that providers consider the risks or new technologies and services. The main weakness identified was that the US failed to measures in relation to money service businesses, and simply focussed on new technologies and services in the banking sector, something that they have now addressed. The US should be praised overall for its preventive measures, they have adopted a strong approach however an area of concern is with regards to the reporting regime, although they are not alone in this area.

Confiscation of the proceeds of crime is a crucial bite point of the US AML and CTF regime. There are three main methods of confiscation: criminal forfeiture, civil forfeiture, and administrative forfeiture. The US has performed well in this area in relation to compliance with international standards, which has led many academics to note that the US utilise forfeiture as a powerful enforcement tool. Although a number of academics have criticised the existence of a civil regime due to the low burden of proof. The US, through the FBI Investigation in relation to the Silk Road, were the first country to deal with the confiscation of bitcoins. Their approach to auction off the bitcoins has been adopted by Australia, in order to recover the proceeds of crime. This is a good approach to take and ensures that the State will not be out of pocket for the AML or CTF investigation that took place leading up to the

confiscation. Most other NTPM will be picked up by the confiscation regime in the traditional manner as they utilise fiat currency, which law enforcement agencies are well used to dealing with. The difficulty is whether the funds are ever detected to be confiscated.

The importance of mutual legal assistance in relation to NTPMs should not be underestimated, the US through the Department of Treasury Office of Intelligence and Analysis is noted as having a strong and robust procedure for assistance. The US has placed a firm emphasis on encouraging mutual legal assistance which must be commended, in particular through its policy of sharing any assets in recovers in conjunction with countries who assisted in the investigation. It has been noted that the US aggressively pursue international cooperation and that approach cannot be faulted as the globalised threat from NTPMs cannot be countered with a localised approach.

So then, whilst it is clear that traditional methods pose by far and away the biggest threat to the US in terms of monetary value it cannot be argued that NTPMs do not pose a significant risk. The US's approach of overlooking a wire transfer SAR due to its low value was a poor choice, that transfer was linked to 9/11. Overall, the US legal framework is strong and robust, and they rightly should be regarded as a leader in terms of AML and CTF.

Chapter 5 – Australia

Australia's implementation of the international AML and CTF framework to tackle abuse of NTPMs

> "Our greatest challenge is to ensure we maintain the edge to detect and monitor money laundering and terrorism financing threats. Criminals use diverse methods to launder money or other ill-gotten property or to support acts of terrorism. These methods evolve to sidestep regulatory and law enforcement measures and exploit market and technology developments, including harnessing new products or technologies such as e-commerce."[1]

5.1. Introduction

The fifth chapter of this thesis investigates and scrutinises how Australia, in implementing the international anti-money laundering and counter-terrorist financing framework (identified in chapter 2), has sought to address the increasing risks associated with the criminal abuse of non-traditional payment methods.

[1] AUSTRAC, Intelligence Strategy 2012-14. Available at: <http://www.austrac.gov.au/intelligence-strategy-2012-14> accessed 01/09/2016.

Whilst like the US and UK, Australia has a longstanding history of implementing measures to counter money laundering and terrorist financing, the primary driver for selecting Australia as a case study is the fact that it underwent, relatively recently, a complete overhaul of its anti-money laundering and counter-terrorist financing framework. Australia has a strong regime to fight money laundering and terrorist financing.[2] The framework, similarly to the UK and US, incorporates the legislative measures of the United Nations (UN), as well as following the Recommendations of the Financial Action Task Force (FATF). As such, in order to meet these objectives, it is crucial that they address all methods of transferring funds, including the use of non-traditional payment methods.

In the FATF 2015 Mutual Evaluation of Australia it found that 'Australia legal framework to combat terrorist financing is comprehensive'[3] however for money laundering it found that 'Australia focusses on what it considers to be the main three proceeds generating predicate threats (drugs, fraud and tax evasion)… it needs to expand its focus to ensure a greater number of cases of money laundering are being identified and investigated adequately.'[4] Unlike the UK and the US, because Australia received its fourth round of Mutual Evaluation by the FATF in 2015, it is possible to view the above comments of FATF in light of criminal use of the non-traditional payment methods identified in chapter 2 of this thesis. Australia's 2015

[2] Australian Government, Attorney General's Department, 'Anti-Money Laundering and Counter Terrorism Financing' <https://www.ag.gov.au/CrimeAndCorruption/AntiLaunderingCounterTerrorismFinancing/Pages/default.aspx> accessed 22 September 2016.

[3] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (April 2015), 6. Available at <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 22 September 2016.

[4] Ibid, 5.

report states that Australia is 'largely compliant' with Recommendation 15 (on New Technologies) and has demonstrated 'it has assessed the money laundering and terrorist financing risks associated with some new products and technologies.'[5] It also notes that AUSTRAC (introduced below) has conducted research and issued a policy on virtual currencies such as Bitcoin.[6] Whilst this is not perfect, like the UK and US there can be no doubt that its compliance with its international obligations can only stand it in good stead to deal with newly emerging NTPMs. Indeed, it is stated 'Australia has a strong institutional framework for combatting money laundering and terrorist financing.'[7]

'Money laundering threatens Australia's prosperity, undermines the integrity of our financial system and funds further criminal activity which impacts on community safety and wellbeing… [it is] a critical risk to Australia.'[8] As noted in chapters 3 and 4, in relation to the UK and US, calculating the amounts of money laundered through Australia each year is challenging. Again, a number of bodies have attempted to quantify the extent of the problem in Australia, and as with the other case study countries the numbers vary significantly. An Australian government estimate of the amount of money laundered estimated that the amount of money laundered through the country is between $2-3 billion per year.[9] The Australian Crime Commission has given a wider range of figures stating it is somewhere

[5] Ibid, 16-17.

[6] Ibid, 161.

[7] Ibid 7.

[8] AUSTRAC, Money laundering in Australia 2011 (2011), 2. Available at: <http://www.austrac.gov.au/files/money_laundering_in_australia_2011.pdf> accessed 22 September 2016.

[9] Financial Action Task Force, Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism' (14 October 2005), 15. Available at <https://www.imf.org/external/pubs/ft/scr/2006/cr06424.pdf> accessed 23/06/2016.

between $2.8bn and $6.3bn.[10] Whilst Sathye believes the figure to be significantly larger at $11.5bn per year.[11] Meanwhile as AUSTRAC report on money laundering, praised for its detailed effort, has concluded that it is actually between AUS $1.0 billion and A$ 4.5 billion, further stating that with some confidence it is around A$3.5 billion.[12] As with the statistics from the US and UK we know that these are not in contemplation of the money laundered via NTPMs like digital currencies and mobile payments. The important part is that significant sums are laundered through Australia each year, and that because of the risks associated with NTPMs they need to be regulated for the purposes of money laundering and terrorist financing. In terms of terrorism, Australia is not at the same threat level as the UK or US, with its threat level described as 'probable'[13], meaning it is perhaps less likely that terrorist funds would be channelled through the country, though no less important that it is countered.

Similarly to the UK and US, the most common way for criminals to move funds in Australia is through the formal financial sector. Indeed, Australia's financial sector is the 12th largest globally and is dominated by banks with total sector assets amounting to over 200% of GDP (over AUD 321.1 billion).[14] From ATM withdrawals, as well as debit card and credit card

[10] Australian Crime Commission, Organised crime in Australia 2009, Canberra: Australian crime Commission, 2010, p.9.

[11] M. Sathye, 'Estimating the cost of compliance of AMLCFT for financial institutions in Australia', Journal of Financial Crime, 2008, 15(4), 347-63, at 350

[12] John Walker Consulting Services, 'Estimates of the Extent of Money Laundering in and through Australia, AUSTRAC, (September 1995) <http://www.criminologyresearchcouncil.gov.au/reports/200304-33.pdf> accessed 22 September 2016.

[13] Australian National Security, 'National Terrorism Threat Advisory System', <https://www.nationalsecurity.gov.au/Securityandyourcommunity/Pages/National-Terrorism-Threat-Advisory-System.aspx> accessed 22 September 2016.

[14] Financial Action Task Force, Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism' (n.9), 15.

transactions we know that there are around 589.8 million transactions per month in Australia.[15] All of this would indicate that like the UK and US, Australia's formal financial sector provides vast cover for criminals seeking to make illicit transactions. As with the UK and US, there are clear signs that NTPMs are used to launder funds, the FATF noting that remittance businesses are one of the most common.[16] Whilst AUSTRAC (introduced below) also noted that electronic payments and emerging NTPMs present high money laundering risks.[17] It is therefore important that Australia's AML and CTF framework focusses on both traditional methods as well as NTPMs as a means of moving illicit funds. The next part of this chapter will assess the UK's implementation of the international AML and CTF framework, and in particular the parts of relevance to NTPMs.

5.2. Global Role and Implementation of the International AML/CTF Framework

This section will outline both the role that Australia plays in the international framework, as well as highlighting the international AML and CTF measures that it has implemented.

The UN was introduced in Chapter 2[18], Australia like the UK and US, has a long connection with the UN; it was one of 51 states to sign the UN Charter in 1945, with it becoming a

[15] Australian Payments Clearing Association, 'Payment Statistics – Transaction Statistics – Cards' available at <http://www.apca.com.au/payment-statistics/transaction-statistics/cards> accessed 22 September 2016.

[16] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 50.

[17] Australian Transaction Reports and Analysis Centre, 'Money Laundering in Australia 2011', (2011), 10. Available at: <http://www.austrac.gov.au/sites/default/files/documents/money_laundering_in_australia_2011.pdf> accessed 22 September 2016.

[18] See section 2.3.1.1. for an explanation of the role of the UN in the international AML & CTF Framework.

founding member.[19] Australia is 'firmly committed to effective global cooperation, including through the UN and its specialised agencies and regional commissions.'[20] Australia is currently the 12th largest contributor to the UN's regular budget.[21] Australia is represented at the UN by the Government Department of Foreign Affairs and Trade. In terms of AML and CTF, it has ratified the following UN Conventions:

- Vienna Convention (signed 1992);
- Palermo Convention (signed December 2000 and ratified in 2004);
- International Convention for the Suppression of the Financing of Terrorism (ratified in 2002).

Alongside the above Conventions the provisions of S/RES/1267(1999) and S/RES/1373(2001) are also in effect in the Australia owing to its membership of the UN. Australia's close links to international efforts is highlighted by the fact that it took the first Presidency of the Security Council in 1946.[22]

Of course implementation of the legislative instruments only tells one side of the Australia's role in the international framework, there are also international standards and best practices to be considered.

[19] United Nations Association – UK, 'What is the United Nations' <http://www.una.org.uk/content/what-un> accessed 22 September 2016.

[20] Australian Government, Department of Foreign Affairs and Trade, 'United Nations (UN)' <http://dfat.gov.au/international-relations/international-organisations/un/pages/united-nations-un.aspx> accessed 22 September 2016.

[21] Ibid.

[22] Ibid.

The most important set of standards come from the FATF. Australia, like the UK and US, is a founding member of the FATF and has chaired the organisation twice: once in 1992[23], and again in 2014[24]. The Attorney General's Department acts as Australia's lead delegation to the FATF.[25] As well as deriving significant benefit from its membership of the FATF, Australia plays a key role on an international level, 'consistently providing input in relation to the policy direction of the international community to combat money laundering and the financing of terrorism and proliferation.'[26] It has further been noted that Australia plays an important role in reviewing and supporting regional implementation of the FATF Recommendations.[27]

Further to its commitments to the FATF, it also has roles in relation to FATF-Style Regional Bodies (FSRBs). In comparison to the UK and US, Australia is a member of far fewer FSRB's, although arguably its role in the APG is of more importance that the UK and US's membership

[23] Financial Action Task Force on Money Laundering, *Annual Report: 1992-1993* (29 June 1993) <http://www.fatf-gafi.org/media/fatf/documents/reports/1992%201993%20ENG.pdf> accessed 22 September 2016.

[24] Financial Action Task Force, 'Objectives for FATF XXVI (2012-2015): Paper by the Incoming President' <http://www.fatf-gafi.org/media/fatf/documents/Objectives%20for%20FATF%20XXVI%202014%202015.pdf> accessed 22 September 2016.

[25] Financial Action Task Force, 'Australia' <http://www.fatf-gafi.org/countries/#Australia> accessed 22 September 2016.

[26] Australian Transaction Reports and Analysis Centre, Parliamentary Joint Committee on Law Enforcement: Inquiry into Financial Related Crime, Australian Transaction Reports and Analysis Centre Submission (May 2014), 38. Available at: <http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Financial_related_crime/~/media/Committees/le_ctte/Financial_related_crime/report.pdf> accessed 22 September 2016.

[27] Ibid, 38.

of similar regional groups. As its founding member[28], Australia has played a prominent role in the APG since its inception – a reflection of the importance that Australia places on the regional response to global AML/CTF efforts and implementation of the FATF Recommendations.[29] They host the APG secretary in Sydney and is a permanent co-chair, highlighting its importance to the regional effort. Through AUSTRAC they also support international initiatives by providing technical assistance and training to FIUs in Africa, Asia and the Pacific.[30]

Australia has experienced a mixed history in terms of its compliance with the FATF Recommendations, in its 2005 Third Mutual Evaluation Report[31], it performed poorly and was criticised by the FATF for a number of AML and CTF deficiencies. However, in its 2015 Fourth Mutual Evaluation Report[32] it performed significantly better. Australia was assessed as being fully compliant with 12 of the 40 Recommendation, largely compliant with 12, partially compliant with 10, and non-compliant with 6. Given that these stats are based on a new evaluation period with different criteria conclusions are difficult to draw in comparison to the UK and US, and using the third Evaluation Report is not useful given the significant change in Australia's framework since its completion. Australia has compliant with a large number of

[28] Australian Transaction Reports and Analysis Centre, 'International Organisations' <http://www.austrac.gov.au/about-us/international-engagement/international-organisations> accessed 22 September 2016.

[29] Australian Transaction Reports and Analysis Centre, Parliamentary Joint Committee on Law Enforcement: Inquiry into Financial Related Crime, Australian Transaction Reports and Analysis Centre Submission (n.26), 39.

[30] Ibid 37.

[31] Financial Action Task Force, Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism' (n.9), 14.

[32] Ibid.

recommendations, however that it is still non-compliant with 6 Recommendations stands out. In relation to the NTPM Recommendations, Australia does reasonably well. It is largely compliant with Recommendation 14 on 'money or value transfer services', largely compliant with Recommendation 15 on 'new technologies', and partially compliant with Recommendation 16 on 'wire transfers'.[33] So it is clear that Australia has improved its overall compliance with the FATF Recommendations, however it is also apparent that there is still room for improvement. In relation to NTPMs, Australia has done well in relation to the areas where the FATF has specific standards. Overall, the FATF has stated that Australia has a strong institutional framework for combatting money laundering, terrorist financing and proliferation financing.[34]

Alongside the above, and as with the UK and US, Australia is also a member of various other international organisations. AUSTRAC, Australia's FIU, is a founding member and lead Commonwealth agency to the Egmont Group of Financial Intelligence Units.[35] Australia is also a member of the Basel Committee on Banking Supervision.

5.3. Competent Authorities

Australia has designated a number of competent authorities to the fight against money laundering and terrorist financing. It has more similarities with the UK than the US, in terms of the number of authorities in the area.

---

[33] Ibid.

[34] Ibid.

[35] Australian Transaction Reports and Analysis Centre, 'About Us' < <http://www.austrac.gov.au/about-us/international-engagement/international-organisations> accessed 22 September 2016.

5.3.1. Primary Authorities

5.3.1.1. Attorney General's Department (AGD)

The aim of the Attorney General's Department (AGD) is to deliver 'programs and policies to maintain and improve Australia's law and justice framework, and strengthen its national security and emergency management.'[36] The AGD has primary responsibility for supporting the Australian Government in protecting and promoting the rule of law, as part of that they have policy responsibility for AML and CTF. This is a different approach to that adopted in the UK and US where HM Treasury and the Department of Treasury manage money laundering and terrorist financing policies. On policy matters, the AGD chairs the AML IDC, which meets three times per year to share information and inform the strategic direction and priority setting of federal agencies working on domestic AML/CTF initiatives.[37] The AGD is also the central authority for extradition and mutual legal assistance in criminal matters. Further, the Australian Transaction and Analysis Centre (AUSTRAC) comes under its portfolio.

The AGD provides international legal assistance through its Anti-Money Laundering Assistance Team (AMLAT). In particular AMLAT partners with countries in the Asia-Pacific Region to strengthen laws and processes on AML and CTF, in line with international standards.[38]

---

[36] Ibid.

[37] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 50.

[38] Attorney-General's Department, 'Anti-Money Laundering Assistance' <https://www.ag.gov.au/Internationalrelations/InternationalLegalAssistance/Pages/AntimoneyLaunderingAssistance.aspx> accessed 22 September 2016.

The AGD in its National Organised Crime Response Plan[39] highlights the use of NTPMs by criminals as a key issue to be tackled. Whilst further, the AGD acted as Chair of the Working Group on Remittance Account Closures, underlining its commitment to understanding and investigating NTPMs. One of the focuses of the Working Group being to prevent across-the-board de-risking[40] of alternative remittance providers by banks as a result of their AML and CTF obligations.

5.3.1.2. The Department of Foreign Affairs and Trade (DFAT)

The Department of Foreign Affairs and Trade (DFAT) has primary responsibility for compliance with sanction requirements. In terms of AML and CTF it performs a similar role as the US Department of State and the UK Foreign and Commonwealth Office. To that end, DFAT also maintains Australia's Consolidated List of persons and entities who are subject to targeted financial sanctions or travel bans.[41] The Consolidated List is available on the DFAT website[42], importantly from the perspective of this thesis it contains all those listed in the UN Security Council Resolution (UNSCR) 1267. Where there are changes to UNSCR 1267 then DFAT

[39] Attorney-General Department, *National Organised Crime Response Plan 2015-18* (2015). Available at: <https://www.ag.gov.au/CrimeAndCorruption/OrganisedCrime/Documents/NationalOrganisedCrimeResponsePlan2015-18.pdf> accessed 22 September 2016.

[40] De-risking is the process whereby a bank chooses not to keep an account for its customer on the basis that it perceives it to be of risk. De-risking causes a problem where banks decide to de-risk whole groups of customers across-the-board without considering their individual risk.

[41] Department of Foreign Affairs and Trade, 'Consolidated List' <http://dfat.gov.au/international-relations/security/sanctions/Pages/consolidated-list.aspx> accessed 22 September 2016.

[42] Department of Foreign Affairs and Trade, 'Regulation 8 Consolidated' <http://dfat.gov.au/international-relations/security/sanctions/Documents/regulation8_consolidated.xls> accessed 22 September 2016.

updates the Consolidated List the next day.[43] DFAT also maintain a mailing list for people interested in receiving updates on Australian sanction laws, including updates on the Consolidated List.[44] The Consolidated List also contains individuals and groups contained in UNSCR 1373.[45] The FATF criticised DFAT in its 2015 Fourth Mutual Evaluation Report, stating that DFAT does not adequately monitor or supervise the financial sector for compliance with the FATF Recommendations in the way they would expect of a supervisory authority.[46]

5.3.2. Secondary Authorities

5.3.2.1. Australian Transaction Reports and Analysis Centre (AUSTRAC)

The Australian Transaction Reports and Analysis Centre (AUSTRAC), is Australia's financial intelligence agency with regulatory responsibility for AML and CTF.[47] It was created by the Financial Transaction Reports Act 1988.[48] It is an independent agency which operates within the portfolio of the AGD.[49] Its vision is an Australia that is hostile to money laundering, financing of terrorism and serious and organised crime'.[50] It believes that it achieved this vision through industry regulation and the collection, analysis and dissemination of financial

[43] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 74.

[44] Department of Foreign Affairs and Trade, 'Consolidated List' (n.41).

[45] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 74.

[46] Ibid, 9.

[47] Australian Transaction Reports and Analysis Centre, 'About' <http://www.austrac.gov.au/about-us/austrac> accessed 22 September 2016.

[48] Financial Transaction Reports Act 1989, s.35.

[49] M. Sathye and C. Patel, 'Developing financial intelligence: an assessment of the FIUs in Australia and India', Journal of Money Laundering Control, 2007, 10(4), 391–405, at 396.

[50] Australian Transaction Reports and Analysis Centre, *AUSTRAC Annual Report 2014-2015* (2015), 6. Available at: <http://www.austrac.gov.au/sites/default/files/austrac-ar-14-15-web.pdf> accessed 22 September 2016.

intelligence.[51] AUSTRAC has two key roles; first, it; it acts as Australia's financial intelligence unit (FIU); and second, as Australia's AML and CTF regulator. AUSTRAC moved from being an intelligence focussed unit, to having a general regulatory ambit under the AML/CTF Act 2006. Intelligence is now only one of a range of functions it covers, alongside regulatory direction, compliance monitoring and enforcement, and education.[52]

AUSTRAC has been described as a 'well-functioning financial intelligence unit (FIU).'[53] It is Australia's primary source for financial intelligence used to fight serious and organised crime and terrorism financing.[54] FATF has praised the role of AUSTRAC in the Australia's AML and CTF framework, noting that 'the amount of financial transaction data it holds in its database, and the fact that all relevant competent authorities have access to this database and can use its integrated analytical tool, are strengths of Australia's AML/CTF system.'[55] A key role which AUSTRAC fulfils is the development of the AML/CTF Rules which provide guidance to businesses in relation to practical application of AML and CTF measures.

The AML/CTF Act significantly increased AUSTRAC's compliance monitoring role. In collecting its data, AUSTRAC oversees the compliance of more than 14,000 Australian businesses ranging from major banks and casinos to single-operator businesses.[56] AUSTRAC also cover

[51] Ibid.

[52] Stuart Ross and Michelle Hannan, 'Australia's New Anti-Money Laundering Strategy' (2007) 19(2) *Current Issues in Criminal Justice* 135, 145.

[53] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 8.

[54] Australian Transaction Reports and Analysis Centre, 'About' (n.47).

[55] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 5.

[56] Australian Transaction Reports and Analysis Centre, 'About' (n.47).

remittance service providers[57] whilst it has been noted that virtual currency exchanges should also fall under their ambit.[58]

In terms of disseminating information and gaining intelligence on CTF, AUSTRAC hosted the inaugural Counter-Terrorist Financing Summit in 2015, and co-hosted the second Summit with Pusat Pelaporan Dan Analisis Transaksi Keuangan (PPATK).[59] The aim of these CTF Summits is to develop regional solutions to terrorism financing issues and risks. Following the 2016 Summit, a Regional Risk Assessment was produced.[60] AUSTRAC's prominence in this initiative is symptomatic of the active role it plays in relation to countering financial crime globally, regionally, and nationally. AUSTRAC's regional work is funded by DFAT.[61]

[57] Ibid.

[58] For more see: Australian Transaction Reports and Analysis Centre and Attorney-General's Department, Review of the AML/CTF Regime (December 2013). Available at: <https://www.ag.gov.au/Consultations/Documents/issues-paper-review-aml-ctf-regime-20131202.doc> accessed 22 September 2016.

[59] Australian Transaction Reports and Analysis Centre, 'Counter-Terrorism Financing Summit 2016' <http://www.austrac.gov.au/about-us/international-engagement/counter-terrorism-financing-summit-2016> accessed 22 September 2016.

[60] Australian Transaction Reports and Analysis Centre, *Terrorism Financing South-East Asia & Australia, Regional Risk Assessment 2016* (2016). Available at: <http://www.austrac.gov.au/sites/default/files/regional-risk-assessment-SMALL_0.pdf> accessed 22 September 2016.

[61] Australian Transaction Reports and Analysis Centre, 'International Assistance and Training' <http://www.austrac.gov.au/about-us/international-engagement/international-assistance-and-training> accessed 22 September 2016.

AUSTRAC also produces annual typology reports.[62] Both the 2013[63] and 2014[64] Reports focusses on variety of typologies including NTPM's such as digital currencies and remittance providers. These reports also highlight the fact that AUSTRAC is committed to collecting intelligence on the use of NTPMs by launderers and terrorist financers.

Alongside the above, AUSTRAC has produced two key documents which provide an oversight of current money laundering and terrorist financing activity, vulnerabilities and threats: Terrorist Financing in Australia 2014[65] and Money Laundering in Australia 2011[66].

5.3.2.2. Australian Criminal Intelligence Commission (ACIC)

The Australian Criminal Intelligence Commission (ACIC), formerly known as the Australian Crime Commission, was formed to strengthen the ability to respond to crime that affects Australia.[67] Under the Australian Crime Commission Amendment (National Policing Information) Act 2016 the Australian Crime Commission and CrimTrac were brought together

---

[62] Available from: Australian Transaction Reports and Analysis Centre, 'AUSTRAC typologies and case studies reports' <http://www.austrac.gov.au/publications/corporate-publications-and-reports/typologies-and-case-studies-report> accessed 22 September 2016.

[63] Australian Transaction Reports and Analysis Centre, *AUSTRAC Typologies and Case Studies Report 2013* (2013). Available at: <http://www.austrac.gov.au/sites/default/files/documents/typ13_full.pdf> accessed 22 September 2016.

[64] Australian Transaction Reports and Analysis Centre, *AUSTRAC Typologies and Case Studies Report 2014* (2014). Available at: <http://www.austrac.gov.au/sites/default/files/typologies-report-2014.pdf> accessed 22 September 2016.

[65] Australian Transaction Reports and Analysis Centre, *Terrorism Financing in Australia 2014* (2014). Available at: <http://www.austrac.gov.au/sites/default/files/documents/terrorism-financing-in-australia-2014.pdf> accessed 22 September 2016.

[66] [66] Australian Transaction Reports and Analysis Centre, *Money laundering in Australia 2011* (2011). Available at: http://www.austrac.gov.au/sites/default/files/documents/money_laundering_in_australia_2011.pdf

[67] Australian Criminal Intelligence Commission, 'About us' <https://www.acic.gov.au/about-us> accessed 22 September 2016.

under a single heading, to form ACIC. ACIC is an entity of the AGD's portfolio. Their aim is to 'make Australia safer through improved national ability to discover, understand and respond to current and emerging crime threats and criminal justice issues.'[68] It does so through working collaboratively with all other Commonwealth, State and Territory law enforcement and regulatory agencies to enhance their intelligence and enforcement capabilities in relation to significant organised crime, in particular large scale money laundering.[69]

ACIC is Australia's national criminal intelligence agency, it has a focus on understanding and combatting serious and organised crime of national significance.[70] The ACC also maintains a national criminal intelligence database and provides strategic advice to its Board in the form of national criminal threat assessments and national law enforcement priorities.[71] The Organised Crime Threat Assessment, which is produced every two years by ACIC, supplements the two AUSTRAC reports on national money laundering and terrorist financing risks, mentioned above. The most recent version, released in 2015, was titled Organised Crime in Australia[72].

Alongside the above, ACIC has since 1999 hosted the Proceeds of Crime Case Studies Desk. Its aim is to share information between Australian law enforcement agencies on money

[68] Ibid.

[69] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 22.

[70] Ibid, 36.

[71] Ibid, 22.

[72] Australian Crime Commission, Organised Crime in Australia 2015 (2015). Available at: <https://www.acic.gov.au/sites/g/files/net1491/f/2016/06/oca2015.pdf?v=1467241691> accessed 22 September 2016.

laundering and tax evasion methodologies and investigative techniques.[73] This body will likely pick up emerging trends and disseminate knowledge and best practice in terms of investigation, in relation to them.

Also of relevance is the ACIC led National Criminal Intelligence Fusion Capability (NCIFC). NCFIC was established in July 2010 and is seen as a key asset of ACIC.[74] NCIFC comprises of subject matter experts, investigators and analysts, data and tools from across a range of government agencies at the national, state and territory levels to:

- Enhance understanding of the national picture of organised crime; and
- Discover previously unknown organised criminal activity and entities.[75]

It is clear then the NCIFC allows Australia's law enforcement agencies, in particular ACIC, to respond to newly emerging threats before they get embedded. NCIFC will have a key role to play in tackling newly emerging NTPMs. NCIFC provides insights from existing intelligence, narrowing gaps in collective intelligence holding and discovering previously unknown criminal threats.[76]

[73] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 22.

[74] Australian Criminal Intelligence Commission, 'National Criminal Intelligence Fusion Capability' <https://www.acic.gov.au/about-crime/taskforces/national-criminal-intelligence-fusion-capability> accessed 22 September 2016.

[75] Ibid.

[76] Ibid.

5.3.3. Tertiary Authorities

5.3.3.1. Australian Federal Police (AFP)

At a Federal level, the majority of money laundering investigations are conducted by the Australian Federal Police (AFP). The AFP is the principal law enforcement agency through which the Commonwealth pursues its law enforcement interests. AFP's areas of operation emphasis include:

- Investigating complex, transnational, serious and organised crime;
- Protecting Australian and Australian interests from terrorism and violent extremism;
- Principal international representative for Australian police and law enforcement;
- Develop unique capabilities and exploit advanced technology to provide utmost value to Australia's national interest.[77]

A Counter Terrorism Division was established in April 2003 to undertake intelligence-led investigations to prevent and disrupt terrorist acts, there are now Joint Counter Terrorism Teams comprising AFP members and State and Territory police.[78]

5.3.3.2. Australian Intelligence Community (AIC) Agencies

The Australian Intelligence Community (AIC), is an informal term used to describe the six Australian security and intelligence agencies: The Office of National Assessments, The Australian Security Intelligence Organisation, The Australian Secret Service, The Australian

[77] Australian Federal Police, 'About us' <https://www.afp.gov.au/about-us/our-organisation> accessed 22 September 2016.

[78] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 22.

Signals Directorate, The Defence Intelligence Organisation, and The Australian Geospatial-Intelligence Organisation.[79]

5.3.3.3. Australian Bankers' Association

The Australian Bankers' Association is one of the main tertiary authorities in Australia, like its counterparts in the UK and US it is concerned with the implementation of preventative AML measures.[80] The Australian Bankers' Association has an Anti-Money Laundering Technical Working Group which holds informal meetings and conferences surrounding emerging threats and areas of AML interest.

5.3.3.4. ELIGO National Task Force

The ELIGO National Task Force, was established to address criminal vulnerabilities and the potential for exploitation by serious and organised crime within the alternative remittance sector.[81] The Task Force is endorsed by ACIC and comprises ACIC, AUSTRAC, the Australian Federal Police, State and Territory law enforcement and key Commonwealth agencies. The Task Force was set up in response to the threat of alternative remittance being used for organised crime, as more than AUS$ 30 billion is moved into and out of Australia through this sector.[82]

---

[79] Inspector-General of Intelligence and Security, 'The Australian Intelligence Community' <https://www.igis.gov.au/australian-intelligence-community> accessed 22 September 2016.

[80] N. Ryder, *Financial Crime in the 21st Century* (Edward Elgar, 2011; Cheltenham, UK), 113.

[81] Australian Transaction Reports and Analysis Centre, 'Task Force Eligo' <http://www.austrac.gov.au/sites/default/files/documents/eligo_fact_sheet.pdf> accessed 22 September 2016.

[82] Ibid.

5.4. Application of a Risk-Based Approach to AML and CTF

The Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Act 2006 introduced the change from a compliance to a risk-based approach.[83] Ross and Hannan have noted that this is 'part of a wider move away from prescriptive, compliance-based approaches.'[84] The Australian Government is of the view that businesses have the best knowledge of money laundering and terrorist financing risks, and as such should be given freedom in how to identify, mitigate and manage the risk.[85] For this reason, under the AML/CTF Act, businesses are required to adopt the RBA by performing a risk-assessment that determine whether the 'designated services' they provide could assist in the transfer of illicit funds.[86] The RBA requires reporting entities to 'have programmes that identify mitigate and manage money laundering.'[87] If AUSTRAC does not believe that a sufficient effort has been made to 'identify, mitigate and manage risk' then it can require under s.165 of the AML/CTF Act that a risk assessment be carried out, or under s.161 of the AML/CTF Act can require that an external auditor be appointed to carry out a risk assessment. The aim of the RBA is to direct resources and effort towards customers and transactions with a higher potential for money laundering.[88]

---

[83] Stuart Ross and Michelle Hannan, 'Australia's New Anti-Money Laundering Strategy' (n.52), 142.

[84] Ibid.

[85] Milind Sathye and Jesmin Islam, 'Adopting a Risk-Based Approach to AMLCTF Compliance: The Australian Case (2011) 18(2) Journal of Financial Crime 169, 170.

[86] See, Law Council of Australia, Anti-Money Laundering Guide for Legal Practitioners, Canberra: Law Council of Australia, 2009, p. 17.

[87] Stuart Ross and Michelle Hannan, 'Australia's New Anti-Money Laundering Strategy' (n.52), 146.

[88] Attorney-General's Department (2004) Anti-Money Laundering Law Reform: Issues Paper 1, Financial Services Sector Canberra, Attorney General's Department.

It should be noted at this stage that AUSTRAC has the power to grant exemptions to specified persons from all or parts of the AML/CTF Act, it does so rarely, but has done so in the case of various applicants operating in the prepaid cards sector.[89] AUSTRAC only takes such a course of action on a case-by-case basis. However, the FATF were critical stating that they were 'not convinced that the exemptions were sufficiently justified as low risk.'[90] The consensus would seem to be that exemptions from the AML/CTF Act obligations in relation to NTPMs is not desirable.

The AML/CTF Act 2006 is supplemented by the AML/CTF Rules Instrument 2007, issued by the AUSTRAC's CEO pursuant to section 229 of the AML/CTF Act.[91] The 2007 Rules set out the requirements on reporting entities' risk assessments, and include provisions on their adoption of a risk-based approach.[92] Under the 2007 Rules, a reporting entity can vary its own AML rules depending on the level of risk associated with a particular transactions.[93] It was noted by Geary that the Rules 'bring this risk-based approach to life by permitting regulated entities to put in place appropriate risk-based systems and controls for certain requirements in the AML/CTF Rules, taking into account the nature, size and complexity of their business.'[94]

[89] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 85.

[90] Ibid.

[91] Ibid, 84.

[92] Ibid.

[93] J. Geary, 'Light is the Best Antidote' (2009) 12(3) *Journal of Money Laundering Control* 215, 215.

[94] Ibid.

The RBA is not without its critics, it has been noted that such an approach causes 'considerable disadvantages' for 'small medium enterprises'.[95] It is clear then that there is a danger that the RBA unduly burdens NTPM providers, particularly where they are operating in a newly emerging field as they tend to be smaller businesses.

5.5. Criminalisation of Money Laundering and Terrorist Financing

5.5.1. Money Laundering

Australia has improved its compliance rating in relation to the criminalisation of money laundering from being 'largely compliant' in the FATF's Third Mutual Evaluation to being 'compliant' in the FATF's Fourth Mutual Evaluation.[96] Indeed, even in the third round of evaluations, FATF described Australia's approach towards criminalisation of money laundering as 'comprehensive'.[97] However, Ryder has noted that it must be questioned due to their apparent 'lacklustre attitude towards investigating allegations of money laundering.'[98]

Money Laundering is criminalised by Division 400 of the federal Criminal Code Act 1995, as amended by the Proceeds of Crime Act 2002. The Criminal Code Act implements Article

[95] J. Gurung, M. Wijaya and A. Rao, 'AMLCTF Compliance and SMEs in Australia: A Case Study of the Prepaid Card Industry' (2010) 13(3) *Journal of Money Laundering Control* 184, 185.

[96] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 131-132.

[97] Financial Action Task Force, Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism' (n.9), 5.

[98] Nicholas Ryder, *Money Laundering – An Endless Cycle?* (1st edn, Routledge, 2012), 116.

3(1)(b) of the Vienna Convention and Article 6(1) of the Palermo Convention.[99] A person is guilty of money laundering if they deal with money or property which 'is the proceeds of crime and believed by the person to be such, or is intended to become an instrument of crime', or 'is the proceeds of a crime, or there is a risk it will become an instrument of crime or the fact that there is a risk that it will become the instrument of crime', or 'is the proceeds of a crime, or there is a risk that it will become an instrument of crime, and the person is negligent to the fact that it is a proceeds of crime or the fact that there is a risk that it will become an instrument of crime.'[100] The FATF have outlined that Division 400.2 covers 'receipt, possession, concealment, disposal, import, export and engaging in banking transactions, which also covers transfer, conversion, disguising, and acquisition.'[101] Part 2.4 of the Criminal Code Act 1995 extends criminal responsibility to attempts, complicity, joint commission, commission by proxy, incitement and conspiracy. It is worthy of note at this stage that the Act states in Division 400.1 that 'a reference in this Division to money or other property includes a reference to financial instruments, cards and other objects that represent money or can be exchanged for money, whether or not they have intrinsic value.' Therefore, it is clear that NTPMs fall under the scope of the criminalised offence. The definition is cleverly phrased to cover the wide range of NTPMs. Per 400.2A, an individual will 'deal with money or property' if they do one of the following:

a) Receive, possess, conceal or dispose of money or other property;

---

[99] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 131.

[100] A. White, 'Australia', in W. Muller, C. Kalin and J. Goldsworth, *Anti-Money Laundering International Law and Practice* (1st edn, John Wiley & Sons, 2007), 749.

[101] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 131.

b) Import money or other property into Australia;

c) Export money or other property from Australia; or

d) Engage in a banking transaction relating to money or other property.[102]

There is no requirement under the Criminal Code Act 1995 for the prosecution to prove a particular offence, or that a particular person committed an offence in relation to the money or property, in order for them to be consider the proceeds of crime.[103] All they have to do is prove beyond a reasonable doubt that the proceeds are either the proceeds of a crime, or are intended to become, or are at risk of becoming, an instrument of crime.[104] So the Act sets the standard for being considered the proceed of crime relatively low in order to capture as many possible instances of money laundering as possible, it would not make sense to set a high standard for prosecutors to prove. It is worthy of note that case law in Australia has restricted the ability to charge for both the predicate offence and for self-laundering where the criminality of the money laundering offence is completely encompassed by the predicate offence.[105] Despite this, a significant difficulty with the Australian model is that there are 19 offences of money laundering, a marked difference from the UK and US which only have three.[106]

[102] Division 400.2A of the Criminal Code Act 1995.

[103] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 131.

[104] Ibid.

[105] As examples see: New South Wales Court of Criminal Appeal in Nahlous v R(2010) 201 ACrimR 150; Thorn v R (2010) 198 ACrimR 135; and Schembri v R (2010) 28 ATR 159.

[106] Nicholas Ryder, *Money Laundering – An Endless Cycle?* (n.98), 119.

5.5.2 Terrorist Financing

Australia has maintained its compliance rating in relation to the criminalisation of terrorist financing, it was rated as 'largely compliant' in both 2005[107] and 2015.[108] It has been noted that Australia's efforts to criminalise terrorist financing largely follow the International Convention for the Suppression of the Financing of Terrorism.[109] Indeed, this is stated in the Explanatory Memorandum to the Suppression of Financing of Terrorism Bill 2002.[110] The Suppression of the Financing of Terrorism Act 2002 amended the Criminal Code Act 1995 in relation to counter-terrorist financing. There are two prominent offences in Australia's counter-terrorist financing armour, financing terrorism per Division 103.1, and financing a terrorist per Division 103.2.

As per, Division 103.1 of the Criminal Code Act 1995, 'a person commits an offence' in relation to the financing of terrorism, if:

a) the person provides and collects funds; and
b) the person is reckless as to whether the funds will be used to facilitate or engage in a terrorist act.

It is notable that unlike the money laundering offence, for the offence of terrorist financing to have been committed the individual must satisfy all strands of the above offence. It should

[107] Financial Action Task Force, Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism' (n.9), 33.

[108] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 142.

[109] Ibid, 141.

[110] Explanatory Memorandum, Suppression of the Financing of Terrorism Bill 2002, 5.

also be noted that the mental requirement is set purposely low so as to capture as many cases of terrorist financing as possible.

In the 2005, Third Mutual Evaluation Report it was noted that Division 103.1 did not adequately cover the FATF standards relating CTF.[111] As a result Australia introduced Division 103.2 to address offences relating to the wilful provision or collection of funds, intending or knowing that they will be used by a terrorist. As per, Division 103.2 of the Criminal Code Act 1995, 'a person commits an offence' in relation to the financing of a terrorist, if:

(a) the person intentionally:

    (i) makes funds available to another person (whether directly or indirectly); or

    (ii) collects funds for, or on behalf of, another person (whether directly or indirectly); and

(b) the first-mentioned person is reckless as to whether the other person will use the funds to facilitate or engage in a terrorist act.

For both offences, the person commits the offence, even if (a) a terrorist act does not occur; (b) the funds will not be used to facilitate or engage in a specific terrorist act; or (c) the funds will be used to facilitate or engage in more than one terrorist act.[112] Both offence also carry a life sentence.

McGarrity has questioned the introduction of the Division 103.2 offence, stating that 103.1 would have covered it, and that aside from the political pressure to adopt the FATF's suggestions in their 3rd Mutual Evaluation of Australia, they should have just stuck with

[111] Financial Action Task Force, Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism' (n.9), 32-33.

[112] Criminal Code Act 1995, Division 103.1(2).

Division 103.1.[113] McGarrity further notes that the overlap between the two offences is significant.[114] The only significant difference between the two offences being that 103.2 requires the funds to have been collected on behalf of another person.

Australia has two further groups of offences which criminalise the provision of funds to particular individuals or organisations. The first, contained in Division 102.6 of the Criminal Code Act 1995, was introduced by the Security Legislation Amendment (Terrorism Act 2002) as a response to UNSCR 1373. The offences under 102.6 relate to the intentional receipt of funds from, or intentionally making of funds available to, a terrorist organisation (whether directly or indirectly). It also covers the intentional collection of funds for, or on behalf of a terrorist organisation (whether directly or indirectly).

The second group of offences are found in the UN Charter Act, as amended by the Suppression of the Financing of Terrorism Act 2002. Section 20 of the UN Charter Act makes it the offence for a person or corporate body who holds a 'freezable asset' to use or deal with the asset, allow the asset to be used or dealt with, or facilitate the use or dealing with asset, where the use or dealing is not in accordance with a s.22 notice..S.21 of the UN Charter Act states that it is an offence for a person or corporate body to make an asset available to a 'proscribed person or entity' where it is not in accordance with an s.22 notice.

It is clear from act that these offences would cover all NTPMs, as 'funds' is defined very broadly within the Criminal Code to include '(a) property and assets of every kind, whether

[113] Nicola McGarrity, 'The Criminalisation of Terrorist Financing in Australia' (2012) 38(3) *Monash University Law Review* 55, 63. Available at: <http://www.austlii.edu.au/au/journals/MonashULawRw/2012/23.pdf> accessed 22 September 2016.

[114] Ibid, 63-64.

tangible or intangible, movable or immovable, however acquired; and (b) legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such property or assets, including, but not limited to bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, debt instruments, drafts and letters of credit.'[115] In the case of the two offences under the UN Charter Act, an 'asset' would also cover NTPMs as they would either be considered a 'list asset, an asset owned or controlled by a proscribed person or an asset derived or generated from an asset in either of the previous categories.[116]

McGarrity criticises the Australian system for CTF, stating that 'the existence of six separate terrorist financing offences is both unnecessary to combat terrorist financing and undesirable.'[117]

5.6. Preventive Measures

Whilst Australia did not implement preventive measures in the speedy fashion that the UK and US did, they are the leader in the Asia / Pacific region. There can be no doubting the importance of preventative measures given the prominence of Australia within that area of the world. Australia's preventive measures are found between the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and the Anti-Money Laundering and Counter-Terrorism Financing Rules 2007. The AML/CTF Act applies to 'designated services' under which it is stated that this means anyone who the AML/CTF Rules apply to. The AML/CTF rules apply to money transmitters which would cover most NTPMs, it also has a section on e-

[115] Criminal Code Act 1995, Division 100.1.

[116] UN Charter Act, s.14.

[117] Nicola McGarrity, 'The Criminalisation of Terrorist Financing in Australia' (n.113), 84.

currency which covers 'digital currency' such as Bitcoin. The FATF confirm that it applies to 'remittance dealers'.[118] Of course, as already noted in other chapters Bitcoin provides a challenge due to its decentralised nature, however, bitcoin (digital currency) exchanges would fall under the above definition for the purposes of AML and CTF preventive measures. Stored value cards[119] are covered by the Act, provided their value is of greater than AUS $1,000 if the amount can be withdrawn in cash, and AUS $5,000 if it cannot. Van der Zahn et al, confirmed that the covered bodies were expanded to money transmitters under the previous legislation, the Financial Transactions Reports Act 1988.[120]

5.6.1. Customer Due Diligence

The FATF in 2015 found that Australia were only 'partially compliant in terms of customer due diligence, an improvement on previous mutual evaluation reports where they were deemed non-compliant.[121] It is a requirement under the Anti-Money Laundering and Counter-Terrorist Financing Rules 2007 that a reporting entity should verify their customer's identity if they are providing a designated service. It is a requirement of the AML/CTF Act 2006 that applicable customer identification procedures are applied prior to the provision of a designated service, including operating an account or carrying out occasional transactions, including wire

[118] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 84.

[119] Stored value cards are identified in Australia's National Threat Assessment as presenting potentially high ML threats.

[120] Mitch Van der Zahn, Mikhail I. Makarenko, Greg Tower, Alexander Kostyuk, Dulacha Barako, Yulia Chervoniaschaya, Alistair Brown, and Helen Kostyuk, 'The Anti-Money Laundering Activities of the Central Banks of Australia and Ukraine' (2007) 10(1) *Journal of Money Laundering Control*, 116–33.

[121] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 157.

transfers.[122] As with the other case study countries, Australia, in line with its risk-based approach to AML and CTF has provision for enhanced due diligence.[123] However, it was criticised in the last FATF Mutual Evaluation Report for not have provision for simplified due diligence, due to proven low risk.[124] It is a requirement that financial institutions keep such records for a period of five years.[125]

5.6.2. Reporting Requirements

Under the 2007 Act, reporting entities are required to report a number of transactions: international funds transfer instructions, international currency transfers, significant cash transactions, suspect-transaction reports and threshold transactions.[126] AUSTRAC acts as Australia's FIU and is responsible for collecting and assessing reports, as well as sharing and gaining information from the Egmont Group.

Australia's main mechanism for reporting is the suspicious matter report (SMR), the FATF has noted that 'reporting obligations are generally well understood.'[127] This matches the UK and US's suspicious activity reports regime. A SMR would be filed in the following circumstances:

- The reporting entity suspects on reasonable grounds that the individual is not who they claim to be;

[122] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.32.

[123] Anti-Money Laundering and Counter-Terrorism Financing Rules 2007, Paragraph 15.10.

[124] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 156.

[125] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.286.

[126] Anti-Money Laundering and Counter-Terrorism Financing Act 2007, Part 3, Division 3.

[127] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 90.

- The reporting entity suspects on reasonable grounds that an agent of the first person who deals with the reporting entity in relation to the provision or prospective provision of the designated service is not the person the agent claims to be;
- The reporting entity suspects on reasonable grounds that information that they have concerning the provision (or prospective provision), of the service may be relevant to the enforcement of the Proceeds of Crime Act 2002 or regulations under that Act.[128]

Compliance cost, as in the UK and US are undoubtedly high in relation to the AML and CTF obligations in Australia. Sathye has put the figure at around AUS $1 billion.[129] Whilst this figure relates to the banking sector, conclusions can still be drawn from it, given the comparable scales between NTPMs providers and traditional financial institutions, the cost of compliance is likely to impact on them harder. Whilst, the risk-based approach will be of some relief to them, it will not remove all of the obligations and costs that they face.

Another area of issue, is the rising number of financial transaction reports, between July 1990 and April 1993 there were '1.6 million such significant transactions reported.'[130] That figure rose to 11 million in 2004.[131] Whilst AUSTRAC has placed the number at 96.3 million reports in 2014-15.[132] Whilst in 2014-2015 81,074 SMRs were received,[133] up 21% on the previous

[128] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.41(1).

[129] Milind Sathye, ''Estimating the Cost of Compliance of AMLCTF for Financial Institutions in Australia' (2008) 15(4) *Journal of Financial Crime* 347, 350.

[130] M. Levi, 'Evaluating the "New Policing": Attacking the Money Trail of Organised Crime' (1997) 30 *Australian and New Zealand Journal of Criminology* 1, 9.

[131] Financial Action Task Force, Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism' (n.9), 50.

[132] Australian Transaction Reports and Analysis Centre, *AUSTRAC Annual Report 2014-2015* (2015), 27. Available at: <http://www.austrac.gov.au/sites/default/files/austrac-ar-14-15-web.pdf> accessed 22 September 2016.

[133] Ibid, 61.

year.[134] It is undoubtable that the significant number of reports means that many SARs will not be fully investigated, and the potential for NTPM related reports to be overlooked due to the lower size of transactions is increased. This, in part is due to the same definitional issues surround suspicion seen in the UK and US. AUSTRAC have noted that a suspicious transaction includes:

- Customers who avoid, or attempt to avoid, transaction reporting obligations;
- Customers who use multiple reporting entities and/or branches to avoid arousing suspicion and detection;
- Customers who undertake transactions that appear inconsistent with their profile;
- Customers who conduct multiple transactions within a short time frame;
- Customers who exhibit irregular behaviour or patterns of transactions;
- Use of currency that is in an unusual condition (for example, dirty, wet, smelly);
- Frequent exchanges of currency denominations (for example, exchanging $20 notes for $100 notes) or currency types (for example, exchanging Australian dollars for euros) where such exchanges are inconsistent with the customer's profile;
- Regular transfers of funds between a customer's personal account and a business or commercial account;
- International funds transfers to high-risk countries, where such transactions are inconsistent with the customer's profile. High-risk countries include:
    - Countries commonly associated with the production or transport of drugs
    - Countries known to be tax havens*
    - Countries associated with phishing scams and card skimming.

[134] Ibid, 26.

- Customers who regularly use stored value cards and frequently add value to the card below the card's threshold limits, particularly when the card is used domestically.[135]

It is clear then, that there is a lack of certainty as to what amounts to suspicion and this leads to over-reporting. In one sense it is helpful that AUSTRAC provides a list of ways in which a transaction would be deemed suspicious, on the other hand it gives a wide ambit for the reporting of transactions and does not assist designated entities in deciphering what is worthy of a report.

5.6.3 Specific NTPM Measures

5.6.3.1. New Technologies

Unlike the UK and US, Australia has already undergone its Fourth Mutual Evaluation Report, and therefore the information on compliance with Recommendation 15 is far more accurate of current technological developments and their threats. The Fourth Mutual Evaluation marks a vast improvement in this area by Australia as they are rated as 'largely compliant'.[136] In their 2006 Third Mutual Evaluation they were rated as 'non-compliant' owing to a complete 'absence of an AML/CTF regime applicable to new technologies.'[137]

However, since then Australia has engaged in understanding the threats posed from new technologies, most notably through it National Threat Assessment.[138] Markedly, the National

---

[135] Australian Transaction Reports and Analysis Centre, *Typologies and Case Studies Report 2009* (2009), 10. Available at: <http://www.austrac.gov.au/sites/default/files/documents/typ09_full_rpt.pdf> accessed 22 September 2016.

[136] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 162.

[137] Ibid, 161.

[138] Australian Transaction Reports and Analysis Centre, Money Laundering in Australia 2011 (2011). Available at:

Threat Assessment focusses on 'electronic payment systems and new payment methods' which cover NTPMs including stored value cards, online remittance and digital currencies.[139] It is an obligation under Australian law that reporting entities 'adopt and maintain an AML/CTF programme'[140] which has the objective of 'identifying, mitigating and managing' money laundering and terrorist financing risk.[141] A reporting entity must 'assess the money laundering and terrorist financing risk posed by:

(a) all new designated services prior to introducing them to the market;

(b) all new methods of designated service delivery prior to adopting them;

(c) all new or developing technologies used for the provision of a designated service prior to adopting them; and

(d) changes arising in the nature of the business relationship, control structure or beneficial ownership of its customers.'[142]

The FATF notes finally that 'there is no specific obligation' for new technologies.[143] It is therefore advisable that Australia goes beyond simply requiring reporting entities to assess the risks of new technology.

<http://www.austrac.gov.au/sites/default/files/documents/money_laundering_in_australia_2011.pdf> accessed 22 September 2016.

[139] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 161.

[140] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.81(1).

[141] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.84(2).

[142] Anti-Money Laundering and Counter-Terrorism Financing Rules 2007, 8.1.5 and 9.1.5.

[143] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 162.

5.6.3.2. Wire Transfers

Australia also struggled with in its compliance with the FATF Recommendation on 'wire transfers' in the last assessment, again being classed as 'non-compliant'.[144] The FATF criticised Australia at the time because there was 'no obligation to verify that the sender's information was accurate or meaningful', 'no requirements to record originator information on domestic transfers', and 'no requirement to include originator information with the transfer instruction.'[145] All this created a clouded picture when it can to the transfer of funds by wire. In its Fourth Mutual Evaluation Report Australia improved and is now rated as 'partially compliant' with the wire transfer Recommendation.[146] It acted to fix the wrongs of its old regime, with FATF noting that Australia have 'extensively updated' its position compared to at the time of the Third Mutual Evaluation.[147] It is worthy of note, that Australia still has a number of areas to improve to gain full compliance with Recommendation 16, they need to implement the most recent updates relating to 'verification of the accuracy of the information, beneficiary information, intermediary financial institutions, and record keeping (for the information that is not required).[148] Further they need to make sure that freezing is undertaken in the context of this Recommendation.[149]

[144] Financial Action Task Force, Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism' (n.9), 83.

[145] Ibid.

[146] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 162.

[147] Ibid.

[148] Ibid.

[149] ibid.

5.6.3.3. Money or Value Transfer Services

Australia has improved slightly on its compliance with Recommendation 14 on 'money or value transfer services' from being 'partially compliant'[150] in 2006 to being 'largely compliant'[151] in the 2015 Fourth Mutual Evaluation Report. Australia has addressed its issues surrounding the registration of money or value transfer services. The AML/CTF Act has a specific section on the Remittance Sector Register[152] and s.74 contains provisions relating to the registration of remittance services. It is a requirement that all remitters apply for registration with AUSTRAC either as an independent remittance dealer,[153] a remittance network provider[154] or an affiliate of a remittance network provider.[155] Further under the new regime which began on 1 November 2011, even if a remitter was on the old Providers of Designated Remittance Services (PoDRS) register, they must still reapply to be on the new Remittance Sector Register,[156] maintained by AUSTRAC. The punishment for breaching the registration requirements is imprisonment for 2 years or 500 penalty units, or both,[157] highlighting the seriousness which Australia has placed on registration. The section is

[150] Financial Action Task Force, Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism' (n.9), 109.

[151] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 162.

[152] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Part 6.

[153] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.74(1A).

[154] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.74(1).

[155] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.74(1B).

[156] Australian Transaction Reports and Analysis Centre, 'Remittance Sector Register' <http://www.austrac.gov.au/businesses/enrolment-and-remitter-registration/remittance-sector-register> accessed 22 September 2016.

[157] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.74(2).

breached simply by engaging in conduct[158] when they are not registered. Individuals can search a remitter on the AUSTRAC website to see if they are registered.[159] Australia has engaged in activity to encourage individuals to identify unlicensed remitters through mechanisms such as advertisements, awareness raising and training sessions and material, as well as relying on larger remitters to detect unlicensed remitters.[160] The biggest weakness identified by the FATF is that agents of the money or value transfer provider are not obliged to be part of the providers AML/CTF programme.[161]

5.7 Confiscation of the Proceeds of Crime

Confiscation of the proceeds of crime are 'actively pursued as a policy objective' in Australia.[162] They have been rated as compliant with the FATF standards on 'confiscation and provisional measures' for the last two Mutual Evaluations in 2006[163] and 2015[164], implementing the relevant international measures outlines in chapter 2. Indeed, in the FATF's Third Mutual Evaluation Report, Australia were complimented on their asset recovery mechanisms for being 'comprehensive and generally effective'.[165]

---

[158] Anti-Money Laundering and Counter-Terrorism Financing Act 2006, s.74(2)(b).

[159] To check if a remitter is registered visit: Australian Transaction Reports and Analysis Centre, AUSTRAC Online <https://online.austrac.gov.au/ao/public/rsregister.seam> accessed 22 September 2016.

[160] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 160.

[161] Ibid.

[162] Ibid.

[163] Ibid, 37.

[164] Ibid, 133.

[165] Ibid, 6.

Confiscation provisions, for both money laundering and terrorist financing, are found in the Proceeds of Crime Act (POCA) 2002. The Act includes both criminal and civil recovery mechanisms.[166] The asset recovery measures available under the Act, include:

- Restraining orders;[167]
- Forfeiture orders;[168]
- Forfeiture on conviction of a serious offence;[169]
- Pecuniary penalty orders;[170] and
- Literary proceeds order.[171]

Restraining Orders are contained in Part 2-1 of POCA and may be applied for by a 'proceeds of crime authority.'[172] The restraint order freezes the property and may lead to confiscation at a later stage. A court will grant a restraining order where 'it decides it is more probably than not, that the person committed a serious offence and that the assets in question are the proceeds of that conduct.'[173]

---

[166] Julie Walters, Carolyn Budd, Russell G Smith, Kim-Kwang Raymond Choo, Rob McCusker and David Rees, Anti-Money Laundering and Counter-Terrorism Financing Across the Globe: A Comparative Study of Regulatory Action (AIC Reports, Research and Public Policy Series, 2011), 9. Available at: <http://www.aic.gov.au/media_library/publications/rpp/113/rpp113.pdf> accessed 22 September 2016.

[167] Proceeds of Crime Act 2002, Part 2-1.

[168] Proceeds of Crime Act 2002, Part 2-2.

[169] Proceeds of Crime Act 2002, Part 2-3.

[170] Proceeds of Crime Act 2002, Part 2-4.

[171] Proceeds of Crime Act 2002, Part 2-5.

[172] Proceeds of Crime Act 2002, s.25.

[173] Andrew White, 'Australia', in Wouter H. Muller, Christian H. Kalin and John G. Goldsworth, *Anti-Money Laundering International Law and Practice* (1st edn, John Wiley & Sons, 2007), 747.

Forfeiture Orders are contained in Part 2-2 of POCA and may be applied for by a 'proceeds of crime authority'[174] except in limited situations.[175] A forfeiture order will be made if the court is satisfied that property is the proceeds of crime, there is no need to find that there has been 'the commission of a particular offence' but instead can be 'based on a finding that some serious offence or other was committed.'[176] Grono expands on how the order is calculated 'the courts assess the benefit from the commission of any other offence that constitutes unlawful activity committed within six years of the application of a pecuniary order or the application for a restraining order, whichever is earlier.'[177]

A 'forfeiture on the conviction of a serious offence' is contained in Part 2-3 of POCA and is generally ordered by the court. An order will be made when a person is convicted of a serious offence, any property which had been subject to a restraining order in relation to the offence is forfeited to the Commonwealth unless the property is excluded from forfeiture.[178] The offence requires the defendant to rebut the presumption that property they own was purchased with illicit funds.[179] Generally, this section is used 'where conviction-based

[174] Proceeds of Crime Act 2002, s.59.

[175] Contained in the Proceeds of Crime Act 2002, s.60

[176] Anthony Kennedy, 'Designing a Civil Forfeiture System: An Issues List for Policymakers and Legislators' (2006) 13(2) Journal of Financial Crime 132, 135.

[177] Sylvia Grono, 'Civil Forfeiture – The Australian Experience', in Simon N. M. Young, *Civil Forfeiture of Criminal Property – Legal Measures for Targeting the Proceeds of Crime* (1st edn, Edward Elgar, 2009), 126.

[178] Proceeds of Crime Act 2002, s.91.

[179] Proceeds of Crime Act 2002, s.92.

forfeiture action is to be taken, or an application for a conviction-based pecuniary penalty order is to be made.'[180]

Pecuniary penalty orders are found under Part 2-4 of POCA, an order will be made by the court requiring a person to pay an amount to the Commonwealth where a 'proceeds of crime authority' applies for an order; and the court is satisfied that the person has committed a serious indictable offence, from which they derived financial benefit.[181] However, it is not always a requirement that a person has been convicted of the offence.[182]

The final order is a literary proceeds order and is found under Part 2-5 of POCA, as with the other orders it can be applied for by a proceeds of crime authority.[183] If 'certain offences have been committed, literary proceeds orders can be made, ordering payments to the Commonwealth of amounts based on the literary proceeds that a person has derived in relation to such an offence.[184] There is no requirement that a person is convicted of the offence.[185] Grono states that a 'restraining order can be obtained over a suspect's property or property under a suspect's effective control where the court is satisfied that there are

[180] Louise Blakeney and Michael Blakeney, 'Counterfeiting and Piracy – Removing the Incentives Through Confiscation' (2008) 30(9) *European Intellectual Property Review* 348, 353.

[181] Proceeds of Crime Act 2002, s.116(1).

[182] Proceeds of Crime Act 2002, s.115.

[183] Proceeds of Crime Act 2002, s.152(1).

[184] Proceeds of Crime Act 2002, s.151.

[185] Ibid.

reasonable grounds to suspect that the suspect has committed an indictable offence or a foreign indictable offence and that person has derived literary proceeds.'[186]

In 2011 a new multi-agency Criminal Assets Confiscation Taskforce was established to provide a more coordinated and integrated approach to identifying and removing the proceeds of crime.[187] Its primary policy objective is to draw on agency skills to target the criminal economy and take the profit out of crime.[188] The FATF state that this Taskforce has increased Australia's efforts to confiscate the proceeds of crime[189], adding further that the Criminal Assets Confiscation Taskforce shows 'early signs of promise as the lead agency to pursue confiscation of criminal proceeds.'[190] The only exclusion to the Taskforce's powers to confiscate are where a conviction is required and no prior restraint order has been obtained.[191]

The Australian Federal Police in the 2010-11 financial year seized AUS$40.1 in assets, compared with AUS$18.9 million in 2009-10.[192] That figure was better in 2013-14, standing at

[186] Sylvia Grono, 'Civil Forfeiture – The Australian Experience', in Simon N. M. Young, *Civil Forfeiture of Criminal Property – Legal Measures for Targeting the Proceeds of Crime* (1st edn, Edward Elgar, 2009), 130.

[187] Australian Transaction Reports and Analysis Centre, Money Laundering in Australia 2011 (2011), 26. Available at: <http://www.austrac.gov.au/sites/default/files/documents/money_laundering_in_australia_2011.pdf> accessed 22 September 2016.

[188] Financial Action Task Force, Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report (April 2015), 61. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf> accessed 22 September 2016.

[189] Ibid, 5.

[190] Ibid, 15.

[191] Ibid, 61.

[192] Australian Transaction Reports and Analysis Centre, Money Laundering in Australia 2011 (n.187), 26.

AUS$ 65.74 million.[193] The bulk of confiscated funds are either related to the drugs trade or tax evasions,[194] this matches the risks identified in Australia's National Threat Assessment.[195] The FATF are still critical of Australia's efforts in the area noting that 'it is unclear how successful confiscation measures are across all jurisdictions, and total recoveries remain relatively low in the context of the nature and scale of Australia's money laundering and terrorist financing risks', the add further that the amount of funds recovered has 'only modestly increased in recent years.'[196] The funds from confiscated asset are deposited into the Confiscated Assets Account and is used to do good; examples include crime prevention, intervention or diversion programs or other law enforcement initiatives.[197]

Alongside the above, Australia also implements targeted financial sanctions in relation to terrorist financing. These are contained in the Charter of the United Nations Act 1945. The FATF have noted that Australia's has a 'sound legal framework'[198] that is a 'good example for other countries' and that the 'automatic, direct legal obligation to freeze assets as soon as an entity is listed by the UN and the numerous designations made under the domestic regime are to be commended as best practices for other countries.'[199] As with the AML provisions,

---

[193] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 61.

[194] Ibid, 47.

[195] Australian Transaction Reports and Analysis Centre, Money Laundering in Australia 2011 (n.187).

[196] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 6.

[197] Australian Transaction Reports and Analysis Centre, Money Laundering in Australia 2011 (n.187), 26.

[198] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 9.

[199] Ibid, 5.

Australia is rated as 'compliant' with the Recommendation on 'targeted financial sanctions'.[200]

In relation to NTPMs, the forfeiture laws are generally applied in quite a simple way, most of the NTPMs merely facilitate the transfer or storage of fiat currency, the only difficulty for law enforcement agencies from these would be identifying the funds in the first place. However, cryptocurrencies have caused more of a problem, in terms of what to do after confiscation. Australia have approached the issue of what to do next by auctioning the confiscated bitcoins.[201] The challenge, in part is that due to fluctuations in the price of Bitcoin, law enforcement need to decide on the best time to sell. Of course, confiscation itself can also prove difficult where law enforcement cannot gain access to the digital wallet key.

Australia's forfeiture laws have been said to have accomplished their 'intended objectives of deterrence, punishment, and deprivation of the fruits of a crime, the Act uses an effective regime of civil forfeiture.'[202]

5.8. Mutual Legal Assistance

It was noted in chapter 2 that cooperation and in particular mutual legal assistance are integral parts of the international effort to tackle the misuse of NTPMs by launderers and terrorist financers, a globalised crime cannot be solved with a localised approach. The FATF

[200] Ibid, 18.

[201] The Guardian, 'Australian Police to Auction $13 in Confiscated Bitcoins' (The Guardian, 31 May 2016) <https://www.theguardian.com/technology/2016/may/31/australian-police-to-auction-13m-in-confiscated-bitcoins> accessed 22 September 2016.

[202] Andrew White, 'Australia', in Wouter H. Muller, Christian H. Kalin and John G. Goldsworth, *Anti-Money Laundering International Law and Practice* (1st edn, John Wiley & Sons, 2007), 747.

has noted that Australia 'cooperates well with other countries in mutual legal assistance matters'[203] and has 'robust systems'[204] in place. Per year, it is estimated that Australia receives around '300-400 mutual legal assistance requests which are processed in a timely manner in accordance with the case prioritisation framework.'[205] In ratifying the Vienna, Palermo, CTF, and Merida Conventions, Australia has given itself firm foundations to build upon in relation to international cooperation. At present Australia has around 30 bilateral mutual assistance treaties in place.[206]

Australia's mutual legal assistance regime is led by the AGD which acts as the central authority.[207] In particular it is the International Crime Cooperation Central Authority that is responsible for dealing with all the case work related to: mutual assistance, extradition, international transfer of prisoners, requests for assistance from the International Criminal Court, and requests for assistance from the International War Crimes Tribunal.[208] Australia's system is governed by the Mutual Assistance in Criminal Matters Act 1987 which has three key objectives:

---

[203] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 10.

[204] Ibid, 12.

[205] Ibid, 115.

[206] For more information on Australia's mutual legal assistance treaties, see: <https://mlat.info/country-profile/australia> accessed 22 September 2016.

[207] Attorney-General's Department, 'Mutual Assistance' <https://www.ag.gov.au/Internationalrelations/Internationalcrimecooperationarrangements/MutualAssistance/Pages/default.aspx> accessed 22 September 2016.

[208] Attorney-General's Department, International Crime Cooperation Division, Fact Sheet – Mutual Assistance Overview (2016), 2. Available at: <https://www.ag.gov.au/Internationalrelations/Internationalcrimecooperationarrangements/MutualAssistance/Documents/Mutual%20assistance%20overview.pdf> accessed 22 September 2016.

- It seeks to 'regulate the provision by Australia of international assistance in criminal matters when a request is made by a foreign country;[209]
- It aims to facilitate the transportation of individuals to foreign countries to give evidence or assist in an investigation;[210]
- It aims to 'facilitate the obtaining by Australia of international assistance in criminal matters.[211]

It is worthy of note, that the AGD can decline a request for assistance, but the Attorney-General and the relevant government minister would have to consider the grounds for doing so.[212]

The FATF have praised Australia for elements of their mutual legal assistance framework noting 'Australia cooperates well in extradition, both making and receiving request in money laundering and terrorist financing related matters, and informal cooperation is generally good across agencies.'[213]

5.9. Conclusion

Australia has a long-running history in efforts to tackle money laundering and terrorist financing, it was viewed as an early leader in the field – given its location and importance to the Asia / Pacific region this is important. However, it experienced a dip in these standards in

[209] Mutual Assistance in Criminal Matters Act 1987, s.5(a).

[210] Mutual Assistance in Criminal Matters Act 1987, s.5(b).

[211] Mutual Assistance in Criminal Matters Act 1987, s.5(c).

[212] Mutual Assistance in Criminal Matters Act 1987, s.8.

[213] Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report' (n.3), 115.

the mid 2000's. In 2005, the FATF was particularly scathing of its regime and it scored in relation to a number of significant Recommendations. This resulted in the introduction of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006, alongside the Anti-Money Laundering and Counter-Terrorism Financing Rules 2007 that sought to bring about a radical overhaul in Australia's AML and CTF regime. In the recent 2015 Mutual Evaluation Report there were signs of improvement in relation to the FATF standard, particularly in terms of preventative measures and those relating to NTPMs. As was seen in this chapter the Act builds on the amendments to the Financial Transaction Reports Act 1988, and bring AML and CTF regulation to a broader range of financial institutions (which encompass the NTPMs laid out in chapter 1). Irrespective of its success so far, Australia should be applauded for its approach of bringing AML and CTF regulation under one Act, it makes it easier for designated entities to know what is required in terms of compliance when everything is in one place. This can be contrasted with the UK and US where they have a patchwork of different instruments.

It has been highlighted that whilst NTPMs are not as much of a threat to Australia as traditional forms of money laundering and terrorist financing, their threat is not insignificant either. Australia's National Threat Assessment's on money laundering and terrorist financing, in 2011 and 2015 respectively, highlighted the risks to Australia from methods such as wire transfers and stored value cards in particular. To that end, we have seen that a number of Australia's competent authorities have concerned themselves in the risks associated with the developments in NTPMs. Of particular note, are the AGDs work through its National Organised Crime Response Plan, as well as its role as Chair of the 'Working Group on Remittance Account Closures'. Alongside the AGD's work in the area, AUSTRAC have also played a prominent role in attempting to understand and disseminate information on NTPMs through their annual typology reports which provide an oversight of newly emerging NTPMs,

alongside more traditional methods of laundering and terrorist financing. In recent years digital currencies and remittance providers have feature prominently in these. One tertiary authority of interest is the ELIGO National Task Force which addresses criminal vulnerabilities and the potential for exploitation of alternative remittance systems, the Task Force had a key role given that around AUS$ 30 million was moved through the sector.

With regards to the criminalisation of money laundering and terrorist financing it has been noted that Australia approach is comprehensive, implementing the main measures found in the Vienna, Palermo and the Terrorism Financing Convention. The use of NTPMs does not make an impact on criminalisation as the offences are construed broadly to be committed through any mechanism. In relation to preventative measures it was noted above that Australia has improved on these in the 10 years between FATF assessment periods, the main preventative measures are found in the Anti-Money Laundering and Counter-Terrorism Financing Act 2006, supplemented by the Anti-Money Laundering and Counter-Terrorism Rules 2007. Australia needs to have strong preventative measures given its location in the world and the attractiveness for criminals in the region to move funds through the jurisdiction. Unfortunately, whilst there is signs of improvement they are still not as strong in these areas as the UK and US. Overall, the preventive measures are construed broadly so that they apply to NTPMs. Australia uses the term ‘designated services’ to cover NTPMs, this covers anyone that the Anti-Money Laundering and Counter-Terrorism Financing Rules 2007 apply to. It is noted by the FATF in their 2015 report that whilst Australia has measures relating to customer due diligence, the fact that they lack provisions relating to simplified due diligence, due to writing it off as low risk, is a weakness in the Australian system. In relation to reporting requirements, Australia faces the same kind of difficulties that other nations face relating to ‘defensive reporting’ and ‘compliance costs’, it is perhaps symptomatic of the

constant battle to improve compliance, that the costs increase. These two issues can have a knock on effect in relation to NTPMs, a report in relation to a suspicious transaction through a NTPM may get lost in the system, and that smaller NTPM providers may struggle to meet the costs of compliance with the AML and CTF preventive measures. Australia also has specific provisions for NTPMs. In relation to wire transfers (or 'electronic transfers') they now require a plethora of information surrounding the transaction, this will follow the transaction and the wire transfer provider will keep a record of it. This seeks to create a paper trail to negate the risks associate with quick transactions that cross borders. With regards to money or value transfer providers generally, Australia require that they are registered with AUSTRAC which again address the risks associated with the ability to set up a NTPM more easily than a traditional financial institution, importantly it means that AUSTRAC have a record of providers in case of involvement in money laundering or terrorist financing cases, as well as for wider consumer protection matters. The final specific measure relating in part to NTPMs is in relation to new technologies, Australia have performed well in this area, improving dramatically between FATF assessments, it can be noted that their National Threat Assessments assist with this, whilst the Anti-Money Laundering and Counter-Terrorism Act and Rules make it compulsory for all reporting entities to adopt and maintain an AML/CTF programme that assesses the risks posed by new services or technologies. Australia, should be praised for this and it will serve them well in terms of any emerging NTPMs as the providers will be required to understand the risks before introducing them.

Australia, like the other case study countries actively pursues the proceeds of crime as a policy objective. It was noted that they have five main methods for the recovery of assets: restraining orders; forfeiture orders; forfeiture on conviction of a serious offence; pecuniary penalty orders; and literary proceeds order. This is an area of Australia's AML and CTF

framework that is particularly strong, and indeed can been seen as an authority of 'good practice' for the Asia / Pacific region. Taking this further, Australia is one of the first countries to deal with the confiscation of bitcoins, they chose to auction them so as to regain the proceeds of crime, and this too should be seen as good practice around the world where a law enforcement agency is able to confiscate the digital currency.

The importance of mutual legal assistance in relation to NTPMs should not be underestimated, Australia through the Attorney-General's Department has been noted as being particularly strong in this area as they cooperate well with other countries. They have a successful framework for the exchange of information, extradition of individuals and for making requests, this is imperative as the global nature of NTPMs means that a localised solution would not be appropriate.

So then, whilst this chapter cannot argue that NTPMs are the most pressing problem that Australia faces in terms of money laundering and terrorist financing, it can be noted that it is a problem. Australia's specific NTPM responses are relatively good, and they have taken a number of steps to understand the risks associated with them. However, it has also been seen that Australia's general AML and CTF framework is still not at the standard that it should be at and this is a concern. Some of the general measures have an impact in relation to the regulation of NTPMs.

Chapter 6 – Conclusions

6.1. Introduction

The aim of this thesis has been to examine the criminal abuse of NTPMs by adopting a comparative method focussing on the implementation and application of international standards in the United Kingdom, United States and Australia. Its primary objective has been to investigate whether or not the case study countries are sufficiently prepared to tackle criminal abuse of NTPMs, and what good practice they can take from one another. The appeal of exploring legal responses to NTPMs (broadly) is driven by a firm belief that all methods of money laundering and financing of terrorism should be tackled and that the framework, to an extent, needs to be futureproof in order to deal with newly emerging typologies. Simply, aiming to deal with the most current typology or indeed needing to draft new legislation for each new typology would be a waste of resources and prove futile. What has been seen, is that there is no miracle solution to the challenge of money laundering and terrorist financing, particularly in relation to NTPMs. However, what is true, is that there are many interesting and unique initiatives being used across the case study countries that need to be utilised more widely. Given the grave impacts of each crime, there should always be a push to make the international AML/CTF framework work harder.

At present, it is fair to say, attention in the area remains predominantly focussed on traditional means of laundering and terrorist financing, after all this is the way in which the majority of funds are transferred. It is worthy of note and useful that, any improvements made in this area generally benefit the AML/CTF framework as a whole, including the efforts to counter the abuse of NTPMs. However, it should be noted, that recently, on both an international and national level, increasing efforts have been made to tackle misuse of

NTPMs. On an international level, framework innovation, engaging stakeholders in the development of international standards, and emerging typology reports have all played a role in highlighting the significance of the threat and in kick-starting efforts to curb NTPMs abuse. On a national level, it has been witnessed via the case study countries that legislation development, engagement in public consultation and investment in understanding new typologies are all evident. Whilst academic interest has mainly focussed on individual NTPMs, the renewed focus on an international level of dealing with them by similar means will undoubtedly spark interest around adapting to newly emerging payment methods and future proofing the framework as much as possible. As this thesis has identified, individual countries are doing this, however even amongst the case study countries which are considered to be 'developed' and have comparatively successful AML and CTF frameworks, this appears to be done in an ad-hoc manner and approaches can differ significantly in places. It is imperative that FATF members work together to improve international standards, and that good practice on a national level is filtered up to be disseminated amongst FATF and FSRB members. As of yet, there appears to be little effort to have standardised approaches to implementing the international AML and CTF framework in relation to NTPMs. It has been largely assumed that individual members enjoy a great deal of autonomy in achieving the aims of the international framework.

6.2. Key Findings

The first part of this thesis, sought to challenge the preconceptions that exist around terrorist financing, and particularly money laundering. Namely, that criminals engage in fairly traditional forms of transfer. Money laundering and terrorist financing have long been recognised as pressing challenges for regulators, supervisors and law enforcement agencies. They act as threats to a countries security and financial industry, that are prime drivers in the

efforts to counter both crimes. It was outlined that one thing that has not and will not change is the ingenuity and intelligence of individuals who seek to evade detection when transferring illicit funds. In this section, it was recognised that NTPMs are an increasingly popular way for launderers to profit from their criminal activity, or for terrorist financers to evade detection in transferring their funds to the final destination. The chapter then turned to focus on these NTPMs and analysing each one in turn for their susceptibility to abuse. The phrase 'non-traditional payment methods' is a broad one, designed to encapsulate the many and varied payment systems that have emerged. It was argued, that as with traditional methods of transfer, it is believed that these NTPMs began with legitimate intentions, simply that they have subsequently been abused because of factors that appeal to criminals.[1] A number of commonalities / factors that would be appealing to criminals were pulled out, notably: efficiency of transfer, reduced cost of transfer, anonymity, advancing technology and lack of widespread understanding of how it works, facilitating cross-border payments and ease of access. Criminals can use NTPMs to: attempt to avoid the regulatory system; move funds freely across borders; and lose less of their illicit funds to bank charges. Whilst it cannot be stated that the volume of abuse through NTPMs is comparable to that through the traditional financial system, what the factors highlighted above (and in more detail in chapter 1) do show is the potential for abuse. It is this potential for abuse that makes it imperative for regulators,

[1] Note, that an argument could easily be advanced that in the future a NTPM could be set up that has completely illegitimate intentions. However, in an ideal world there are two things that any criminal abusing NTPMs wants the NTPM to be; first, it should be incapable of being identified as a mechanism purely used for moving illicit funds; and second, it should protect individual transactions being easily identifiable as being moved for criminal purposes. In order for a NTPM set up from the outset with illegitimate intentions, it would have to attract a sufficient number of legitimate users to disguise the illicit transactions of its criminal users, otherwise individuals would be easy to identify.

standard setters, law enforcement agencies and private entities to act to prevent abuse. It was further argued in this section, that rather than focussing on individual NTPMs going forward it is these themes that the international framework should work on so that it is flexible and responsive to newly emerging challenges. So, by way of example, when a new NTPM comes along with new characteristics regulators and standard setters simply have to assess whether the customer due diligence requirements are still adequate in relation to dealing with that NTPM. This process can be done for each area of the AML/CTF framework. It would mean that only areas deemed insufficient would need revision, or explanation as to how they apply to the new NTPM. Responding to each NTPM as and when they arise would entail the investment of significant resources each and every time a new method emerges, and result in a delayed response time. By working on themes rather than the NTPM itself, individual jurisdiction should be more responsive.

After establishing the need to tackle abuse of NTPMs for the purposes of money laundering and terrorist financing, and advocating an approach which focusses on particular characteristics of specific NTPMs, rather than on specific NTPMs as and when they arrive, the thesis then:

- Established a thematic structure to identify and analyse the relevant parts of the international AML and CTF framework, in relation to NTPMs; and
- Using the thematic structure, assessed the compliance of three case study countries (the UK, US, and Australia) with the parts of the international AML and CTF framework that are relevant to NTPMs.

The thesis stated that there were seven key criteria by which each country should be assessed, they were:

1. Global Role and Implementation of the International AML/CTF Framework;
2. Establishment of Competent Authorities and their Roles;
3. Application of a Risk-Based Approach;
4. Criminalisation of Money Laundering and Terrorist Financing;
5. Preventive Measures;
6. Confiscation of the Proceeds of Crime; and
7. Mutual Legal Assistance.

It is the aim of this concluding section to highlight the key findings from the above thematic analysis, identifying areas of best practice and areas for improvement.

6.2.1. Global Role and Implementation of International Framework

Under this heading the thesis established the global role of the case study countries and their overall implementation of the international standards. It should come as no surprise, given the nature of the countries chosen, that overall their compliance with international standards can be described as respectable. Indeed, they were partly picked as in places their AML and CTF measure have been identified as exceeding the international community's responses.

In terms of implementation of international obligations, all three countries were founding members of the UN Charter in 1945, and have subsequently signed and ratified the main UN AML and CTF Conventions, notably: the Vienna convention, the Palermo Convention and the SFT Convention. It is interesting to note, that all countries are relatively quick in signing and then ratifying UN Conventions. The only exception being the SFT Convention where the UK was one of only four jurisdictions to ratify it prior to 9/11. The US and Australia, signing it alongside a host of other countries when there was increased political will to counter terrorism post-9/11. Although the UK itself is not entirely consistent in meeting its

international obligations, indeed it received criticism from the House of Lords for not implementing the Council of Europe's Warsaw Convention in a timely manner. Indeed, the House of Lords doubted that there was ever any good reason for not implementing it as soon as practicably possible. On the whole then, the three case study countries tend to be quick in adopting international measures. As noted elsewhere in this thesis, whilst these Conventions have no explicit mention to NTPMs, because they inform the underlying AML and CTF preventive measures that are applicable to NTPMs then it is pleasing to see that the three case study countries ratifying them.

In relation to the international standards, all three case study countries are full members of the Financial Action Task Force and therefore as well as being assessed on the basis of FATF's Recommendations, they also play a prominent role in shaping these Recommendations. By virtue of this membership, the US and UK are revolving members of several of the FATF-Style Regional Bodies, this enables them to share good practice and encourage the development of AML and CTF measures around the world. It is perceived that this is a way for the most developed nations in terms of AML and CTF to bring other jurisdictions up to speed, this is an important role, particularly in relation to NTPMs. Weaker jurisdictions may not have the resources or expertise to develop and counter measures in their own right, the full-FATF members should assist them in doing this. Australia, are not members of as many FSRB's but they arguably have just as important a role as the UK and US as they are the FATF member which sits on the Asian-Pacific Group FSRB. Australia, therefore play a significant role in developing AML and CTF measures for the whole of the Asia-Pacific region. It is therefore clear that it is essential the UK, US and Australia have strong and robust AML/CTF regimes, and also that they are capable of responding quickly to emerging threats and then disseminating their practices widely.

6.2.2. International Bodies and Establishment of National Competent Authorities

In terms of developing the international framework for AML and CTF, at the core there are only a few key bodies: the UN and the FATF. They are often assisted by the IMF, World Bank and FSRB's. Whilst bodies such as the Basel Committee on Banking Supervision have very limited interaction in relation to customer-due diligence measures.

Undoubtedly, the most important body is the FATF, its 40 Recommendations are the gold standard in terms of AML and CTF provisions, and as such a number of the Recommendations either directly relate to NTPMs or are applicable to them. The FATF also undertakes typology reports on emerging threats and new trends – they are assisted in this role by the FSRB's[2] and member jurisdictions. It is often through these typology reports that the FATF get a first glimpse of emerging NTPMs. They then go on to conduct full research on them, producing guidance papers. These documents are imperative to the international effort to counter money laundering and terrorist financing through NTPM, and the competent authorities in all three case study countries identify them as important documents. Further, they identify risk factors and red flags which inform the efforts national authorities. The FATF have produced guidance documents in relation to all the NTPMs discussed in this thesis. There can be no doubt of the value of the FATF and its FSRB's on an international level, both in terms of the AML/CTF framework generally, and specifically in relation to NTPMs. Often, it is the only body dealing with these NTPMs in relation to AML and CTF. The FATF provides an excellent forum for co-operation, knowledge building, and standard setting. It should only be encouraged to flourish and continue its efforts to improve AML and CTF standards globally, going forwards. Indeed, it has been an oft-stated phrase in this thesis, but a global problem cannot be solved

[2] The FSRB's play an invaluable role in disseminating the FATF Recommendations and good practices in relation to NTPMs to their 189 member states.

with a localised approach, the international framework and the bodies that comprise have an invaluable role to play in tackling the abuse of NTPMs. On that theme, the European Union also does in good job in setting minimum standards within the Union, as well as funding projects in the area, the most notable being the project with GAFILAT on the 'cocaine route' which yielded some outcomes in relation to NTPMs.

All three case study countries have a number of competent authorities tasked with AML and CTF responsibilities, a number of which have engaged with the process of understanding NTPMs and analysing their risk factors. However, a number of academics have criticised the US for the volume of competent authorities it has designated AML and CTF responsibilities to. All three countries have competent authorities that are responsible for the production of National Threat Assessments; these have proven to be successful methods for assessing the risks associated with NTPMs. One initiative worthy of special note is HM Treasury's call for information in relation to the risks of digital currencies such as bitcoin, it utilised the knowledge base of experts to play a role in the UK's response.[3] The resulting response paper gives an indication of the path the UK wishes to pursue in relation to NTPMs. Another factor that stands the UK in good stead in relation to tackling abuse of NTPMs is the fact that the National Crime Agency have a competition objective. This competition objective means that the FCA has an interest in NTPMs, and from an AML and CTF perspective needs to make sure that they are sound. Further, through its Innovation Hub it wants to ensure that innovation is not being stifled by regulatory barriers, an important consideration in relation to NTPMs.

[3] See appendix for the document that I, alongside Dr. Robert Stokes submitted in response to this call.

6.2.3. Risk-Based Approach

As identified earlier in the thesis, the risk-based approach is one of the key concepts promoted by the FATF. It is argued throughout the thesis that this is an imperative part of the international framework in relation to NTPMs. It means that where the risks are sufficiently serious, then more rigorous AML and CTF preventive measures should be put in place. But, by the same token, where there is little risk, then there is room for regulators to permit the NTPM to flourish, without the weight of cumbersome AML/CTF measures. This is particularly important for NTPMs due to the consumer benefits they bring – if they are not too risky, then it would be unduly burdensome to apply the same level of AML and CTF measures to them, as we do to the formal financial system. All of the case study countries note that they are committed to implementing a risk-based approach in all of the sectors they regulate. The biggest issue in the area is in relation to the businesses operating in the area, will they apply AML and CTF measures on a risk-based basis correctly? This is a challenging for even traditional financial businesses, never mind NTPM businesses which do not necessarily have the same level of resources.

6.2.4. Criminalisation

In relation to criminalisation, all three countries have implemented the criminalisation measures found in the Vienna, Palermo and SFT Conventions and so its standards in relation to this should not come as a surprise. All three adopt an approach that means that the use of NTPMs would be capture under this, as the criminal offence does not have regard for the payment method used to commit it.

6.2.5. Preventive Measures

Turning to preventive measures, the international framework has a number of measures applicable to NTPMs, including: customer due diligence, the reporting regime, measures in relation to new technologies, wire transfer measures, and rules in relation to money or value

transfer services. The US was one of the first countries to introduce some of the measures we now consider synonymous with AML and CTF, whilst the UK was the first to do so in the EU. It has been noted that Australia's Anti-Money Laundering and Counter-Terrorism Financing Act 2006 should be praised for housing all of Australia primary AML and CTF measures in one place, in comparison to the UK and US who have adopted a patchwork approach to their legislation. Australia meanwhile has a key role to play in disseminating best practices in relation to the preventive measures across the Asia / Pacific region through the Asia / Pacific Group FSRB. In the UK and US, the preventive measures apply to NTPMs by virtue of money service business falling under the definition of 'financial institution', whilst in Australia they fall under the definition of 'designated services'. One point of note in this area is that ad bitcoin is decentralised the AML and CTF preventive measures cannot be applied directly onto it in the way it can with other NTPMs as it has no 'provider'. Therefore, it has been indicated, by all three countries, that digital currency exchanges which turn digital currency into fiat currency will be the point at which AML and CTF preventive measures bite. In relation to customer due diligence both the UK and US provide for both enhanced and simplified due diligence measures, Australia on the other hand lacks provisions for simplified due diligence and has been criticised by the FATF for this approach. All three countries operate a suspicious transaction reports regime (Australia call these suspicious matter reports). A common problem experienced across all three countries relates to the fact that the SARs regime results in defensive reporting as well as high compliance costs. Defensive reporting results in spurious reports making it difficult for the countries Financial Intelligence Unit to identify SARs requiring attention. The US has been criticised for its approach in relation to this of devoting analytical resources to those SARs that are considered most valuable to law enforcement. Indeed, this choice led to FinCEN overlooking an SAR with links to 9/11. On an international,

the Egmont Group of Financial Intelligence units, founded by FinCEN, plays an essential role in disseminating emerging threats and typologies across a wide range of countries via their financial intelligence units. This can be particularly important where a country has yet to experience risks associated with NTPMs. All three countries have also implemented the FATF measures relating specifically to NTPMs. With regards to the Recommendation on wire transfers, all three countries now require extensive information from the originator that is recorded and held for a five-year period, but that also travels with the wire transfer. In relation to this the US implemented a threshold of $3,000, they have been extensively criticised for this as it potentially leaves a whole host of transactions without an adequate paper trail and leaves a gap that criminals may seek to exploit. In relation to money or value transfer services, all three countries identify them as money service businesses and operate a registration regime. Failure to register, results in a penalty. The final specific measure relating in part to NTPMs is in relation to new technologies. Their rules make it compulsory for all reporting entities to adopt and maintain an AML/CTF program that assesses the risks posed by new services or technologies.

6.2.6. Confiscating the Proceeds of Crime

All three case studies recognize the importance of pursuing the proceeds of crime, indeed it was the US that initiated this a policy choice. All of the case study countries have been assessed highly by the FATF in this area. There are a number of confiscation measures across the jurisdictions, all three have criminal and civil measures. The US have lead the way in dealing with the confiscation of digital currencies. Their approach to auction off the bitcoins has been adopted by Australia, in order to recover the proceeds of crime. This is a good approach to take and ensures that the State should not be out of pocket for the AML or CTF investigation that took place leading up to the confiscation. Most other NTPM will be picked

up by the confiscation regime in the traditional manner as they utilise fiat currency, which law enforcement agencies are well used to dealing with. The difficulty is whether the funds are ever detected to be confiscated.

6.2.7. Mutual Legal Assistance

The importance of mutual legal assistance in relation to NTPMs should not be underestimated, all three case study countries engage strongly in this area. The US has placed a firm emphasis on encouraging mutual legal assistance which must be commended, in particular through its policy of sharing any assets in recovers in conjunction with countries who assisted in the investigation. An approach that the UK has also adopted. Of all the jurisdictions, it is noted that the US in particular, aggressively pursue international cooperation and that approach cannot be faulted as the globalised threat from NTPMs cannot be countered with a localised approach. A final good initiative in this area comes from the UK, where the NCA will create International Liaison Officer posts to improve its international outreach. Significant emphasis needs to be placed on the international community working together to share intelligence on current cases and then engage in joint intelligence-led investigations.

6.3. Recommendations to UK Government

Following on from the key findings of the thesis, it is perhaps of use to give some important recommendations that the UK government should seek to follow when aiming to tackle criminal misuse of NTPMs. These are:

1. **Ensure the swift and effective implementation of international legal measures in the area of AML and CTF**. On the whole, the UK has been first-rate in doing this, although the catastrophe that was the implementation of the Council of Europe's Warsaw

Convention is a reminder to all that this process could be improved. Whilst, these measures tend not to directly relate to NTPMs, they do have an indirect impact.

2. **Close and sustained engagement with international standards**. The UK has consistently been assessed as one of the best countries when it comes to implementation of FATF standards. It is important that they continue with this trend as the FATF are the one international body that actively and regularly publish guidance in relation to NTPMs and adapting a countries legal framework to tackle their abuse.
3. **A clearer delineation of the respective roles of HM Treasury and Home Office**. It is not always abundantly clear which authority is dealing with which aspect of the AML and CTF framework. Indeed, in the recent plan for improvement of the UK's AML and CTF framework responsibility for different areas almost seems to have been awarded on an ad-hoc basis.
4. **A single body responsible for oversight of NTPMs**. At present, NTPMs seem to fall through the cracks. Though they are picked up by the FCA in most instances in terms of AML and CTF measures. But, maybe going forwards it would be best to expand the role of the new Payment Services Regulator to cover NTPMs as well. This would allow greater insight into NTPMs and their trends beyond just AML and CTF tendencies.
5. **Greater focus in the National Threat Assessments on the abuse of NTPMs**. The NTA's have been a positive development, and they do include reference to NTPM cases and issues. However, it is questionable whether enough is being done. Whilst, the number of NTPM cases is without doubt smaller than those through traditional methods, what cannot be doubted is that they are occurring and need further light shone on them.
6. **Continued public engagement in relation to NTPMs**. One good thing that the government did in relation to bitcoin, and digital currencies more generally, was to

consult on the risks and benefits of it. This enabled them to receive expert advice and resulted in a variety of viewpoints. The value of engaging experts cannot be understated, particularly in relation to these newly emerging NTPMs, as they are highly technical and often require different views to create the whole picture.

7. **Remember to focus on the benefits and not just the AML/CTF risks**. Again, the government has done this well in relation to bitcoin, but it is an important recommendation none-the-less. The temptation to say that bitcoin is bad and therefore should be heavily regulated is an easy one to advance particularly in light of the Silk Road but more important is to recognise its utility as a new medium of exchange. After all, one should remember that fiat currency is particularly susceptible to laundering, perhaps to a far greater extent that bitcoin.
8. **Invest in digital education**. At the moment, understanding of NTPMs by the general public is low. This cause many problems, not least that it is easy for NTPM detractors to advance arguments about the criminal risks of them, and deter the public from using them. However, with education about the benefits of these alternate payment systems, the public would realise that they are not all bad and see through misleading statements. Further, there can be no doubt that with advances in technology it is only a matter of time before these methods or ones based on them become the norm.
9. **More stringent enforcement of customer due diligence measures outside the financial sector**. CDD measures tend to be stringently applied within the financial sector, however at the moment this is still a weakness in relation to certain NTPMs.
10. **Encourage more SARs reporting from NTPM providers**. At the moment, there is a lack of reporting from NTPM providers. Whilst it is important not to go down the route of over-reporting, under-reporting is also a significant problem.

11. **International cooperation**. At a time when there is a fear that the UK will become more insular, it is important that in terms of security, we continue to cooperate with our international neighbours. It cannot be stated often enough that an international problem cannot be solved on a local level, it requires full cooperation. We need to continue to explore avenue for further cooperation.
12. **Focus on themes, and not specific payment methods**. As outlined above, focussing on specific payment methods can duplicate workload and lead to poor response times. Rather it would be a better use of resources for the government to focus on characteristics that make NTPMs challenging to deal with.

Of course, this is not an exhaustive list, rather the areas that are most important to address going forward.

6.4. NTPMs – Looking Forward

This thesis then, has looked at the development of NTPMs, using examples up to digital currencies like bitcoin – the most recent NTPM to gain notoriety. We are however already seeing adaptations on bitcoin which exploit some of its characteristics and aim to be more anonymous. None of these have yet flourished, but there is no doubt that going forward standard setters, regulators, and law enforcement will continue to be challenged by new developments in payment methods that facilitate criminal activity. Remember the adage that criminals are increasingly sophisticated and are limited only by their own imagination, then the challenge for regulators is to be as responsive as possible to new developments.

Bitcoin is still developing and increasing in usage, similarly the regulatory response to bitcoin is still emerging. However, what is for certain is that their threat will change over time for instance the more well known a NTPM gets, the more techniques such as (cuckoo) smurfing

are used to make them even more difficult to trace. In the same way as in the formal sector. Or, the criminal may decide to move funds through several types of NTPM to further obscure the paper trail. Of course, we cannot rule out bitcoin failing and disappearing. That is a possibility. However, what can be guaranteed is that something based on the blockchain will emerge and continue as a payment method.

At present, as with the other NTPMs, it is still of most use to move bitcoin back into the formal financial sector at some point, to realise its value in fiat currency. This allows the traditional gatekeepers to step in and detect suspicious activity and impose customer due diligence measures. However, the worry is, going forward, that payment methods like bitcoin will flourish to the point where they have wide acceptance and removing the need to channel funds through the formal financial sector. This would have the effect of removing a layer of protection against abuse.

At present, in terms of digital currencies, most of the big sites on the dark web only accept bitcoin. This is advantageous in the sense that law enforcement agencies know to just focus their efforts on one payment method. This could also get more challenging should they change the way in which the accept payment.

It is relevant to conclude this section by noting that where NTPMs go and what comes next depends fully on technological development. The best we can hope for is that the government is well prepared to deal with new threats and typologies.

6.5. Potential Impact of this Research

Throughout the course of this thesis, the work has sparked a lot of interest. During a research trip to Australia, I engaged with ANZ Bank, Commonwealth Bank, Westpac Bank, the Australian Banker's Association, Monash University, as well as presenting to both the

Australian Banker's Association Anti-Money Laundering Technical Working Group and the PIS conference hosted by ANZ Bank. Back in the UK I have engaged in Government consultation and presented to AIG in London. I am also currently involved in a research project with Greater Manchester Police, on the policing of bitcoin which received funding from the N8 through this I have also made contacts at the National Crime Agency. Whilst, pieces written for the Conversation have been republished in America, Australia and South Africa. What is clear from this, is that interest in understanding NTPMs from an AML and CTF prospective is high. I have no doubt that the research found in this thesis will be of use to: government, law enforcement agencies, private sector bodies and researchers. The research also leaves me well placed to:

- Comment on and analyse future NTPMs;
- Expand my analysis into further countries e.g. less developed countries to see what challenges they face;
- To apply it to other sectors e.g. the charity sector;[4]
- Funded research into countries that are not primarily English speaking.

6.6. Final thoughts

Being realistic, as with traditional means, we know that complete prevention is not possible but that reduction should be the aim. This thesis has analysed the legal response to the abuse of NTPMs and laid out some responses that should be undertaken. It is worthy of note at this stage that we need to be mindful of how we deal with NTPMs, often they are the only

[4] As an example, see: *Shillito, M. R. '*Countering Terrorist Financing via Non-Profit Organisations: Assessing why few States Comply with the International Recommendations' (2015) 6(3) *Nonprofit Policy Forum* 325.

mechanism for transferring funds for certain groups of people, we need to ensure that we do not disproportionately disadvantage them by imposing stringent AML and CTF measures. But, this should not stop measures being implemented where they are needed and follow a risk-based approach.

Added to this there are questions whether the AML framework is a sufficient mechanism for tackling terrorist financing due to the challenges of cheap terrorism and legitimate funds being used – if this was the case then it makes it very difficult and in many cases impossible for the preventive measures to bite. The wider question therefore has to be whether the whole CTF regime needs to be revisited.

The UK is currently undergoing significant change to its AML and CTF regime in advance of the fourth mutual evaluation. We can however be sceptical of the benefits of this renewed emphasis in updating the framework. It is by no means the first time the government has focussed on AML and CTF, owing to this we know that it will not make drastic improvements to the framework. It is however, a commendable step none-the-less. Though sceptics would suggest a belated attempt to make sure the framework is up to scratch for the FATF assessment.

These are then, interesting times for anti-money laundering and counter-terrorist financing, and academics conducting research into this area of law. Globalisation and advances in technology mean that the area is advancing rapidly and new variations on familiar NTPM themes are being developed. There are signs that the framework for AML and CTF, both domestically and internationally is quick to respond, however the old adage that launderers are one step ahead of regulators still seems fitting. It only seems fitting to conclude, criminal abuse of NTPMs is a global problem, it can only truly be tackled with a coordinated

international response – we should not underestimate the size of the challenge and the importance of working together – we are only as strong as the weakest jurisdictions AML / CTF regime.

Bibliography

- Abbott, K. W. and Snidal, D. 'Hard and Soft Law in International Governance' (2000) 54(3) *International Organisation* 421;
- Alford, D. 'Anti-Money Laundering regulations: A Burden on Financial Institutions' (2004) 19 *Carolina Journal of International Law and Commercial Regulation* 437;
- Alldridge*, P. Money Laundering Law: Forfeiture, Confiscation, Civil Recovery, Criminal Laundering and Taxation of the Proceeds of Crime*, (1st edn, Hart Publishing, 2003);
- Alldridge, P. 'Proceeds of Crime Law Since 2003 – Two Key Areas (2014) 3 *Criminal Law Review* 171;
- Alexander, K. 'The International Anti-Money Laundering Regime: The Role of the Financial Action Task Force' (2001) 4(3) *Journal of Money Laundering Control* 231;
- Alexander, R *Insider Dealing and Money Laundering in the EU: Law and Regulation* (1st edn, Ashgate, 2007);
- Alhosani, W. *Anti-Money Laundering: A Comparative and Critical Analysis of the UK and UAE's Financial Intelligence Units* (1st edn., Palgrave Macmillan, 2016).
- Aron, J. 'Future of Money: Virtual Money Gets Real' (New Scientist, 2011) <https://www.newscientist.com/article/mg21028155-600-future-of-money-virtual-cash-gets-real/>;
- Arnone, M. and Borlini, I. 'International anti-money laundering programmes: empirical assessment and issues in criminal regulation' (2010) 13(3) J.M.L.C. 226;
- Azarian, R. 'Historical Comparison Re-Considered' (2011) 7(8) *Asian Social Science* 35;
- Azarian, R. 'Potentials and Limitations of Comparative Method in Social Science' (2011) 1(4) *International Journal of Humanities and Social Science* 113;
- Baldwin Jr., F. N. 'Money Laundering Counter-Measures with Primary Focus on Terrorism and the USA Patriot Act 2001', 2002 6(2) *Journal of Money Laundering Control* 105;
- Bantekas, I. 'The International Law of Terrorist Financing' (2003) 97 *American Journal of International Law* 315, 316; and Nimrod Raphaeli, 'Financing of Terrorism: Sources, Methods, and Channels' (2003) 15(4) Terrorism and Political Violence 59.Barnes, B. D. 'Confronting the One-Man Wolf Pack: Adapting Law Enforcement and Prosecution Responses to the Threat of Lone Wolf Terrorism' (2012) 92 *Boston University Law Review* 1614;
- Bell, R. E. 'The Confiscation, Forfeiture and Disruption of Terrorist Finances' (2003) 7(2) *Journal of Money Laundering Control* 105;
- Benning, J. F. 'Following Dirty Money: Does Bank Reporting of Suspicious Activity Pose a Threat to Drug Dealers?' (2002) 13(4) *Criminal Justice Policy Review* 337;
- Blakeney, L and Blakeney, M. 'Counterfeiting and Piracy – Removing the Incentives Through Confiscation' (2008) 30(9) *European Intellectual Property Review* 348;

- Bleicher, S. A. 'The Legal Significance of Re-citation of General Assembly Resolutions' [1969] 63 AJIL 444;
- Biersteker, T. J. and Eckert, S. E. 'Introduction: The Challenge of Terrorist Financing', In Thomas J. Biersteker and Sue E. Eckert, *Countering the Financing of Terrorism* (1st edn, Routledge, 2008);
- Brown, G. and Evans, T. 'The Impact: The Breadth and Depth of the Anti-Money Laundering Provisions Requiring Reporting of Suspicious Activities' (2008) 23(5) *Journal of International Banking Law and Regulation* 274;
- Bryans, D. 'Bitcoin and Money Laundering: Mining for an Effective Solution' (2014) 89 (44) *Indiana Law Journal* 441;
- Bunt, H. V. D. 'The Role of Hawala Bankers in the Transfer of Proceeds from Organized Crime' in Dina Siegel and Hans Nelen, *Organised Crime: Culture, Markets and Policies* (Volume 7, Springer, 2008). Available at: <http://link.springer.com/chapter/10.1007%2F978-0-387-74733-0_9> accessed 22 September 2016;
- Carr, I. and Goldby, M. 'Recovering the Proceeds of Corruption: UNCAC and Anti-Money Laundering Standards' (2011) 2 *Journal of Business Law* 170;
- Cassella, S. D. 'An Overview of Asset Forfeiture in the United States', in Simon N. M. Young, *Civil Forfeiture of Criminal Property: Legal Measures for Targeting the Proceeds of Crime* (1st edn, Edward Elgar, 2009);
- Casella, S. D. 'Forfeiture of Terrorist Assets under the USA PATRIOT Act of 2001' (2002) 34 *Law and Policy in International Business* 7;
- Chodosh, H. E. 'Neither Treaty nor Custom: The Emergence of Declarative International Law' (1991) 26 TEX. INT'L L.J. 87;
- Choo, K-K. R., 'Money Laundering Risks of Prepaid Stored Value Cards' (Australian Institute of Criminology No. 363, 2008) 1, 2. Available at: <http://aic.gov.au/media_library/publications/tandi_pdf/tandi363.pdf> accessed 22 September 2016.
- Choo, K-K. R. 'New Payment Methods: A Review of 2010 - 2012 FATF Mutual Evaluation Reports' (2013) 36 *Computers and Security* 12;
- Chowdhry, A. 'Overstock.com Is Going To Accept Bitcoin in 2014' (Forbes, 21 December 2013) <http://www.forbes.com/sites/amitchowdhry/2013/12/21/overstock-com-is-going-to-accept-bitcoin-in-2014/?utm_campaign=techtwittersf&utm_source=twitter&utm_medium=social>;
- Chung, S. 'Criminalizing Money Laundering as a Method and Means of Curbing Corruption, Organised Crime and Capital Flight in Russia' (1999) 8(3) *Pacific Rim Law & Policy Journal Association* 617;
- Cole, M. 'Money Laundering' (1993) 8(4) *Journal of International Banking Law*, 129;

- Cordero, I. B. *El Delito de Blaqueo de* Capitals (3rd edn, Thomson Reuters Aranzadi, 2012), in: Miguel Abel Souto 'Money Laundering, New Technologies, FATF and Spanish Penal Reform' (2013) 16(3) *Journal of Money Laundering Control* 266
- Doyle, T. 'Cleaning Up Anti-Money Laundering Strategies: Current FATF Tactics Needlessly Violate International Law' (2002) 24 *Houston Journal of International Law* 279;
- The Economist (2001), 'Cheap and Trusted: Homing in on Networks of Informal Money Transfers' (2001). Available at: <www.economist.com/node/877145>;
- The Economist, 'Mobile Money in Africa: Press 1 for Modernity' (28 April 2012). Available at: <http://www.economist.com/node/21553510>;
- Fisher, J. 'Part 1 of the Serious Crime Act 2015: strengthening the Restraint and Confiscation Regime' (2015) 10 Criminal Law Review 754
- Fisher, J. and Bewsey, J. 'Laundering the Proceeds of Fiscal Crime' (2000) 15(1) J.I.B.L. 11;
- Fisher, J. 'Recent development in the fight against money laundering' (2002) 17(3) Journal of International Banking Law 67;
- Freeman, M. D. *Lloyd's Introduction to Jurisprudence* (8th edn, Sweet and Maxwell Limited, 2008);
- Forbes, Q2 2015 US Banking Review: Total Deposits, September 1st 2015 available at <www.forbes.com/sites/greatspeculations/2015/9/01/q2-2015-u-s-banking-review-total-deposits/#4e2f6dcf1e7d>;
- Gallivan, J. 'First Bitcoin ATM to Debut in NYC' (New York Post, 12 January 2014) <http://nypost.com/2014/01/12/first-bitcoin-atm-to-debut-in-nyc/>;
- Geary, J. 'Light is the best antidote', Journal of Money Laundering Control, 12(3), 215;
- Gentle, S. Spinks, G. and Harris, T. 'Legislative Comment, Proceeds of Crime Act 2002: Update' (2016) 139 (Sep) Compliance Officer Bulletin 1;
- Gilmore, W. C. *Dirty Money – The Evaluation of International Measures to Counter Money Laundering and the Financing of Terrorism* (3rd edn, Council of Europe Publishing, 2004);
- Glenn, H. P. 'The Aims of Comparative Law, in: J.M.Smits, Elgar Encyclopedia of Comparative Law (1st edn., Cheltenham; Edward Elgar, 2006);
- Gongloff, M. 'So, Bitcoin is Crashing' (Huffington Post 12 June 2013). Available at: <http://www.huffingtonpost.com/2013/12/06/bitcoin-crashes_n_4400392.html>;
- Greenberg, A. 'FBI Says It's Seized $28.5 Million in Bitcoins from Ross Ulbricht, Alleged Owner of Silk Road' (Forbes, 25 October 2013) <http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/#3f56f1161440>;
- Grono, S. 'Civil Forfeiture – The Australian Experience', in Simon N. M. Young, *Civil Forfeiture of Criminal Property – Legal Measures for Targeting the Proceeds of Crime* (1st edn, Edward Elgar, 2009);
- Gurung, J, Wijaya, M and Rao, A. 'AMLCTF compliance and SMEs in Australia: A Case Study of the Prepaid Card Industry' (2010) 13(3) Journal of Money Laundering Control 184

- Hardister, A. 'Can We Buy Peace on Earth?: The Price of Freezing Terrorist Assets in a Post-September 11 World' (2003) 28 *North Carolina Journal of International Law and Commercial Regulation* 601;
- Higgins, R. 'The Role of Resolutions of International Organisations in the Process of Creating Norms in the International System', in William .E. Butler, *International Law and the International System* (1st ed., Martinus Nijhoff Publishers 1987);
- The Hindu Times, 'Vietnam Bans Bitcoin' (28 February 2014). Available at: <http://www.thehindu.com/business/vietnam-bans-bitcoin/article5736019.ece>;
- Hopton, D. *Money Laundering: A Concise Guide for All Businesses* (1st edn, Gower, 2009), 33; and Steven Mark Levy, *Federal Money Laundering Regulation: Banking Corporate and Securities Compliance* (1st edn, Aspen Publishers, 2003);
- Irwin, A. S. M, Choo, K-K. R and Liu, L. 'An Analysis of Money Laundering and Terrorist Financing Typologies' (2011) 15(1) Journal of Money Laundering Control 85;
- Johnson, B. T. 'Restoring Civility – The Civil Asset Forfeiture Reform Act of 2000: Baby Steps Towards a More Civilized Civil Forfeiture System' (2002) *35 Indiana Law Review* 1045;
- Johnston, M. *Consent and Commitment in the World Community: The Classification and Analysis of International Instruments (*1st ed., Brill| Nijhoff, 1997).
- Kemp, K. 'Mobile Payments: Current and Emerging Regulatory and Contracting Issues' (2013) 29 *Computer Law and Security Review* 175;
- Kennedy, A. 'Designing a Civil Forfeiture System: An Issues List for Policymakers and Legislators' (2006) 13(2) Journal of Financial Crime 132;
- Kirgis Jr., F. L. 'Customs on a Sliding Scale' (1987) 81 AJIL 146;
- Koh, J-M. *Suppressing Terrorist Financing and Money Laundering* (1st edn, Springer, 2011);
- Kyriakos-Saad, N. PNG, C. A. and Thony, J. F., 'Recent Developments in International Monetary Fund Involvement in Money Laundering and Combating the Financing of Terrorism Matters' <http://www.imf.org/external/np/leg/amlcft/eng/pdf/cdmfl_v4.pdf> accessed 22 September 2016;
- Kocka, J. 'The Use of Comparative History' in Ragnar Bjork, *Societies Made up of History: Essays in Historiography, Intellectual History, Professionalizations, Historical Social Theory and Proto-Industrialisation* (1st ed., Akedemitryck AB, Stockholm, 1996);
- Lacey, K. A. and George, B. C. 'Crackdown on Money Laundering: A Comparative Analysis of the Feasibility and Effectiveness of Domestic and Multilateral Policy Reforms (2003) 23(2) *Northwestern Journal of International Law & Business* 262
- Lee, T. B. This Senate Hearing is a Bitcoin Lovefest (The Washington Post, 18 November 2013) <https://www.washingtonpost.com/news/the-switch/wp/2013/11/18/this-senate-hearing-is-a-bitcoin-lovefest/> ;
- Levi, M. 'Evaluating the "New Policing": Attacking the Money Trail of Organised Crime' (1997) 30 *Australian and New Zealand Journal of Criminology* 1;
- Levi, M. 'Combatting the Financing of Terrorism: A History and Assessment of the Control of "Threat Finance"' (2010) 50(4) *British Journal Criminology* 650

- Levi, M. 'Crimes of Globalisation: Some Measurement Issues' in Matti Joutsen, 'New Types of Crime: Proceedings of the International Seminar Held in Connection with HEUNI's Thirtieth Anniversary' (1st edn, European Institute for Crime Prevention and Control, 2012);
- Levi, M. and Reuter, P. 'Money Laundering' (2006) 34 *Crime and Justice* 289;
- Liargovas, P. and Repousis, S. 'Underground Banking or Hawala and Greece-Albania Remittance Corridor' (2011) 14(4) *Journal of Money Laundering Control* 313;
- Lilley, P. *Dirty Dealing – The Untold Truth about Global Money Laundering* (3rd edn, Kogan Page, 2006);
- Leong, A. 'Assets Recovery under the Proceeds of Crime Act 2002: the UK Experience', in Simon N. M. Young, Civil Forfeiture of Criminal Property: Legal Measures for Targeting the Proceeds of Crime (1st edn, Edward Elar, 2009);
- Lijphart, A. P. 'Comparative Politics and the Comparative Method' (1971) 65(3) *American Political Science Review* 682; and Arend P. Lijphart, 'The Comparable-Case Strategy in Comparative Research' (1975) 8(2) *Comparative Political Studies* 158.
- Low, L. Tilen, H. and Adendschein, K. 'Country report: the US anti-money laundering system', in M. Pieth and G. Aiolfi (eds), *A comparative guide to Anti-money Laundering: A critical analysis of systems in Singapore, the Uk and USA* (Cheltenham: Edward Elgar, 2004), 346.
- MacNeil, C. 'Australian Anti-Money Laundering Reform in the International Context' (2007) 22(6) *Journal of International Banking Law and Regulation* 340;
- Maimbo, S. M. and Ratha, D. Remittances: Development Impact and Future Prospects (1st edn., World Bank Publications, 2004);
- Malik, S. and Fox-Brewster, T. 'Six Britons Arrested Over Silk Road 2.0 Amid Dark-Web Takedown' (The Guardian, 7 November 2014). Available at: <https://www.theguardian.com/technology/2014/nov/07/six-britons-arrested-silk-road-dark-web-takedown-online-drugs>;
- McCulloch, J. and Pickering, S 'Supressing the Financing of Terrorism – Proliferating State Crime, Eroding Censure and Extending Neo-Colonialism' (2005) 45 *British Journal of Criminology* 470;
- McCusker, R. 'Underground Banking: Legitimate Remittance Network or Money Laundering System?' (July 2005) 300 *Trends & Issues in Crime and Criminal Justice* 1, 2. Available at: <http://aic.gov.au/media_library/publications/tandi_pdf/tandi300.pdf>;
- McGarrity, N. 'The Criminalisation of Terrorist Financing in Australia' (2012) 38(3) Monash University Law Review 55;
- Menon, S. and Siew, T. G. 'Key Challenges in Tackling Economic and Cybercrimes: Creating a Multilateral Platform for International Co-operation' (2012) 15(3) *Journal of Money Laundering Control* 243;
- Merlonghi. G. 'Fighting Financial Crime in the Age of Electronic Money: Opportunities and Limitations' (2010) 13(3) *Journal of Money Laundering Control* 202;

- Mills, H. Skodbo, S. and Blyth, P. *Understanding Organised Crime: Estimating the Scale and Understanding the Social and Economic Costs* (Home office, October 2013). Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246390/horr73.pdf>;
- Mitsilegas, V. and Gilmore, B 'The EU legislative framework against money laundering and terrorist financing: a critical analysis in the light of evolving global standards (2007) 56(1) International & Comparative Law Quarterly 119;
- Moores, E. 'Restoring the Civil Asset Forfeiture Reform Act' (2009) 51 *Arizona Law Review* 777;
- Morais, H. V. 'Fighting International Crime and its Financing: The Importance of Following a Coherent Global Strategy Based on the Rule of Law' (2005) 50 *Villanova Law Review* 583;
- Morris-Cotterill, N. 'Money Laundering Update' (2006) 34 (March) *Compliance Officer Bulletin* 1;
- Nelson, S. 'The Supreme Court Takes a Weapon from the Drug War Arsenal: New Defences to Civil Drug Forfeiture' (1994) 26 *Saint Mary's Law Journal* 157;
- Padfield, N. 'Depriving Criminals of the Proceeds of Their Crimes (2016) 10 *Criminal Law Review 695;*
- Popa, C. 'Money Laundering using the internet and electronic payments' (2012) 17(8) *Metalurgia International* 219;
- Peck, M. E. 'Bitcoin: The Cryptoanarchists' Answer to Cash', (IEEE Spectrum, June 2012) <http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash>;
- Pieth, M. and Aiolfi, G. *A Comparative Guide to Anti-Money Laundering: A Critical Analysis of Systems in Singapore, Switzerland, the UK and the USA* (1st edn., Edward Elgar, 2004).
- Pieth, M. and Aiolfi, G. 'The Private Sector Becomes Active: The Wolfsberg Process' (2003) 10(4) J.F.C. 359
- Piller, G. and Zaccariotto, E. 'Cyber-Laundering: The Union Between New Electronic Payment Systems and Criminal Organisations' (2009) 16(1) *Transition Studies Review* 62;
- Podgor, E. S. 'Money Laundering and Legal Globalisation: Where Does the United States Stand on This Issue?' 5(1) Washington University Global Studies Law Review 151;
- Png, C. 'International Legal Sources I – The United Nations Conventions', in William Blair QC and Richard Brent, *Banks and Financial Crime – The International Law of Tainted Money* (1st edn, Oxford University Press, 2008);
- Prost, K. 'No Hiding Place – How Justice Need Not be Blinded by Borders', in Steven David Brown, *Combating International Crime: The Longer Arm of the Law* (1 edn, Routledge Cavendish, 2008);

- Provost, M. A. 'Money Laundering' (2009) 46(1) *American Criminal Law Review* 837;
- Putman, R. D. 'Diplomacy and Domestic Politics: The Logic of Two-level Games' (1988) 42(3) *International Organisation* 427;
- Radomyski, R 'What Problems Has Money Laundering Posed for the Law Relating to Jurisdiction?' (2010) 15(1) *Coventry Law Journal* 4;
- Ragin, C. C. *The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies* (1st edn., 1987, University of California Press, California);
- Raymond, N. 'U.S. Auctions Some 30,000 Bitcoins from Silk Road Raid' (Reuters, 27 June 2014) <http://www.reuters.com/article/us-bitcoin-auction-idUSKBN0F22LG20140628>;
- Reuter, P. and Truman, E. M. *Chasing Dirty Money* (1st edn, Peterson Institute for International Economics, 2005);
- Richard, A. C. *Fighting Terrorist Financing: Transatlantic Cooperation and International Institutions,* (1st edn, Centre for Transatlantic Relations, 2006), 6.
- Robinson, J. 'Laundrymen: Inside the World's Third Largest Business' (2nd edn, Pocket Books, 1998);
- Roth, J. Greenburg, D. and Wille, S. 'Monograph on Terrorist Financing' (Staff Report to the National Commission on Terrorist Attacks Upon the United States), 3. Available at: <http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf> ;
- Rosdol, A. 'Are OFCs Leading the Fight Against Money Laundering?' (2007) 10(3) *Journal of Money Laundering Control* 337;
- Ross, S. and Hannan, M. 'Australia's New Anti-Money Laundering Strategy' (2007) 19(2) *Current Issues in Criminal Justice* 135;
- Ryder, N. *Financial Crime in the 21st Century* (1st edn, Edward Elgar, 2011);
- Ryder, N. *Money Laundering: An endless cycle* (1st edn, Routledge 2012);
- Ryder, N. 'To Confiscate or Not to Confiscate? A Comparative Analysis of the Confiscation of the Proceeds of Crime Legislation in the United States of America and the United Kingdom' (2013) 8 *Journal of Business Law* 767;
- Ryder, N and Turksen, U. 'Islamophobia or an Important Weapon? An Analysis of the US Financial War on Terrorism' (2009) 10 *Journal of Banking Regulation* 307;
- Sartori, G. 'Comparing and Miscomparing' (1991) 3(3) *Journal of Theoretical Politics* 244.
- Sathye, M. 'Estimating the Cost of Compliance of AMLCFT for Financial Institutions in Australia' (2008) 15(4) *Journal of Financial Crime* 347;
- Sathye, M. and Islam, J. 'Adopting a Risk-Based Approach to AMLCTF Compliance: The Australian Case (2011) 18(2) Journal of Financial Crime 169;

- Schott, P. A. *Reference Guide to Anti-Money Laundering and Combatting the Financing of Terrorism* (2nd edn, World Bank / IMF, 2006);
- Schramm, M. and Taube, M. 'Evolution and Institutional Foundation of the Hawala Financial System' (2003) 12(4) *International Review of Financial Analysis* 405;
- Shelton, D. *Commitment and Compliance: The Role of Non-binding Norms in the International Legal System* (1st ed., OUP 2000);
- Shelton, D. 'Normative Hierarchy in International Law' [2006] 100 AM. J. Int'l L. 291;
- *Shillito, M. R. '*Countering Terrorist Financing via Non-Profit Organisations: Assessing why few States Comply with the International Recommendations' (2015) 6(3) *Nonprofit Policy Forum* 325;
- Shillito, M. and Stokes, R. *Governments want to regulate bitcoin – is that even possible?,* (The Conversation, March 26th 2015).
- Shillito, M. The Fall of Silk Road isn't the End for Anonymous Marketplaces, Tor or Bitcoin (The Conversation, June 2nd 2015);
- Solin, M. and Zerzan, A. *Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks*, (GSMA Discussion Paper, January 2010), available at: <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/09/amlfinal35.pdf>;
- Soloman, P. 'Are Money Launderers All Washed Up in the Western Hemisphere? The OAS Model Regulations' (1994) 17 *Hastings International and Comparative Law Review* 433;
- Souto, M. A. 'Money Laundering, New Technologies, FATF and Spanish Penal Reform' (2013) 16(3) *Journal of Money Laundering Control* 266;
- Sparkes, M. 'UK's First Bitcoin Cash Machine Launches in Shoreditch' (The Telegraph, 7 March 2014). Available at: <http://www.telegraph.co.uk/technology/10682842/UKs-first-Bitcoin-cash-machine-launches-in-Shoreditch.html>;
- Southall, E. and Taylor, M. 'Bitcoins' (2013) 19(6) C.T.L.R. 177, 178.
- Stokes, R. A. 'Anti-Money Laundering Regulation and Emerging Payment Technologies' (2013) 32 (5) *Banking and Financial Services Policy Report* 1;
- Stokes, R. A. 'Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar' (2012) 21(3) *Information & Communications Technology Law* 221;
- Sultzer, S. 'Money Laundering: The Scope of the Problem and Attempts to Combat It' (1995) 63 Tennessee Law Review 143;
- Sutton, G. W. 'The New FATF Standards' (2013) 4(1) Geo. Mason J. Int'l Com. Law 68;
- Teasdale, S. 'FSA to FCA; Recent Trends in UK Financial Conduct Regulation' (2011) 26(12) J.I.B.L.R. 583;
- Trautsolt, J. and Johnson, J. 'International Anti-Money Laundering Regulation of Alternative Remittance Systems: Why the Current Approach Does Not Work in Developing Countries' (2012) 15(4*) Journal of Money Laundering Control* 407;

- Tripathi, D and Misra, P *Towards a New Frontier: History of the Bank of Baroda*. (1st edn., Manohar Publications, 1985);
- Tsingou, E. 'Global Governance and Transnational Financial Crime: Opportunities and Tensions in the Global Anti-Money Laundering Regime' (2005) Centre for the Study of Globalisation and Regionalisation Working Paper. Available at: <http://wrap.warwick.ac.uk/1959/1/WRAP_Tsingou_wp16105.pdf>;
- Unger, B. *The scale and impacts of money laundering* (1st edn, Edward Elgar 2007);
- Unger, B and Waarden, F. 'How to Dodge Drowning in Data? Rule –and Risk – based Anti-Money Laundering Policies Compared' (2009) 5(2) *Review of Law and Economics* 953
- Van der Zahn, M. Makarenko, M. I. Tower, G. Kostyuk, A. Barako, D. Chervoniaschaya, Y Brown, A. and Kostyuk, H. 'The Anti-Money Laundering Activities of the Central Banks of Australia and Ukraine' (2007) 10(1) *Journal of Money Laundering Control*, 116–33
- Viles, T. 'Hawala, Hysteria and Hegemony' (2008) 11(1) *Journal of Money Laundering Control* 25, 28.
- Vittori, J. *Terrorist Financing and Resourcing* (1st edn, Palgrave Macmillan, 2011);
- Vicek, W. 'Development vs. Terrorism: Money Transfers and EU Financial Regulations in the UK' (2008) 10(2) *British journal of Politics and International Relations* 286
- Vlcek, W. 'Global Anti-Money Laundering Standards and Developing Economies: The Regulation of Mobile Money' (2011) 29(4) *Development Policy Review* 415;
- Wadsley, J. 'Money Laundering: Professionals as Policemen' (1994) July/August *Conveyancer and Property Lawyer* 275;
- Walters, J. Budd, C. Smith, R. G. Choo, K-K. R. McCusker, R. and Rees, D. Anti-Money Laundering and Counter-Terrorism Financing Across the Globe: A Comparative Study of Regulatory Action (AIC Reports, Research and Public Policy Series, 2011), 9. Available at: <http://www.aic.gov.au/media_library/publications/rpp/113/rpp113.pdf>;
- Wang, J. R. 'Regulating Hawala: A Comparison of Five National Approaches' (2011) 14(3) *Journal of Money Laundering Control* 210;
- Wile, 'What Is Litecoin: Here's What You Need to Know About The Digital Currency Growing Faster Than Bitcoin' (Business Insider, 27 November 2013) <http://www.businessinsider.com/introduction-to-litecoin-2013-11>;
- White, 'Australia', in Wouter H. Muller, Christian H. Kalin and John G. Goldsworth, *Anti-Money Laundering International Law and Practice* (1st edn, John Wiley & Sons, 2007);
- Zweigert, K. and Kotz, H. *An introduction to Comparative Law* (3rd edn, Oxford University Press, 2011).

Official Documents

ocuments

- APG, '2013 APG/EAG Joint Typologies and Capacity Building Workshop, 23–27 September, Ulaanbaatar, Mongolia' (September 2013) <http://www.apgml.org/events/details.aspx?e=309020bb-b42b-4ebf-8249-b2c7d3016bea>;
- Australian Criminal Intelligence Commission, 'About us' <https://www.acic.gov.au/about-us>;
- Australian Criminal Intelligence Commission, 'National Criminal Intelligence Fusion Capability' <https://www.acic.gov.au/about-crime/taskforces/national-criminal-intelligence-fusion-capability>;
- Australian Crime Commission, *Organised Crime in Australia 2009* (2010), 9;
- Attorney-General's Department, 'About us' <https://www.ag.gov.au/About/Pages/default.aspx>;
- Attorney-General's Department, 'Anti-Money Laundering Assistance' <https://www.ag.gov.au/Internationalrelations/InternationalLegalAssistance/Pages/AntimoneyLaunderingAssistance.aspx>;
- Attorney-General's Department (2004) Anti-Money Laundering Law Reform: Issues Paper 1, Financial Services Sector Canberra, Attorney General's Department.
- Attorney-General Department, *National Organised Crime Response Plan 2015-18* (2015). Available at: <https://www.ag.gov.au/CrimeAndCorruption/OrganisedCrime/Documents/NationalOrganisedCrimeResponsePlan2015-18.pdf>;
- Australian Government, 'Australian National Security' <https://www.nationalsecurity.gov.au/Securityandyourcommunity/Pages/National-Terrorism-Threat-Advisory-System.aspx>;
- Australian Government, Attorney General's Department, 'Anti-Money Laundering and Counter Terrorism Financing' <https://www.ag.gov.au/CrimeAndCorruption/AntiLaunderingCounterTerrorismFinancing/Pages/default.aspx>;
- Australian Government, Department of Foreign Affairs and Trade, 'United Nations (UN)' <http://dfat.gov.au/international-relations/international-organisations/un/pages/united-nations-un.aspx>;
- The Australian Government the Treasury, *Australian Government Response to the Senate Economics References Committee Report: Digital Currency* (May 2016) <http://www.treasury.gov.au/~/media/Treasury/Publications%20and%20Media/Publications/2016/Gov%20response%20to%20Digital%20Currency/Downloads/PDF/Government_response_Senate-Committee_Digital-Currency-report-prod.ashx>;
- Australian National Security, 'National Terrorism Threat Advisory System', <https://www.nationalsecurity.gov.au/Securityandyourcommunity/Pages/National-Terrorism-Threat-Advisory-System.aspx>;

- Australian Taxation Office, 'ATO Delivers Guidance on Bitcoin' (QC 42160, 20 August 2014) <https://www.ato.gov.au/Media-centre/Media-releases/ATO-delivers-guidance-on-Bitcoin/>;

- Australian Transaction Reports and Analysis Centre, 'About Us' < <http://www.austrac.gov.au/about-us/international-engagement/international-organisations>;
- Australian Transaction Reports and Analysis Centre, *AUSTRAC Annual Report 2014-2015* (2015), 6. Available at: <http://www.austrac.gov.au/sites/default/files/austrac-ar-14-15-web.pdf>;
- Australian Transaction Reports and Analysis Centre, 'International Assistance and Training' <http://www.austrac.gov.au/about-us/international-engagement/international-assistance-and-training>;
- Australian Transaction Reports and Analysis Centre, 'International Organisations' <http://www.austrac.gov.au/about-us/international-engagement/international-organisations>;
- AUSTRAC, Money laundering in Australia 2011 (2011), 2. Available at: <http://www.austrac.gov.au/files/money_laundering_in_australia_2011.pdf>;
- Australian Transaction Reports and Analysis Centre, Parliamentary Joint Committee on Law Enforcement: Inquiry into Financial Related Crime, Australian Transaction Reports and Analysis Centre Submission (May 2014), 38. Available at: <http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Financial_related_crime/~/media/Committees/le_ctte/Financial_related_crime/report.pdf>;
- Australian Transaction Reports and Analysis Centre, 'Task Force Eligo' <http://www.austrac.gov.au/sites/default/files/documents/eligo_fact_sheet.pdf>;
- Australian Transaction Reports and Analysis Centre, *Terrorism Financing in Australia 2014* (2014). Available at: <http://www.austrac.gov.au/sites/default/files/documents/terrorism-financing-in-australia-2014.pdf>;
- Australian Transaction Reports and Analysis Centre, *Terrorism Financing South-East Asia & Australia, Regional Risk Assessment 2016* (2016). Available at: <http://www.austrac.gov.au/sites/default/files/regional-risk-assessment-SMALL_0.pdf>;
- Australian Transaction Reports and Analysis Centre, *AUSTRAC Typologies and Case Studies Report 2013* (2013). Available at: <http://www.austrac.gov.au/sites/default/files/documents/typ13_full.pdf>;
- BCBS, 'Consolidated know your Customer (KYC) Risk Management' (2004) <http://www.bis.org/publ/bcbs110.pdf>;
- BCBS, 'Customer Due Diligence for Banks' (2001) <http://www.bis.org/publ/bcbs85.htm>;

- BCBS, 'Prevention of Criminal Use of the Banking system for the Purpose of Money-Laundering' (December 1988) <http://www.bis.org/publ/bcbsc137.pdf>;
- British Bankers' Association, 'BBA Brief – 4 February 2016', available at: <https://www.bba.org.uk/news/bba-brief/bba-brief-4-february-2016/#.V8y6l_krKUk>;
- British Bankers' Association, 'Divorcing Blockchain from Bitcoin', available at: <https://www.bba.org.uk/news/insight/divorcing-blockchain-from-bitcoin/#.V8y5DfkrKUk>;
- Charity Commission, *Protecting Charities from Harm: Compliance Toolkit – Chapter 1, Module 1* (2013), 3. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/396183/CT-1-M1.pdf>;
- Comptroller and Auditor General, "Confiscation Orders" HC738 Session 2013-2014, 17 December 2013;
- Department of Foreign Affairs and Trade, 'Consolidated List' <http://dfat.gov.au/international-relations/security/sanctions/Pages/consolidated-list.aspx>;
- Department of Justice, 'Asset Forfeiture and Money Laundering Section (AFMLS)' <https://www.justice.gov/criminal-afmls>;
- Department of Justice, 'Asset Forfeiture Program' <https://www.justice.gov/afp>;
- Department of Justice, 'Counterterrorism Section' <https://www.justice.gov/nsd/counterterrorism-section>
- Department of Justice, 'Participants and Roles' <https://www.justice.gov/afp/participants-and-roles>;
- Department of State, '2015 Agency Financial Report: Advancing America's Interests through Global Leadership and Diplomacy' (16 November 2015) 7 <http://www.state.gov/documents/organization/249770.pdf>;
- Department of State, 'Bureau of Economic and Business Affairs' <http://www.state.gov/e/eb/>
- Department of State, Bureau for International Narcotics and Law Enforcement Affairs, *International Narcotics Control Strategy Report Volume II Money Laundering and Financial Crimes* (March 2010), 223. Available at: <http://www.state.gov/documents/organization/137429.pdf>;
- Department of State, 'DEA: Money Laundering' <https://www.dea.gov/ops/money.shtml>;
- Department of State, 'DEA History' <https://www.dea.gov/about/history.shtml>;
- Department of State, 'Mission' <http://www.state.gov/j/ct/about/mission/index.htm>;
- Department of State, 'DEA Mission Statement' <https://www.dea.gov/about/mission.shtml>;
- Department of State, 'Who We Are' <http://www.state.gov/j/ct/about/>;

- Department of Treasury, 'About: Terrorism and Financial Intelligence'<https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx>;
- Department of Treasury, 'About: Terrorism and Financial Intelligence: Terrorist Financing and Financial Crimes' <https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorist-Financing-and-Financial-Crimes.aspx>;
- Department of the Treasury, 'Joint Treasury and US Mission to the United Nations Fact Sheet: UN Security Council Meeting of Finance on Countering the Financing of Terrorism', available at: <https://www.treasury.gov/press-center/press-releases/Pages/jl0307.aspx>;
- Department of the Treasury, National Money Laundering Risk Assessment (2015), 93. Available at: <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf>;
- Department of Treasury, 'Office of Foreign Assets Control: Specially Designated Nationals and Blocked Persons List' (September 2016) <https://www.treasury.gov/ofac/downloads/sdnlist.pdf>;
- Department of Treasury, 'Resource Center' <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/Money-Laundering.aspx>;
- Department of Treasury, 'Strategic Direction Fiscal Years 2012-2015', 3 <https://www.treasury.gov/about/organizational-structure/offices/Documents/Strategic%20Direction%2008-13-12.pdf>;
- Egmont Group, 'Annual Report 2014-2015' (2015). Available at <http://www.egmontgroup.org/library/annual-reports>;
- Egmont Group, 'Interpretive Note Concerning the Egmont Definition of a Financial Intelligence' (2004) <*www.egmontgroup.org/library/download/8>;*
- Egmont Group, 'Summary Strategic Plan 2014-2017' (2014), 1 <*www.egmontgroup.org/library/download/355>;*
- The Egmont Group, 'Strategic Plan 2014-2017' (May 2015).
- European Commission, 'Financial Crime' <http://ec.europa.eu/justice/civil/financial-crime/index_en.htm>;
- Egmont Group of Financial Intelligence Unites, Annual Report 2014-2015 (2015), 16. Available from: <http://www.egmontgroup.org/library/annual-reports>;
- European Commission, 'Frequently Asked Questions: Anti-Money Laundering' <http://europa.eu/rapid/press-release_MEMO-13-64_en.htm?locale=en>;
- European Commission – Press Release: Commission Presents Action Plan to Strengthen the Fight Against Terrorist Financing' (2 February 2016) <http://europa.eu/rapid/press-release_IP-16-202_en.htm>;
- European Commission, 'Register of Commission Expert Groups and Other Similar Entities: Expert Group on Money Laundering and Terrorist Financing (E02914)' (11 May 2015) <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2914&Lang=EN>;

- FBI, Department of Justice, 'FBI: About'<https://www.fbi.gov/about>;
- FBI, Department of Justice, 'FBI: A Brief History' <https://www.fbi.gov/history/brief-history>;
- FBI, Department of Justice, 'FBI Revamps Money Laundering Investigations' (March 2016) <https://www.fbi.gov/audio-repository/news-podcasts-thisweek-fbi-revamps-money-laundering-investigations.mp3/view>;
- FBI, Department of Justice, 'FBI: History: Timeline' <https://www.fbi.gov/history/timeline>;
- FBI, Department of Justice, 'Intelligence Assessment: (U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity' (24 April 2012) <https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf>;
- Financial Action Task Force, Annual Report 1995 – 1996 (June 1996). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/1995%201996%20ENG.pdf>;
- Financial Action Task Force, *Annual Report 2004 – 2005* (June 2005), Foreword. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2004%202005%20ENG.pdf>;
- Financial Action Task Force, *Annual Report 2007 – 2008* (June 2008), i. Available at: < http://www.fatf-gafi.org/media/fatf/documents/reports/2007-2008%20ENG.pdf>;
- Financial Action Task Force, *Annual Report 2009 – 2010* (July 2010), 19. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2009%202010%20ENG.pdf>;
- Financial Action Task Force, *Annual Report 2010 – 2011* (June 2011), 13. Available at: < http://www.fatf-gafi.org/media/fatf/documents/reports/FORMATTED%20ANNUAL%20REPORT%20FOR%20PRINTING.pdf>;
- Financial Action Task Force, *Emerging Terrorist Financing* Threats (October 2015) <http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf> accessed 22 September 2016;
- Financial Action Task Force, 'Financial Action Task Force on Money Laundering: Annual Report 2001–2002' (June 2002), 2. Available at <http://www.fatf-gafi.org/media/fatf/documents/reports/2001%202002%20ENG.pdf>;
- Financial Action Task Force, *FATF Annual Report 2007 – 2008* (June 2008), annex. Available at: <http://www.oecd.org/dataoecd/58/0/41141361.pdf>;
- Financial Action Task Force, 'Frequently Asked Questions' <http://www.fatf-gafi.org/faq/moneylaundering/>;
- Financial Action Task Force, 'FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion' (Report, February 2013) 29 <https://perma.cc/RN8Y-98Q9>;

- Financial Action Task Force, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (June 2013), 3. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf>;
- Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (June 2015). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>;
- Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (February 2012, update June 2016), 7. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf>;
- Financial Action Task Force, 'Members and Observers' <http://www.fatf-gafi.org/pages/aboutus/membersandobservers/>;
- Financial Action Task Force, 'Methodology: For Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems' (February 2013). Available at <http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf>;
- Financial Action Task Force, 'Money Laundering through Money Remittance and Currency Exchange Providers' (June 2010) <http://www.fatf-gafi.org/media/fatf/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf>;
- Financial Action Task Force, *Money Laundering Using New Payment Methods* (October 2010), 66. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>;
- Financial Action Task Force, *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems* (June 2008). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20TF%20Vulnerabilities%20of%20Commercial%20Websites%20and%20Internet%20Payment%20Systems.pdf>;
- Financial Action Task Force, Money Laundering Through Money Remittance and Currency Exchange Providers (June 2010). Available at: <http://www.fatf-gafi.org/media/fatf/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf> accessed 22 September 2016; and Financial Action Task Force, *Guidance for a Risk-Based Approach Money or Value Transfer Services* (February 2016). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf>;
- Financial Action Task Force, 'National Money Laundering and Terrorist Financing Risk Assessment' (February 2013). Available at: <http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf>;

- Financial Action Task Force, *Report on Money Laundering Typologies 2002 – 2003* (February 2003), 6-7. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2002_2003_ML_Typologies_ENG.pdf>;
- Financial Action Task Force, *Money Laundering & Terrorist Financing Typologies 2004 – 2005* (June 2005), 3. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2004_2005_ML_Typologies_ENG.pdf>;
- Financial Action Task Force, *Report on New Payment Methods* (October 2006). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf>;
- Financial Action Task Force, *The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing* (October 2013) <http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf>;
- Financial Action Task Force, Third Mutual Evaluation Report on Anti-Money Laundering and Combatting the Financing of Terrorism, Australia (October 2005). Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Australia%20full.pdf>;
- Financial Action Task Force, *FATF Third Mutual Evaluation Report: Anti-Money Laundering and Combatting the Financing of Terrorism, The United Kingdom of Great Britain and Northern Ireland* (June 2007), 15. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20UK%20FULL.pdf>;
- Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Countering the Financing of Terrorism, United States of America* (June 2006), 14. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20US%20full.pdf>;
- Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* (June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>;
- Financial Action Task Force, *Vulnerabilities of Casinos and Gaming Sector* (March 2009) <http://www.fatf-gafi.org/media/fatf/documents/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf>;
- Financial Action Task Force on Money Laundering: report of 6 February 1990, reproduced in William C. Gilmore, *Dirty Money – The Evaluation of International Measures to Counter Money Laundering and the Financing of Terrorism* (3rd edn, Council of Europe Publishing, 2004);
- Financial Action Task Force, 'United States' available at: <http://www.fatf-gafi.org/countries/#United States>;
- Financial Conduct Authority, 'Financial Crime', available at: <https://www.fca.org.uk/firms/financial-crime>;
- FCA, 'Disruptive Innovation in Financial Markets' (October 2015) <https://www.fca.org.uk/news/speeches/disruptive-innovation-financial-markets>;

- FCA, 'Innovation: The Regulatory Opportunity' (October 2014, updated November 2014) <https://www.fca.org.uk/news/innovation-the-regulatory-opportunity>;
- Financial Conduct Authority, 'Thematic review: Mobile banking and payments' (September 2014) <https://www.fca.org.uk/static/documents/thematic-reviews/tr14-15.pdf>;
- FCA, 'Payment Systems Regulator Limited: Annual Report and Accounts 2015/2016' (HC 386, 12 July 2016) 30 <https://www.psr.org.uk/sites/default/files/media/PDF/PSR-annual-report-2015-2016.pdf>;
- FCA, 'The FCA's Risk Based Approach to AML Supervision' (CNBV Workshop on AML and CFT, Mexico City, 8-9 September) <http://www.cnbv.gob.mx/PrevencionDeLavadoDeDinero/Documents/Presentation%20for%20Mexico%20City%20workshop%20FINAL%2020150901.pdf>;
- FinCEN, 'Mission' <https://www.fincen.gov/about/mission>;
- Financial Crimes Enforcement Network, *Application of FinCEN's regulations to Persons Administering, Exchanging, or using Virtual Currencies 1* (2013) <http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf>;
- Financial Crimes Enforcement Network, Prepared remarks of James H. Freis, Jr, Kewellers Vigilance Committee AML Seminar, 10 March 2008. Available at: <https://www.fincen.gov/news/speeches/prepared-remarks-james-h-freis-jr-director-financial-crimes-enforcement-network-3>;
- Financial Crimes Enforcement Network, 'Prepared Remarks of FinCEN Associate Director for Enforcement Thomas Ott, delivered at the National Title 31 Suspicious Activity and Risk Assessment Conference and Expo' (17 August 2016). Available at: <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-associate-director-enforcement-thomas-ott-delivered-national>;
- Financial Crimes Enforcement Network, *The Hawala Alternative Remittance System and its Role in Money Laundering*, 5. Available at: <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/FinCEN-Hawala-rpt.pdf>;
- Financial Crime Enforcement Network, 'William J Fox, Director, Financial Crime Enforcement Network: Women in Housing and Finance' (25 February 2004) <https://www.fincen.gov/news/speeches/william-j-fox-director-financial-crimes-enforcement-network-1>;
- FSA, 'Review of Firms' Implementation of a Risk-Based Approach to Anti-Money Laundering (AML)' (March 2008) <http://www.fca.org.uk/static/documents/fsa-aml-implementation-review.pdf>;
- Financial Services Authority, 'What is financial crime?' <www.fsa.gov.uk/pages/About/What/financial_crime/money_laundering/faqs/index.shtml>;
- Future Market Insights, 'Mobile Payment Transaction Services Market: Money Transfer & Merchandise Purchase Key Application Segments' (20 July 2015)

<http://www.futuremarketinsights.com/press-release/global-mobile-payment-transaction-market>;

- GAFISUD, 'Guide on New Payment Methods: Prepaid Cards, Mobile Payment and Internet Payment Services' (June 2013) <http://www.cocaineroute.eu/wp-content/uploads/2014/08/GUIDE-ON-NEW-PAYMENT-METHODS2.pdf>;
- General Accounting Office, *Money Laundering: Needed Improvements for Reporting Suspicious Transactions Are Planned* (1995), 2. Available at: <http://www.gao.gov/assets/160/155076.pdf>;
- General Accounting Office, 'Money Laundering: Extent of Money Laundering through Credit Cards is Unknown' (Washington, DC: General Accounting Office, 2002), 1. Available at: <http://www.gao.gov/assets/240/235231.pdf>;
- HM Government, *Serious and Organised Crime Strategy* (October 2013), 34. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf>;
- HM Revenue & Customs, 'Money Laundering Regulations: Money Service Business Registration' <https://www.gov.uk/guidance/money-laundering-regulations-money-service-business-registration>;
- HM Treasury, 'About Us', available at: <https://www.gov.uk/government/organisations/hm-treasury/about>;
- HM Treasury, 'Anti-Money Laundering and Counter Terrorist Finance Supervision Report 2010-11' (November 2011) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204350/amlctf_supervision_report_201011.pdf>;
- HM Treasury, Anti-Money Laundering and Counter Terrorist Finance Supervision Report 2014 – 2015 (May 2016). Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/525355/anti-money-laundering-counter-terrorist-report-2014-15.pdf>;
- HM Treasury, *Anti-Money Laundering Strategy* (2004) available at: <http://webarchive.nationalarchives.gov.uk/+/http:/www.hm-treasury.gov.uk/media/D57/97/D579755E-BCDC-D4B3-19632628BD485787.pdf>;
- HM Treasury, 'Appointment of the UK President of the Financial Action Task Force'. Available at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/534959/hmt_advisory_notice_june_2016.pdf>;
- HM Treasury, 'Digital Currencies: Call for Information' (3rd November 2014) <https://www.gov.uk/government/consultations/call-for-information-anti-money-laundering-supervisory-regime/call-for-information-anti-money-laundering-supervisory-regime>;
- HM Treasury, 'The Financial Challenge to Crime and Terrorism' (February 2007) <http://webarchive.nationalarchives.gov.uk/+/http:/www.hm-treasury.gov.uk/d/financialchallenge_crime_280207.pdf>;

- HM Treasury, Financial Services Bill receives Royal Assent, available at: <https://www.gov.uk/government/news/financial-services-bill-receives-royal-assent>;
- HM Treasury, *Policy Paper: Preventing Money Laundering* (June 2013). Available at: <https://www.gov.uk/government/publications/preventing-money-laundering/preventing-money-laundering>;
- HM Treasury, Report to the European Parliament and to the Council on the Application of the Directive 2005/60/EC on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing (June 2012). Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200634/fin_response_ec_report_application_directive_on_prevention_of_money_laundering_terrorist_financing.pdf>;
- HM Treasury and Home Office, 'Biggest reforms to Money Laundering Regime in Over a Decade' (21 April 2016). Available at: <https://www.gov.uk/government/news/biggest-reforms-to-money-laundering-regime-in-over-a-decade>;
- HM Treasury, 'Research and Analysis: Anti-Money Laundering and Counter Terrorist Finance Supervision Report' (Updated 26 May 2016) <https://www.gov.uk/government/publications/anti-money-laundering-and-counter-terrorist-finance-supervision-reports/anti-money-laundering-and-counter-terrorist-finance-supervision-report-2012-13>;
- HM Treasury and the Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (October 2015), 3. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf>;
- Home Office, *Requests for Mutual Legal Assistance in Criminal Matters: Guidelines for Authorities Outside of the United Kingdom* (12th Edition, 2015), 4. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415038/MLA_Guidelines_2015.pdf>;
- IMF, 'Anti-Money Laundering and Combating the Financing of Terrorism: Observations from the Work Program and Implications Going Forward – Supplementary Information' (August 2005) 18 <https://www.imf.org/external/np/pp/eng/2005/083105s.pdf>;
- [1] IMF, 'Anti-Money Laundering and Combating the Financing of Terrorism: Regional Videoconference: Central and West Africa Region—BCEAO (Banque Centrale des Etats de l'Afrique de L'Ouest), BEAC (Banque des Etats de l'Afrique Centrale), angola, Cape Verde, Democratic Republic of Congo, and Rwanda' (2003) <http://documents.worldbank.org/curated/en/879731468781780843/pdf/271850Anti1mon1entral010West0Africa.pdf>;
- IMF, Anti-Money Laundering / Combating the Financing of Terrorism: Technical Assistance on AML / CFT <http://www.imf.org/external/np/leg/amlcft/eng/aml3.htm>;

- International Monetary Fund, *Approaches to a Regulatory Framework for Formal and Informal Remittance Systems: Experiences and Lessons* (2005). Available at: <https://www.imf.org/external/np/pp/eng/2005/021705.pdf>;
- IMF, 'The IMF and the Fight Against Money Laundering and the Financing of Terrorism' (March 2016) <http://www.imf.org/external/np/exr/facts/aml.htm>;
- International Monetary Fund, 'Anti-Money Laundering / Combating the Financing of Terrorism – Topics' <http://www.imf.org/external/np/leg/amlcft/eng/aml1.htm>;
- IMF, 'Compliance with the AML / CFT International Standard: Lessons from a Cross-Country Analysis' (2011) WP/11/177, 11. Available at: <http://www.imf.org/external/pubs/ft/wp/2011/wp11177.pdf>;
- IMF Staff Discussion Note: Virtual Currencies and Beyond: Initial considerations' (SDN/16/03, January 2016) <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>
- IMF, 'Ongoing IMF Research Projects on Anti-Money Laundering / Combating the Financing of Terrorism: An Overview' (April 2007) <http://www.imf.org/external/np/leg/amlcft/eng/orpaml.htm>;
- IMF Working Paper: Oversight Issues in Mobile Payments' (WP/41/123, July 2014) <https://www.imf.org/external/pubs/ft/wp/2014/wp14123.pdf>;
- Inspector-General of Intelligence and Security, 'The Australian Intelligence Community' <https://www.igis.gov.au/australian-intelligence-community>;
- Joint Money Laundering Steering Group, 'Welcome to the Joint Money Laundering Steering Group Website', available at: <http://www.jmlsg.org.uk/>;
- Joint Money Laundering Steering Group, Prevention of Money Laundering / Combatting Terrorist Financing (2014 Revised Version), Part I 5.5.10 – 5.5.17. Available at: <http://www.jmlsg.org.uk/download/9803>;
- John Walker Consulting Services, *Estimates of the Extent of Money Laundering in and through Australia* (AUSTRAC, September 1995). Available at: <http://www.criminologyresearchcouncil.gov.au/reports/200304-33.pdf>;
- MI5, 'Threat Levels' <https://www.mi5.gov.uk/threat-levels>;
- Middle East & North Africa Financial Action Task Force, *Typology Report on "Existing / Emerging Cross Border Payment Methods and their vulnerabilities to ML/TF"* (2007), 2. Available at: <http://www.fiu.gov.om/files/TCBEng.pdf>;
- Money Laundering Threat Assessment Working Group, *US Money Laundering Threat Assessment (*December 2005), 20. Available at <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf>;
- Moneyval, 'Research Report: Criminal Money Flows on the Internet: Methods, Trends and Multi-Stakeholder Counteraction' (March 2012) <http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)6_Reptyp_flows_en.pdf>;
- National Commission on Terrorist Attacks on the United States, '9/11 Commission Report' (2004), 170. Available at: <http://govinfo.library.unt.edu/911/report/911Report.pdf>;

- The Home Office, The National Crime Agency: A Plan for the Creation of a National Crime Fighting Capability, London: Home Office, 2011.
- National Crime Agency, 'NCA Annual Plan 2015/2016 (2015), 4. Available at: <http://www.nationalcrimeagency.gov.uk/publications/541-nca-annual-plan-2015-16-v1-0/file>;
- NCA, 'National Crime Agency: Annual Report and Accounts' (HC 35, 13 July 2015) 30 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/444184/NCA_Annual_Report_2014-15__web_.pdf>;
- National Crime Agency, 'JMLIT Executive Summary of FTI Report', available at: <http://www.nationalcrimeagency.gov.uk/publications/708-jmlit-executive-summary-of-fti-report/file>;
- National Crime Agency, 'Joint Money Laundering Intelligence Taskforce', available at: <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit>;
- National Crime Agency, 'National Strategic Assessment of Serious and Organised Crime 2015' (23rd June 2015) <http://www.nationalcrimeagency.gov.uk/publications/560-national-strategic-assessment-of-serious-and-organised-crime-2015/file>;
- National Crime Agency, 'What We Do', available at: <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do>;
- National Crime Agency, 'What We Do: Economic Crime Command', available at: <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime>;
- Organisation for Economic Co-operation and Development, 'Budget' <http://www.oecd.org/about/budget/>;
- Organisation for Economic Co-operation and Development, 'Financial Statements of the Organisation for Economic Co-operation and Development as at 31 December 2015' (23 June 2016), 47. Available at: <http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=BC(2016)20&docLanguage=en>;
- Security Council Counter-Terrorism Committee, 'About the Counter-Terrorism Committee' <https://www.un.org/sc/ctc/about-us/>;
- Terrorist Financing Convention 1999, Preamble. Available at: <http://www.un.org/law/cod/finterr.htm>;
- Topical Trust Fund, 'Anti-Money Laundering / Combating the Financing of Terrorism' (April 2009) <http://www.imf.org/external/np/otm/2009/anti-money.pdf>;
- The United Nations Association – UK, 'What is the United Nations?' <http://www.una.org.uk/content/what-un>;
- United Nations Counter-Terrorism Implementation Task Force, 'Tackling the Financing of Terrorism' (CTITF Working Group Report, October 2009), ii. Available at: <http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_financing_eng_final.pdf>;
- United Nations Office on Drugs and Crime, *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organised Crimes (Research report)*

(October 2011), 5. Available at: <http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf>;

- United Nations Office on Drugs and Crime, 'Illicit Money: How Much is Out There?' <http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html>;
- United Nations Office on Drugs and Crime, 'Money Laundering and the Financing of Terrorism: The United Nations Response', 20. Available at: <http://www.imolin.org/pdf/imolin/UNres03e.pdf>;
- United Nations Office on Drugs and Crime, Political Declaration and Plan of Action on International Cooperation Towards an Integrated and Balanced Strategy to Counter the World Drug Problem (High-Level Segment Commission, March 2009), iii. Available at: <https://www.unodc.org/documents/ungass2016/V0984963-English.pdf>;
- United Nations Office on Drugs and Crime, 'Technical Assistance Against Money-Laundering' <https://www.unodc.org/unodc/en/money-laundering/technical-assistance.html>;
- United Nations Office on Drugs and Crime, 'United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988' <https://www.unodc.org/unodc/en/treaties/illicit-trafficking.html>;
- US Department of Homeland Security, 'National Terrorism Advisory System Bulletin' (15 June 2016). Available at <https://www.dhs.gov/sites/default/files/ntas/alerts/16_0615_NTAS_bulletin.pdf>
- US Department of State*, International Narcotics Control Strategy Report: Mobile Payments a Growing Threat* (March 2008). Available at: <http://www.state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm>
- United States Government Accountability Office, *Report to Congressional Requesters, Moving Illegal Proceeds: Challenges Exist in the Federal Government's Effort to Stem Cross-Border Currency Smuggling* (October 2010), 2. Available at: <http://www.gao.gov/new.items/d1173.pdf>
- The White House (Office of the Press Secretary), 'Fact Sheet: Obama Administration Announces Steps to Strengthen Financial Transparency, and Combat Money Laundering, Corruption and Tax Evasion' <https://www.whitehouse.gov/the-press-office/2016/05/05/fact-sheet-obama-administration-announces-steps-strengthen-financial>
- Wolfsberg Group, 'Comment letter on the FATF consultation process', (6th January 2011), 1 <http://www.wolfsberg-principles.com/pdf/Wolfsberg_Group_Comment_Letter_on_FATF_Consultation_Paper_Jan-6th-2011_unsigned.pdf>;
- Wolfsberg Group, 'Global Banks: Global Standards' 2012 <http://www.wolfsberg-principles.com/>;
- Wolfsberg Group, 'The Wolfsberg Global Anti-Money Laundering Guidelines for Private Banking' (2002) <http://www.wolfsberg-principles.com/pdf/Wolfsberg_AML_Guidelines_for_PB_(2002).pdf>;

- Wolfsberg Group, 'Wolfsberg Anti-Money Laundering Principles for Correspondent Banking' (2014) <http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg-Correspondent-Banking-Principles-2014.pdf>;
- Wolfsberg Group, 'Wolfsberg Guidance on Mobile and Internet Payment Services (MIPS)' (2014) <http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg-Group-MIPS-Paper-2014.pdf>;
- The Wolfsberg Group, *Wolfsberg Guidance on Prepaid and Stored Value Cards* (2011), 2. Available at: <http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14,_2011.pdf>;
- The World Bank, *Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide* (2009), 12. Available at: <http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/CombattingMLandTF.pdf>.

Appendix

Digital currencies: Call for information

Robert Stokes (Lecturer in Law) and Matthew Shillito (Doctoral Researcher)

The School of Law and Social Justice, University of Liverpool

Question 1: What are the benefits of digital currencies? How significant are these benefits? How do these benefits fall to different groups e.g. consumers, businesses, government, the wider economy? How do these benefits vary according to different digital currencies?

Digital currencies offer a number of advantages to business and consumers, many of which derive from the challenges they pose to some of the fundamental assumptions which underpin our conception of money e.g. decentralised issue, use of cryptography without a third-party to solve the 'double-payment' problem etc. In brief, we identify the key benefits of digital currencies for merchants and consumers to be:

(1) Global application

Digital currencies have the technical ability to act as a de facto global currency. Digital currencies are not limited by geographical area, whether country or region, and allow for payments to be made without regard to international borders. The only limitation on this would be those of end-user technology limitations and the current lack of general acceptance amongst retailers. As digital currencies become accepted more widely, something that would be thought likely with regulatory intervention, end-user adoption is likely to spread and in turn the commercial incentive to solve the technology problem increases. A similar pattern can be identified with regard to the development of M-PESA as a payment mechanism via mobile devices.

(2) Quick transaction times

Transaction times for digital currencies are swift. Clearance is usually received within 5 minutes. In relation to Bitcoin, for example, in 2014 the average transaction confirmation time has been between 6 to 9 minutes.[5] In contrast, transfers using the standard banking systems tend to receive confirmation over a longer time frame, e.g. BACS takes 3 working days to clear; CHAPS is same day for instructions made before 2pm; and the Faster Payments service, will take up to two hours. Moreover, digital currency is not restricted by banking hours. In essence, the user is in full control of their money.

(3) Low transaction costs

A key feature of digital currencies is their low transaction fees, for example, within Bitcoin the transaction fee, when applied, is charged at 0.0005 BTC irrespective of value. As at December 2, 2014, that equates to $0.19 (with a BTC valued at $382.59). Fees may also payable to merchant processor at the point of conversion into fiat currency. As this separate process (between merchant and merchant processor) also utilises the Bitcoin system, the associated transaction fees are lower than other payment systems like PayPal and Western Union.

In contrast it is worth noting that for users with access to the traditional financial systems, BACS is free but limited to under £10,000. CHAPS transfers cost around £20. Faster Payments are also free (but are subject to institution limits).

(4) Security in transactions

Security is a key feature of digital currencies, particularly those like Bitcoin which are based on the blockchain system. Bitcoin and many other similar digital currencies operate on the basis of a 'push' system. This means that the value is transferred to the

[5] Average transaction confirmation time: <https://blockchain.info/charts/avg-confirmation-time>

merchant, but they have no further control.[6] There is no ability for the merchant to re-charge the account. Conversely, the merchant in turn has additional security over alternative payment mechanisms where 'charge-backs' (e.g. credit cards) are possible for a substantial period of time following the transaction. Bitcoin transactions are secure, irreversible, and do not contain customers' sensitive or personal information.

(5) Enhanced Information Security

Further, there is no identifiable material attached to a Bitcoin, meaning that the merchant has no database of customer information that can be targeted by hackers for the purposes of theft or identity theft.

(6) Security in Storage of Value

Whilst it may be acknowledged that there are a number of deficiencies in digital currencies with regard to security of stored value (for both businesses and consumers alike), e.g. volatility of exchange rates, cyber-risks around encryption keys being 'hacked' or otherwise compromised, it is clear that in comparison to other payment methods digital currencies have utility around the security they offer e.g. no large cash sums requiring special security procedures for business, security for consumers in avoiding the need to carry large sums of cash etc.

(7) Transparency

Perhaps counter-intuitively given the anonymity concerns surrounding the operation of some digital currencies, they offer unprecedented levels of transparency. All information concerning transactions is available on the public ledger for anybody to use and verify. As previously noted, for decentralised digital currencies, given they are not particularly susceptible to manipulation by a single entity. This level of trust within digital currencies is further enhanced by the use of cryptography to secure transactions and key information and it is likely in many cases, also by the fact that digital currencies are not part of the traditional financial 'establishment'.

Significance of the benefits

Where a currency is not backed by an asset e.g. gold, nor underpinned by guarantee (e.g. by a central state issuer) the adoption of that currency is in a very significant way driven by the benefits it offers users, whether businesses or individuals. Using Bitcoin as an example, the benefits are clearly significant enough to warrant 100,786 unique transactions[7] of 8,116.67 Bitcoins (hereafter BTCs) on the 2nd of December 2014.[8] At the current exchange rate that equates to over $3,000,000 transferred in the last 24 hours. The significance of this cannot be understated, and whilst the future of Bitcoin specifically is unknowable, points to substantial interest in the use of digital currency as an alternative to other currencies or payment mechanisms, albeit not, perhaps in the UK at present (e.g. a recent YouGov survey indicated that 71% of respondents were not interested in digital currencies).

[6] Credit cards for instance are the inverse. They operate on the basis of a 'pull' system. Customers agree to merchants taking money from their account by providing them with the necessary data to access the account.

[7] <https://blockchain.info/charts/n-transactions?timespan=30days&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=>

[8] <http://www.bitcoinwatch.com/>

Question 2: Should the government intervene to support the development and usage of digital currencies and related businesses and technologies in the UK, or maintain the status quo? If the government were to intervene, what action should it take?

In the UK specifically, it is unclear to us what the imperative would be for the Government to directly support the *development* of digital currencies. Certainly, digital currencies have the potential to fulfil a social good, e.g. around the unbanked, however, with regard to the relatively small percentage of unbanked persons within the UK, it is by no means clear that digital currencies are the solution in our case. This may be contrasted with populations where the causes (and extent) of individuals not having access to banking services is more amenable to useful intervention through the development of digital currencies. The potential, for example, for a digital currency such as Bitcoin to develop so as to facilitate financial inclusion where more formal financial systems have struggled is potent e.g., in Africa where 80% of the adult population are unbanked.[9] The Bitcoin structure would be easier to implement; fundamentally requiring only improved access to the internet and compatible devices.

One matter which should form a key part of the Government's response here is to invest in education. This can be done in two main ways: first, investment in skills; and second investment in educating the public as to the use of digital currencies and risks thereof. Digital currencies and the blockchain technology which underpins them, represent a significant opportunity to further the technology and information based economies within the UK. This point will be addressed further below but in short, the technology has implications far beyond digital currencies, e.g. self-executing contracts using blockchain technology. The key is not to stifle innovation by over regulation/intervention whilst also ensuring that where consumers (in particular) utilise digital currencies, they do so fully aware of the advantages and risks, just as is the case for currency (or payment mechanisms) generally. Regulatory intervention is necessary here, but the nature of the intervention must be appropriate to the specific risks it is intended to mitigate. In the case of digital currencies, we would identify the core drivers for intervention by Government to be limited to (i) consumer protection and (ii) financial (and other) crime risks.

It should also be recognised that whilst there may be 'unintended' consequences of regulatory intervention, e.g. costs, which will ultimately reduce current advantages of digital currencies, i.e. transaction costs will rise particularly with regard to third-party services, this may be a necessary step in the development of digital currencies. With regulation comes legitimacy and increased uptake and usage ought to follow where regulatory measures increase consumer (and business) confidence in digital currencies. This may be thought of as a crucial step in the evolution of digital currencies, albeit one which has potential negative impacts and may be thought of by some users as contrary to the principles on which some digital currencies were developed (e.g. Bitcoin).

Question 3: If the government were to regulate digital currencies, which types of digital currency should be covered? Should it create a bespoke regulatory regime, or regulate through an existing national, European or international regime? For each option: what are the advantages and disadvantages? What are the possible unintended consequences (for instance, creating a barrier to entry due to compliance costs)?

[9] < http://www.mckinsey.com/insights/financial_services/counting_the_worlds_unbanked >

When considering regulatory responses to any phenomenon, Government must consider two potentially conflicting interests: on the one hand, Government should encourage an environment suitable for innovation to flourish whilst, on the other, it should ensure that firms performing similar functions are regulated in similar ways. All of this must be done in such a way as to protect the consumer and, potentially in the case of digital currencies, the financial system more broadly. The challenge to be overcome here is that of how to effectively regulate digital currencies when one considers the key features, e.g. decentralised architecture, no inherent value or guarantee of value, pseudo-anonymity etc.

Should the Government decide to regulate digital currency then a uniform approach needs to be developed with regard to the regulatory environment active on firms fulfilling similar functions, e.g. third-party exchanges should face the same level of regulatory intervention where their risk factors are broadly similar (e.g. distribution channels, geographical coverage, self-imposed monetary limits etc). However, the different drivers for intervention should be reflected within the nature of the intervention itself. Thus, with regard to the financial crime imperative, a risk-based model could be of use similar to that which underpins much of the domestic, European and global anti-money laundering framework. In contrast a risk-based approach would not seem appropriate to ensure consumer protection risks are properly mitigated and so a different approach is required there, perhaps using licensing/registration mechanisms.

This approach will mean that the regulation is multi-faceted, reflecting the different aspects warranting regulatory intervention yet fair to all commercial actors within the emerging digital currency sector by creating a level playing field. Whichever driver, however, regulatory measures should apply to all digital currencies (though not virtual currencies as defined in the consultation). This has the effect of future-proofing, as far as possible in a field as fast-paced as this, the regulatory coverage and enhancing consumer protection and reducing criminal utility of digital currencies. It also prevents the framework from becoming reactive and dependent on understanding new products and technologies before it is able to include them within its scope.

The FCA's policy unit responsible for 'project innovate' could be further empowered to cover digital currencies. It currently works with firms who have developed innovative approaches in the financial sector; which is not explicitly covered by regulation, or for which application of regulation is ambiguous. It is very much a supportive role and could be of use here, notwithstanding the decentralised nature of digital currencies by supporting associated businesses e.g. exchange services; secure online wallet services etc.

Question 4: Are there currently any barriers to digital currency businesses setting up in the UK? If so, what are they?

No particular view.

Question 5: What are the potential benefits of this distributed ledger technology? How significant are these benefits?

The distributed ledger technology solves issues relating transaction security, i.e. preventing a unit of digital currency from being spent more than once without any third-party intervention or observation. Further, it also enhances customer information, privacy and data security protection. Most significantly however, is the potential utility of the blockchain technology coupled with the decentralised architecture of digital currencies, to broader applications rather than digital currencies, i.e. next-generation or Bitcoin 2.0 platforms. As an example of such platforms, for social media there is Twister (decentralised, effectively anonymous version of Twitter) and Ethereum which is geared towards autonomous contracts. Smart, self-executing,

contracts are likely to be a significant development over the coming years with numerous possibilities, e.g. smart loans with automated interest rate adjustment according to set parameters e.g. repayment history over the course of the loan. Similarly, decentralised cloud storage services are in development.

This is an area where, with Government support, the UK could become a leader in this emergent area of technology, particularly given the potential cross over between smart contracts and smart property, e.g. driver-less cars with the UK's investment in such technology continuing through the Autumn Statement.[10] Further, developments such as Ripple have the potential to take the application and usefulness of the blockchain further. Ripple allows for lower-cost avenues for worldwide money access due to giving servers the ability to establish transaction veracity without crunching number intensive calculation as is the case, for example with Bitcoin.

Question 6: What risks do digital currencies pose to users? How significant are these risks? How do these risks vary according to different digital currencies?

The risk that digital currencies pose to users, is in many ways the threat that users pose to themselves when using digital currencies. Users need to be educated about using digital currency in a safe, secure manner. Users should be clear that without their cryptographic key, they have, effectively, lost their BTCs. Information technology literacy around back-ups, malware protection etc is crucial as is ensuring that each user controls access to their key in the same way that PINs are not to be circulated. One of the obvious risks that digital currencies pose to users is the fact that they are easy to lose, similar in many respects to cash. By way of illustration, an individual lost 7,500 Bitcoins when he discarded the hard-drive that he had them stored on.[11] The hard-drive contained the crypto-graphic "private key" without which there is no way to access and spend the BTCs. A solution of sorts was created when third party deep storage websites like Elliptic Vault began providing 'deep cold' storage systems for these keys. The issue with this is that access to a consumer's BTCs is being placed in the hands of start-up third-party companies with little or no track record. These third-party service providers are a potential area of regulation.

Another risk with digital currencies is that they tend to be extremely volatile in terms of their exchange rate into fiat currency. Bitcoin prices fluctuate wildly. This again, is an area which could prove to be a significant blocker to large scale uptake amongst consumers (certainly, businesses can use contract terms to protect themselves against price fluctuations, however, such volatile movements will do little to inspire confidence within consumers, and ultimately (digital currency as with fiat) confidence is everything.

Question 7: Should the government intervene to address these risks, or maintain the status quo? What are the outcomes of taking no action? Would the market be able to address these risks itself?

Yes, intervention to protect consumers should be welcomed. Education as to the risks (and advantages to consumers) of digital currencies is crucial. The growth of BTCs as a speculative investment is one which will be hard to prevent (as a market response) but it is a matter which requires further thought and research since the volatility created by speculative investment in digital currencies is a significant bar to wider adoption as a token of value by consumers. The

[10] http://www.bbc.co.uk/news/technology-30316458

[11] < http://www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site >

advantages of digital currencies are in its use as a means of transferring value, and not as an investment opportunity.

Question 8: One of the ways in which the government could take action to protect users is to regulate. Should the government regulate digital currencies to protect users? If so, should it create a bespoke regime, or regulate through an existing national, European or international regime?

For each option: what are the advantages and disadvantages? What are possible unintended consequences (for instance, creating a barrier to entry due to compliance costs)? What other means could the government use to mitigate user detriment apart from regulation?

As noted elsewhere in this response, we would support regulatory intervention to protect users from the risks identified in the manner suggested in the different responses to other questions.

Question 9: What are the crime risks associated with digital currencies? How significant are these risks? How do these risks vary according to different digital currencies?

Money is the lifeblood of crime. Thus, with the uptake of digital currencies comes the risk of criminal operations responding, adapting, and utilising such currencies. Every currency or indeed store of value and payment mechanism has criminal utility whether cash, plastic cards, wire transfer or other. One of the most obvious crimes that can be committed on digital currencies is theft and with increased uptake and acceptance of a digital currency comes a corresponding increase in the risk of theft. There are three key ways in which theft of digital currencies has occurred:

1. Attack on a third-party website
2. Malware programmes
3. Third party companies exploiting consumers

As an example of the first category, the third-party website, BIPS (Bitcoin Internet Payment System) suffered a denial-of-service attack, however, that was merely a smokescreen for a digital heist that quickly drained numerous wallets, netting the criminals a reported 1,295 BTCs (worth nearly $1 million). As a technology-based development, digital currencies are vulnerable to malware specifically designed to infect a user's computer and cede control to the criminal.

The final way is third part companies exploiting consumers. One such example is Mt.Gox. Mt.Gox which lost $600m in BTCs in uncertain circumstances. Another example is a China based Bitcoin exchange called GBL launched in May. Almost 1,000 people used the service to deposit BTCs worth about $4.1 million. The exchange was revealed to be an elaborate scam after the perpetrator closed the site later that year and absconded with the funds. Where businesses create a centralized body to operate as an adjunct to a decentralized structure, but with no corresponding oversight for the centralized body, fraud is both possible and, in general terms, predictable.

A further criminal risk associated with digital currencies is money laundering. Digital currencies provide opportunities for criminals to exploit its interconnectedness, accessibility and anonymity to achieve their illicit objectives without detection or sanction. The ongoing revolution around payment technology and specifically, peer-to-peer transfer of money using the internet, has heightened regulatory concern around what is being termed

"cyberlaundering". Essentially, Bitcoin and analogous digital currencies *could* enable money launderers to move illicit funds more quickly, with little expense, and even less scrutiny, than technology has allowed in the past.

The general approach of AML regulation (whether at a global or national level) has focussed upon the use of key professions as de facto policemen, guarding entry points into the financial (and other) systems and limiting the ability of criminals to transfer value without scrutiny. Digital currencies, such as Bitcoin, evade these key professions for as long as the user is content to keep the value as digital currency, i.e. unless and until the digital currency is exchanged for fiat currency (or goods or services) where the business, whether merchant or exchange service, is amenable to anti-money laundering regulation.

It should be pointed out, however, that the extent of these risks is by no means fully understood. There are, for example, significant limitations on digital currencies as currently operative from the perspective of a serious organised launderer. The volatility of the exchange rates e.g. BTC to US dollar would represent a significant risk to criminal organisations. This is true in two distinct ways. First, the value of the BTCs will be unpredictable and second, where a criminal organisation buys/sells significant sums of BTCs, that could in itself trigger a response within the exchange rate markets, thus fuelling the volatility. Most fundamentally, the scale of money laundering globally is such that the relatively limited uptake of digital currencies in effect hampers the laundering utility of that currency – one can only fail to see the wood for the trees where there are sufficient trees to obscure the wood.

Question 10: Should the government intervene to address these risks, or maintain the status quo? What are the outcomes of taking no action?

We would support regulatory intervention to address the criminal risks associated with digital currencies. As noted previously, together with consumer protection, these are the most pressing imperatives for regulating digital currencies. Given the difficulties of attempting to regulate digital currencies as currency (no central issuer; no control over supply/demand; no central organisation to impose regulatory requirements upon) it would seem futile to attempt such an approach. On the other hand, the commercial element of digital currencies, i.e. where they are accepted as payment for goods and/or services, would seem amenable to certain anti-financial crime regulatory measures, e.g. customer due diligence measures when high-value goods are purchased using digital currency. In this sense, digital currencies can be regulated in the same way as cash (e.g. the high-value dealers regime within the MLR 2007). The other avenue to mitigate crime risks associated with digital currencies would be to focus regulatory attention on the exchange services i.e. use the need for digital currencies to be converted into fiat currency as a regulatory choke point.[12] Two key AML initiatives noted elsewhere in this report, CDD and SARs could be of some utility at that stage. There are also arguments to support controlling, perhaps through a positive licensing scheme, access to that form of business venture, from the criminal risk perspective.

In our view, with decentralised, pseudo-anonymous currencies such as Bitcoin, it is only that commercial side of the network which could or should be regulated to mitigate criminal risks. To attempt to regulate peer-to-peer transfers of BTCs would seem to be an exercise in futility.

Question 11: If the government were to take action to address the risks of financial crime, should it introduce regulation, or use other powers? If the government were to

[12] See further, 'Anti-Money Laundering Regulation and Emerging Payment Technologies' (2013) 32(5) *Banking & Financial Services Policy Report* 1; 'Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar' (2012) 21(3) *Information and Communications Technology Law* 221.

introduce regulation, should it create a bespoke regime, or regulate through an existing national, European or international regime? For each option: what are the advantages and disadvantages? What are possible unintended consequences (for instance, creating a barrier to entry due to compliance costs)?

Regulation through the existing anti-financial crime mechanisms would seem the most beneficial approach. However, certain core aspects of that regime e.g. Suspicious Activity Reporting obligations on third-party exchanges would require further consideration. Most fundamentally the limited knowledge and understanding as to legitimate usage of digital currencies e.g. Bitcoin is such that it would be very difficult for an exchange service provider to identify an abnormal i.e. suspicious Bitcoin transaction (as opposed to say, wire transfers where we have an understanding of laundering behaviour). Government should support multi-agency, cross-disciplinary research into this area so that the aspects of digital currencies which are more amenable to regulation under the existing financial crime measures are fully utilised, whilst accepting that certain aspects of digital currencies, e.g. P2P transfers are simply not susceptible to or indeed, suitable for, regulatory intervention. Moreover, in general terms, the role of the third-party exchange service is vital to serious organised crime (unless and until digital currencies are accepted as a de facto global currency in their own right, in which case, third-party exchanges will be defunct in any event.) At that point, effective regulation of digital currency will be challenging to say the least.

What has been the impact of FinCEN's decision in the USA on digital currencies?

The impact of FinCEN's decision to issue guidance on 'Virtual Currencies and Regulatory Responsibilities' is still relatively new, but its impact is already reasonably clear. The guidance provides that "administrators" or "exchangers" of virtual currency are considered MSB's for the purposes of the Bank Secrecy Act. Therefore, a virtual currency transmitter must be licensed whether starting or continuing relevant business activities. The guidance has provided a certain level of certainty in the market place, classification as an MSB is made based upon clear factual criteria, and all businesses which fall within that definition are subject to the rules.

What is significant is the choice of money transmitters as the first target for regulation of virtual currencies. They are the 'players' that are on the surface, visible to the outside world. As third parties to transactions they present a lot of the risks discussed above in the crime section. By classifying them as MSBs it brings these Bitcoin exchanges and payment processors into the regulatory framework, where previously they were unregulated. As a result of the US approach businesses may simply choose to locate overseas to evade regulation, digital currencies are not restricted by borders and in that sense it is not important where they are operating from. To register in all of the states could take a significant amount of time; such a requirement would not be as burdensome for virtual currency transmitters in the UK.

In terms of impact, the Department of Homeland Security ("DHS") issued a seizure warrant for a bank account held by a US subsidiary of Mt.Gox, because it failed to register as a money transmitter. This highlights that the guidance has had an almost immediate impact.

Question 12: What difficulties could occur with digital currencies and financial sanctions?

In terms of the key characteristics of financial sanctions, they must be: capable of application; and either restrictive or coercive in nature. If they are not capable of application then they offer

little deterrent to financial crime. Digital currencies provide a barrier to the effective implementation of financial sanctions.

The 'Consolidated List of Financial Sanctions Targets in the UK' is a good illustration of the difficulties here. It provides a list of individuals and entities, by country, which should have their assets frozen. Key to it functioning is that those individuals or entities can be identified. The problem is that digital currencies mean that the transaction could be taking place anywhere in the world with originator information masked. Further, unlike other non-traditional payment methods (such as wire transfers) there is no need for a third-party intermediary, due to the decentralised structure and the technology used; therefore there is no one that can freeze the funds. Quasi-anonymity is another issue, even though every transaction is recorded on the blockchain (and freely available) as mentioned in response to Question One there is no personally identifiable information on it. This means that there would be a need to link wallets with real people, which can be difficult when the transactions are simple, but is particularly tough when users operate numerous wallets. This problem is further compounded by "dark" wallets which have been termed 'super-anonymous'; it encrypts and mixes users' payments so as to make flows of money online untraceable. The effort required to source an individual or entity, if possible, would not justify the resources it would undoubtedly take.

So, it seems that sanctions are only of use where there is some other kind of information which facilitates sanctions, e.g. as was the case where the CIA was able to confiscate BTCs as part of the closure of Silk Road. Consideration is needed as to how confiscation and asset freezing systems within the UK could operate in the realm of digital currency.

Question 13: What risks do digital currencies pose to monetary and financial stability? How significant are these risks?

The risks here are potential not actual, and given the scale of use and rate of growth, unlikely to be relevant at a systemic level for a significant period of time.