MONEY LAUNDERING, TERRORIST FINANCING AND NEW TECHNOLOGIES: POTENTIAL FOR MISUSE OF NEW PAYMENT METHODS IN THE UK AND IRELAND?

Padraig J. McGowan, JFSD, QFA

to be submitted for the award of MA

at Dublin City University

under the supervision of Dr. Maura Conway

School of Law and Government

July, 2014

DECLARATION

I hereby certify that this material, which I now submit for assessment on the programme of study leading to the award of MA, is entirely my own work, and that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

Signed: _____

Candidate ID No.: 11100117

Date: September 18, 2014

TABLE OF CONTENTS

ABSTRACT

Money Laundering, Terrorist Financing and New Technologies: Potential for Misuse of New Payment Methods in the UK and Ireland?

Padraig J. McGowan

The increased popularity of Internet-based financial services has led to the introduction of many new innovations. Often described as New Payment Methods, they are frequently offered by providers outside the mainstream financial services industry. While offering improved services to a widened customer base, there is the potential for money laundering and terrorist financing usage, concerns recognised by the European Council. To explore potential misuse, this research focused on a range of new payment methods within the European Union. Analysis included their various features, practical usage and customer identity requirements. Two of the most popular and widely available new payment methods—prepaid credit cards and online payment systems—were selected for more in-depth analysis focusing on those available in the Republic of Ireland and the United Kingdom. This involved applying for, and/or purchasing relevant products and services, and assessing the customer identification and profile-building process. Their practicality for money laundering or terrorist finance was reviewed along with the regulations pertinent to their provision. Evidence suggests that, while there are some matters of concern, many online payment providers closely monitor customer applications and use of services. However a number of serious shortcomings were evident in relation to some prepaid card providers in their verification of customer identity and profile details, and the controls in place to prevent multiple card holdings by individual customers.

ABBREVIATIONS AND ACRONYMS

ABCUL – Association of British Credit Unions Limited

AML – Anti-Money Laundering

ATM – Automated Teller Machine

CDD – Customer Due Diligence

CFT – Countering the Financing of Terrorism

CU – Credit Union

DCE – Digital Currency Exchange

E-Money – Electronic Money

EC – European Council

EFT – Electronic Funds Transfer

EMI – Electronic Money Institution

EU – European Union

FATF – Financial Action Task Force

FIU – Financial Intelligence Unit

FSP – Financial Service Provider

IP – Internet Protocol

ISP – Internet Service Provider

IT – Internet Technology

KYC – Know Your Customer

ML – Money Laundering

MLRO – Money Laundering Reporting Officer

NPM – New Payment Method

OSFI – Office of the Superintendent of Financial Institutions

PEP – Politically Exposed Person

ROI – Republic Of Ireland

SAR – Suspicious Activity Report

SEMI – Small Electronic Money Institute

TF – Terrorist Finance

UCITS – Undertakings for Collective Investment in Transferable Securities

UK – United Kingdom of Great Britain and Northern Ireland

US – United States of America

ACKNOWLEDGEMENTS

There are a number of people who I would like to thank for the help and support provided during the course of this research.

Firstly my supervisor, Dr. Maura Conway, without whose dedication, guidance, and encouragement, this thesis would not have been completed. Thanks must also go to my family, Lisa and Daria, for their practical help and encouragement. Finally, I must acknowledge those organisations, and the individual members of staff of those organisations, who responded to various queries and requests for information. Those responses aided this research in no small way.

CHAPTER 1

INTRODUCTION

In the financial world, the ever-increasing importance of the World Wide Web has resulted in a significant expansion of online services. These have included various products and services which have become known as New Payments Methods (NPMs). However, while these methods have provided benefits for legitimate users, they may also have introduced new opportunities for those involved in terrorist financing (TF) or criminal money laundering (ML).

The importance of countering ML and TF is seen by many governments and international bodies as being vital. The United States of America (US) addressed ML as early as 1970. With its requirements for the recording of transactions and reporting of high value transactions, the *Currency and Foreign Transactions Recording Act* (United States, 1970, pp.1114-1125) cited such actions as having a 'high degrees of usefulness' in criminal investigations and prosecutions. The European Council (EC) first addressed the issue of ML in its 1991 Directive, *91/308/EEC*, and acknowledged the importance of ML in the growth of general crime (European Council, 1991, p. 77). It has continued to focus on Anti-Money Laundering (AML) measures with updates and directives in 2001(European Council, 2001a, 2001b) and 2005(European Council 2005). In a reflection of the increasing awareness of the global impact of ML, the Financial Action Task Force (FATF)[1] was established in 1989 to help prevent ML through the monitoring of national and international AML responses, and the issuance of reports and guidance notes.

[1] Financial Action Task Force, see http://www.fatf-gafi.org/

However, it wasn't until much later that TF was addressed by many national governments or trans-national bodies, the catalyst for increased awareness being the 2001 terrorist attacks in the US. Since then Countering the Financing of Terrorism (CFT) has become a major focus of attention. The EC issued *Council regulation (EC) No 2580/2001,* (European Council, 2001b) in which it stated CFT was 'decisive' in the fight against terrorism, and has since issued Directive 2005/60/EC (European Council, 2005). The FATF, whose role was to monitor AML, had its responsibilities widened to include CFT, recognizing its 'vital importance' (FATF, 2001, p. 2). Both, former US Treasury Secretary Paul O'Neill [2], and former Under Secretary for Terrorism and Financial Intelligence, Stuart Levey [3], have confirmed the vital role that has been, and will continue to be played by the detection of TF.

In 2009 the EC addressed the possible misuse, by terrorists, of NPMs. The Stockholm programme (Council of the European Union, 2009, pp. 51-52) stated:

> 'The European Council considers that the instruments for combating the financing of terrorism must be adapted to the new potential vulnerabilities of the financial system, as well as cash smuggling and abuse of money services, and to new payments methods used by terrorists.'

It further called upon the European Commission to take NPMs 'into account' in future updates of CFT measures (*ibid*, p. 52).However it is not just the EC that has recognised the potential for NPMs and other online financial services to be misused

---

[2] Paul O'Neill, "Remarks by Paul H.O'Neill United States Secretary of the Treasury, Before the extraordinary plenary meeting of the Financial Action Task Force.", October 29, 2001. Accessed November 20, 2010. http://www.ustreas.gov/press/releases/po735.htm

[3] Stuart A.Levey, "Prepared remakes by Stuart A.Levey, Under Secretary for Terrorism and Financial intelligence, Before the American Bar Association's 22nd Annual National Institute on White Collar Crime", March 6, 2008. Accessed November 20, 2010 . http://www.ustreas.gov/press/releases/hp863.htm

for ML or TF. The FATF first addressed the potential misuse of NPMs in 2006 in its '*Report on New Payment Methods*' (FATF 2006). Since then the FATF has continued to issue regular reports on ML/TF issues related to various NPMs including, '*Money Laundering using New Payment Methods*' (FATF 2010), and '*Virtual Currencies, Key Definitions and Potential AML/CFT Risks*'(FATF 2014). Additionally, the US Department of Justice produced a report on the potential use of digital currencies for ML (U.S. Department of Justice, 2008) while the US Financial Crimes Enforcement Network's *2007 National Money Laundering Strategy* report (Fincen, 2007, pp. 39-41, 43-45) saw potential concerns with such NPMs as digital currencies, online payment systems and prepaid cards.

This research analyses that potential for NPMs to be used for the illicit financial transactions involved in ML or TF. It examines this under a number of headings, but the core questions were: Can these NPMs be obtained, funded and used anonymously, provide sufficient practical features such as fund storage, Automated Teller Machine (ATM) withdrawals or fund transfers, and could their use for ML or TF remain undetected?

The initial examination of NPMs was carried out to assess their usefulness under the headings listed above. A number of internet-based services not normally recognised as NPMs were also selected for examination, if they were capable being used for movement or disguising the origin or destination of funds. These included online share dealing, internet based banks or online gambling, along with such 'normal' NPMs as digital currencies, online payment systems, prepaid cards and payment-capable mobile phones. Having examined a number of the products/services another deciding factor came into play: familiarity with the product/service. This ease of use, along with potential compatibility with all of the other factors, made the

decision on the two NPMs to be looked at in detail, even easier. Prepaid cards were chosen because of their potential for anonymity, practical features, and easy funding. Online payment systems were chosen for almost the same reasons, although they cannot be used for cash withdrawals unless linked to one of the aforementioned prepaid cards. As previously stated, another deciding factor was familiarity and ease of use: Prepaid cards have virtually the same features and uses as standard, mainstream issued cards, while many people are familiar with online payment systems through their involvement with online auction sites or, in some cases, fund transfers from and to friends and family overseas.

The research concentrated on two of the primary NPMs, prepaid cards and online payments systems. The research was conducted by examining the products and services, the regulations pertaining to their use, and by practical experimentations, such as obtaining, activating and using a card.

Few concerns were apparent with online payment systems, although there were some issues around the use of prepaid cards as a funding source and source of customer verification with one online payment provider. However, the researcher discovered that there were serious concerns around the sale of prepaid cards. This was due to the potential for those involved in ML or TF to be able to move relatively large amounts of money anonymously using multiple cards from a single provider. This problem extended to a number of providers.

Argued within this thesis is that there are serious deficiencies in the internal monitoring controls of card providers, from customers obtaining multiple cards to the poor monitoring of transactions or customer activities for suspicious behaviours. While the products are classified as at low risk of criminal or terrorist

misuse, that status is only appropriate were their use is restricted. This is patently not the case with multiples cards capable of being obtained by one customer. The solutions to these problems would entail more efficient monitoring by the providers of accounts and account applications along with the centralisation of the certification of documents and/or the provision of the customer's personal social security number.

Synopsis

In Chapter two the researcher reviews the existing ML or TF literature on various online financial services. The EC's regulation of NPMs, the implementation of those regulations and the impact of other regulatory requirements in the Republic of Ireland (ROI) and United Kingdom (UK) are examined in Chapter three. A review of various NPMs and online financial services available in either the ROI or UK, is detailed in Chapter four, as is the methodology used in the assessment of the two NPMs, prepaid cards and online payment systems, selected for in-depth investigation. Chapter five examines some of the prepaid cards and online payment services available in the ROI and UK, before Chapter six provides details and analysis of the research findings. Finally, Chapter seven reviews the findings, lists the limitations placed on the research, and details the researcher's suggestions for solutions to the concerns highlighted in the thesis. The researcher also provides suggestions for future research to be carried out in the field.

CHAPTER 2

LITERATURE REVIEW

The need to hide the source of illicit wealth has been an essential part of illegal or criminal activity since society started taking countermeasures to prevent such activities. While there are some questions as to the origins of the term 'money laundering' (Hunt, 2011, p. 134; Masciandaro *et al*., 2007, pp. 103-104), it is very descriptive of the age old process of turning 'dirty' criminal-originated funds into 'clean' funds. The monetary values involved in ML on a worldwide or even regional basis are a mystery and subject to much debate (Schneider, 2011, pp. 5-8; Stokes, 2012, p. 221), as are the values of ML transactions made via NPMs (Melongi, 2010, p. 209). What is unquestionable is that the monetary values involved in crime, and therefore the amounts being laundered, are significant. However the idea that ML is a victimless crime (Sienkiewicz, 2007, p. 5) could be disclaimed when one considers the possible fines imposed on Financial Service Providers (FSPs), and therefore their shareholders, for deficient AML measures.

The laundering of funds traditionally entails three stages: (1) the initial placement of the illegal funds within the legal economic system. (2) the layering of the funds which entails the movement of the funds between different accounts or into different items of value to disguise their source, and (3) the integration of the now disguised funds into the legitimate economy (Hunt, 2011, pp. 134-135; Masciandaro *et al*., 2007, pp. 104-105). The methods by which dirty funds are disguised are as varied as the criminal acts that generate them. Any business with a high cash turnover is attractive to those wishing to disguise the origin of their funds (Mills, 2001, p. 80; Schneider, 2011, p. 5). To that end public houses, gambling casinos, betting shops, grocery shops, petrol stations, foreign exchange bureaus, etc. can all

become useful ML tools. These could be either an existing legitimate business purchased by the launderers or one specifically setup for ML (Fossat et.al, 2012, pp. 9-11; Horgan and Taylor, 2003, pp. 17-35; Schneider, 2011, p. 5) and used to contribute financially to the criminal activity (Chargualaf, 2008, pp. 16-17; Schneider, 2011, pp. 8-9; Stringer, 2011, p. 104). Personal financial products can also be used for ML. Funds are easily moved between accounts in different financial institutions and in different countries, Cash withdrawn in substantial amounts via ATMs, personal borrowing repaid with 'dirty' funds and the items related to the borrowing then sold as a source of 'clean' funds etc. However as regulatory requirements and greater watchfulness in mainstream financial services has made it more difficult for money laundering to take place, those involved have looked elsewhere for less well regulated systems which can provide similar, and in some cases, more ML user-friendly alternatives (Linn, 2008, p. 163; Sienkiewicz, 2007, pp. 9-10).

Advances in 'new' technology, such as the internet or mobile phones, have provided many new ML opportunities with their own unique attractants (Filipkowski, 2008, pp. 16-17; Fosset *et al*., p. 7; Hunt, 2011, p. 136; Jacobson 2010, p. 355, 357; Stokes, 2012, p. 231; Villasenor *et al*., 2011, p. 20). They can also introduce modifications that make older ML methods even more attractive (Bronk et.al, 2012, p. 129; Feldman, 2006, pp. 361-363; Hunt, 2011, pp. 135-136). The very features, such as anonymity, transaction speed, accessibility and ease of use, which attract legitimate users, can also attract those who would use them for illegal purposes (Bronk et.al, 2012, p. 130; Hunt, 2011, pp. 137-138; King, 2013, p. 1; Merlongi, 2010, p. 204, 210). Additionally the variety of different systems will prove attractive to those wishing to disguise the source or destination of funds (Bronk et.al, 2012, p. 130).

To address the many varied forms of NPMs and the literature dealing with them, this chapter is divided into six sections. These look at internet based gambling, prepaid credit cards, online payment systems, digital/virtual currencies and virtual worlds, mobile phone based financial services, and online banking services from mainstream FSPs.

Internet based gambling

One of the favoured methods of traditional ML was in the area of gambling through either casinos or betting shops. Given previous history it is obvious that online gambling has been used both for ML and TF (Jacobson, 2010, p. 355; McMullan and Rege, 2010, p. 62, pp. 66-67; Simser, 2013, p. 47).

Online gambling has greatly increased in popularity over the last 10 years as more and more people turn to the internet for entertainment. Registration with an online gambling site is simple, usually requiring an active email address, name, and for those wishing to gamble for real money, date of birth, address, and the provision of scanned copies of documents via email (Levi, 2009, pp. 539-540). Funding of the account can be made via a variety of methods including bank transfer, credit card and various online payments systems such as *Paypoint, Paysafecard, Ukash* or *Moneybooker*s.

Concerns have been raised with a number of features which could be used for ML or TF. On some sites, players have the option to either play against whoever is available, or against chosen opponents. This latter option could be misused in a number of ways: a player could have a number of virtual identities/avatars, and choose to play one against the other. By 'loosing' against the chosen avatar, funds are moved to that avatar's owner, thus facilitating an illicit transfer. Alternatively,

and again using multiple avatars and deliberate losses, funds could be switched between players and then withdrawn, giving the appearance of 'clean 'funds (Stokes, 2012, p. 229). A simpler method would be to lodge funds to the account, gamble some of the money and then request a refund (Hornle, 2011, p. 258). The funds may have been paid in, for example, via a cash lodgement, but can be withdrawn as a cheque which can then be lodged as clean funds, disguised as gambling winnings. Other issues would include the use of FSPs with poor regulatory compliance, funding via unregulated digital currencies, cash lodgements allowed which could be untraceable as regards their origin, identity fraud aided by the lack of face-to-face contact, etc. While some view the facility to lodge and withdraw funds by different methods as something which is an issue not specific to online gambling (Levi, 2009, p. 536), this, as well as many of the other commonplace problems, remains an issue. Funding of the account can also be a matter of concern. Prepaid credit cards are seen as potentially problematic (Levi, 2009, p. 539), perhaps due to their minimal Know Your Customer[4] (KYC) requirements and the ease with which they can be loaded with cash. Another issue is the potential establishment by terrorists or money launderers, of an online gambling site purely for the purposes of TF or ML (Filipkowski, 2008, p. 22; Hunt, 2011, p. 136), probably based in one of the less well regulated countries (Levi, 2009, p. 537; Mills, 2001, p. 86).

Many of the online gambling companies are committed to preventing misuse, as a societal duty and a desire to protect their industry (Brooks, 2012, p. 304, 309, 311-312; Levi, 2009, p. 542). However this cannot be said for all providers (Brooks,

[4] KYC is a process of establishing or updating a customer's profile details. Initially confined to name, postal address, contact details and date of birth, it can also include, where appropriate, details of employment, income and financial standing. Confirming the customer's identity usually requires the provision of documents such as a passport or driving licence and a utility bill showing the customer's full name and address and must usually be less than 3 months old.

2012, p. 309). Online gambling companies, operating within the EU, implemented AML and CFT directives on a voluntary basis (Levi, 2009, p. 537). These self-imposed regulations followed many of the requirements imposed on mainstream FSPs such as banks and credit card companies: Customers must be properly identified under enhanced Customer Due Diligence[5] (CDD) rules due to the lack of face-to-face contact, which may entail checking databases to verify the customer's name and address details. Phone numbers are verified as the customers by the use of phone calls and codes sent online. Watch lists of suspected or known money launderers or terrorists must be checked and continual monitoring of customer actions for suspect behaviours. Additionally, value limits are imposed, direct cash lodgements prohibited and suspect behaviours (such as large deposits withdrawn after minimal usage) resulting in closures of accounts (Levi, 2009, pp. 537-541).

However, these measures do have some drawbacks, namely the availability of unregistered mobile phones and there remains the option of lodging cash via a number of FSPs who do not require identification. While those in the EU voluntarily imposed AML/CFT regulations, those within the UK were obliged to comply with a robust regulatory regime since 2007. Requirements include many of the EU requirements already detailed: Enhanced CDD around the provision of identity

[5] The EU Third AML Directive states that CDD shall comprise of the following:

(a) Identifying the customer on the basis of documents, data or information obtained from a reliable and independent source;
(b) Identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to understand the ownership and control structure of the customer;
(c) Obtaining information on the purpose and intended nature of the business relationship;
(d) Conducting ongoing monitoring of the business relationship including ensuring that the transactions being conducted are consistent with the knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that documents, data or information held are kept up-to-date.
http://www.pearse-trust.ie/blog/bid/69446/What-Is-Customer-Due-Diligence

documents, limits on the total value of transaction, record keeping and the reporting of suspicious transactions (Stokes, 2012, pp. 229-230).

Dealing with the US, Mills (2001) sees potential misuse of online gambling for ML (*ibid*, pp. 77-78). Citing the location of many online gambling companies in countries with poor or non-existent regulation, Mills sees the need for international cooperation (*ibid*, p. 86, 96), and advocates that an enforcement body should be established with jurisdiction over online gambling companies (*ibid*, p. 93), He suggests various solutions to the problem of non-resident providers, citing previous law cases in the US (*ibid*. pp. 87-90) Mills expresses concerns at the possible side effects of badly designed regulation (*ibid*, p. 96). Levi (2009) views the risk of online gambling or online card games being used for ML as being modest (*ibid*, p. 533). However his claim that online transactions are traceable through the internet service provider (ISP) (*ibid*, p. 541) ignores the possibility of those involved in the illegal acts using technical expertise to hide their location, utilising internet cafes and free Wi-Fi services to preserve anonymity (Filipkowski, 2004, p. 3; Hinnen, 2004, p. 11; Jacobson, 2010, p. 358, 360). Additionally, some jurisdiction's internet providers are not obliged to provide such information to investigating authorities (Bensted, 2012, p. 244, 253). Similarly Levi's assumption that a link to a regulated FSP reduces concerns about KYC requirements as these are already complete, is hardly a dependable solution (Levi, 2009, p. 543), given that some mainstream FSPs have been found to be lacking in relation to full regulatory compliance.[6]

[6]For example; Irish FSPs deficient in compliance, see Irish Central Bank presentation at Assoc. of Compliance officers in Ireland conference. See pages 28, 31-32, 34-39. http://www.centralbank.ie/regulation/processes/enforcement/Documents/Central%20Bank%20Slides%20for%20ACOI%20presentation%2027%2009%2012.pdf

Prepaid credit cards

Pre-paid cards, alternatively known as stored value cards, are attractive to many legitimate users for the payment of salaries or government allowances, providing bank services to the 'unbanked'[7] or used by those who worry about using mainstream credit cards online (Choo, 2009, p. 13; Linn, 2008, pp. 146-147; Sienkiewicz, 2007, p. 1). Pre-paid cards are normally issued under licence from one of the major credit card companies, usually *Visa* or *MasterCard* (King, 2013, p. 1; Zerzan, 2010, p. 5), but are not readily available through mainstream FSPs. They share many of the features of standard credit or debit cards, for example; being able to conduct cash withdrawals from ATMs, purchases at real-world or online outlets, for online fund transfers, and are not limited by geographical location (Linn, 2008, p. 147; Sienkiewicz, 2007, pp. 2-3, p. 11).

While King, Linn and Sienkiewicz deal mostly with the pre-paid market in the US, and Choo's paper relates to the Australian market, all four identify concerns which are pertinent within the EU and elsewhere. Prepaid credit cards are available in two main formats. Closed loop cards are usually restricted to retail sales in one location or with one chain of stores having effectively taken over from paper gift vouchers. Usually sold via non-financially regulated outlets, they normally cannot be exchanged for cash or used to withdraw funds from an ATM. Considering the latter point, they would appear to be of minimal use for either ML or TF, their only usage would be the purchase of goods to be retained for the use of the criminals/terrorists, or sold for cash. Alternatively the cards could be sold on for cash (Linn, 2008, pp. 148-149; Sienkiewicz, 2007, pp. 10-12; Zerzan, 2010, p. 5), but this would be in a

[7] People who for various reasons are unable to access mainstream banking services. This could be due to poor quality bank services, bad credit records or poor infrastructure.

very limited market. Open loop Cards have much more in common with standard credit/debit cards, sharing all their functionality for cash withdrawals, retail or online purchases or funding online fund transfers. Where they differ is in their availability, purchasable either online or in retail outlets with minimal or no regulatory requirement for the provision of KYC documentation or information. This, especially where there is a lack of face-to-face contact, allows for a great degree of anonymity (Choo, 2009, p. 17; King, 2012, p. 1; Linn, 2008, p. 147, 156, 162; Sienkiewicz, 2007, pp. 12-15; Zerzan, 2010, p. 5), especially when online provision of scanned documentation is required, allowing for the easier use of altered, stolen or counterfeit items. This anonymity, in addition to ready availability, ease of use and the ability to transfer the card to a third party, is very attractive for either ML or TF (King, 2013, p. 1). Even where regulations require provision of identity documents and AML/CFT compliance, there would be concerns around the competence of untrained staff at retail outlets or a lack of AML/CFT qualified staff (Choo, 2009, p. 17) Some of these cards are also available with large balance limits (King, 2013, p. 8; Linn, 2008, p. 150, 154; Sienkiewicz, 2007, p. 3, 13). Almost all can be funded via unregulated outlets often with no identification requirements (Choo, 2009, p. 15; Simser, 2013, p. 44), and frequently with cash (Linn, 2008, p. 147; Sienkiewicz, 2007, p. 16, 19, 20). This makes the tracing of transactions or those who made them almost impossible, while the removal of the need to carry bulky hard currency is also advantageous for illicit use (Hunt, 2011, p. 135; Linn, 2008, p. 147). It is also possible to buy numerous prepaid cards thus facilitating the movement of large amounts of currency with minimal risk of detection (Choo, 2009, p. 17; Linn, 2008, p. 154; Sienkiewicz, 2007, pp. 20-21)

Linn (2008, p. 164), suggests technical solutions should be found which would identify pre-paid cards originating from countries with poor regulatory regimes, and

which therefore need to be closely examined for potential illegal usage. While this solution may be sufficient where people are searched it is unclear how this will affect those who are not checked on arrival into a country. In addition this does not address the possible loading of the card from outside the country, after border controls have been passed. King (2013, p. 1, 4, 8), sees the current US restrictions on value limits, US$10,000 per customer, as being an effective counter measure. However the ability to move this amount of currency, per customer, per bank should be a matter of concern. For example, the 1998 bombings of US embassies in East Africa cost approximately US$10,000 and the 2005 London attacks, US$ 15,600 (Hett, 2008, pp. 1-2). Sienkiewicz (2007, pp. 20-21), suggests that while it is not possible to prevent every case of misuse it should be possible to make it more difficult through limiting the loading and reloading speed of cards, preventing multiple card acquisitions and controlling the number of permitted ATM transactions. He does not however address how to prevent the purchase or use of cards from other jurisdictions, the use of 'mules' [8] or 'smurfs' [9] in both the purchase and loading of cards, or how to prevent launderers purchasing multiple cards from various different providers. Choo (2009) acknowledges the cost impact of increased compliance on the pre-paid card industry, expressing concerns that any increase in same will result in their moving to less costly or restrictive jurisdictions (*ibid*, p. 26). He suggests that the movement of funds held on pre-paid cards should be regulated with an obligation to declare same in line with requirements for the movement of hard currency (*ibid*, p. 28). This, however, does not address the possibility, as

[8] Mules are people who allow their bank accounts to be used for the transmission of illicitly gained funds. Alternatively they may be recruited to open accounts in their own name for the same purpose.

[9] Smurfs are individuals who are recruited to make numerous small value financial transactions in an attempt to disguise the total value of the transaction. Their actions are known as 'smurfing'

already mentioned, of a card being loaded remotely from a foreign country after it passes any border checks. Zerzan (2010, p. 5, 7) suggests greater emphasis on collecting KYC information where higher value transactions or certain geographical usage are requested. He also claims that such measures would have little effect on the availability of these services to those who cannot access mainstream bank services. However the provision of KYC documentation may be a barrier for some of those legitimate users, especially amongst those with low incomes, and as such would require careful consideration of what amount constitutes 'higher value'. He also calls for countries to recognise the significance of these items as financial products to ensure that they are dealt with under financial regulation.

Online Payment Systems

Online payment systems evolved from the expansion in online shopping, the need for a convenient payment system and for some users, risk concerns about using mainstream credit cards online. These issues have been addressed with the provision of intermediary financial services such as *PayPal*, *Moneybookers* or *Neteller*, some also providing virtual and/or real pre-paid credit cards. Online payments systems are available either to those acting on a personal basis, as a charity or as an online business. As with many NPM's, these systems will have been examined by criminals and/or terrorists as potential ML or TF tools. With increasing popularity, *PayPal* claims 200 million users' worldwide (Zerzan, 2010, p. 21) and *Moneybookers*, over 33 million users, [10] providing the potential to hide ML or TF transfers in the midst of numerous legitimate transactions, leaving these systems liable for criminal or terrorist misuse (Jacobson, 2010, pp. 356-357; Tibbetts, 2002,

[10] https://www.moneybookers.com/app/

pp. 22-23). Customers can, in certain countries, register for these services with either no or minimal provision of identity documents. Even where they are required they are provided on the basis of no face-to-face contact, which lends itself to identity theft (Zerzan, 2010, p. 22), or use of forged documentation. The accounts can then be funded by various methods, including prepaid credit cards, bank accounts, etc (Filipkowski, 2008, p. 21). Many online payment service providers depend on a customer's bank or credit cards details providing some level of AML/CFT compliance (Zerzan, 2010, p. 21).

Once registered, customers can process transactions to and from virtually anywhere in the world and with great speed. This speed of transaction, which is very attractive to legitimate customers, could also aid illicit use, funds could be transferred onwards or withdrawn before any counteraction was taken (Zerzan, 2010, p. 21). Additionally, with no means of verifying that goods or services were actually exchanged, there is great potential for 'trade based' money laundering (Melongi, 2010, p. 208; Smith, 2012, p. 38; Tibbetts, 2002, p. 22). These facilities are not provided by regulated, mainstream FSPs (Filipkowski, 2008, p. 21; Melongi, 2010, p. 206; Zerzan, 2010, p. 21), and what designation they fall under is a matter of some debate (Gonzalez, 2004, pp. 7-12), a confusion which would be an asset to those who would use them for illicit purposes. In addition, a lack of training, understanding and commitment to countering terrorist use of the internet, TF and ML in at least some countries is a concern (Jacobson, 2010, pp. 359-360). While terrorists in particular have become wary of detection while using online payments, there is a strong probability that there will be a continued expansion in misuse of internet based financial systems (Jacobson, 2010, pp. 358-359), some even going so far as to see online payments systems as being amongst those most at risk (Smith, 2012, p. 38). There is a lack of record keeping which will be a serious impediment for law

enforcement agencies who may wish to trace particular transactions made via these services (Zerzan, 2010, p. 21). As with all internet based financial services, the 'no-border' nature of the internet and the problems that it causes for law enforcement, allied with the slowness or unwillingness to respond to change which blights some governmental & international countermeasures, could cause problems (Jacobson, 2010, pp. 359-360; Smith, 2012, p. 38).

Dealing with the needs for customer identification and profile details, Zerzan (2010, p. 21), notes than many of these systems require the customer's bank or credit card details before they can be used for significant transaction values. He sees this as a solution to regulatory requirements around CDD and also provides an opportunity for detection of suspect transactions. However, as previously discussed, a reliance on a different entity, for example a mainstream bank or credit card company, having completed proper identification and CDD procedures is a risk. In addition, prepaid credit cards, which can be used to fund some online payments systems, are available with minimal KYC information or documents, and it should be noted that the detection of suspect transactions is made more difficult as more layers are added to transactions. Additionally, a mainstream FSP might not suspect an incoming or outgoing transfer from an online payment service such as *PayPal* as being ML or TF. For example, an international transfer of cash might trigger a warning but this information will not normally be available to them when an online payment system is used.

Zerzan does note some efforts at mitigating the risk, by the sending of post, the placing of telephone calls or the processing of a small transaction from and to the customer's account which necessitates the customer's verification of the amount as a proof of ownership. While the later may be effective, providing the bank account

has not been compromised, the idea that post sent to an address confirms the person's permanent residency is not. It is comparatively easy to have the use of an address with no real connection to it, via short term rental, illegal use or interception of post. In the same way a phone call, to a number registered on the customer's profile details, may not be sufficient where that number is an unregistered mobile phone. These are readily available in many countries with no requirement for either KYC information or documents. In recognising the need for regulation, Zerzan also identifies the need for international cooperation in regulation to ensure that standards are maintained equally, but also ensuring that they do not stifle further growth (*ibid*, pp. 23-24).

Melonghi (2010), speaking in general terms about internet payment systems, calls for greater involvement from government bodies such as Financial Intelligence Units (FIUs) and Central Banks. He urges a concentration on general solutions rather than a concentration on individual misused products and that services should not be repressed. Problems, and solutions to those problems, should be watched for and addressed when the product is being designed. Products should encourage licit users while hindering or blocking illicit use. Features such as immediate transfers of funds and anonymity should be prevented and records of transactions maintained. He recommends that attention should be paid to the initial placement phase, when the funds are changed from hard currency into electronic form, that restrictions may need to be placed on the maximum amount of cash transactions, and that even newer payment methods should be monitored as they become available (*Ibid*, pp. 210-211).

Digital currencies, Virtual currencies and Virtual worlds

Alongside online payments systems, digital or virtual currencies are becoming increasingly popular for the payment of online sales of goods and services. First appearing in the 1990s the expansion of the World Wide Web has increased their popularity in the last ten years. Digital currencies take many different forms ranging from those simply held in a national denomination or linked to precious metals, used with avatar based virtual worlds such as Entropia Universe, or held in internet-based currencies with no tie to real world currencies, existing purely online. Usually set-up for practical reasons, allowing for online payments for sales or services, others were established due to a political viewpoint rejecting centralised government involvement in financial affairs and state-regulated banking systems (Grinberg, 2012, p. 165, pp. 172-173; Kaplanov, 2012, p. 11). Once established, intermediary involvement with the customer ends, with no further involvement in the same way that, for example, banks process card transactions (Zerzan, 2010, p. 26).

As with many NPMs, high transaction speeds, potential anonymity, the security of not using a credit card for online transactions as well as the ease with which digital currencies can be sourced, makes them attractive to those who need to move funds locally or globally. For many businesses knowing that, unlike a credit card transaction, a digital currency transaction cannot be cancelled is reassuring. With many transactions, for example using *Bitcoin*, a transaction is difficult to trace back to an individual in the real world. The identifying address is usually only used once and, as such, cannot be linked to an identifiable person or organisation (Stokes, 2012, pp. 225-226). Digital currency accounts are often available with the provision of an email address and a real or fictitious name, no KYC process takes place and no verification to ensure the details are valid (Hett, 2008, p. 3, 9). Even where some

form of identification process takes place, the risk of misuse remains high, added to by a lack of face-to-face contact (Hett, 2008, pp. 8-9; Stokes, 2012, pp. 224-225).

While there have been some moves to address the issue of unregulated digital currencies in some countries, the problem of countries that have not taken action remains a serious one. This lack of regulation can allow the safe passage of illicit funds that might otherwise be reported by a regulated FSP (Hett, 2008, p. 3, 4; Stokes, 2012, pp. 224-225), while the lack of any account monitoring or reporting of suspect transactions, and confusion around industry regulation adds to their vulnerability (Zerzan, 2010, pp. 26-28). Funding of the accounts can take many forms often involving a Digital Currency Exchange (DCE). Real world currency can be exchanged for various digital currencies, paid for by cash, cheque, bank transfer, prepaid credit card, etc. (Hett, 2008, pp. 9-10). Digital currencies can be used in a number of ways, including as a funds transfer via a DCE to a bank account or to load a prepaid credit card (Hett, 2008, pp. 11-12).This ability to transfer funds into a bank or prepaid credit card anywhere, but especially to countries with poor regulation and AML/CFT compliance, would be useful for illicit purposes (Hett, 2008, pp. 9-11; Stokes, 2012, pp. 224-225). The speed with which transactions can take place is also helpful for TF or ML, making any subsequent attempt to retrieve the funds difficult if not impossible where funds rapidly move onwards (Stokes, 2012, pp. 225-226; Zerzan, 2010, p. 26). Digital currencies can also make the employment of 'smurfs' very effective, allowing them to process multiple, high speed, small value transactions instead of one larger transaction, diverting attention and making any subsequent investigation extremely difficult (Brezo, *et al*., 2012, p. 23; Stokes, 2012, p. 226).

Overall, features such as anonymity, ease of use and lack of traceability or record keeping, make digital currencies attractive for ML or TF (Hett, 2008, p. 2). Digital currencies can be used for purchases at a limited number of real world retail outlets but are more readily accepted on various online retail sites. While the majority are legitimate, concerns have been raised about their acceptance at entities such as *Silk Road*, an online facility which it is allegedly used for the illegal sale of drugs, drawn to *Bitcoin* by the lack of regulation, the ability to remain anonymous and the lack of transaction traceability (Brezo *et al*., 2012, p. 23; Christin, 2012, pp. 2-4; Villasenor *et al*., 2011, pp. 6-7). An example of how digital currencies can be misused for ML or TF is seen in the case of *e-Gold*. This digital currency operator pled guilty to various crimes including ML and operating an unlicensed money transmitting business. Investigators found that accounts were opened by the provision of an email address, could be funded with real world currency through various DCEs and once opened could be used to conduct anonymous transactions (Villasenor *et al*., 2011, pp. 7-8). It is claimed that one US official described *e-Gold* as "*PayPal* for terrorists" (Hett, p. 7). It is also claimed that *e-Gold* staff were aware of the ML, did nothing to deal with it, even noting their customer's crimes (Zerzan, 2010, p. 28). Where *e-Gold* differed from other digital currencies was that despite claiming that it was based outside the US (*ibid*, p. 28), some of its senior company officers were known to be living there (Villasenor *et al*., 2011, p. 8). These company officers could therefore be charged under US law.

Examining the situation in the US, Hett cites issues around attempts to regulate the market and the problem around the cross-border nature of the internet, seeing a need for strong international co-operation (Hett, 2008, pp. 4-5, p. 12). His recommendations include a review of digital currencies features, the elimination or reduction of customer anonymity and greater limitations on worldwide usability. He

also recommends comprehensive record keeping and limitations on the total funding allowed, transaction size and transaction type. Hett identifies a need for specific regulations relating to the industry, and possible bans on the use of digital currency funded, prepaid credit cards from less well-regulated countries (*ibid*, pp. 35-36, p. 42).

As a solution to his concerns, Zerzan suggests greater international regulation and cooperation, due to the cross-border nature of the internet. He also suggests a greater focus by individual governments given the example of the *e-Gold* case. Zerzan acknowledges that some providers have already implemented enhanced CDD procedures and sees that as proof that such measures will not adversely affect the market (Zerzan, 2010, p. 28). However his claim that a lack of known ML or TF cases indicates a lack of misuse has to be questioned. The prosecutions for ML from the *e-Gold* case may just be an example of where digital money launderers were unlucky.

Stokes (2012) argues that the possibility of *Bitcoin*[11] or *Second Life's*[12] *Linden dollars* being used for large scale ML or TF are slim. He recognises a factor facilitating the use of mainstream banking for ML or TF, as being the immense number of legitimate transactions, in the midst of which illicit transactions can be hidden in a cloak of legitimacy (Stokes, 2012, p. 226; Stringer, 2011, pp. 104-105). As high numbers of transactions are not yet available in either *Bitcoin* or *Second Life's* financial systems, large value transactions are noticeable. In addition any such large funds transfers from or to real world currencies could seriously affect the exchange rate and

[11] Bitcoin, see https://bitcoin.org/en/
[12] Second Life, see http://secondlife.com/

stability of the virtual currency. In particular any such exchange rate movement would be noticed by the *Linden Dollar Exchange*, who suspends dealings if values fluctuate too markedly. As an extra protection the Linden exchange has placed restrictions on the total value of any transaction therefore making large withdrawals a lengthy process (Stokes, 2012, pp. 226-227). However while these factors may prevent large scale illicit usage they do little to prevent the smaller scale ML or TF that occurs with greater frequency. Not every money launderer or terrorist needs to move US$ 100,000, and while it is not possible or practical to prevent every case of ML (*ibid*, p. 233), detection of smaller value, suspect transactions is possible where proper KYC has been performed. *Second Life* may have a US$5000 individual limit for monthly transfers but that amount of money, possibly multiplied by other individual accounts of the activists involved, would have been of great use to the terrorists that attacked the London and Madrid transport systems in 2005 and 2004. Stokes does acknowledge that digital currencies could be used for small scale ML, and the need for greater caution, preferably pre-emptive, should digital currencies become more popular (ibid, p. 232). In an examination of current legislation in the UK he cannot identify any that is suitable for the regulation of either virtual world currencies or digital currencies. He draws comparisons with the UK's online gambling market, examines how it is regulated and suggests that it is a suitable model (*ibid*, pp. 227-230). He further suggests that the DCE's and currency providers should each establish procedures for the monitoring of transactions for suspicious activity. Stokes especially views the need for the involvement of DCEs, and the application of correct CDD procedures, as that is the entry point for those involved in ML or TF (*ibid*, p. 230). He also identifies problems with this in relation to the decentralised nature of *Bitcoin*, as there is no central organisation on which rules can be imposed. Therefore, he sees a need for even greater concentration on the regulation and registration of DCEs that handle entities such as *Bitcoin* (*ibid*, pp.

230-231). Stokes also cites the need to ensure that legitimate use of the system is not burdened with regulations, thus stifling growth.

As shown in Stoke's (2012) paper, digital currencies have found a niche in such virtual worlds and role-playing games as *Second Life*, *Entropia*[13] and *World of Warcraft*[14]. Initially used for leisure purposes these 'worlds' have developed many other uses, including various forms of training including medical, business, military and law enforcement. Universities employ them for various educational purposes while business's use virtual worlds for training, meetings, advertising or sales. However any sales are conducted via a link to their real world website thus placing those transactions in the real rather than the virtual world (Keene, 2012, pp. 26-28). Players or residents join these worlds or games easily, just requiring a computer, a good internet connection and email address. They can then set up an account giving very basic or even fictional profile details, which are usually not verified, and an avatar (Keene, 2012, p. 27). Payment systems are initially used for the payment of an entry fee into some virtual worlds. Real world funds, exchanged for digital/virtual world currencies either within the virtual world or at independent DCEs, can be used to pay for these transactions. In addition, within the virtual world itself, it is possible to buy or sell various enhancements, or to create virtual items and facilities which can then be sold on to other residents or players (Irwin & Slay, 2010, p. 43; Keene, 2012, pp. 27-29; Villasenor *et al*., 2011, pp. 9-10). This ability to conduct economic transactions, with real world exchanged for virtual world currency, then back into real world currency after the sale, opens up the possibilities of the virtual worlds being misused for ML or TF (Chambers, 2012, pp. 342-343;

[13] Entropia, see http://www.entropiauniverse.com/
[14] World of Warcraft, see http://us.battle.net/wow/en/

Landman, 2009, p. 5177). As previously outlined, DCEs accept various means of payment which could allow misuse, including cash, prepaid credit cards or bank transfer (Hett, 2008, pp. 9-10). In many ways these virtual worlds have developed many of the features of real world economies, and inevitably will have attracted the attention of those who would use their financial facilities for illicit use (Chambers, 2012, p.343; Landman, 2009, p. 5172). However, unlike large parts of the real world economy, there are no financial regulatory bodies monitoring misuse for ML or TF. KYC documents are not required on joining most virtual worlds or before allowing use of their financial systems, something which promotes anonymity (Landman, 2009, p. 5172). As with many online only FSPs, problems are faced in identifying customers, with the potential difficulty of recognising counterfeit or stolen identity documents which are forwarded via email (Landman, 2009, p. 5172). *Second life*, one of the biggest virtual worlds in existence is viewed as particularly vulnerable, lacking in verification of identity procedures, leaving them incapable of providing meaningful information or intelligence in the event of customers or transactions being investigated (*ibid,* p. 5173). However, *Entropia*, another popular virtual world, is said to be more comprehensive in their processes (*ibid*, p. 5173). One consequence of the lack of financial regulation is that there appears to be no meaningful account monitoring for suspicious transactions, no retention of transaction records, no transaction value limitations and no ability to identify end recipients when funds are transferred back into real world currencies (Keene, 2012, p. 32; Landman, 2009, pp. 5172-5174). In addition there appears to be some confusion about what actually constitutes a real life crime when committed in a virtual world, leading to further confusion regarding potential regulation (Keene, 2012, p. 29). As with other digital currencies and NPMs, the ease with which accounts can be set up could result in 'smurfs' being used to disguise the origins or destination of funds and create seemingly clean funds (Keene, 2012, pp. 32-33).

Similar methods could be used as an illicit TF transfer of funds. These various factors; anonymity, accessibility, funding methods, the ease with which accounts can be set-up, are almost tailor made to meet the demands of ML (Landman, 2009, p. 5166, 5171) or TF. Crimes of theft do occur on virtual worlds (Keene, 2012, pp. 30-31), and while there is no evidence of terrorist involvement, one has to ask if such crimes have, in a reflection of the real world, been committed in the past as a form of TF. There is also no evidence of misuse of virtual worlds for ML or TF with effect January 2012, this does not mean they have not occurred (Landman, 2009, pp. 5172-5173), but could be more indicative of the lack of regulation, account monitoring, etc. that appears to be prevalent in most virtual worlds.

Reviewing the regulatory regime in the US, Landman (2009) feels that existing legislation is sufficient, so that once notified, virtual worlds will have to comply (*ibid*, pp. 5180-5182). He sets out various requirements that they will have to meet, including enhanced identification processes, maintenance of records and monitoring of governmental watch lists. Landman states that a link must be capable of being proven to an identity and address, and also to a bank account. He suggests that checks are carried out to ensure that the information provided is correct, in so far as it is possible to be checked. Aware that such measures will have cost implications he suggests that virtual worlds should have two membership levels, one for members who wish to engage in financial transactions and one for those who don't (*ibid*, pp. 5182-5183). However, these suggestions do not address a number of issues. Firstly there is the possibility of identity theft where someone may have someone else's social security number, address, date of birth etc. If no face-to-face contact is made and no real world post sent out, how can it be confirmed that the avatar is actually the person named and listed at the address given? Secondly, while it is to be hoped that US banks are well regulated and complaint with their AML & CFT requirements,

this would not be the case in at least some European Banks[15]. Therefore dependence on them as part of the KYC process would be inadvisable. However where funds can only be transferred from and to a bank account it severely reduces the possibilities of misuse unless the account has been compromised.

Keene (2012) calls for clarification on where the real world ends and the virtual world begins regarding crime, what constitutes a crime in a virtual world, and for improved regulatory requirements on CDD, identification and monitoring/reporting. She also calls for risk analysis to be performed on certain support systems, including currency exchanges, and, where appropriate, brought in under a regulatory umbrella requiring mandatory suspicious transaction reporting. In identifying anonymity as an issue, she suggests that the monitoring of Internet Protocol (IP) addresses and the information available from the customer's credit card should provide sufficient to allow identification (*ibid*, p. 33). However, this is not always the case. As previously noted an IP address can be disguised by the use of technology (Christin, 2012, p. 2, 4; Hinnen, 2004, P. 11; Irwin *et al*., 2013, p. 21), more and more people are using free Wi-Fi, and internet cafes are often available, all of which render the chances of tracing someone through their computer usage virtually impossible (Irwin *et al*., 2013, p. 7). With regards to credit card information, compliance issues may be just as serious with credit cards accounts as routine bank accounts. Prepaid credit cards are increasing in popularity and available with minimal KYC requirements. One prepaid credit card provider, which advertises itself as a virtual world 'friendly' card, offers limits up to E2500/US$3500, complete anonymity and no identification requirements. Finally, Keene (2012, p. 34) identifies the need for international cooperation in countering

[15] As detailed in Chapter three, see footnote 66 for details.

criminal exploitation of the systems, also calling for continued vigilance in monitoring emerging technology for potential criminal misuse and as a means of fighting criminality.

Mobile phone-based financial services

The popularity and importance of mobile communication devices such as mobile/cell phones impacts almost every part of the world (Bronk *et al*., 2012, p. 135; Merritt, 2010, p. 2; Villasenor *et al*., 2011, p. 12; Vlcek, 2011, p. 416; Zerzan, 2010, p.15). Initially used purely for communications they now provide access to the internet, gaming, music, films and, of interest in the study of ML and TF, financial services. Mobile phone banking services have two main types. The first is linked to the customer's mainstream bank account while the second is linked to the funds held in an account with their telecommunications provider. In some cases this latter service is provided by a combination of mainstream bank and telecommunications provider. The demand for these services has been particularly noticeable in areas of the world where mainstream financial services are difficult to access; due to poor infrastructure, a lack of nearby mainstream FSPs, or are not readily available to some sections of the community (Villasenor *et al*., 2011, p. 11; Vlcek, 2011, p. 421). Initially these mobile phones or devices only provided enquiry facilities for mainstream bank accounts, something which in itself posed no great threat. But as demand grew they developed into a means of conducting transactions, in effect another expansion in customer services (Merritt, 2010, p. 4, 7).

Effectively these mobile phone services provided by regulated FSPs, have no greater risk of ML/TF than any of the other options available to customers such as online banking or ATM withdrawals (Zerzan, 2010, pp. 10-11). But this is only the case where good compliance is in place. The provision of similar services by providers

from outside the mainstream FSPs does raise some concerns. As with many NPMs, anonymity is an issue with either minimal, or no, identification being required by some providers, and the popularity of unregistered prepaid phones (Zerzan, 2010, p. 11). Even where identification is provided at the initial stage, there are problems with potential misuse of a system operating on a remote basis. For example, the provider cannot be sure who is using the facility; the phone could be used as a 'community' phone, could have been stolen or passed on to criminals, or passed on by a wealthy owner to an employee or subordinate family member[16]. This latter scenario could even be a problem where customer profiling has been completed. The phone could be misused by the designated user, large transactions taking place which would appear to fit the profile of the owner, but passing undetected and unknown by them (Zerzan, 2010, pp. 11-12). Another commonplace concern shared with other NPMs is transaction speed. This can lead to a rapid movement of funds (Merritt, 2010, p. 19), with difficult to unravel, layering of transactions disguising the origin of the funds. This can easily be achieved by one or more people with access to several payment-capable mobile phones (Zerzan, 2010, p. 11; pp. 16-17). Looking at cross-border transfers via these facilities multiple transfers are amalgamated by the provider for ease of transmission before being divided out to their destination networks. When this occurs the chances of detection are reduced as regulatory bodies in the sender or receiver's country cannot immediately access information on the originator of the transaction (Zerzan, 2010, p. 16). While this information may be available eventually from the service provider, delays are critical and there is the risk that the funds would have moved on. There is also the potential lack of relevant regulation and oversight, in part due to the newness of

[16] While some of these examples are more relevant to particular societies, they may impact on Europe with the increasing numbers of migrant workers entering the EU.

services which, in many cases, will have arrived after many countries had implemented their AML/CFT regimes (Zerzan, 2010, p. 12) In addition many countries experience problems in identifying which government department or agency is responsible for regulation (Merritt, 2010, p. 18; Vlcek, 2011, pp. 423-424; Zerzan, 2010, p. 12). There are also issues around differing standards of regulation in different jurisdictions (Merritt, 2010, p. 25).

Having identified various concerns, Zerzan looks at possible solutions. Specialised KYC requirements, tailored to suit a countries individual situation, would include limits on the value and type of transactions processed through the phone where CDD was minimal, customer identity established by reference to various reliable databases, and compulsory registration of phones. However these identity and address confirmation measures would be of little use where identity documentation is either not normally held, perhaps in a poorer economy, was not available from a customer due to their individual circumstances or, for example, where the customer is resident in a rental property. Zerzan does mention various technical solutions such as biometric authentication and electronic signatures as means of authorising transactions. But how this would work without excessive costs where customers are living in remote areas is unclear (Zerzan, 2010, p. 13). Customer profiling, the monitoring of accounts and internal controls are also mentioned as potential solutions, and while these would allow for the detection of potential large scale ML and potential launderers or terrorists on various governmental and international watch lists (Zerzan, 2010, pp. 14-15), they would do little to prevent ML by smurfing or small value TF transactions, a concern which is raised by Merritt (2010, pp. 18-19). However Zerzan's suggestion of a centralised registry of account holders has great merit and could in fact be useful to mainstream FSPs across the world. With this facility, customer profile details could be checked to ensure that multiple

accounts were not in operation in different institutions, thus making ML layering operations between multiple accounts in the same name difficult. In addition it could be the solution to an age old fraud problem of 'kiting' where a customer moves funds between various accounts in their own or a false name, eventually hoping to leave one account in debt, a debt they do not intend to repay. Government provided guidance and the registration of providers is also suggested. Guidance would provide new or existing providers with details of their responsibilities and duties regarding AML/CFT compliance. If correctly drawn up, they would leave little room for uncertainty with registration of providers ensuring that these guidelines were complied with (Zerzan, pp. 14-15). Zerzan's claim, that the lack of any detected cases of mobile phones being used for TF is a positive sign, may be optimistic. Ehrenfeld (2009) as cited by Vlcek, (2011, p. 424), illustrates how funds could be moved in an anonymous, untraceable manner very suitable for TF. Given Zerzan's own analysis of their potential usefulness for illicit purposes, allied with the difficulties in detecting same, it is very possible that TF or ML misuse of mobile payment systems has occurred. TF or ML in a financial system is difficult to detect even in a well regulated environment with trained financial services and regulatory staff available. How much more difficult will it be to detect TF in an unregulated system where, for example, anonymity is often not only possible but the norm? In addition Zerzan does not address the problems around the inexperience of staff employed in retail outlets or by the provider, in AML/CFT compliance issues (Merritt, 2010, p. 18, 19), or the possibility of some of those staff being complicit in illicit use of the system (Villasenor *et al*., 2011, p. 12-13).

Merritt (2010), in response to potential misuse of the systems, suggests various solutions to the situation in the US, but with lessons that may be relevant elsewhere. She sees that greater cooperation needs to be implemented between the financial

and communications regulators to allow knowledge sharing, as neither understands the entire complexity of both systems, and suggests that a single entity should be set up to regulate the industry. She also urges better international cooperation to counter any potential illicit cross border transfers and that industry should establish appropriate AML and counter fraud procedures (Merritt, 2010, pp. 25-28).

Vlcek (2011), sees the organisation of regulatory bodies as being vital, and the decision as to which will be responsible for a provider as equally so. He suggests a risk-based approach which will find a balance between ensuring that growth is sustained, and that misuse of the system is minimised (Vlcek, 2011, pp. 426-427). Vlcek also advocates that anonymity should not be allowed and that proper identification should be required (*ibid*, pp. 424-425).

Online banking services

As well as allowing access via mobile technology applications, most mainstream banks now offer online banking, in many cases this being their preferred way of dealing with customers. However the remoteness of these contacts may leave a potential for same to be abused where a launderer has access to various accounts by way of identity fraud or bribery. The launderer can then create layers of transactions using multiple accounts, some of which can take place instantaneously (Filipkowski, 2008, p. 19). The ability to transfer funds in a rapid, convenient and potentially global basis will make online banking attractive for illicit use (Bensted, 2012, p. 242; Hinnen, 2004, p. 12). The different regulatory requirements relating to online banking, in different jurisdictions, are also seen as creating vulnerabilities (Filipkowski, 2008, p. 21; Hinnen, 2004, p. 28). The lack of face-to-face contact is also identified as making the establishment of the customer's real identity difficult (Bensted, 2012, p. 243). However in comparison with various NPMs, mainstream

FSP's online banking services are less at risk of being misused for ML or TF(Bensted, 2012, p. 244), forming an extension of existing services, with enhanced security measures to reduce fraud (Zerzan, 2010, pp. 19-21). This, however, does not address the provision of services by mainstream, regulated banks that operate on a completely remote basis, never meeting their customers on a face-to-face basis, with all the associated problems of customer identification etc. Fossat *et al*., (2012), recognises the many advantages that online banking provides for criminals or terrorists, including lack of face-to-face contact, ease of use, etc. They also recognise the important role that mainstream banks have had in CFT and AML in the past, and call for an even greater focus in future with the expansion of online banking services. But their call for the same levels of regulatory requirements for those opening accounts remotely or face-to-face is a matter for concern (*ibid*, 2012, p. 8-9). Where this occurs enhanced CDD should be implemented to compensate for increased risk levels.

Summary

This chapter reviewed existing literature dealing with NPMs and other less obvious means of laundering or moving funds based on the internet. After briefly looking at the impact of ML, its constituent parts and types of ML, it moved on to look at the interaction of old and new world ML. The potential misuse of online gambling was reviewed along with the reaction of both industry and regulators. The following section examined prepaid credit cards, their practical uses, potential for anonymity and solutions addressing their potential misuse. Online payment systems are addressed in the next section, with details of what makes them attractive for misuse before moving on to look at possible solutions. In the third section digital/virtual currencies were reviewed, looking at the reasons for their existence, the ease with which they can be obtained, risks and actual cases of misuse along with potential

solutions. Finally the potential misuse of virtual words for financial crime is examined as are solutions to that misuse. The final section looks at payment capable mobile phones. It reviews the various types of service available, their popularity in different regions, the potential for misuse as well as preventative measures. The section ends with a brief look at online banking services.

Comparing the researcher's findings to those in this review we can see, despite none of the papers having dealt with the ROI or UK, some commonality in the issues addressed. With regards to prepaid cards, the anonymity allowed by non face-to-face contact between provider and customer noted by Choo (2009, p.17), King (2012, p. 1), Linn (2008, p. 147, 156, 182), Sienkiewicz (2007, pp. 12-15) and Zerzan (2010, p. 5) is also a major factor in both the ROI and UK. Additionally, the anonymous lodgements cited by Choo (2009, p. 15) and Simser (2013, p.44) are also present in the UK and ROI as are the cash lodgements noted by Linn (2008, p. 147) and Sienkiewicz (2007, p. 16, 19, 20). Choo's (2009, p. 17) concern that provider staff may not have sufficient AML/CFT training could also explain why ROI card provider staff did not know which number from a driving licence was the correct identification number to use or that use of a centralised delivery address should not be permitted. As noted by Choo (2009, p17), Linn, (2008, p. 154), Sienkiewicz (2007, pp. 20-21) it was feasible to buy a number of prepaid cards without detection, thus opening the possibilities of higher value ML or TF. However, the potential noted by Linn (2008, p. 164) and Zerzan (2010, p. 5,7) for control of funds coming into a country by way of a declaration on entry, was proven wrong by the loading in the ROI of a card while it was being used in the US.

Looking at online payment systems, again we see some similarities between the researcher's findings and those shown on the papers, but not as many as in the

prepaid card section. For example, Filipkowski (2008, p. 21) notes the funding of the accounts by prepaid card or bank account. Zerzan (2010, p. 21) notes the dependence on a link to an account with a regulated FSP as providing part of the provider's compliance requirements. However, his view that this can safely be used as part of that requirement (*ibid*, p. 21) is at variance with the researcher's concerns about regulatory compliance at some mainstream FSPs. Similarly Zerzan sees the contacting of a customer by post, or the receipt of a phone call as being a positive matter (ibid, pp. 23-24). However, this has been disproved in both the ROI and UK, by the researcher's ability to open payment accounts using unattached addresses and untraceable phone numbers. Melonghi (2010), sees the prevention of immediate transfers and anonymity, and a cap on transaction values as being important (*ibid*, pp. 210-210). While the researcher certainly agrees that removing anonymity is vital, and that a limitation of transfer values is an important measure already in place in the EU, placing delays on transactions may result in a fall-off in popularity. A far better solution would be to make any rapid transfer traceable, through the use of a certified KYC document scheme or the provision and verification of the social security number of at least one of those involved in the transfer.

The next chapter examines the EC's electronic-money (e-money) regulation and its implementation in the ROI and UK, as well as assessing the impact of other relevant regulations on AML/CFT compliance.

CHAPTER 3

THE REGULATION OF E-MONEY IN THE REPUBLIC OF IRELAND AND UNITED KINGDOM

This chapter examines the history of e-money regulation in the EU, comparing and contrasting the implementation of those regulations in the ROI and UK. It also looks at the impact of other EC and local regulations on the e-money industry, as well as the history of AML and CFT regulation. The regulatory measures implemented to increase customer confidence are charted as well as those created to help the growth of the e-money market.

The e-money market in the EU has been heavily influenced by the regulations it is obliged to operate under. As will be seen later on in this chapter, the idea that early e-money regulation was hindering rather than helping the growth of the market led to concerns for the EU. By the time the second e-money directive had been implemented the burden on providers had been considerably reduced by the risk-based analysis of e-money as low risk and therefore eligible for simplified CDD. This allows FSPs, and specifically those e-money products that qualify, to operate with significantly reduced levels of KYC information or documentation. It is this reduced level of regulatory requirements, along with the lack of face-to-face contact between provider and customer that may have left e-money products and services vulnerable to misuse.

The need for regulation in the 'new world' of electronic financial transactions was recognised by the EC as early as 1987. While mainly dealing with card based transactions on accounts held with mainstream FSPs, *Commission Recommendation 87/598/EEC* (European Commission, 1987) set out some basic principals which hold

true to this day. These included the benefits of flexible regulation, the need for cross-border compatibility and the use that could be made of electronic payments to expand the internal market of the European Economic Area, as well as modifying and widening the provision of financial services (European Commission, 1987, pp. 72-73). This latter feature would facilitate an increasing variety in the types of service available, encourage innovation and the development of new products, and therefore aid, rather than stifle, the growth of this particular financial services market. A decade later, in 1997, the EU addressed the greatly expanded and diversified use of ICT by the financial services sector with *Commission Recommendation 97/489/EC* (European Commission, 1997). This document dealt with the advances that had occurred over the previous ten years in such 'mainstream 'banking services as credit cards and online banking. The recommendation also addressed, to a limited extent, examples of e-money systems such as stored value cards and computer-stored electronic tokens, although the recommendation specifically excluded non-reloadable financial instruments (European Commission, 1997, p. 51). However, neither recommendation contained any specific details of AML or CFT requirements. In April 2001 an EU-commissioned report (European Commission 2001) into the effectiveness of the directive was published, but by then the EC had already issued a new directive, which specifically dealt with the issue of what became commonly designated as e-money.

Directive 2000/46/EC: The EC's first e-money directive

On October 27 2000 the EC issued *Directive 2000/46/EC* (European Council, 2000c). The directive dealt specifically with e-money, addressing many of the unique characteristics of products such as prepaid cards and online payment systems. One of its chief aims was to provide a single market for these products across the EU, irrespective of national borders, by harmonising the relevant regulations of the

individual member states. In so doing it was hoped that the directive would lead to the development of e-money to its full potential and prevent the stifling of new providers or technologies entering the market. Effectively this meant that an operator, once authorised, could provide services across all member states. Amongst other issues, the directive recognised the need for specific regulations for e-money and that it was a supplementary form of currency (European Council, 2000c, p. 39). The directive set the parameters for the creation and operation of Electronic Money Institutions (EMIs). The specification of what constituted e-money was detailed in *Article 1*, namely that it should be issued at parity with the funds used to pay for it and must be accepted by entities other than the issuer. The article also restricted EMI activities to the issuance of e-money, banned the granting of credit, and instructed that providers must be registered as Credit Institutions to operate as an EMI. EMIs had been designated as Credit Institutions in *Directive 2000/28/EC* (European Council, 2000b) under *Article 1(1) (b)*. However *Article 2* of *Directive 2000/46/EC* (European Council, 2000c) established the responsibilities of EMIs for compliance with other directives such as *Directive 91/308/EEC* (European Council, 1991) and *Directive 2000/12/EC* (European Council, 2000a). For example, the right of an EMI to establish a branch in another member state is set out in *Article 20* of *Directive 2000/12/EC* (European Council, 2000a), while the right to provide services in other member states was set out in *Article 21*. Exemptions were also detailed in *Article 2*, for example, the initial capital requirements of mainstream providers or the need for each authorisation of a provider to be notified to the European Council. E-money transactions were also exempted from designation as a deposit-taking activity, with an exemption whenever funds were immediately exchanged for electronic currency. However, if there was a surplus of customer funds held by the EMI after the transaction had taken place this surplus was regarded as being covered under *Directive 2000/12/EC* (European Council, 2000a, p. 39). The

redeemability of funds was dealt with in *Article 3*, with funds to be available at parity, minimum fees or charges and a minimum transaction limit of no greater than €10. While based on existing regimes relevant to mainstream banking, *Articles 4* and *5* set out the unique capital, 'own funds', [17] and investment rules pertaining to EMIs. Where operating solely as an e-money issuer, either new or existing EMIs were allowed to operate with lower levels of initial set-up capital. EMIs were required to have a minimum initial capital of €1,000,000 rather than the €5,000,000 required for mainstream institutions. Mainstream institutions were also required to hold 'own funds' of 8% (European Council, 2000a, Article 47), whereas EMIs were only required to hold 2%. The monitoring of compliance with these requirements was set out in *Article 6*, while *Article 7* dealt with the requirements for internal procedures and controls. The authorisation of waivers from some or all of the directive's requirements was dealt with in *Article 8*. Member states could grant these waivers once the EMI did not normally exceed €5 million, and never exceeded a maximum balance of €6 million in outstanding e-money. It was also required to restrict the issue of e-money only to subsidiary entities or for use within a small geographic area, imposing a storage limit of €150. Such EMIs could only operate within the national borders of the member state where they were authorised. The continued operation and authorisation of existing EMIs is dealt with in *Article 9*, while *Article 10* required member states to have enacted the directive by 27 April 2002. A review of the directive by the EC to examine its application was detailed in *Article 11*, and was required to be completed by 27 April 2005. This requirement for a review, while looking at capital requirements, waivers, the possible need to introduce

[17] "To be able to absorb losses in a going or in a gone concern situation, institutions need 'own funds' in sufficient quantity and quality in accordance with applicable European legislation."
http://www.eba.europa.eu/regulation-and-policy/own-funds

customer protection and prohibit the payment of credit interest, made no mention of a need to examine the possible misuse of e-money for ML or TF. *Articles 12* and *13* dealt with the directive's entry into force and addressed the directive to the member states. The importance of a dependable, stable and properly regulated e-money sector was acknowledged in the directive as being vital to the stability of the financial system in general (European Council, 2000c, p. 40).

As set out in *Article 10*, member states were required to have enacted the directive by 27 April 2002. The UK did so on the due date with *The Financial Services and Markets Act 2000 (Regulated Activities) (Amendment) Order 2002* (United Kingdom 2002). Ireland followed suit on 29 May 2002, implementing a Statutory Instrument, the *Regulations entitled European Communities (Electronic Money) Regulations 2002* (Ireland 2002).

EMIs were also impacted by other EC directives. For example, *Directive 2002/65/EC* (European Council, 2002) which dealt with consumer rights under 'distance marketing' based financial contracts. But this along with a number of others did not affect the EMIs AML or CFT compliance issues. However EMIs did have AML and CFT responsibilities and these were set out in various EC directives that dealt with countering the laundering of criminal funds and the financing of terrorism.

Anti-Money Laundering: The first and second directives

At the time of the implementation of the first e-money directive, *Directive 2000/46/EC* (European Council, 2000c), the responsibilities of FSPs in relation to AML had been set out in *Directive 91/308/EEC* (European Council, 1991), the EC's directive on the prevention of ML. It should be noted that the directive was seen as a response to the growing problem of illegal drugs, and while mentioning other

criminal activity, TF was only mentioned as a minor part of the overall criminal use of ML (European Council, 1991, p.78). EMIs were regulated under the directive due to their designation as credit institutions. These responsibilities included the requirement to obtain copies of customer identification documents as set out in *Article 3*, while *Article 4* obliged the providers to retain them or details of same for five years after the end of the customer relationship along with details of the customer's transactions. They were also required to monitor customer transactions and report any suspicious occurrences to the appropriate authorities under *Articles 5* and *6*, and to ensure, under *Article 8*, that customers were not advised whenever their accounts or transactions were being investigated. *Article 11* obliged providers to implement adequate AML controls and provide adequate AML training for staff. The directive also set a monetary limit for 'occasional transaction'[18] at ECU15,000[19] in *Article 3*. There were various amendments to the directive but the main focus continued to be ML. Enacted on 4 December 2001, *Directive 2001/97/EC*, *Article 1, (2)*, (European Council, 2001a) amended various parts of the first AML directive, bringing other entities outside the financial services industry within the remit of AML legislation. It also widened the scope to include other criminal financial activities rather than just the sale of illegal drugs(European Council, 2001a, p. 76). While it contained no specific mention of e-money, it contained several aspects particularly relevant to FSPs acting on a distance marketing basis. For example, the verification of customer identification details by 'supplementary measures' or the use of a link to a customer's account with a regulated provider as part of the

[18] ' "Occasional transaction" means a transaction (carried out other than as part of a business relationship) amounting to €15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked' http://www.legislation.gov.uk/uksi/2007/2157/pdfs/uksi_20072157_en.pdf (p. 5)

[19] "The European currency unit, abbreviated as ECU, was the former currency unit of the European Communities, from its adoption on 13 March 1979 (replacing the 'European Unit of Account') to its own replacement by the euro on 1 January 1999, at a ratio of 1:1." http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Glossary:ECU

customer identification process is authorised under *Article 1(3) (11)*. Once again TF, for the most part, remained as a crime within a crime and was not dealt with as a separate issue.

Following the terrorist attacks on the US on 11 September 2001, *Council regulation (EC) No 2580/2001* (European Council, 2001b) was issued on 27 December 2001. Dealing specifically with TF, this represented a major change in attitude with the regulation stating that CFT was a "decisive aspect of the fight against terrorism" (European Council, 2001b, p. 70). *Article 1* of this regulation covered all types of financial services, including insurance, normal banking services such as consumer or business finance, foreign exchange, and all payment and money transmission services. The implementation of this regulation was, however, limited to a constantly reviewed list of individuals and organisations provided to the member states by the European Council in *Article 2*. The directive required the reporting of any suspected occurrences of TF to the relevant authorities was set out in *Article 4*. Responsibility as the competent authority for the implementation of this regulation was vested with the Central Bank of Ireland and, in the UK, HM Treasury department and the Bank of England which acts as the UK's central bank (*ibid*, p. 74). In addition to the EC issued regulations, the FATF issued recommendations specifically targeting TF which were implemented by many countries within the EU. For example, in 2003, Ireland issued 'guidance notes' to FSPs outlining concerns about TF. (Ireland 2003)

The Third EC Anti-Money Laundering Directive: 2005/60/EC

In 2005, the EC issued *Directive 2005/60/EC* (European Council, 2005), which, unlike the previous AML directives, dealt with the financing of terrorism as a separate issue alongside ML. It also specifically mentioned e-money. The directive

saw a major change from a rules-based system of regulation to a risk-based approach (Della Pellegrina and Masciandaro, 2009, cited in van den Broek, 2011, pp. 170-171). The directive was applicable, as set out in *Article 2*, to all aspects of financial service provision and to those involved in other activities, including the legal professions, accountants and external auditors. While EMIs had responsibilities under most articles of the directive, some had a particular significance and relevance to EMIs and those involved in their regulation. CDD was dealt with in Chapter 2, *Articles 6* to *19*, setting out the parameters for standard, simplified, and enhanced CDD. Member states were prohibited from allowing the opening or continued operation of existing anonymous accounts by *Article 6*. Standard CDD was specified in *Article 7* as a requirement to be applied when establishing a business relationship, or where there were suspicions of ML or TF, or when carrying out a transaction or transactions amounting to or greater than €15,000, or, finally, where previously provided customer data was inadequate or suspect. Confirming the identity of the customer or the beneficial owner of the account or service, and the information provided by them was set out in *Article 8*. Confirmation was to be by documentary evidence, collection of data or, and directly impacting on some EMIs, the use of information from a "reliable and independent source". Equally important to EMIs, while obliged to comply with all requirements set out under CDD, was the option for them to determine the extent of the CDD measures dependent on the risk-level of the product, customer profile, transaction type, or business relationship. The timescale for the receipt of this customer information was confirmed in *Article 9*. While normally to be received prior to the establishment of a business relationship, member states had the option of allowing it to occur during the establishment of a business relationship, but it had to be fully completed prior to any transactions taking place. Where the requirements were not complied with, the business relationship was to be terminated and consideration

given to reporting the event to the appropriate authorities. The article also confirmed that these provisions were also to be applied to existing customers, again on a risk-sensitive basis. The responsibility of casino operators to identify their customers was set out in *Article 10*.

It is in the second section of chapter 2 of the 2005 directive, which dealt with simplified CDD, that we find the most significant issues for EMIs/NPMs. Containing only two articles, the first, *Article 11*, covers those customers, products and services which are eligible for either complete or partial exemption from the requirements set out for standard CDD. Customers such as other regulated credit and financial institutions covered under the directive, similar non-EC institutions operating under equivalent regulations or public authorities were permitted to avail of simplified CDD, as were certain insurance or pension scheme policies. But of most significance to EMIs was the specific exemption granted to EMIs operating under the auspices of *Directive 2000/46/EC* (European Council, 2000c). These EMIs were granted an exemption, under *Article 11, subsection 5 (D)*, from certain provisions of *Articles 7, 8* and *9* of the directive. The exemption from *Article 7(a, b, and d)* removed the need to apply standard CDD when establishing a business relationship, when conducting a transaction or transactions equal to or greater than €15,000 or, surprisingly, when suspicions were raised about the veracity or adequacy of previously obtained customer identification data. The exemption from *Article 8*, removed the requirement for the provider to confirm the customer or beneficial owner's identity, the intended nature and purpose of the business relationship and to monitor the use of the account/product to ensure it matched the information provided by the customer. This exemption also removed the need for the provider to perform a risk analysis on their customer or their use of the product when deciding on a level of CDD. With the removal of *Article 8, Article 9* which dealt with the timetable for

verifying a customer's identity, the non-provision by a customer of identity verification items and the need to apply CDD to new and existing customers, was also removed. All of these exemptions for EMIs were only permitted for products with certain transactional limitations. They were restricted to storing a maximum of €150 when not capable of being reloaded, or €2,500 where reloadable. The redemption of funds was also limited to a maximum of €1,000. Finally, *Article 11* had a proviso allowing for the future addition of any low risk customer, product, service or transaction to the list of those eligible to be accessed under simplified CDD. However the application of simplified CDD to credit or financial institutions or to listed companies from countries which had, or was found to have, a weaker regulatory regime was prohibited under *Article 12*.

Also assessed on the basis of risk-analysis, Enhanced CDD was addressed in *Article 13*. This enhanced CDD would be applicable to EMIs where their customer was not eligible under the exemptions of *Article 11*, for example where the customer required higher transaction limits than those permitted under the exemption. This version of CDD called for more stringent and extended requirements to be implemented where a product, service, or customer demonstrated a greater risk of involvement in ML or TF. There was a focus on a number of issues, including trans-national relationships with non-EC based banks. Any regulated entity operating under the directive could only provide services once the relationship was approved by senior management, were required to establish the bone-fides of the non-EC FSP, ensure that they had adequate AML/CFT procedures in place, and had properly verified the identity of any customers that would operate 'payable-through' [20]

[20] "The Term *payable-through account* refers to correspondent accounts that are used directly by third parties to transact business on their own behalf."

accounts. They were also prohibited from continuing or entering into business relationships with 'shell banks'[21]. Politically Exposed Persons (PEPs)[22] from outside the home state of the service provider were also seen as a concern. Those operating under the directive were required to have procedures in place to identify such customers and to only allow the opening of accounts with the approval of senior management. Additionally, they were required to clearly establish the source of wealth and funds transacted through the account as well as closely monitoring any such customer for suspicious activity. This led to a requirement for the implementation of additional measures during the identification of customers where there was no face-to-face contact between customer and provider. Identifying such activity as being of a higher risk of ML or TF, *Article 13 (2)* required that a customer's identity be verified by one of more of the following: the provision of additional documents, data or information to that required under standard CDD, additional verification or certification of any documentation received or, finally, ensuring that a link to a regulated credit institution was made by receipt of a payment from an account in the customer's name. In an instruction to all FSPs, *Article 13* required that they pay special attention to, and prevent, the misuse of any service or product that could provide anonymous financial transactions.

As previously outlined in *Article 13(2)(c), Article 14* confirmed that EMIs, and those covered under the directive, could rely on another independent, but similarly regulated, provider's CDD as part of their compliance obligation. To do so they had

---

http://www.fatf-gafi.org/pages/glossary/n-r/

[21] "*Shell Bank* means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision." http://www.fatf-gafi.org/pages/glossary/s-t/

[22] Politically Exposed Persons or "*PEPs* are individuals who are or have been entrusted with prominent public functions" http://www.fatf-gafi.org/pages/glossary/n-r/

to be able to provide a valid link between their customer and the account held with the other provider. But even where this had been proven, the ultimate responsibility for compliance remained with the entity opening the account or providing a service for a new customer. Member states had the option, confirmed in *Article 14*, of ratifying or not ratifying this facility. However, having permitted the use of this third party CDD on a domestic basis, member states had to grant similar facilities to other providers based in other member states. This was outlined in *Article 15* and also permitted the acceptance of this form of CDD even where the requirements of the two states were not identical. This facility was also extended, under *Article 16*, to states which were not regulated under the directive but had equivalent levels of regulation and supervision. The use of regulated entities, for CDD, from states not operating under the directive could be prohibited under *Article 17*, while *Article 18* set out the duties of providers, on whose CDD other providers had depended. This required them to provide copies of their CDD documentation immediately upon request. As detailed in *Article 19*, entities that were employed as an outsourced processor or agent for the FSP were deemed to be acting under the auspices of the FSP and not covered by *Articles 13* to *18.*

The remaining articles dealt with a variety of issues. The obligations of both provider and member state regarding the reporting of suspicious activity were set out in *Articles 20* to *27*. For example, member states had to ensure that those operating under the directive, monitored customer's activities for suspicious activity under *Article 20* and reported them under *Article 22*, while *Article 24* required that transactions would not be carried out unless a refusal might warn those suspected of ML or TF. Disclosures to customers of AML or CFT investigations were prohibited in *Article 28*, although it permitted the sharing of information with member state bodies, normally the FIU, or other financial institutions. The retention of records and

customer documentation were detailed in *Articles 30* to *33*. Providers were required under *Article 30*, to retain CDD information and documentation as well as transactional information for a period of five years after the end of the business relationship. Entities operating under the directive were required by *Article 31*, to enforce equivalent regulations on their branches or subsidiaries based outside the community. Where this was not possible they were required to advise their regulatory authority and impose additional AML/CFT measures. Where an AML or CFT investigation by a FIU, lead to a request for information, the provider was required to comply with that request fully and promptly, as detailed in *Article 32*. Ongoing monitoring of the effectiveness of member state's AML/CFT measures was required under *Article 33*.

The implementation of appropriate policies and procedures and the on-going training of staff by those regulated by the directive were set out in *Articles 34* and *35*. Additionally, *Article 35* detailed the responsibility of member states to provide up to date information on ML and TF typologies to the public sector, as well as feed-back on any submitted Suspicious Activity Reports (SAR). The remaining articles of the directive dealt with issues such as the supervision and implementation of the directive, penalties imposed for non-compliance, and the repeal of *Directive 91/308/EC* (European Council, 1991). However, *Article 40* has relevance to those involved in the e-money industry. The article provides for the establishment of technical criteria to re-assess the risk level of e-money as defined under *Article 11 (5d)* and the risk level of simplified and enhanced CDD. The implementation of the new directive was outlined in *Directive 2006/70/EC* (European Commission, 2006c). Of particular interest to EMIs was the direction that the numbers of those availing of simplified CDD should be restricted and that the providers should monitor their customers actions for suspicious activities, (European Commission, 2006c, p. 29)

additionally noting that money transmission and remittance services were more likely to be used for Ml or TF (*ibid* p. 30).

Member states were required to implement the directive by 15 December 2007. The UK implemented their legislation, *The Money Laundering Regulations 2007* (United Kingdom 2007), with effect from 15 December 2007. Ireland did not meet the 2007 deadline, with its directive, *The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010* (Ireland 2010), not appearing on the statute books until the 5 May 2010. There were a number of variations in the application of the directive in Ireland and the UK when compared to other member states. For example, in both jurisdictions the exemptions from CDD available for restricted financial products did not have to be applied for by a provider, being applied automatically (European Commission, 2011, p. 5). Both states were also seen as implementing a wider interpretation of what constitutes ML than some other member states (*ibid*, p. 30). However, of more significance to EMIs, is that both states implemented the exclusion clause outlined in *Article 11* of the directive, allowing EMIs to apply simplified CDD to their customers. The UK retained the basic monetary levels for these products, €150 for non-rechargeable, €2500 for rechargeable with a €1000 limit on redemptions, (United Kingdom 2007, p. 15). However, Ireland availed of the increased limits on non-rechargeable products allowing a maximum of €250 or €500 where the product could only be used within Ireland. (Ireland 2010, p. 36) The UK issued *The Money Laundering (Amendment) Regulations 2012* (United Kingdom 2012) which made adjustments to their 2007 ML regulations. Of relevance to EMIs was the addition of certain professional bodies and consumer credit financial institutions to the list of those who could be depended upon as part of a CDD process (United Kingdom 2012, p. 2, 3. pp. 4-5). Additionally it added to the powers of UK regulatory authorities to share information with other regulatory authorities

(*ibid*, p. 2). In Ireland, an amendment to the 2010 act was undertaken with *The Criminal Justice Act 2013* (Ireland 2013) to improve compliance with the AML/CFT standards set by the FATF (Ireland 2012). Of relevance to EMIs, were a number of issues. For example, those covered by the act were required to carry out on-going assessments of new technological developments in their products, practices, or the means by which they delivered those products with a view to their potential misuse for ML or TF (Ireland, 2013, p. 9). Additionally a reduction in the transactional limit for "occasional transfers" would impact the transfer of funds into some customer's accounts. Payment service providers were now required to complete CDD for wire transfers for amounts equal to or greater than €1000 (Ireland 2012; Ireland 2013, p. 6).

General directives and regulations and their impact on the EU e-money market

Several other EC directives or regulations were also issued which would impact on the AML/CFT responsibilities of EMIs. *Regulation (EC) No. 1781/2006* (European Council, 2006c) dealt with the provision of information about the payee of a transaction accompanying the transfer of funds. This regulation, under *Article 3(3)*, created a derogation from its requirements were an EMI had availed of the waiver available under *Article 11(5)(d)* of *Directive 2005/60/EC*(European Community, 2005) and the customer was conducting a transfer of less than €1000. In further exemptions, *Article 3(4, 5)* allowed an exemption for any mobile phone or IT-based prepaid transfer of less than €150 or, alternatively, where CDD had been carried out and the customer paid for the transfer after the transaction had taken place, effectively meaning that the customer must have a previously opened account with the provider from which the payment was taken. However, for those transactions or customers that did not fall within the exemptions granted for low-value e-money transactions, there were requirements around the provision of a payer's details to

the receiving FSP, and the retention of customer and transaction information for a period of five years. Simplified information on the payer was permitted for transfers within the EC by *Article 6*. However *Article 7* specified that complete information, the payer's name, address and account information, had to accompany any transfer to a non-member state. In a final reference to e-money, *Article 19* called for a review, to be completed by 28 December 2011[23], of its possible misuse in ML or TF. This regulation was enacted, with direct applicability to all member states, on 20 January 2007. Also introduced in 2007, *Directive 2007/64/EC* (European Council, 2007) dealt with payment services within the EC. Its impact on AML or CFT relating to EMIs was limited, dealing with, amongst other issues, consumer rights and the establishment of a new classification of FSP, namely Payment Institutions. These new Payment Institutions were specifically barred from issuing e-money in *Article 16 (2).* The directive did impact on e-money through its directions on the timescales allowed for funds transfers, potentially to accounts held with EMIs, in *Articles 64, 69, 71, 72* and *73*, with the requirement for the rapid transfer of funds aiding those wishing to hide funds with a series of quick transfers.

Looking to the growth of e-money: The EC conducts a review of its directive

In one of its final instructions, detailed in *Article 11*, *Directive 2000/46/EC* (European Council, 2000c) had required the EC to present a report to the European Parliament and Council on the application of the directive, concentrating on such issues as the protection of consumer rights, capital requirements, waivers, and the need to prohibit the payment of interest on funds received for exchange. This report,

[23] With effect January 2014, this review appears to be at the proposal stage and has not been ratified.
http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/0024%28COD%29

which was due to be furnished by 27 April 2005, was subsequently expanded to undertake a comprehensive review of the directive's effectiveness and its relevance to current and future market conditions (European Commission, 2006a, p. 2)[24]. This was due to a perception that the e-money market had not developed to the extent expected and that the e-money directive may have hindered rather than helped the development of the market (European Council, 2008, pp. 3-5). However, there was no specific requirement for the report, even in this expanded version, to address any potential misuse of e-money for ML or TF purposes. Subsequently, while AML and CFT were mentioned, it was as an impediment to the growth of the e-money market through the cost of compliance and the inconvenience caused to customers (*ibid*, p. 5). However, these AML/CFT cost concerns had been, to some extent, addressed by *Directive 2005/60/EC* (European Council, 2005), which introduced simplified CDD to the provision of e-money services (European Commission, 2006b, pp. 13-14).

Having reviewed the findings of the report, the EC implemented many of the report's recommendations in its second directive on e-money.

Directive 2009/110/EC: The Second EC directive on E-money

Following its review of the first e-money directive the EC issued *Directive 2009/110/EC* (European Council, 2009). This Directive, repealed the previous e-money directive, amended aspects of both *Directive 2005/60/EC* (European Council, 2005) and *Directive 2006/48/EC* (European Council, 2006a), and

[24] A summary of the findings of this report and other feedback received during the review of EMD1 can be found in European Council (2008).

> "...focused on modernising EU rules on electronic money, especially bringing the prudential regime for e-money institutions, into line with the requirements for payment institutions in the Payment Services Directive."

Some aspects of the new directive remained the same as its predecessor, for example, e-money could only be issued by those authorised to do so, could only be issued at parity and funds received from customers must be converted into e-money without delay. However the directive introduced some significant changes, implementing many of the findings of the review which was summarised in the European Commission's 2008 document, *Impact Assessment accompanying the Draft Proposal for a Directive of the European Parliament and of the Council amending Directives 2000/46/EC on the taking up, pursuit of and prudential supervision of the business of electronic money institutions* (European Commission, 2008). Those changes included a clarification of what services and products could be designated as e-money and permitted the involvement of EMIs in non e-money related financial services and business activities. Additionally EMIs were designated as financial institutions rather than their previous designation as credit institutions under *Directive 2000/46/EC* (European Community 2000c). EMIs were also given a distinct status from mainstream FSPs and the directive authorised a new sub-type of EMI with restricted regulatory requirements and services.

Article 1 of the directive set out the subject matter and scope of the second e-money directive. Included was a separate designation of EMI as a sub-type of financial institution, distinct from the credit institutions involved in the market. However those credit institutions could continue to issue e-money. In addition, Post offices, European Community and national central banks, member states, and their local government bodies were all permitted to issue e-money. It exempted electronic payment instruments that could only be used with a limited number of service providers or for a limited range of goods or services, as specified in *Article 3(k)* and

3(l) of *Directive 2007/64/EC* (European Council, 2007). This would include travel payment cards, loyalty cards, and gift cards for use in chain-stores or shopping centres. It also exempted the sale of goods or services that were for use by an electronic device and delivered through that electronic device without the involvement of an intermediary. This effectively removed the purchase of such goods as games or apps, provided directly by mobile phone operators to their customers, from the remit of the new directive.

Defining an EMI as a 'legal person' authorised to issue e-money or those operating under a waiver agreement, *Article 2* also widened the definition of e-money to include all forms of electronically stored, monetary value accepted by a third party. Setting out the requirements for the commencement of an e-money business, but also covering continued operations and the prudential supervision of existing EMIs, *Article 3* refers to the prudential rules outlined in various articles in *Directive 2007/64/EC* (European Council, 2007). That directive's *Articles 5* and *10-15* set out such matters as the need to provide a business plan and evidence of initial capital held, together with requirements for internal controls, structural organisation and statutory auditing requirements and detailed the authorisation process. Importantly for many EMIs, *Article 17(7)* also applied to them, dealing with the need to advise regulatory authorities when using third parties as part of their payment system. Additionally, *Article 18* of the same directive confirmed that the EMIs must ensure, within reason, that their third party provider was compliant with the regulations. It is noteworthy that the responsibility for any problems rested with the EMI. *Article 19* required the EMI to retain customer's records for a period of five years, while *Articles 20* to *24* set out the duties of the member states, for example in the supervision of providers and the exchange of information with other member states. Finally, in respect of *Directive 2007/64/EC* (European Council, 2007), *Article 25*

detailed the right to, and the requirements for, the establishment of a branch or branches, and the freedom to provide services, in other EC member states.

Moving back to Article 3 of the new e-money directive, it required an EMI to advise their 'home' state's regulatory body of any changes to its safeguarding of customer funds and of any changes in its ownership profile. It also authorised an EMI to process its sales and purchases of e-money through other agents, although only if those agents were registered with the authorising authority and were complaint with the requirements detailed in *Article 17* of *Directive 2007/64/EC* (European Council, 2007). One of the most significant changes in the directive is found in *Article 4*. Where previously initial capital of at least €1,000,000 was required, this requirement reduced the requirement to €350,000. *Article 5* set the minimum level of 'own funds' required as the amount of initial capital invested or 2% of the average outstanding balance of customer's funds, which ever had the highest value. Where an EMI had not operated for a sufficient period, the assessment would be made on the projected value of customer funds which would be held. Those requirements were applicable to the part of the operation which dealt exclusively with e-money. While many of these requirements effectively mirrored the first e-money directive, member states were allowed some discretion in applying them. Where a particular EMI was seen as having a higher risk of failure, the member state could require an increase of up to 20% on the amount of 'own funds' required. Alternatively, where an EMI was part of a larger operation, for example a FSP involved in other parts of the financial services market, the member states were given the option of not applying the 'own funds' criteria of the directive.

Article 6 detailed the activities that EMIs could be involved in. They were allowed to engage in the basic activity of issuing e-money and the receipt of customer funds for

payment of same. These activities included the processing of direct debits and standing orders from customer accounts as well as transfers from payment cards. Where the granting of any form of credit had been strictly prohibited in the first e-money directive, some exceptions were now permitted. However these were mostly of a technical nature, around potential short term delays in the receipt of funds from a customer's payment card, internet based payment system or through the direct debit system. In a major change to the previous directive, *Article 6* allowed for the conduct of business activities other than those involved in the issuance of e-money. However the taking of deposits remained as a prohibition, with customer funds received being exchanged into e-money 'without delay'. The previous edict of the first directive, which saw surplus customer funds held by the EMI falling under the regulations pertinent to deposit taking, was absent. Any transactions conducted by the EMI, which did not involve e-money, were deemed to have fallen under the remit of *Directive 2007/64/EC* (European Council, 2007).

The safeguarding of customer funds was dealt with by *Article 7*, under the auspices of *Directive 2006/49/EC* (European Council, 2006b), annex 1, points 1 to14, and *Directive 2007/64*/EC (European Council, 2007), *Article 9 (1, 2).* Customers were to be safeguarded against financial loss by the segregation of their funds from those of the provider or the provision of an insurance policy or guarantee from an independent insurance company or credit institution. Additionally customer funds were to be protected from any claims against the EMI by its creditors. These safeguards had to be in place whether the funds were for immediate use by the customer or stored with the EMI for future use. Interestingly, one dictate of the safeguarding provisions contained within *Directive 2007/64/EC* (European Council, 2007) does not apply to EMIs, namely the provision for member states to remove safeguarding from users with a balance of less than €600. Had this been

implemented it would have impacted many of the customers of providers covered by the second e-money directive. However, where EMIs were providing additional services other than the provision of e-money they would find themselves obliged to comply with the full safeguarding regulations set out in *Article 9* of *Directive 2007/64/EC* (European Council, 2007). The type of investment permitted for EMIs is set out in Annex 1 of *Directive 2006/49/EC* (European Council, 2006b). As required with the first e-money directive, the emphasis was on low-risk, secure investments which would protect the customer's funds. These included securities issued by national and regional government, development banks and certain UCITS[25]. The new e-money directive allowed member states to prohibit the use of some low-risk assets.

The provision of services by providers based outside the EC is dealt with in *Article 8*. It required all member states to ensure that they did not provide more favourable terms to providers headquartered outside the community and to advise the European Council whenever it authorised a branch of a non-EC based EMI. It also retained the right of the EC to set up agreements with non-member states to allow access for their EMIs to the EC market. These agreements were to be on equal terms with those for EMIs based in the EC. In a significant measure, but which echoed some elements of the first e-money directive, the option for member states to apply waivers to certain parts of the new directive was set out in *Article 9*. With the aim of helping to expand the e-money market, individual member states were permitted to allow reduced or complete non-compliance with the prudential, initial capital, 'own funds' and customer fund-safeguarding requirements of the directive. These

[25] Undertakings in Collective Investments in Transferable Securities.
http://www.dilloneustace.ie/download/1/DE%20UCITS%20Brochure%20FA%20Web.pdf

providers, known as Small EMIs (SEMIs), were prohibited from providing services in other member states. To be eligible as a SEMI, the provider was required to have an average of less than €5,000,000 in e-money balances held for customers, have its headquarters in the member state concerned, and ensure that none of those involved in the management or operation of the provider had been involved in financial crimes. The provider was also required to provide information on the amount of outstanding e-money on at least an annual basis, which would form part of that member states annual report to the European Council. However, unlike the first e-money directive, there was no requirement for a value based limitation on the products, although individual member states could choose to impose such a measure if they desired. These waivers did not reduce or remove their responsibilities for AML/CFT compliance as set out in *Directive 2005/60/EC* (European Council, 2005). *Article 10* prohibited the provision of e-money by those not registered to do so. The issuance and redemption of e-money was dealt with in *Article 11*, establishing that it should be issued and redeemed at parity, must be available for redemption without notice, that any fees or conditions relating to redemption must be made known to the customer before purchase and that during the period of the contract between the EMI and the customer, funds could be withdrawn in full or in part. The payment of any form of benefit, including interest, related to the length of time that a customer holds e-money was prohibited by *Article 12*, while *Article 13* designated the complaint and redress regime detailed in *Directive 2007/64/EC* (European Council, 2007) as being implemented for e-money services. In an attempt to deal with some of the perceived problems of the first directive, *Article 14* allowed for the amendment of the e-money directive to reflect changes in the rate of inflation, but also advances in technological and called for one standard across all member states relating to what products or services were or were not designated as e-money. *Article 15* called for the assistance of the Payments

committee set up under the *Directive 2007/64/EC* (European Council, 2007). Under *Article 16*, member states were required to adhere to the provisions in the directive. In a reflection of a similar requirement for a review of the first e-money directive, *Article 17* called for a review of the new directive to be completed and provided to the European Parliament and Commission by November 2012[26]. However, this was to concentrate on its impact and implementation, as well as reviewing the prudential requirements for EMIs. Again, there was no mention of a review of any potential misuse for ML or TF. *Article 18* dealt with the effect of the new directive on existing EMIs and their continued operations. Existing EMIs were not required to reapply for authorisation. However, by 30 October 2011, they were required to provide sufficient information to allow an assessment of their compliance with the new directive. Once completed to the satisfaction of their home-state regulatory authority, they would be entered on the new register of EMIs. If found to be non-compliant, they would be advised of what corrective measures were needed, with a requirement for implementation by 30 October 2011. Failure to comply with the new directive would result in the withdrawal of their authorisation to issue e-money. Issuers who had operated under a waiver were allowed to continue their operations, which were restricted to their home-state, until 30 April 2012, by which stage they would have to have complied with the relevant sections of the new directive or cease trading.

Articles 19 and *20* amended the various directives impacted by the new EMD. *Directive 2005/60/EC* (European Council, 2005) was amended by *Article 19* to reflect the new designation of a 'credit institution', but also to amend the derogation

[26] A requirement for a review of the 'efficient functioning' of the directive is detailed as being required three years after the deadline for its transposition. This review would therefore be due by the 30 April 2014 (European Council, 2009, p. 10 (22)).

that permitted e-money issuers to forgo full CDD. This amendment retained the previous limit on rechargeable instruments at €2500, with an annual redemption limit of €1000, but increased the limit on non-rechargeable instruments from €150 to €250. In addition it permitted member states to raise that limit to €500, but only for instruments restricted to use within their own national border. The new designation of credit and financial institutions, which listed EMIs as a financial institution, was implemented by *Article 20*. The previous e-money directive, *Directive 2000/46/EC*, (European Council, 2000c), was repealed in *Article 21*. The remaining articles dealt with the implementation of the directive and the responsibilities of member states.

Member states were given until 30 April 2011 to implement *Directive 2009/110/EC* (European Council, 2009). The ROI implemented the directive with effect from 30 April 2011 in its *European Communities (Electronic Money) Regulations 2011* (Ireland 2011). The UK introduced some aspects of the directive on 9 February 2011, before implementing *The Electronic Money Regulations 2011* (United Kingdom 2011) in full on 30 April 2011. The implementation of the directive in both jurisdictions was identical in many aspects. For example, both specifically authorised Credit Unions (CUs) and their national Post Offices to issue e-money (Ireland, 2011, p. 12; United Kingdom, 2011, pp. 35-36). Additionally, both states implemented the new e-money directive's *Article 19* option for increased monetary limits on basic e-money products, the UK amending its *Money Laundering Regulations of 2007* (United Kingdom, 2007, p. 62), with Ireland having enacted the amendments when implementing its *Criminal Justice Act 2010* (Ireland, 2010, p. 36). However, there was at least one major disparity, the 'outstanding e-money' clause for SEMIs. In Ireland the maximum permitted average amount of outstanding e-

money was set at €1million (Ireland, 2011, p. 31), whereas in the UK it was set at €5million (United Kingdom, 2011, p. 12).

The impact of the various pieces of legislation on the EU's e-money market can be seen in a number of ways. The promotion of e-money can be seen as helping grow the EU's internal market through the promotion of internet-based sales, while also providing financial services to some of those who are excluded from the mainstream market. However, the first e-money directive (European Council, 2000c), and other relevant regulation in place at that time, had been seen by some as impeding rather aiding the growth of the market, through its stringent requirements on start-up capital, internal controls and KYC/AML requirements for customers. However, by the time that the review of that directive had been undertaken and the new e-money directive was implemented, the AML/CFT regime had been eased by the implementation of the risk-based approach of Directive 2005/60/EC (European Council, 2005) and its subsequent amendments. This allowed FSPs to register e-money customers using simplified CDD and, while certainly making the market more accessible, has also opened up the potential for anonymity, thus increasing the possibilities of misuse. Effectively, providers are required to ensure that each customer can only process €2,500 p.a. through an e-money product before satisfying full CDD requirements. However, as will be seen in *Chapter 6* controls to prevent customer's exceeding that limitation are either not in place or not effective with regards to the provision of prepaid cards. There also appears to be nothing to prevent a customer obtaining a number of cards from different providers, an issue which is of particular concern in the UK, with its numerous providers. It therefore appears possible, even without obtaining multiple cards from one provider, to break the value limitations imposed under the e-money regime, certainly in the UK and to a lesser extent in the ROI.

The following chapter details the researcher's assessment of various NPMs and online financial services with a view to their potential for misuse in ML or TF. The decision to concentrate on two particular NPMs is explained, followed by details of the various methods used during the in-depth research and experimentation carried out on them.

CHAPTER 4

CASE SELECTION AND METHODOLOGY

An assessment of the compatibility of NPMs and online financial services for money laundering or terrorist finance

Having decided to investigate the potential for NPMs and other online financial services to be misused, the researcher had to assess which of them would best meet the needs of those involved in ML or TF. Terrorist financiers[27] share many of the needs of money launderers but, having some unique requirements of their own, also differ in some crucial ways. For example, terrorists may wish to move funds to individual activists or other organisations and use those funds immediately, while launderers are usually only concerned with hiding illicitly gained finances. However, in many cases, they do share one key commonality: the need for anonymity in their financial dealings.

With that in mind, the next step was to examine NPMs and other online financial services to assess which would best satisfy that need for anonymity while remaining practical and user-friendly. The initial stage of the investigation was completed by the examination of provider websites, visits to FSP offices, the forwarding of email and telephone queries as well as some limited experimentation around account opening and product acquisition.

[27] The term 'terrorist-financier' is used here to describe all of those involved in the financing of terrorism, from the person making a donation to the activist using that donation to buy explosives .

Online account opening with mainstream banks

Mainstream or 'High Street' banks are increasingly turning to remote, non face-to-face dealings with their customers. From a profitability point of view this seems very plausible, even desirable as it reduces staff and premises costs, from the customer point of view it often removes the need to physically call into a branch. However it does remove significant opportunities to detect suspicious personal behaviours or transactions[28].

During this part of the research process the researcher examined banks operating from physical offices, but also opening accounts under 'distance marketing' [29] conditions. In contacting various FSPs by email in various European countries, the researcher met with varying degrees of success from a complete lack of response to detailed information on account opening requirements. The consensus was that where accounts are opened remotely, certified copies of KYC documents[30] are required. Various banks in Denmark, France, Germany, Italy, The ROI, Spain and the UK, declined a request for an interview with their Money Laundering Reporting Officer (MLRO)[31], and failed to respond or provided incomplete answers to email queries. It is therefore unknown if or how they independently verify the genuineness of copies. *Barclays Bank* and *H.S.B.C* (UK), *CommerzBank* (Germany), *Intesa Sanpaolo* (Italy) and *CGD* (Portugal) all advised that they do not open

[28] On numerous occasions during his career in retail financial services, the researcher detected criminal or illegal activity by watching for facial expressions, nervous behaviours or noting a tone of voice, thus foiling various attempted frauds or the theft of funds.
[29] Distance marketing refers to the provision of services by remote means where there is no physical contact between the customer and the service provider's staff.
[30] KYC documents refer to documents required to confirm a customer's profile details. This would usually mean a passport or driving licence to confirm identity, and a utility bill or bank statement to confirm their residential address/
[31] The MLRO is a designated official or officer appointed by a financial service provider to ensure that AML and CFT requirements are complied with. http://www.pearse-trust.ie/blog/bid/77047/MLRO-Who-Are-They-What-Do-They-Do

accounts remotely: prospective customers must call into a branch with their identification documents. *Nationwide* (UK) appear willing, when certified copies are not provided, to rely on uncertified photocopies of passports, driving licences etc., allied with a cheque drawn on an existing personal account in the name of the customer. *Credit Agricole* (France) require certified identity documents, a bank reference and a blank cancelled cheque to be submitted with any online application.

With such a focus on the provision of KYC documentation, the potential for ML or TF using these providers would appear to have been substantially reduced.

Online only banks

As with many aspects of the financial services industry there has been a marked increase in the number of banks operating on an 'online-only' basis with no physical contact between customer and bank staff. Regulated in the same way as banks with physical branches, some of these FSPs offer full account facilities while others concentrate on the savings market.

Having examined the account opening requirements of a number of these providers, it soon became evident that most operate under strict KYC regulations. There are requirements for certified copies of the normal KYC documentation but some providers also require proof of a personal tax number and a cheque drawn on the customer's account in a regulated bank. This link to a regulated FSP is to be found with several NPMs as will be seen, for example, in the section dealing with online share dealing. As occurred with their High street counterparts a number of providers were contacted with requests for interviews. Unfortunately none of these requests were accommodated so it cannot be confirmed if the providers conduct verifications when documents are received.

However, the requirements around certification of KYC documents should deter many potential cases of ML or TF.

Online Gambling sites

Real world gambling casinos, with high cash holdings as an integral part of their day to day business, provided an advantageous means of laundering funds for many years, mostly where criminals owned the casinos used (Beasley and Whitcomb, 2009). The researcher's concerns that this could have been transferred over to the world of online gambling were supported at a later date by the arrest of a number of online gambling site owners on charges of ML and associated crimes (Wilson, 2011). Initial research concentrated on the need for those involved in ML or TF to move funds without attracting attention. Therefore, the researcher explored various online gambling sites to ascertain if it was possible to select your opponent. This would allow someone to 'lose' a card game thus paying the 'winnings' to their chosen opponent. The research took the form of an examination of and/or contact with card-gambling sites such as *Bwin*[32], *Partypoker*[33], *Wild Jack Casino*[34], *Friendbet*[35] *and Paddypower*[36]. The researcher also joined a number of online gambling forums and set up Google-alerts for any news items relating to online gambling. Any queries took the form of someone wishing to play card games only against friends. In this initial research none of the sites allowed players to choose against whom they played. But following a query on one of the online gambling forums two sites, *Pokerstar Homegames*[37] and *RPM*[38], were advised as providing the facility of

[32] Bwin, see https://www.bwin.com/
[33] Partypoker, see http://www.partypoker.net/
[34] Wild Jack Casino, see http://www.wildjackcasino.com/
[35] Friendbet, see http://friendbet.com/
[36] Paddy Power, see http://poker.paddypower.com/
[37] Pokerstar, see http://www.pokerstars.com/poker/home-games/

choosing your opponent. While at least one of these appears to be an American domiciled company, both sites and any others offering similar facilities would bear further investigation.

As part of the investigation of online card-game gambling the researcher discovered some features of online sports betting that could be misused. For example, it is possible to set up a *Paddypower* online betting account with an attached card which can then be en-cashed at shops. While this *Paddypower* facility is restricted to Ireland at the moment there may be other companies offering more extensive services of this kind. This and many other aspects of the online gambling industry would certainly warrant further investigation.

Online share dealing

The introduction of electronic share certificates has seen an increasing move to online share dealing with no face-to-face contact between seller and stock broker employees. Previously many people bought and sold their shares via their bank or other FSP, physically presenting their share certificate and a transfer of ownership document, known as a 'crest' form, or a signing a share purchase order at an office. Now, stockbrokers provide online sales, purchases and ownership transfers. Payments can often only be processed via the customer's bank account by cheque, card payment or electronic funds transfer (EFT). Where funded via bank account, certain providers do not require any KYC documents. When required, some providers will accept uncertified, emailed copies of identification and address confirmation documents, while others require fully certified copies. At least one

---

[38] RPM has ceased operations during the course of this research.

provider will accept copy documentation certified by local, non-professional or unregulated persons such as a religious cleric.

While those who require either a link to a regulated FSP or certified documentation are in all probability compliant, there are potential AML/CFT problems with those who do not. There has been at least one case of an online share dealing provider being fined in the UK for poor AML/CFT compliance.[39]

Digital Currencies

Alongside many other NPMs, digital/virtual currencies are increasing in popularity as a payment mechanism for online sales of real or virtual goods and services. First launched in the 1990s they are now reaching a wider audience with the greater availability of the World Wide Web. There are many different variations with some simply held in a national denomination or linked to precious metals. Others are issued in conjunction with virtual worlds such as *Second Life* or held in currencies which only exist online having no formal ties to any 'real world' currency. The reasons for their existence are varied. Usually set-up for practical reasons, for payments for online sales or services, others were set up due to a political viewpoint which rejects regulated banking systems and centralised government involvement in financial affairs.

Once a customer is established, there is often no intermediary involvement in the same sense as, for example, banks are involved with debit card transactions. The ease with which they can be sourced, high transaction speeds, potential anonymity

[39] '*FSA issues fines totalling £250,000 for transactions reporting failures*' http://www.fsa.gov.uk/library/communication/pr/2012/096.shtml

and the privacy of not using your credit card online, makes digital currencies attractive to individuals wishing to move funds locally or internationally. Additionally the security of knowing that the transaction is instantaneous reassures business users that, unlike a credit card, sales transactions are final and cannot be cancelled.

In many cases transactions can only be traced with great difficulty if at all. For example, with *Bitcoin* the identifying address is usually only used once, is non-permanent and as such, difficult to link to an individual or organisation. Most digital currencies can only be purchased through a DCE. Purchases can be paid for by credit/debit card, electronic transfer from a bank account, cash lodged via providers such as *Western Union* and through online payment systems such as *Moneybookers*[40]. Some implement various AML/CFT measures of their own with at least one digital currency provider making the provision of customer bank account details a requirement for membership. Another saw the acceptance of illicit funds into their system as being the sole responsibility of the bank which handles the initial transaction. Digital currency accounts can often be opened simply with the provision of an email address and a real or fictitious name. Often no customer identification process takes place, with no verification of the customer's identity.

Many of these features, which attract legitimate users, also make digital currencies attractive to those involved in illegal activity. Digital currency advocates claim that the comparatively small number of transactions, allied with the low total monetary value of all transactions, would make any suspicious or large transaction stand out. However, a number of cases have arisen recently where charges, including ML, have

[40] For details on these providers see Chapter Two.

been brought against individuals heavily involved in the industry (*The Guardian*, 2013; Pagliery, 2014). Balanced against that is the lesson of *Mt. Gox* one of the biggest DCEs which went into liquidation with severe losses to some of its account holders (Hals, 2014). Would those involved in ML or TF take the risk of losing their funds?

Digital/virtual currencies are constantly evolving with some proponents now citing the need for greater co-operation with regulatory authorities (Shubber, 2014). However, with potential for anonymous funds transmission, little in the way of KYC requirements and a distinct lack of traceability, there must be serious concerns around their potential for ML or TF.

Mobile phone payments

The use of mobile phones as a means of accessing financial services has proven to be very popular in parts of the world where the more traditional services are not available. Within Europe there is an increasing demand for such services, perhaps due to a migration of workers from areas of the world where they are already established. Enquiries addressed to most of the mobile phone providers showed that those in the ROI and UK who replied, did not provide this facility and had no plans to provide such services in the near future. While there are facilities available, such as *Barclay Bank's Pingit* service in the UK, these cater for the withdrawal of funds from a bank account rather than from the value held in the mobile phone account of the customer. What became evident at a later stage was that funds could be processed from some of these accounts, including the payment of purchase fees for prepaid credit cards, as will be seen in chapters two and five.

Having assessed the services and products detailed above, it was decided to conduct a detailed examination of the two most popular, accessible and easily used NPMs: Online payment systems and prepaid credit cards and their provision in the ROI and UK.

Methodology

Having established the NPMs that should be examined in-depth, it was necessary to purchase a number of prepaid credit cards and open a number of online payment accounts in both jurisdictions.

While the prepaid card market in the ROI is limited there are numerous providers in the UK. The cards that were examined were selected in a number of ways: Retail outlets in both jurisdictions were visited to ascertain which cards were commonly available, online searches for internet-based providers were conducted using search engines such as Google and information was gleaned from online forums, consumer comparison websites and TV or online advertisements. The cards were selected on the basis of availability, popularity and practical features such as ATM use or compatibility with online commerce.

Online payment systems are usually available across all countries in the European Union (EU), with very few systems limited to availability in specific countries. The systems were assessed for practical features such as sources of funding and the ability to move funds within and across national borders. A number of the more popular online payment services were selected for examination. Other providers were selected through online searches and through the monitoring of online forum, consumer advice websites and TV or online advertisements.

As has already been stated, one of the prerequisites for those involved in ML and in most forms of TF is the need for anonymity and the reduction of the potential for government or transnational bodies to trace either the origin and/or destination of funds. To that end the ability of a money launderer or a terrorist financier to hide their real identity is vital. In order to replicate this, the researcher used various methods:

Internet access

Internet access was made through different ISPs. In the ROI these included Dublin City Universities ISP, public Wi-Fi services allowing anonymous usage, the public library, as well as a personal mobile broadband service[41]. In the UK, public Wi-Fi services allowing anonymity were used along with internet access available from a university and the UK's public library service. On one occasion an ISP from outside the EU was used.

Prepaid mobile phone sim cards

Telephone contact details are normally required as part of the application process. A number of prepaid mobile phone sim cards, freely available without customer profile details or identification, were purchased in both jurisdictions. The funds held on the phone account were sometimes used for the payment of online purchase/administration fees.

[41] This mobile service does not have a static IP address and therefore it changes with every reconnection, thus allowing a certain level of anonymity.

Anonymous email accounts

A number of email addresses were set up. These were available without confirmation of the profile details provided or proof of identity.

Postal addresses

As a further aide, a number of different postal addresses were utilised. Firstly, the researcher's own home address, which could be traced when it was used with the correct spelling, in English, of the researcher's name. This search may be possible through electoral records, credit check systems modified to confirm customer addresses, etc. However, this is an address in a rural part of the ROI where there are normally no postal codes, house numbers or definite road names. Therefore, the researcher used several different connotations of his home address which, while known locally, would not be readily apparent as the same address shown on, for example, a register of voters. In addition, for a short period, the researcher had access to two addresses, one in the ROI, one in the UK. On other occasions, during the UK experimentation, business addresses, picked at random from a telephone directory, were used when it was necessary to provide an address at the initial signup stage of the application. These addresses were only used where they could be changed or cancelled before correspondence was posted out or when it would not be posted out at all. Two fictitious addresses were used in the ROI but again only where post was not going to be delivered to them. It should be noted that, with these modified, temporary, fictitious or business addresses, it was impossible to confirm any connection to the researcher.

Additionally, during the latter part of the research, a service facilitating the delivery of letters and packages to either a UK or ROI business address became available. Items are delivered to an automated storage facility, the customer being advised by

text message or email when they arrive. The items are collected without face-to-face contact with delivery service employees. Registration is via the internet with no requirement for identification or address confirmation documents, fees being paid through anonymous prepaid credit cards.

Identities used

On a number of occasions the researcher used his own name. He also used the Irish language version, amended versions of the name in both English and Irish and, on a few occasions, completely fictitious names.

Identity and address confirmation documents

As a number of providers require either a copy of a document or its number, the researcher's own driving licence was used. The number provided was usually the local authority reference number, a number used on numerous similar documents[42], and thus untraceable to an individual driver. Where required, poor quality photocopies or scans would be initially provided. However it would be impossible to provide any evidence of some of the addresses used, so when requested this would have to be declined. Where certified copies were required or the documents presented on a face-to-face basis, effectively preventing anonymity, this requirement would not be complied with.

Card or account funding

With most prepaid cards and payment systems, funds can be lodged in a number of ways. Most offer the option of transfers from the customer's mainstream bank

[42] I was unofficially advised that the number of documents could be in excess of one hundred and fifty and possibly in excess of five hundred documents.

account or credit card. However, these options provide a link to an account with a regulated FSP who theoretically has completed full KYC procedures. This precludes anonymity and therefore was not used. Funding, either directly or indirectly, was normally made via cash lodgements through retail outlets offering services such as *Payzone* or *Paypoint*[43]. These services are readily available across both jurisdictions. Some of the funds lodged to prepaid cards were later used in conjunction with various online payment systems, either as a direct funds source or as a means of transferring funds into the payment system account.

In addition to the measures listed above, a number of behaviors or actions were undertaken to test the provider reactions to suspicious activities. For example, the purchase of prepaid cards funded by existing prepaid cards and transactions conducted in various countries outside the euro/sterling zone, but using a euro/sterling card. Additionally, outside ISPs and phone numbers [44] were used in some applications, cards/accounts were not used or used then allowed to become dormant before being reused, letters received were held and not acted upon, help desks were contacted with real or contrived problems to bring the cards/accounts to the provider's attention and finally euro prepaid cards were used to purchase sterling prepaid cards and vice versa.

To order to preserve their anonymity, prepaid card providers studied in this research are referred to as PCP1IRL, PCP1UK, etc. For online payment systems, the providers are referred to as OPS1 and OPS2.

---

[43] These companies licence retail outlets to accept cash for various entities including utility companies and some FSPs. See http://www.paypoint.co.uk/ http://www.payzone.ie/

[44] In this research a reference to an 'outside' ISP or phone number, refers to the use of a foreign ISP or phone number. For example, UK ISPs used to apply for ROI cards, ROI phone numbers used with UK applications.

CHAPTER 5

PREPAID CREDIT CARDS AND ONLINE PAYMENT SYSTEMS IN THE REPUBLIC OF IRELAND AND UK MARKETS

New developments in the online financial services market are appearing on a regular basis, but two of the longer established NPMs remain the most popular: Prepaid Credit Cards and Online Payment Systems. Both methods gained popularity for the online purchase of products and services, while governments and employers are increasingly using prepaid cards as a means of making payments to either social welfare recipients or employees. Prepaid credit cards offer almost the same facilities and are used in the same way as mainstream credit cards, while online payment systems play an increasingly important role in the movement of funds both locally and internationally. The use of both these NPMs is therefore familiar to many people. This functionality, ease of use and potential for rapid movement of funds and increased anonymity in a less heavily regulated part of the financial services market would attract those involved in ML or TF.This chapter therefore examines in some detail card and payment system availability in Ireland and the UK as well as their product features and application processes. The chapter is divided into three sections. The first section examines prepaid credit cards in general terms and is then divided into three subsections looking at the ROI and UK then comparing the two markets. The second section examines Online Payment Systems before detailing the similarities and contrasts of the two markets. The final section looks at the similarities and differences between prepaid cards and online payment systems.

Prepaid credit cards

There are two principal types of prepaid credit card: Closed loop which are usually restricted in their usability and level of funding, and Open loop which share many of

the characteristics of mainstream credit cards. Closed loop cards have very limited functionality, being confined to use within a geographical area or within a business group. They are normally restricted to use as a means of paying for goods or services on a face-to-face basis, with restrictions on the amounts that can be held on them. Due to these factors their usefulness to those involved in ML or TF would be reduced in comparison to open loop cards. It was therefore decided to concentrate on open loop cards as they appear to have greater potential for ML or TF.

Open loop cards are available in either physical or virtual format. Virtual cards take the form of a voucher or email advice with a unique credit card number which can be used for online transactions. Within physical open loop cards there are some variances. For example, some operate on a "stand-alone" basis with the funds being held on the card. Other cards are attached to online accounts, the funds being held in those accounts with the card as one of a number of methods of fund withdrawal. Additionally, with many open loop cards, there are different levels of functionality which is dependent on how much information customers wish to divulge and the provider's terms and conditions. There are also some differences between the two markets.

The Republic of Ireland

With a smaller target population than the UK, there are fewer providers dealing specifically with the Irish market. Additionally, there have been several closures. For example, *Rubycard*, one of the major providers at the time of the commencement of this research, left the market in August 2012. This also resulted in the withdrawal of several other cards, including some being offered by localised business associations, charities, sports clubs and newspapers, which were being provided under the *Rubycard* umbrella.

Currently the most popular prepaid card providers in Ireland are *Swirl* and *O2*. Other providers include *Neteller, Skrill, 3V, EcoPayz* and *Entropay*, along with some relatively new entrants into the market. For example, the Irish based airline, *Ryanair,* entered the market in autumn 2011 and the state-run postal service, *An Post*, started supplying prepaid travel cards in the first half of 2013. With the exception of *An Post*, most providers do not have any involvement in the mainstream financial service industry.

Many physical prepaid cards in the Irish market are only available online, but there are exceptions, for example, *An Post, O2* and *Swirl*. With *O2*, a face-to-face purchase can only be made via *O2*'s own outlets although cards are also available via their website. *Swirl's* prepaid cards are, on the other hand, readily available at numerous independent retail outlets or, as with the *O2* card, on their own website. *An Post's* cards are only available once the customer has called into a designated post office for the initial part of the application process and as such are not available without face-to-face contact between provider and customer.

An Post

The process to apply for an *An Post*[45] prepaid card, issued by *R.Raphaels & Sons plc*., is much like the opening of any mainstream banking facility, and as such fairly unique in the Irish prepaid market. The prospective customer is required to present themselves at designated post offices with identification documents[46]. They must

[45] An Post, see https://www.anpost.ie/AnPost/MainContent/Personal+Customers/Money+Matters/Foreign+Exchange

[46] To prove their identity a customer will be expected to provide a passport, driving licence or national identity card. To confirm their address, the customer will be expected to provide a utility bill, bank or credit card statement or in some cases a letter from a local authority.

then complete an online application using that same identification documentation provided. As such these *An Post* cards are very different to most of the prepaid cards available in Ireland in that the customer must present both themselves and their identification documents at a real-world office.

Swirl

As previously stated, *Swirl* [47]prepaid cards are amongst the most popular prepaid cards in Ireland and are issued by *Catelli Bank S.A*. in Luxembourg. Both physical and virtual cards are available, either online or at numerous retail outlets. The process of applying for the physical card via the internet entails the applicant providing some very basic profile details, including name, postal and email address and date of birth. The payment of the card fee is limited to a debit/credit card with the card delivered by post. The process then follows the same procedure for cards purchased at a retail outlet, with the card being fully activated once registered on the *Swirl* website. For face-to-face purchases of *Swirl* cards at retail outlets, no identification documentation or details are taken at the time of the initial purchase. These cards can initially only be used for online payments with a maximum one-off loading of €150. When registered online and upgraded by the provision of basic details, the card offers ATM capability and provides a €2500 holding capacity. To avail of these facilities the customer registers the card online, providing the same basic personal details required during an online purchase. There is also a requirement for the provision of the number taken from a government-issued form of identity, such as a driving licence or passport. A verification code is sent via the post, apparently as a

---

With NPMs the providers may request a copy of, for example, the passport but an original proof of address.

[47] Swirlcard, see http://www.swirlcard.com/

means of proving the customer resides at the address supplied, the customer confirming same online. Once this is completed the account is upgraded with full ATM facilities and the €2500 annual holding limit. The customer is limited to having only one card at a time, thus theoretically limiting the value of transactions per person to €2500 p.a. and a total of three cards in their lifetime. Swirl offers the option of increasing the annual transactional limit to €15,000 per card on the provision of a certified copy of the customer's passport or driving licence. The certification can be made by a member of the Irish police, a certified solicitor or accountant, or an embassy official, and must be accompanied by a signed confirmation of the profile information provided online. No address confirmation documents or further customer profile details are required. The card, which can be funded with cash at outlets with *Payzone* facilities, has a limit of €500 per lodgement but allows multiple lodgements per day. Alternatively funds can be sent directly from the customer's bank account by way of an EFT to the provider's bank account in Luxembourg. However, unlike some other cards, funds cannot be transferred directly from one *Swirl* card to another *Swirl* card.

O2 Money

Already established as one of the major mobile phone providers in Ireland, *O2* [48] launched their *'O2 Money Card'* in February 2011 and has since become one of the most popular prepaid cards on the Irish market. *O2*'s card in Ireland is issued through a UK regulated provider, *R.Raphaels & Sons plc*. One of the few prepaid providers using the *Visa*[49] brand, the *O2* card is available through their website or their own retail outlets. For cards purchased at an *O2* outlet, there is no requirement

[48] O2, see http://www.o2online.ie/o2/o2-money/
[49] Visa, see http://www.visa.ie/

to provide any identification documents at the outlet, just the customer's name, address and contact information. A purchase fee of €9.99 is applicable. The card can be loaded immediately, up to a limit of €150, although only one loading can be carried out. It can however, be used almost immediately for ATM, in-store or online purchases. To avail of higher limits and to be able to lodge further funds the customer must register the card online using the same details provided at the O2 outlet. Once this is done the customer will receive a code by post that they must input on the website. Ordering an *O2* card via their website is just as simple. The customer fills out an online application providing their name, postal and email addresses and date of birth. A mobile phone number must also be provided as *O2* send a confirmation code via text as part of the application process. The customer can use credit from their *O2* mobile phone or, alternatively, a credit/debit card in their own name to pay the purchase fee. *O2* posts out the card and a PIN number. Once the card is received the customer inputs confirms the receipt of the card by inputting the customer number printed on the card, along with an activation code received by email, to activate the card.

Initially cards are given a €150 balance limit. However, once registered online, the balance limit is raised to €2500 p.a. The customer can also withdraw a total of €1000 annually to their bank account, €200 per day in cash from an ATM or send €350 to another *O2 Money Card* holder. Total withdrawals, however, are limited to €1000p.a. Where the customer calls in to an *O2* outlet and presents his identification documents to *O2* staff in a face-to-face meeting the limits are substantially increased. Customers can then hold €5000 in their account at any one time, add a total of €25,000 to the account annually and the limitation on transfers to their bank account is removed.

O2 cards can be funded in a number of ways. The customer has the option of transferring funds via their internet banking service or by using an existing debit/credit card in their name. They can also lodge cash via *O2*'s retail network or in retail outlets through *Paypoint*. Funds can also be transferred in from certain gambling sites, such as *Paddy Powers*. *O2* also offers the facility for customers to send funds to other *O2 Money Card* customers. Withdrawals can only be made to the customer's bank account.

Entropay

Entropay [50] previously offered customers the option of either virtual or physical prepaid *Visa* cards. However they appear to be experiencing difficulties with their physical cards and as such, are restricted to only issuing virtual cards[51]. Available via *Entropay's* website, and not through any retail outlet, the customer is initially required to provide their name, email address, country of residence and date of birth. The customer must decide which currency (US dollars, Sterling or Euro) they want to load, create their *Entropay* card, and can then link a card as a funding source. This is the *Starter* account, with a maximum load of €250 and only one virtual card per account. To upgrade to the *Basic* account the customer must complete an online application with the KYC details previously supplied but including their postal address. The customer must verify the email address and add at least one funding method to their profile. They can then avail of an annual funding limit of €2500 and withdrawal limit of €1000. A further upgrade to *Premier* status is allowed when the customer provides uncertified copies of their KYC documents and

[50] Entropay, see https://www.entropay.com/
[51] Since examining the facilities available from this provider, they have recently advised that their physical cards are now available. It should also be noted that they appear to have made some changes to their provision of services since this research was carried out.

copies of the back and front of all cards attached to the account[52]. Once these are accepted the account can be upgraded to allow twenty virtual cards per account, daily withdrawals of €20,000 and lodgements totalling €15,000 every thirty days. The card can be funded by credit or debit card, or transfer from the customer's bank account.

3V

As a provider of 'virtual' prepaid cards, *3V* [53] is available at many *Paypoint* agents. Available in amounts from €30 up to €500, they have a maximum holding of €2500 per customer over a 12-month period. Funding is by cash or credit/debit card at participating retail outlets. The card can be used for online purchases, the funding of physical prepaid cards or the payment of funds into 'mainstream' bank accounts. To avail of the service, the customer must register online beforehand. The customer provides very basic profile information, contact details such as a mobile number, email and postal addresses. There is no requirement for KYC documents or document numbers to be provided. The customer then receives a 'customer card' via the post allowing them to conduct *3V* transactions at participating retail outlets. The customer visits the outlet, pays for the transaction and is given a voucher carrying a code. They must then register the transaction, using the code on the *3V* website. Once the transaction is registered the customer receives a notification of their *Visa* number and attached security numbers by email or text message. They can then use those numbers on any website that accepts *Visa*, for example, loading funds into certain physical prepaid cards, online payment systems or paying for goods and services online.

[52] The provider advises that certain numbers on the card should be blanked out before the copies are sent.
[53] 3V, see https://www.3v.ie/about-3V-vouchers.html

Discussion

In terms of availability, functionality and registration requirements, two providers are considerably better than the others. Both *O2* and *Swirl* offer cards through retail outlets with the same transactional limits and minimal KYC requirements. Both cards can be used for cash withdrawals, online and face-to-face retail purchases. While *Swirl* cards are available at a greater number of retail outlets, *O2* cards have the advantage of more options for funding and allowing funds movements between customers.

United Kingdom

The prepaid market in the UK is considerably larger than the Irish market and as such has considerably more providers. These providers vary in their set-up, some only providing prepaid cards while others offer online accounts with attached prepaid cards and other means of conducting financial transactions.

As is the case in Ireland, the vast majority of providers are not part of the mainstream financial services industry. However, recently some banks, including *Barclays, Clydesdale* and *Yorkshire*, have started to offer prepaid credit cards to their customers. In addition prepaid cards are also available through some CUs and at least one building society. Amongst the providers in the UK market are a few who also operate in Ireland: *3V*, *Entropay* and, a very recent addition, *Swirl*. Other cards available in the UK include *Bread, Pockit, Orange, Travelex, CitizenCard, Western Union*[54]*, Kalixa, Cashplus, Clearcash, Virgin, Tuxedo,* and *Lebera.* UK prepaid cards offer options on the payment of transaction fees. With some cards, the customer can

[54] Western Union offer certain services in the ROI, prepaid cards are not amongst those services.

pay a fixed monthly fee, which does not vary dependant on the number of transactions. They also have the option of paying 'standard' fees on a transaction by transaction basis. In another option, which is not generally available in the Irish market, customers can have their salary or wages lodged to some UK prepaid cards.

Swirl

Swirl [55] are relative newcomers to the UK market, first appearing in 2013. Available through their own website and unaffiliated retail outlets, their cards are issued by *Catella Bank S.A*., a Luxembourg based FSP. Cards purchased through retail outlets do not require the provision of any KYC details, the purchase fee being payable in cash or by card at the outlet. To activate the card it must be registered online with basic KYC details, including name, date of birth, postal and email address as well as phone contact details. The customer must also provide the number from an identification document. Once registered a code is sent by post, which, once confirmed online, activates the card. For online orders, the customer must provide the same KYC details as for cards purchased in retail outlets. The fee can only be paid by credit/debit card. Once completed a code is dispatched by post, which the customer must confirm online also providing their identification document number. The card is then activated with full ATM, online and in-store capabilities. A total of £1700 can be credited to the card annually with funding being available by transfer through the customer's online banking facility or by cash at retail outlets providing *Paypoint* or *Payzone* services. ATM withdrawals are limited to £300 per transaction, but the maximum balance of £1700 can be withdrawn in one day. Customers can increase the lifetime balance limit to £10,000 on the provision of certified copies of their identification.

[55] Swirl, see http://www.swirlcard.com/?country=uk

Cashplus/Clearcash

Cashplus[56] and *Clearcash*[57] prepaid credit cards are both issued by the UK-based, APS *Financial Ltd (AFL). Cashplus* also provide the *Titanium*[58] card which is available through the *Money Shop* chain*. Both Cashplus* and *Clearcash c*ards are only available through their respective websites. Applying for the cards requires the provision of the same basic details as most UK cards. The application fee is payable by cash at Post Offices, by credit/debit card, or by text from a UK mobile. The verification of the customer's address and identity is made by electronic search. If the provider is unable to do so they may offer the customer one of their restricted versions, the *Clearcash Express* or *Cashplus Express Access* account. With these accounts the customer has a balance limit of £2000, and ATM withdrawals of £250 per day to a maximum of £800 p.a. The customer can apply for an upgrade by providing certified copies of their passport or driving licence and an original document confirming their address. If the upgrade is granted, the customer qualifies for a balance limit of £5000 and £500 in daily ATM withdrawals with no annual limit. The customer can also obtain additional cards for friends or family. Either card offers the option of direct debit and standing order payments[59] normally only found with accounts held in mainstream banks. Both cards can be funded by cash lodged through Post offices or certain retail outlets. With the enhanced version of either card those options are available, as is the receipt of the customer's salary or wages, or funds transfer by standing order or internet banking. *Clearcash* also offers the option of being used in conjunction with online payment systems such as *Paypal.*

---

[56] Cashplus, see http://www.mycashplus.co.uk/
[57] Clearcash, see http://www.clearcash.co.uk/
[58] Titanium, see http://www.titaniumcashplus.co.uk/
[59] Regular payments from a customer's bank account, initiated by the FSP in the first case and by the customer in the second.

Orange

A well-established mobile phone operator, *Orange*[60] launched its prepaid credit card, issued by *Barclay's Bank,* in February 2011. Only available via their website, the customer must complete an online application with minimal details, including name, postal and email address and phone number. The application fee can be paid from a mobile phone account or by credit/debit card. *Orange* examine the application and, if able to electronically verify the customer's identity information, will apply a balance limit of up to £5000 and no limit on ATM withdrawals. If the provider is unable to verify the customer's identity, then they may provide a card with a balance limit of £1600 and an ATM withdrawal limit of £600. Should the customer wish to raise these reduced limits, *Orange* will accept an original bank/credit card statement or utility bill to prove residence and uncertified copies of a passport, driving licence, or various government documents to confirm the customer's identity. The card can be funded by cash through UK Post Offices, certain retail outlets or at *Orange* outlets, by standing order or online transfer from the customer's bank account, or by debit/credit card. The customer can also have their wages or salary paid into their *Orange* prepaid card. Both basic and enhanced cards have full functionality for online or real world sales and ATM facilities.

Prime

The *Prime* [61] prepaid card, issued by the Gibraltar-based based *IDT Financial Services Limited,* can be purchased at retail outlets or through their website. When purchased at a retail outlet, the card is available without provision of any customer details and the card fee can be paid in cash or by debit/credit card. Unusually, the

[60] Orange, see http://cash.orange.co.uk/
[61] Prime, see http://www.idtprime.com/index.html

card can only be loaded at UK post offices or at some retail outlets. There is no option for funds to be sent directly from the customer's bank account. At this basic level the card can be loaded to a maximum of £300 p.a., and can be used for real world or online purchases, although there are technical restrictions on some online purchases[62]. However, at this basic level the card cannot be used in ATMs. To purchase the card online, the customer must have an existing credit or debit card for the payment of the card purchase fee. The customer is required to provide basic profile and contact details, and these must match those of the card being used for the payment. Aside from the normal name, date of birth and contact details, *Prime* also require details on the source of funds which will be used to fund the card, for example salary, social welfare payment, maintenance payments, savings etc. They also require certain details for the source of funds chosen. For example, employer's name, bank branch details if the funds are going to come from a savings account, who is providing maintenance payments, etc. The customer is then required to provide the number from either a UK driving licence or any "machine-readable" passport. If the provider is unable to electronically verify the customer's identity from these details, they may request an uncertified copy of a passport or driving licence and an original document showing the address. Once upgraded the *Prime* card can hold a maximum of £5000 at any one time, with an annual limit of £11250. Cards with either limit can be used in an ATM once registered and accepted.

[62] These restrictions revolve around the need for online merchants to be able to verify a customer's profile details when accepting a payment by credit card.

Pockit

Pockit's[63] prepaid MasterCards[64], like *Prime*, are issued by *IDT Financial Services Limited*. Unlike *Prime*, the card can only be applied for via the company's website. As with most prepaid cards the customer can apply for the card by providing their name, date of birth and contact details. There is no initial requirement for documentary proof. *Pockit* also ask for details of where the funding of the card will originate from, seeking details of, for example, the customer's bank, employer or social welfare details. The purchase fee can be paid through debit/credit card, or from the funds held on a mobile phone. The basic card can be funded by cash through UK post offices and retail outlets, or salary transfer. Loading from the customer's existing cards is not permitted. The maximum load is £800 per month, £2000 per year, with ATM withdrawals limited to £120 per day. An upgrade of the card is available on provision of uncertified copies of identity documents, along with original address confirmation documents. This allows the holding limit to be raised to £3000, £20,000 per annum and ATM withdrawals of £250 per day. Pockit reserve the right to ask for information if transactions exceed £12,000 within 12-months.

The mainstream providers

Several providers from the more traditional financial services industry are now providing prepaid credit cards. *Yorkshire Bank a*nd *Clydesdale Bank* are part of *National Australia Bank Group* [65] and have a combined total of more than 330 branches. The card, which has identical features in both banks, is unusual in that it

---

[63] Pockit, see https://www.pockit.com/
[64] Mastercard, see http://www.mastercard.com/index.html
[65] Yorkshire Bank and Clydesdale Bank form the UK arm of National Australia Bank Group. http://www.cbonline.co.uk/about-clydesdale-bank/corporate-profile/

uses *Maestro*[66] rather than *MasterCard or Visa*. The online application is the same for both cards, customers are required to provide the same basic profile and contact details as with other providers. The card fee can be paid by cash at certain retail outlets, by text through a mobile phone, or by credit/debit card, as long as the card is in the applicant's name. However some cards are not acceptable, particularly other prepaid cards. The cards can be funded by cash through various Post offices and retail outlets, debit/credit card (although restricted to one card only), by transfer of the customer's salary/wages, or by transfer of funds from a bank account. Additional cards can be ordered with a limit of five cards per account or household.

There are different levels of capability, dependant on the profile details contained in the application. If the provider is unable to electronically confirm those details, they may offer a restricted card with a limit of £1600 and withdrawals of £600 p.a. These cards cannot be funded by credit/debit card and no additional cards can be ordered. An upgrade is available, with the provision of the normal KYC documents, although it is unclear if these need to be certified or uncertified. Once verified the customer can avail of a £3500 annual limit, and a £500 per day, ATM withdrawal limit.

An increasing number of UK CUs are also offering prepaid cards to their members, including *RedKite, Bristol, Undeb Credyd* and *Cardiff & Vale.* To avail of a *Cardiff & Vale CU*[67] prepaid card the customer can complete their application remotely but must call to the CU's office for a face-to-face meeting, too allow CU staff to witness their signature. Identification of new customers can be made by electronic search, but if unsuccessful the customer will be required to present standard KYC

[66] Maestro, see http://www.maestrocard.com/gateway/index.html
[67] Cardiff & Vale CU, see https://www.cardiffcu.com/

documentation at the CU office. General customer accounts can be funded by various means, including cash lodged at retail outlets and Post offices. Funds can be transferred from those accounts to the card, once the customer provides a signed authorisation and makes a telephone request for the transfer. *Bristol CU* [68]accepts online applications. As with *Cardiff & Vale,* customer identity requirements can be completed via electronic searches. If not completed satisfactorily the customer must present physical documentation to *Bristol CU* staff. Where issued in conjunction with the *Association of British Credit Unions Limited*[69](ABCUL), prepaid *Visa* cards have a maximum limit of £3500, and ATM withdrawals of £300 per day or £1200 over 4 days. These cards are issued under licence from *Clydesdale Bank*. Responsibility for the monitoring of the cards remains with the CU. The researcher contacted a number of ABCUL affiliated CUs. Only one of the respondents had actually issued cards, but they confirmed that remote online account opening was possible, that KYC checks are carried out electronically and where they fail, the customer must call into the office with the necessary KYC documents. Other CUs offer a *Visa* card issued by *credEcard* [70], with a maximum balance of £5000 with ATM limits of £250 per day.

A number of other providers offer prepaid cards, in both the Irish and UK markets, which are linked to an online account offering other capabilities. A number of these are detailed in the section dealing with online payment systems.

Discussion

Despite the multiplicity of cards that are available there are minimal differences between them when examining the basic, entry level cards. A few offer slightly

[68] Bristol CU, see http://www.bristolcreditunion.org/index.asp
[69] Association of British Credit Unions, see http://www.abcul.org/home
[70] credEcard, see https://www.credecard.com/

higher limits, but there is little difference in features unless the higher specification cards can be obtained. For convenience the retail outlet cards can be activated slightly faster than the online cards, but again the difference is marginal.

Comparing the markets

As someone who does not reside in the UK, it is difficult to make an accurate assessment of the advantages of these cards to the average customer. However, as a means of bringing advanced financial facilities to the 'unbanked'[71] they are an excellent tool. To that end their provision through CUs will be welcomed by many. From the point of view of application process and product features most of the cards are very similar. However, the Swirl card with its availability through retail outlets does have a slight advantage. Comparing the two markets, the major difference is that most UK cards cannot be used until registered whereas ROI cards have some, admittedly restricted, facilities from the time of a face-to-face purchase. Additionally while online searches are a standard procedure in the UK, this does not appear to happen in the ROI as many providers use the postal system as proof of someone's existence and address.

Online Payment Systems

There are now many options available to those who wish to make online purchases beyond the use of debit/credit cards. Often motivated by the fear of online fraud or the potential compromise of credit card details, many people now use services which claim to protect them from identity fraud, provide some degree of anonymity and protects card information. The providers of these services are usually non-

[71] These are people who would not normally be able to avail of traditional banking facilities.

traditional FSPs, and may also offer such services as pre-paid credit cards, online vouchers or other financial services. There are numerous providers who provide services to both the Irish and British markets, including *Paypal, Skrill-Moneybookers, Xoom, myCitadel, Nochez, XE, Lebara, Google wallet*, *Neteller*, *Western Union and Allied Wallet*.

Paypal

Paypal[72]can justifiably claim to be the best known of the internet based, non-traditional FSPs. Acquired by auction site *eBay* in 2002, *Paypal Inc.* is a US company with product availability in almost every part of the world. *Paypal's* European operations are operated by *PayPal (Europe) S.à r.l. et Cie, S.C.A*. which is licensed as a credit institution by Luxembourg[73]. A *Paypal* account allows electronic transfers of funds in payment for goods and services, or to send money to friends or family. It many instances it is possible to transfer funds to anyone with an email address or mobile phone number, however to access the funds the recipient will have to open an account with *Paypal*. Account opening is only available online. In the UK, the customer is required to provide their name, email and postal address, date of birth, and mobile phone number. At this stage, they can also choose to link a card. *American Express*[74]*, Discover*[75]*, Maestro*, or various versions of *Visa* and *MasterCard* are all accepted, although it is not a requirement during registration. The customer must then confirm a code sent to their email address. Once this is completed the next step is the setting of security questions and confirmation of nationality. Registration is now complete but the customer has a status of 'unverified'. With

[72] Paypal, see https://www.paypal.com
[73] https://www.paypal.com/webapps/mpp/about
[74]American Express, see https://www.americanexpress.com/
[75] Discover, see https://www.discover.com/

unverified status the customer has transactional limits on the sending and receiving of funds, set at £1900 each, with withdrawals restricted to £650 p.a. The customer can remove these limitations by setting their status as a personal or business customer, confirming the information they have already input as their profile details and inputting their financial details. On their website *Paypal* state that the linking of a bank account, debit or credit card will achieve this, but in the UK the process defaults to the linking of a bank account. Therefore, to achieve verified status, the UK customer links their bank account, completes an authorisation for a direct debit and then confirms the amount of two deposits *Paypal* will make to the customer's bank account. In certain cases the customer is asked to confirm their residency at the address which is shown on their credit card by either receiving a letter with an attached code, or receiving a phone call on a landline registered to that address. If the provider is unable to confirm the customer's profile details, then they will request uncertified KYC documents by email or fax. The account can be funded by the customer's personal debit/credit card, the customer's bank account or by transfer from other *Paypal* customers.

The withdrawal of funds by the customer can only be made to their linked bank accounts. However, *Paypal* also have a debit card, only issued at their discretion, allowing funds in a customer's account to be used at merchant outlets or for ATM withdrawals. Two cards can be attached to each account with a maximum of four per household. The card is subject to similar restrictions as the online account, but with three levels. The *'restricted'* card offers £600 p.a. in ATM withdrawals and an overall yearly withdrawal total of £1600. The *'standard'* card has no annual limits but restricts weekly ATM withdrawals to £500 and point-of-sale purchases to £1500. Similarly, the *'full'* card has no annual limits, allows weekly ATM withdrawals

of £1000 and weekly point-of-sale transactions restricted to £3000. These cards are available for both ROI and UK customers.

For Irish customers the initial process is almost identical. The provision of the same basic customer profile details gives the customer a receiving limit of €2500 p.a., a sending limit of €1500 p.a. and a withdrawal limit of €1000 p.a. Funding is only available by bank account or credit card, debit cards cannot be linked to the account. To upgrade the account, removing the transactional limitations, the customer will be required to provide emailed or faxed copies of their address and identity documents. As with UK customers, certified copies are not required and the withdrawal of funds can only be made to the customer's linked bank account unless they are offered the *Paypal* debit card detailed above.

Nochex

Nochex[76] is a UK-based FSP which provides both personal and business accounts allowing fund transfers. Accepted for payments on internet auction sites *eBay* and *Bumblebee,* the FSP can also provide online, credit card acceptance services for merchants. Unusually, both the personal and basic business accounts are only available to UK Residents, with the full merchant services account being the only one available on a worldwide basis[77]. To avail of either a personal or business account the customer completes an online application. For personal customers the process commences with the provision of their name and email address. A code is sent to the email address, allowing the application process to continue. The customer must then register a UK credit card held in their name, provide their

[76] Nochex, see http://www.nochex.com/
[77] Services to European customers are being launched in July 2014.

postal address and date of birth, and complete a security question. The provider then withdraws a random amount from the credit card, the customer confirming the amount as part of the final verification process. The personal account provides a very small, maximum balance of £90, loading to a maximum of £300 per day or £1000 every seven days, outward transfers limited to £300, and incoming transfers restricted to *Nochex* members. To load funds into the account, a customer must register a debit card provided by a UK bank or building society. UK Credit cards can be used in conjunction with the account but as with a number of other providers, Nochex only acts as an intermediary, a means of transferring the value, funds not being held in the *Nochex* account. Fund withdrawals can only be made to a UK bank account, with limits of £500 per day and £1000 every 7 days. However this can only be achieved after the customer has registered a debit/credit card and the account the funds are being sent to. The customer can upgrade to the *'Seller'* or *'Merchant'* accounts with greater facilities and few, if any, restrictions on balances held. However as these are business accounts they fall outside the scope of this research.

Skrill

As one of the FSPs which provide both an online payment system and a prepaid card, *Skrill*[78] (Formally *Moneybookers*) has been growing in popularity. Both the card and payment system can only be applied for online. But, similarly to many other NPMs, value restricted facilities are available on the provision of basic KYC details and contact information. At the onset of the application process a European customer must designate the currency of the account, choosing from US Dollar, Sterling, Euro or Polish Złoty. Further details of their country of residence, name,

[78] Skrill, see https://www.skrill.com/en/?rid=20317595&gclid=CP2p7OXlnL8CFQF22wodm7IAEg

postal address and mobile phone number are required, followed by email address and date of birth. Once the customer verifies an email the account is automatically opened with certain transactional limits. At this basic level the customer can lodge €1000 into their account from their credit/debit card over a sixty day period, and can remit funds totalling €1000 over ninety days. To enhance these limits the customer has various options. To verify the customers address, *Skrill* will send a letter by post containing a code. Once that code is confirmed online, this adds an additional €5000 to their 'outgoing transaction' limit, while verifying their credit card and bank account adds an additional €10,000. The address verification also adds €5000 to their sixty day, credit/debit card loading limit. Funding of the account can be made by credit/debit card, through the customer's internet banking service or by other *Skrill* account holders . Withdrawals can be made by ROI or UK customers to their bank account or by a *Skrill* issued cheque.

Skrill accounts can be used in conjunction with purchases from online auction sites, such as *eBay, eBid and uBid*. *Skrill* is also popular with numerous online gambling or betting sites including *Bet365, 32Red*, *Pokerstars, Ladbrokes, Paddy Power* and *Betfair*. Funds can be transferred to other account holders as a payment for goods and services or as the transfer of funds to friends and family. Customers can only apply for the prepaid *MasterCard* after they have opened a *Skrill* account. The cards are issued by *Wirecard Card Solutions Ltd*, with any transactions on the card being processed through the customer's *Skrill* account, funds not being held on the card.

The card has full functionality, including online or real world commerce and ATM cash withdrawals[79].

Neteller

As a provider of both online payment systems and prepaid credit cards globally, *Neteller*[80] services are available in many EU states including Ireland and the UK. As part of *Optimal Payments PLC*, which has registered offices in Canada, the UK, and Isle of Man, the provision of these facilities falls under the UK's regulatory umbrella. All services are based around the *Neteller e-wallet*, an online account which allows for the transfer of funds to and from merchants, friends or family, and funds the virtual and physical prepaid cards. To register, customers must do so online. Having confirmed their country of residence, preferred currency and email address, the customer provides basic profile details, including name, address, telephone details and date of birth. They must also set a password and various security questions. The customer is provided with an account number and a 'secure I.D.' for use with online transactions. Some very limited options are available for customers who do not verify their identity. Customers can only fund the account with €100 using a maximum of three credit/debit cards, can only make a single transfer to a *Neteller* account to a maximum of €75 , and withdrawals to bank accounts are not allowed. Effectively, unverified status is only permitted to allow a new customer to test the system. No further transactions are allowed until the customer verifies their identity.

[79] Skrill have made changes to the provision of these services, especially around their requirements for KYC documents, transactional limits etc.
[80] Neteller, see http://www.neteller.com/

To verify their status the customer has several options. In the UK, the provider will undertake electronic checks to verify the customer's details. If successful, the customer has two options to complete the verification process; they can order a *Neteller* prepaid card, which, when received, is seen as proof of identity and residential address. Alternatively, they can link their bank account, in theory providing a link to an account in a regulated institution. *Neteller* processes a lodgement to the account, with the customer confirming the amount. If these options do not work or are not availed of, the customer can email a copy of an identity document. In Ireland the option of an electronic check appears not to be available, the system defaulting to a request for an emailed, uncertified copy of various identity documents or types of work/study visa.

Once verified, transactional limits are significantly increased. With the physical card, ATM withdrawals of €2250, and purchases of €6750 are permitted, while the virtual card can be used to make purchases of €10,500 over the same four day timescale. Additionally, funds can be transferred to the customer's bank account or the customer can request that a cheque be issued. The *Money Transfer* system can be used to pay for goods or services on websites which accept *Neteller*. To send funds to another individual the customer inputs the recipient's email address and amount, the recipient receives an email and must register, or already be registered with *Neteller* to withdraw the funds. Where used by verified account holders, the *Money Transfer* system has maximum balance limits of €7500 per day, €15,000 every seven days, €37,000 every thirty days and a lifetime limit of €185,000. There are numerous funding options: Cash can be lodged via *Paysafecard*[81], *Ukash*[82] or certain

[81] Paysafecard, see https://www.paysafecard.com/en-ie/?gclid=CLautYygsb8CFcbJtAodkhkAqw

prepaid credit cards. Transfers from mainstream bank accounts, once linked by the customer, can be made by a form of direct debit, internet banking, or by credit/debit card. Verified customers can link a total of five credit or debit cards as a funding source. Once verified, members from Ireland, UK and other EU states can lodge €5000 per day, €10,000 per week or €20,000 every 30 days using their credit cards. Debit card holders can deposit €10,000 per day, €20,000 per week, and €40,000 every 30 days. Funds can also be transferred in from gaming or gambling websites.

ecoPayz

ecoPayz[83] *(formally ecoCard)* is a UK-based online FSP which can claim to be one of the longest established, originally entering the market in 2000. Providing online payments services as well as virtual and physical prepaid cards, applications are processed through their webpage. Customers are initially asked to create a username, password and security question, then provide the normal profile details of name, postal and email address, date of birth and phone number. For UK customers, an electronic search is completed to confirm their address. If unsuccessful, the customer is required to provide uncertified copies of their identity document along with a copy of a bank statement or utility bill. For those in the ROI, there is no automated address confirmation and, at this stage, no requirement for proof to be provided of either customer identity or address.

In both countries, the customer now has access to the entry-level, *ecoCard Classic* account. This provides an account with a lifetime, cumulative limit of €2500 on all transactions and restricted funding. For example, card transfers are limited to €50

---

[82] Ukash, see https://www.ukash.com/en-IE/
[83] Ecopayz, see http://www.ecopayz.com/en-GB/Home

per day per card type and daily bank electronic transfers to €800. In addition the customer cannot withdraw funds to their bank account, use ATM facilities, or transfer funds between their accounts or to other customer's accounts. The customer can upgrade their account to either the *ecoPayz Silver* or, after a relatively short period of time, the *ecoPayz Gold* account. To do so both Irish and UK customers need to email uncertified copies of their KYC documents. Once accepted by the FSP, the customer can avail of greatly improved facilities with the *EcoPayz Silver* account. For example, no lifetime limit on the value of transactions, €15,000 can be held at any one time, funding of the account by card transfer is raised to €250 per card type and by bank electronic transfer to €15,000, per day. Payments to affiliated merchants, previously restricted to a daily limit of €800, are raised to €10,000 or €100,000 per month.

Customers can hold multiple accounts, in different currencies, and can transfer funds between those accounts. Transfers can be made to other account holders with a monthly limit of €3000. Funds can be withdrawn to their bank account, restricted to €500,000 per transaction. An ATM capable prepaid credit card is available, and *EcoPayz*'s virtual prepaid was re-launched in late 2013. Additional cards can also be ordered for friends or family members. ATM withdrawals of €750 per day or €4000 every four days are allowed, along with a monthly, combined ATM, point of sale and e-commerce total of €15,000. In a further enhancement of these facilities, the customer can upgrade to the *EcoPayz Gold* account once they have established a relatively short term history with the provider. This final grade of account has no cumulative lifetime value limit and €50,000 can be held at any one time. Funding by card is raised to €5000 per week per card type, with the electronic bank transfer limit raised to €260,000 per week. The customer retains the €500,000 limit on individual transfers to their bank account. The monthly limit on the transfer of funds

to other account holders is raised to €6000, and for transfers to merchants, raised to €100,000.

Moneygram

There are some providers who only offer restricted services in Ireland but full services in the UK. *Moneygram*[84] is a US based provider of funds transfer services which are available either online or, manually, via licensed retail outlets. This latter service is the only one available to Irish customers, who can call into a *Moneygram* agent with cash, cards not being accepted, and transfer funds to another agent where it is picked up by the designated recipient. UK customers can avail of both online or retail outlet based services.

To register for the online service, customers initiate a transaction which allows them to enter the registration page. Initially the customer provides their name, postal and email addresses, phone number and the document number from a passport or UK driving licence. The customer is then asked to provide security questions. The only means of funding is by UK-issued credit/debit card, details of which are added to the customer's profile. *Moneygram* offers two options with their online funds transfer service. Funds can be sent to the recipient's bank or picked up in cash at affiliated retail outlets. To send funds for collection at an agent, the customer provides the full legal name of the recipient, and the destination agent. Once the transaction is processed and confirmed, the sender receives a reference number which is passed to the recipient. The recipient completes a form at the agency, including the reference number, and may be required to provide government-issued identification before collecting the cash. There are limits on how

[84] Moneygram, see https://www.moneygram.com/MGIRewards/Main/index.htm

much can be sent for pick up in cash at an agent, dependent on the destination country. Other FSPs, such as *Paypal* and *Lebara*[85], have reached agreement with *Moneygram* to use their agents for cash transactions from and to their customer's online accounts, while banking institutions such as *First Bank of Nigeria, Forex Bank* and *Banco Espírito Santo* also offer services in conjunction with *Moneygram*.

XE

A Canadian-based foreign exchange company, with an office in Lithuania, *XE*[86] also offers fund transfer services. Operated by *Custom House Financial (UK) Limited*, they are regulated under the UK's regulatory bodies. Only available in certain countries, including the ROI and UK, *XE* offers to exchange all major currencies and/or transfer funds to almost anywhere in the world. Additional CDD requirements are in place for various countries listed on *FATF, OSFI* [87]and *US Treasury Department* warning lists and residents of some countries cannot use *XE's* services. Registration is only available through their website and is relatively simple. The customer must confirm what country they are registering from, are they an individual or business, the anticipated number and value of transactions and a commencement date. They must advise what currencies will be exchanged, choose a user name and answers to security questions. The customer then provides basic profile details such as name, date of birth, postal and email addresses. They must also provide details of their nationality and occupation, the latter stated as being an AML measure. The final stage entails the provision of numbers from two identification documents, one of which must carry a photograph of the customer, and details of both document's country of origin. *Xe* then advises that they may require copies of the identification

[85] Lebara, see https://www.lebara-money.com/
[86] Xe, see http://www.xe.com/
[87] *OSFI,* is the Canadian financial services regulatory body http://www.osfi-bsif.gc.ca/

documents, with an attached certification document for customers in the ROI. Customers may have to receive a phone call as part of the identification process. Limits to the total value of transactions do apply, but these appear to be decided on an individual basis.

Funding of currency exchanges or international transfers is strictly by transfer from a bank account, although that account can be in the customer's name or that of a third party, if 'permitted' by the account holder. Funding by credit card, cash, customer-issued cheque, bank-issued draft or other internet payment system is not allowed. Funds can only be withdrawn by transfer to a bank account or by the issuance of a bank draft or cheque, which effectively means lodgement to the payee's bank account[88].

The ROI and UK markets compared

The provision of services in both jurisdictions is very similar, the only major differences being the means by which the provider's prove their customer's identity. As has been seen previously, UK providers can perform electronic searches to verify their customer's details whereas this seems to be limited in the ROI. In both jurisdictions uncertified copies of KYC documents are accepted and a link to a regulated FSP is a requirement for most upgrades. However in the ROI some providers also use the postal system as proof of identity and address.

[88] Most bank cheques/drafts, certainly for customers in the ROI or UK, are issued in such a way to require lodgement to the payee's bank account.

Conclusion

Many of the internet payment systems and prepaid credit card share the same characteristics when it comes to customer interaction, and their means of proving the identity of those customers. In most cases there is no direct, face-to-face contact between customer and provider, at either the account opening stage or any of the subsequent financial transactions. Customer profile details are usually minimal, normally just name, electronic and residential address, date of birth and telephone number(s). The customer is rarely asked to provide significant levels of information about their financial or personal profile. This holds true at both the initial application stage or when upgrading the facility for higher value transactions. KYC documents, such as passports and utility bills are accepted, either as a customer-provided document number or an uncertified copy received by fax or email. Those email addresses are verified by the customer's confirmation of the receipt of a code. A customer's residential address is often proven by the receipt and activation of a card or the confirmation of a code number, sent by post by the provider. Electronic verification of a person's address is also used extensively in the UK, but apparently less so in the ROI. Where this is not possible, in either jurisdiction, a scanned copy of a utility bill or bank statement is often accepted by email or fax.

Mobile phone numbers and the ability to receive SMS text messages or calls, or pay certain fees using funds held on the phone, are employed as further confirmation of the customer's details through ownership of the phone. Proving that a credit card, or bank account, belongs to the customer is often seen as vital. This is frequently achieved by processing a small value transaction to the card or account, the customer confirming the amount as proof. Linking a debit/credit card often results in substantially increased transaction limits, as does the linking of a bank account. While these measures can be seen as preventing fraudulent use of a stolen or

compromised card, they also provide a link to another, regulated FSP who, in theory, will have completed more comprehensive KYC measures. Both types of NPM can often be funded by cash, either directly through licensed retail outlets or by using other NPMs as an intermediary. Most can also be funded by electronic transfer from the customer's bank account, or by debit/credit card. Both systems can allow customers to purchase goods or services via the internet, with almost no geographic limitations on their origin. Some, for the most part online payment systems but also certain prepaid card providers, allow the option of transferring funds back into the customer's bank account or sending funds to other accounts/cards held with the same provider.

Both systems also have features that they do not share. Unlike online payment systems some prepaid cards can be purchased over the counter at retail outlets, usually without the need for the customer to provide KYC information. Most prepaid cards share the same capabilities as mainstream credit cards once minimal KYC requirements have been met, in some cases even before hand. The physical cards can be used to withdraw cash at worldwide ATMs, and while virtual cards cannot be used in most retail outlets, both physical and virtual are usually accepted for the online purchase of goods and services. Some providers allow customers to add additional cards to facilitate friends and family members. Payment systems offer customers the ability to move funds on a global basis, or alternatively to the person sitting beside them. Cards can do this but mostly in a limited way, i.e., to holders of additional cards linked to the original card. Certain payment systems also offer the potential for customers to exchange one currency for another.

The following chapter details the findings from practical experiments carried out with prepaid credit cards and online payment systems in both the ROI and UK. The

findings look at the application, verification and activation processes, along with the practical features of the NPMs and the level of adherence with the provisions of the e-money directive.

CHAPTER 6

PREPAID CARDS AND ONLINE PAYMENT SYSTEMS: USEFUL TOOLS FOR MONEY LAUNDERING AND TERRORIST FINANCING?

Introduction

Having assessed the regulations pertaining to e-money services, this chapter focuses on an in-depth assessment of the potential misuse of prepaid cards and online payment systems for ML or TF. This details the practical experimentation carried out on some of the prepaid cards and online payment systems detailed in Chapter Two.

The chapter is divided into two sections, the first details the experimentation carried out on prepaid cards, subdivided into three subsections. The first subsection details the findings for the ROI, while the second deals with the UK. These subsections concentrate on two cards from each jurisdiction, comparing and contrasting purchase, verification, KYC requirements and practical usage. It also briefly examines other providers within the individual markets. The final subsection compares and contrasts the two markets. The second section deals with online payment systems. As very few providers only operate in one of the markets, the findings from both jurisdictions are detailed in one section, with any variations detailed in the text. Divided into two subsections, the first details findings related to two providers of online payment systems available in both jurisdictions and compares them to other providers. The second subsection compares and contrasts the two markets.

Prepaid Cards

Most prepaid card providers operate in a similar manner. Cards are usually available through retail outlets and/or the provider's website. Initially available with restricted facilities and transactional limits, improved facilities and limits are usually available once profile details are registered online. As part of the research a number of prepaid cards from various providers were obtained and tested.

Detailed findings from the research carried out on two providers in each jurisdiction are detailed underneath followed by a discussion of the findings and a brief review of the individual markets. Finally, there is also a short analysis comparing the findings for the two markets.

Prepaid Cards: Republic of Ireland

In the ROI prepaid cards are available from retail outlets or provider websites. For most cards obtained in retail outlets there is no requirement for KYC details to be provided at the time of purchase. Most cards initially have a small loading limit and limited facilities. To avail of a higher limit and improved facilities, the card must be registered online with basic KYC information: the customer's name, date of birth, phone number, residential and email address. A code is dispatched by post, the customer inputs it online and qualifies for a €2500 storage limit, ATM functionality, face-to-face or online purchases and the funding of online payment systems. Further upgrades to the limit are available with certified copies of various identification documents. With online orders the same KYC details must be provided at the time of purchase. The customer receives the card by post, inputs a code received with the card and can avail of the same facilities and limits available from cards sourced in retail outlets.

The providers reviewed in the two case studies detailed hereafter, offer prepaid cards in the ROI through their website or via retail outlets. A total of five cards were obtained from PCP1IRL and a further five from PCP2IRL[89] during the course of this research.

Were there any difficulties in obtaining the product, online or through a retail outlet?

No problems were encountered at retail outlets, apart from one occasion, with PCP1IRL, where a member of staff was unaware of the sales process. The researcher simply went to another store and obtained the card there. The purchase fee for cards obtained in retail outlets was paid in cash. Similarly few difficulties were encountered in obtaining cards from provider websites. Only one application, with PCP1IRL, was declined due to limitations around the holding of more than one card per customer. Where purchased online, the registration fee for PCP1IRL's cards were paid via other prepaid cards, although this option was rejected by PCP2IRL because the name on the paying card did not match the application. Payment was therefore paid using the credit held on a mobile phone account.

The ease with which this initial stage of obtaining these cards, remotely via the internet or face-to-face at a retail outlet, would not provide any difficulties for those wishing to use the card for criminal purposes.

[89] I was at a slight disadvantage as I had previously dealt with this provider and it could be expected that they would still hold records of that customer relationship.

What KYC checks were carried out when the products was obtained or applied for by the customer?

Having obtained a number of cards it has become apparent that no independent verification of the customer's profile details takes place. On only one occasion with PCP1IRL, were the researcher's correct, and verifiable, profile details provided. Similarly, with PCP2IRL the correct profile details, although with the name in Irish, were used only once. In all other applications various combinations of incorrect profile details such as a misspelt or fictitious name, unconnected or modified address, correct and incorrect date of birth, were used. Like most ROI providers, PCP1IRL and PCP2IRL apparently rely on the receipt of mail as part of their KYC compliance. While PCP1IRL does require the number from an identity document, PCP2IRL apparently views the delivery of post as not just proof of the customer's residential address but also their identity. It should be said that PCP1IRL, with its insistence on the delivery of post to a residential address, probably views that delivery as a backup to its securing of an identity document number.

However, a matter of great concern was the delivery by PCP2IRL of a card to a centralised postal delivery address, the card subsequently being forwarded to an unmanned pickup point. The provider did send an email query when this address was used during the application process, requesting the researcher's home address. A completely fictitious address was provided after the provider undertook that no correspondence would be sent there. The fact that this central address was accepted indicates a lack of understanding by the provider of the implications of its use or

that it leaves their cards even more susceptible to various criminal activities including ML, TF and bank fraud[90].

Had any independent verification of the details provided in most of the applications taken place, some obvious discrepancies would have been discovered. For example, addresses that did not exist on official records or with no one of the applicant's name living at the traceable addresses. These incidents would, at the very least point, towards potential identity fraud with potential for ML, TF or the theft of funds from a compromised bank account. The lack of provider enquiries or the cancellation of any card indicates that the provider did not detect or recognise any concerns around these issues. This lack of KYC verification could leave this provider's cards susceptible to misuse for TF or ML.

How effective were controls over the receipt of documents/document numbers related to the confirmation of a customer's identity and address?

Most providers, including PCP2IRL, do not require documentary evidence of KYC information relying, as outlined in Point 2 above, on postal deliveries as confirmation of some of the KYC information provided. But, unlike most other providers, PCP1IRL does require confirmation, namely an identity document number. However, they do not appear to verify that the document exists. The number frequently used was not the individual document number, but the local authority reference number. As that number cannot be traced to an individual the retention of the number, as evidence of the customer's identity, is completely meaningless. On one occasion during a call to their helpdesk the member of staff

[90] Bank fraud here refers to the criminal theft of funds from a legitimate bank account by, for example, online hacking of a customer's internet banking facility, the theft of a credit/debit card etc.

was unable to advise which number should be provided and accepted the untraceable number. But this lack of verification has other implications. A check on the number used would have shown that the document was not issued by the local authority of the address used in a number of the applications. While not necessarily a problem in itself, it would have made the provider aware of a potential issue around the address of the customer and a possible case of identity fraud. However, no query was received relating to the provision of this number.

While PCP1IRL may, as outlined in Point 2 above, use postal deliveries as an additional proof of identity, the lack of independent verification of the identity number is a serious issue, indicating poor control during the application process. Any knowledgeable money launderer or terrorist financier could easily ensure that the number used would be useless by the use of the same sort of meaningless reference number used in this case study. Therefore the product remains liable to misuse.

How stringently were controls preventing customers having more than one card or account applied?

The application of this restriction is a core issue for compliance with e-money regulations. Simplified CDD can only be applied on e-money products where the customer is restricted to a maximum annual balance of €2500 with withdrawals of €1000 p.a.[91]. When customers source more than one card, that limit can be broken. The five cards from each provider, obtained during the research, should have been detected in a number of ways. For example, monitoring of the identification number supplied to PCP1IRL would have detected multiple online applications and

[91] European Council 2009, Article 19 (2) d of Directive 2009/110/EC states that: '....a limit of €2500 is imposed on the total amount transacted in a calendar year,'

registrations of outlet sourced cards. There appears to be no monitoring of applications from the same address, multiple cards from both providers using the same numbered address in the mid-west, similar numbers using variations of the address in the north-east. Three PCP1IRL applications had the same date of birth, two of these using the English spelling of the name and the third in Irish, all with slight variations of the address in the north-east. Two PCP2IRL applications had the same date of birth and name, one using a variance of the north eastern address, the other the mid-western address. A third card was sent to the mid-western address with virtually the same spelling of the name and an almost identical date of birth. Two cards, one from each provider were sent to the mid-western address using completely fictitious names. On only one occasion was an order rejected when PCP1IRL detected a second application through the use of the existing card to pay the purchase fee. Surprisingly, despite this apparent breach of e-Money regulations, no further investigation appears to have been made, the original card remaining active.

On a number of occasions applications were delayed as the system automatically detected the reuse of a mobile phone number or email address. Two PCP1IRL and PCP2IRL applications were delayed when existing contact details were used, but completed when new details were provided. However, this does not appear to have triggered any deeper investigations, the existing cards originally tied to those contact details remain active. In total ten cards, with the potential to store €25,000 and allow cash withdrawals of €10,000[92] were obtained. The lack of control over the number of cards held by individual customers has implications not only for potential

[92] The remaining funds could be transferred to online payment systems or used for online or face-to-face purchases.

misuse for ML, TF or fraud, but potentially leaves the providers open to accusations of noncompliance with EC e-money regulations.

How easily could the product be funded?

With both providers, cards can be loaded with funds at numerous retail outlets. No identification or profile details were required. The only difficulty encountered was where retail staff lacked training or knowledge of the procedures for processing a transaction. However while this caused short delays at the outlet, it did not prevent funds being lodged. Small amounts of cash were processed to a number of cards without difficulty, including a number processed at the same time without query. PCP2IRL also offers the option for fund transfers between its customers, a number of these transactions being carried out without difficulty.

The research was limited by a lack of funds which prevented any assessment of the lodgement of larger amounts. However, having discussed same with a number of staff in various outlets, this would not appear to have been a problem. This anonymous lodgement of cash, and the ease with which it could be accomplished, makes this product, and many others in the market, attractive for ML or TF.

What practical day-to-day needs, such as online fund transfers, retail purchases or ATM withdrawals, could be carried out with the product?

With both cards, when purchased through a retail outlet, the customer has the option of making a once off lodgement to the card. The amount allowed is minimal and while PCP2IRL's card has full functionality, PCP1IRL's card cannot be used for ATM withdrawals until registered online. However, once registered both cards have most of the facilities available from mainstream cards and an annual holding limit of €2500. While limited in their monetary value, both cards financed online transfers

of funds to individuals and businesses in various countries, including France, Belgium, China, the US and UK. ATM withdrawals were made in the ROI, UK and US. Goods and services were purchased at retail outlets in the UK, US and ROI. Transfers were also made to various online payment systems, for the purchase of phone credit and other prepaid credit cards. On only a few occasions were difficulties experienced in the use of the cards. Problems occurred due to the lack of a particular security feature on both cards when used for some online purchases. PCP2IRL's cards could not be used for the purchase of UK prepaid cards, the researcher being advised by the provider that a bar on the payment of funds to other 'financial institutions' was in place. However, their cards did work for the purchase of other ROI prepaid cards.

The practical features available on these cards would therefore be attractive for ML or TF, offering as they do much of the same functionality as mainstream cards.

Would certain customer behaviours trigger an enquiry from the provider or the withdrawal of services?

To assess the monitoring of suspicious behaviours or actions, a number of activities were undertaken. During a number of applications and card verifications with both providers, access was gained using various UK ISPs. During one application with PCP1IRL, access was gained using a non-EU ISP for an online application. On this occasion the provider became aware of the application due to the use of an existing PCP1IRL card and the application. However they did not notice, or view as a matter of concern, the use of an outside ISP or the use of a non-EU phone number as a contact detail on that application. This is evidenced by the fact that despite emailing the researcher regarding their decision, no mention was made of either the non-EU phone number or ISP address. The use of a non-ROI phone number is not possible

with PCP2, as the application process does not permit their use. However, PCP1IRL allowed a UK and, as already mentioned, a non-EU phone number to be used. At no point was the use of foreign ISPs and/or phone numbers questioned by either provider. This is a concern for both providers as the use of an outside ISP could indicate a non-resident customer, potentially in breach of their own terms and conditions.

For mainstream banks the reactivation of a dormant account or card normally results in contact being established with the customer. Usually concerned with potential fraud, this contact can also prevent misuse for ML or TF. Therefore, the researcher retained a number of cards for a few months before registering or activating them. While not significant for retail outlet sourced cards, potentially held at the outlet for a considerable time, it was significant for cards ordered online. Other cards were verified, loaded and used before being put to one side and not used for some time. With one PCP1IRL card, the dormant period extended to almost eleven months while another online card was not activated for over two months. With PCP2IRL, a card remained unused for almost ten months with another held for twenty months. A third card was purchased but left unverified for three months. None of these dormant or unused cards resulted in a query being received. This is in marked contrast to the actions taken by a number of providers of online payment services who suspended accounts and issued email reminders when accounts remained unused or unfunded. At the very least they should elicit an email in a similar fashion to what occurred with online payment providers. Cards held for a period of time could indicate preparations pending a large ML or TF operation.

In another action which offered an opportunity for the provider to become aware of multiple card holdings or incorrect profile details, a number of queries were placed

with their help desk by email or phone. Some of the queries occurred during the purchase of the first cards, while others were generated after a number of cards had been obtained and activated. Remarkably, two queries relating to different PCP1IRL cards were submitted using the same email address, a sure indication of a multiple holding. This did not seem to be recognised by the provider. Despite these actions, and even after the cards and, presumably, the activities, applications and verifications had been examined, no queries were received related to multiple card holdings, applications from outside the applicant's home state or dormant cards.

The rejection of some orders indicates that some monitoring is in place. But the absence of provider enquiries indicates a lack of sufficient internal controls or possibly staff training/awareness. Had these been in place the detection of a potential non-resident obtaining cards or the multiple issue of cards to one person would have been possible.

These deficiencies in control or monitoring would make this product very attractive for criminal use.

Does the provider monitor the product for suspicious transactions?

While the researcher could not conduct tests with large value transactions, it was possible to conduct transactions that should trigger some level of attention. PCP1IRL's cards were used to purchase prepaid cards from other providers, including a card from PCP2IRL, a virtual card and cards from UK providers. Cards from PCP2IRL were used to fund the purchase of a card from PCP1IRL and in several failed attempts to purchase UK prepaid cards. Another suspicious transaction occurred when the card purchase fee for another provider's card was being paid for by a PCP2IRL card. This payment was initially rejected as the paying card's KYC

details did not match those on the application. However, when the details were changed to match the application, rather than the paying card's actual details, the payments were processed. This could have indicated a number of things, including card fraud or the holding of cards in fake names. All of these transactions should have triggered investigations by all of the providers involved. Not only was there the possibility of multiple ROI cards being held, indicating potential misuse, but also the purchase of cards from outside the country indicating that the applicant was not a resident. There was also at least one case of potential fraud.

As previously detailed, PCP1IRL's cards transferred funds to private individuals and businesses in different parts of the world, transactions also being carried out in retail outlets in the UK and the US. PCP2IRL cards were used for retail purchases in the ROI, UK and US as well as ATM withdrawals in all three countries. While not suspicious in themselves, such transactions, if paid using a mainstream credit card, would usually have resulted in a query, predominantly to prevent fraud but also to verify what the card was being used for. In a similar vein the transfers of funds from an active PCP2IRL card into a dormant card should have triggered some response.

At no stage did either provider question any of the transactions processed against a card. This indicates either a lack of account monitoring or perhaps a lack of concern that the customer may possess multiple cards issued under e-money regulations, has had their card stolen or is incurring unusual transactions[93]. This additional

[93] This is especially true with the ready availability of other prepaid cards in various currencies allowing reduced transaction fees and greater control over exchange rate used. See,
http://www.cashpassport.com/1/en/ie/Buying-Your-Card/

evidence of a lack of internal controls would again make this product attractive for ML or TF.

Discussion

Both providers operate in a very similar manner to each other and to many other providers in the market. Both operate under EC e-money regulations, offer their products through retail outlets and their websites, and provide full functionality when the cards are registered with minimal KYC information. Both depend on the receipt of post as proof of residency, PCP2IRL also depending on this as evidence of the existence of their customer, while PCP1IRL requires additional proof of identity, namely the number from an identification document.

Both providers also share many of the problems identified in this research. Anonymous, unregistered email and phone contact details were accepted which provide little hope of meaningful links to customers engaged in illegal activity. The receipt of a code sent by post is accepted as proof of residence and by default, proof of the existence of someone of that name at that address. However this is subject to abuse by, for example, the use of derelict or unoccupied properties, the subletting of a rental property or illegal access to someone else's mail. There appear to be few controls in place to prevent multiple card holdings. Despite numerous occurrences where these could have been detected, such detection only occurred once and could be easily avoided. The active monitoring of profile details such as address or date of birth would have brought many of these cards to their attention. Further potential breaches in e-money regulations could have been detected in transactional monitoring or for non-ROI ISPs used during the application/verification process. Both providers appear to have problems related to staff training, with PCP1IRL's lack of staff knowledge about the correct number to be taken from an identity

number and the acceptance of a centralised delivery address by PCP2IRL. While some of the concerns detailed above may be unique to these two providers, at least some of them are relevant to other providers, namely the acceptance of unregistered contact details and the receipt of post as proof of identity and address.

But each provider has its own unique concerns. For PCP1IRL, it was the acceptance of a meaningless identity document number. Had any verification taken place it would have been obvious that the number was untraceable. It is therefore apparent that there are no additional checks were undertaken. While PCP1IRL is unusual in requiring this number at an early stage of a customer relationship, the lack of verification renders it meaningless as a contribution to its compliance duties. For PCP2IRL, the major issue was the delivery of a card and associated documents to a parcel delivery address which effectively removes any link to the customer's home address. While there are problems around the confirmation of addresses by post, the use of this delivery service leaves PCP2IRL's cards open to even greater levels of misuse. With simple, untraceable registrations it would be possible for a money launderer or terrorist financier to open multiple delivery addresses assigned to multiple, fake identities and obtain multiple cards each with a limit of €2,500 thus providing a ready-made system for layering illicit funds.

However, it should be noted that these issues are prevalent with many other providers. The researcher was able to obtain or gain approval for seven cards from four other providers, using similar methods to those detailed in the cases above and without receiving any queries. Another provider even sent a card and PIN to the central delivery address used with PCP2IRL.

Unfortunately, neither the providers nor their issuing banks, agreed to meet the researcher to discuss various aspects of their AML/CFT regime.

In summary, both providers have serious issues regarding their compliance with the EC's e-money regulations and the prevention of the use of their products for ML or TF. These issues would appear to extend to many others within the industry.

Prepaid Cards: The United Kingdom

The prepaid card market in the UK expanded greatly in recent years and includes offerings from banks, building societies and CUs as well as numerous providers operating outside the mainstream market. As many of the mainstream providers operate their prepaid cards under the same KYC requirements as their mainstream accounts, the research concentrated on the provision of cards by non-mainstream providers.

Similarly to the ROI market, cards are available via provider websites and retail outlets. However, most cards have to be registered online with basic KYC details of name, date of birth, residential and email address and phone number before they can be used. Once this has been completed the provider will attempt to confirm the KYC details via electronic searches. Where those searches are unsuccessful the provider will normally offer a card with transactional limits of between £1600 and £2000. Customer's have the option of providing copies of identification documents, usually certified, to remove these restrictions. Once registered and activated the cards offer normal facilities such as ATM withdrawals, online and face-to-face commerce but some cards can also be enhanced to allow payment of direct debits and standing orders as well as the receipt of wage transfers. Some basic cards are

restricted to funding by cash at numerous retail outlets, while others also offer funding by credit card, bank transfer or mobile phone app.

Two cases studies are detailed hereafter, followed by a discussion of the findings and a comparison of the two markets. With both providers, cards are available via their website and through various retail outlets. PCP1UK's card allows some limited use before registration, while PCP2UK's card cannot be used before registration.

Were there any difficulties in obtaining the product, either through a retail outlet or online?

Both providers' cards are available in retail outlets in Northern Ireland. However, there were some problems in rural areas where there are limited numbers of stockists and numbers of cards held. When sourced at a retail outlet, fees were payable in cash, KYC details were not required at the time of purchase but are for the online registration and the postal dispatch of an activation code from PCP2UK. One verification process with PCP2UK was blocked when the researcher refused a request to phone the provider. Online purchases were processed after the provision of normal, basic KYC information. Most were processed without difficulty, although one PCP2UK application was cancelled due to a problem with the loading of funds at the time of purchase. This application was reprocessed successfully at a later date. It was not possible to test the payment of fees for online purchases of PCP1UK's card as these are not payable until after the sale has been approved. Approval for those purchases was not obtained for the reasons detailed in point two below. PCP2UK's online purchase fees were funded by prepaid card. Surprisingly one payment was accepted from a card in a different name to the applicant while on a second application the paying card had not been registered. Those involved in ML or TF would have little difficulty in this initial stage of the process.

What KYC checks were carried out when the product was obtained or applied for by the customer?

There are some differences in the amount of KYC information required by the two providers. With both providers the customer is required to provide the standard KYC information of name, address, date of birth and contact details, but PCP1UK also requires details of employment and income details. As previously stated, the address used in Northern Ireland had no connection to the researcher making it impossible for a successful electronic search to be conducted.

Having applied to obtain full facilities with PCP1UK, the researcher was advised by email that the provider was unable to confirm the KYC details by electronic search. They required certified copies of an identity document along with either an original or certified copy of an address confirming document. Very strict rules around the certification were set, including how the certification should be completed and a requirement for the certifier's contact details. This occurred with both outlet obtained cards and online applications and would make the use of fake or altered documents a high risk option.

With PCP2UK, the inability to perform a successful online search was dealt with very differently. This provider, like many others in the UK market, relies on postal deliveries as proof of the existence of someone of that name at a particular address. Two cards, one sourced in a retail outlet and the other online, were verified in this way, while a third retail sourced card was suspended pending the receipt of a phone call from the researcher. When this was declined the card remained inoperative. It is unclear why this occurred, different identity number and profile details but the same address were used as with the successfully activated cards. Those other cards

remained active so it would appear that there were no suspicions raised against them.

PCP1UK's apparent refusal to use the delivery of post as proof of identity and address, and their requirement for certified copies of identity documents, would create severe difficulties for anyone wishing to use these cards for ML or TF. In comparison the dependence on a delivery of post as proof of identity and address, with no apparent independent verification, leaves PCP2UK and many other providers, liable to misuse for criminal purposes including ML and TF.

How strict were controls over the receipt of documents/document numbers related to the confirmation of a customer's identity and address?

For the majority of providers there is no requirement to provide documents or document numbers to avail of their basic card. However, both PCP1UK and PCP2UK set different standards to each other and in the case of PCP1UK very different standards to the rest of the market.

As set out in the previous section, PCP1UK advised the researcher that they were unable to verify his details and set out their requirements for the provision of original and certified documentation, repeated in every email received. This provision of certified documents would effectively reduce the chance of anonymity so important for ML and TF. The requirement for certified copies and the lack of an address confirming document prevented any further experimentation around the provision of documentation.

PCP2UK requires the provision of an identification document number during the online order or card verification process. While processing the two activated cards, the researcher provided the same meaningless reference number from the driving

licence used in the ROI experiments. This was accepted without query. With a third card a fake number for a passport was used during its verification. This verification was declined pending receipt of a phone call from the researcher, which was not made. It is not known if the verification of the card was refused due to the identification document number or perhaps the receipt of multiple applications from the same address over a short period of time. However, no queries were raised about the other cards which used an equally meaningless reference number and which remain active, so this would seem unlikely.

Overall there seems to be poor control over the document details received by PCP2UK. As previously outlined the reference number from the driver's licence was meaningless and impossible to trace to an individual. The fact that it was not a UK driving licence did not seem to come to the provider's attention. This weakness in internal controls renders meaningless the whole exercise of obtaining the reference number. Such an absence of internal controls and the dependence on postal delivery as identity confirmation, leaves these cards open to misuse for ML or TF.

How stringently were controls preventing customers having more than one card or account applied?

Controlling the number of cards held by individual customers is a vital part of a provider's compliance with the monetary restrictions imposed by e-money regulations. With the refusal of PCP1UK to approve a card without either a successful electronic search or the provision of certified copies of KYC documents, it was not possible to establish if it would be possible to obtain a number of fully capable cards. This level of control would reduce the possibilities of one customer being able to obtain a number of fully capable cards. In the case of PCP2UK, two cards were obtained using similar profile details. The same identity reference

number, address and similar names and dates of birth were used in both applications for the cards that remain active. No queries were received in connection with these cards. As previously detailed a third card, issued using the same address, was obtained but verification was refused. It is unclear if this related to the presence of other cards at the address, but the fact that the other cards remain active would point to this not being so. With the apparent lack of internal controls which would have made it aware of not only a meaningless reference number but that it had been used twice, PCP2UK remains vulnerable to multiple applications from the same person. Not only is there a higher risk of ML or TF misuse through the issuance of multiple cards but also the attendant risk of noncompliance with e-money regulations around the use of simplified CDD.

How easily could the product be funded?

Both providers' cards are easily fundable. PCP1UK only permits funding via cash through retail outlets, while PCP2UK card holders can lodge funds through retail outlets or by transfer from the customer's bank account. Cash was lodged at a number of outlets, staff being able to process the lodgements without identification or KYC details. While the limitation on available funds meant that it was not possible to test large value lodgements of cash, it was confirmed at several outlets that such lodgements were not problematic. This ability to anonymously lodge relatively large amounts of funds, even where it must be done over a few days, would prove attractive to those who would use this card for illegal purposes.

What practical day-to-day needs, such as online fund transfers, retail purchases or ATM withdrawals, could be carried out with the product?

With the refusal to provide an ATM capable card, PCP1UK's cards were of reduced capability. However the cards were used for the purchase of other prepaid cards in

both the UK and ROI, as well as the funding of online payment systems. Both of the activated PCP2UK's cards, once verified, offered full ATM, online and face-to-face retail facilities. ATM withdrawals and retail purchases were conducted in the US, UK and ROI. Online purchases were made with businesses in the UK. Transactions were processed to credit an online payment system and to purchase a prepaid card in the ROI. While this latter transaction was successful, an attempt to buy a UK prepaid card failed due to the absence of a security feature. In terms of practical usage, PCP2UK's cards would be useful to those involved in ML or TF whereas the unverified card from PCP1UK would be of minimal use.

Would certain customer behaviours trigger an enquiry from the provider or the withdrawal of services?

Various actions were implemented which should have drawn the provider's attention. With both providers, during all aspects of the application/verification process, UK and non-UK ISPs were used. Transactions were conducted to purchase other prepaid cards including some from the ROI which would indicate that the KYC details held by both providers were incorrect. However this did not generate any query from either provider.

In another action, cards, ordered via PCP2UK's website, were retained for a period of time before being activated. With one of those cards an email request was made for login details almost two months after the verification letter arrived. A number of PCP2UK's cards were obtained over a relatively short period of time using the same address. Two cards were fully activated, but provider refused to activate the third card unless a phone call was received. This was the second request for a call that was refused. As already stated it is unclear if this was due to the number of applications received or some other issue around the individual application, but the

other cards remained active. In another application the use of a centralised postal address was noticed and declined by PSP2 UK. However it should be noted that despite a number of suspicious applications being brought to the attention of PCP2UK, the provider allowed two cards to remain in use. These cards were based at the same address with similar names and dates of birth and the same identity document number.

The inability to upgrade the card restricted the attempts to evaluate PCP2UK's internal controls or procedures and reduces the value of the findings related to this point. However the lack of response to a number of potential indications of false KYC information being provided is a concern. It is of course impossible to assess how they would have reacted in similar circumstances if this had occurred with a fully capable card.

With PCP2UK, the refusal to accept a centralised delivery address would indicates some level of internal monitoring in place. However, there are still serious issues around the monitoring of accounts for suspicious behaviours, something which would be favourable for those misusing the cards.

Does the provider monitor the product for suspicious transactions?

As outlined in a number of previous sections, the restricted functionality of PCP1Uk's card reduced the potential for this type of assessment. Despite this, a number of transactions were processed which, as described in point 7, should have engendered some interest from the provider. However these did not result in any contact with the researcher.

In a bid to test this aspect of PCP2UK's AML/CFT regime a number of transactions were processed. While these were low value at least some of the transactions should have resulted in a query from the provider. Over a short period of time a number of payments were attempted for prepaid cards issued by other providers including one in the ROI. This should have been a concern for a number of reasons. Firstly, the attempt to obtain numerous cards could be an attempt to circumvent e-money regulations which preclude balance holdings greater than €2500, or to hide or move substantial amounts of illicit funds. Secondly, the purchase of a ROI issued card would indicate that the customer is not resident in the UK, in contravention of EC and local e-money regulations. At no stage was a query received about the use of the cards or what should have been seen as indications of a non-resident having possession of the cards. This lack of monitoring for suspect transactions would be useful for those who would misuse the products.

Discussion

While these providers share some operational similarities there are also many differences. Both offer their cards through retail outlets and online, both cards can provide a full range of services. But the KYC requirements they impose on customers are vastly different. In the case of PCP1UK, the measures they have implemented will discourage those involved in criminal or terrorist activities. To avail of an ATM capable card the requirement for certified customer documentation, when independent verification of a customer's profile details cannot be achieved, will significantly reduce the chances of misuse. Even when these documents are received, the provider appears to be determined to ensure their legality by being capable of contacting the certifier. Where they are unable to verify the customer's details or do not receive the required KYC documents, they do offer some level of services, services which, though limited, could be misused. However, the monetary

limits and reduced capabilities of those cards would make such misuse difficult and hardly worthwhile. It is therefore unlikely that this provider's cards will be misused when so many other UK providers offer much more easily obtained and capable cards for those involved in ML or TF.

One of those providers is PCP2UK. A customer must provide almost the same amount of information but is not required to provide the same levels of proof. Where the provider is unable to verify the customer's profile details, they dispatch a letter, the receipt of which is confirmed by the customer. This is accepted as proof of the customer's existence and address. However, all that proves is the customer's access to post delivered to that address. The provider also requires the customer to provide an identity document number. But again this is of no value, the researcher being able to use a meaningless number which is useless for customer identification. But the provision of this number also demonstrated another concern: the lack of control over multiple card applications. Despite using it on a number of applications, sharing very similar profile details and the same address, the researcher was able to obtain and activate two cards without difficulty. In marked contrast to PCP1UK, this lack of application monitoring leaves this provider very open to abuse for various forms of criminal misuse including ML or TF.

However, while the contrast might be marked with PCP1UK, it is much less so when PCP2UK is compared to other providers. Using the same methods as those used in the detailed cases, the researcher was able to obtain or gain approval for a further seven cards from four other providers. None of the providers were able to trace the customer profile details provided, relying on the delivery of post as proof of the customer's existence and place of residence. Only one other provider requested any form of documentation, but unlike PCP1UK accepts uncertified copies. The only

queries received from these providers were connected to the delayed payment of application fees. In one case a staff member told the researcher of the problems around the use of prepaid cards to pay for their services, but did not question the researcher's procession of two prepaid cards which had been used in an attempt to pay the fee.

Perhaps, what was even more surprising was that the researcher would later receive an offer of a preapproved standard credit card with a £2000 overdraft limit from one of these providers. This despite the fact that the card had not been fully activated and there would have been no possible trace of their customer using the details held.

Having examined these various providers it has become obvious that many of them shared the same problems evident with PCP2UK and are as open to abuse by those who would misuse their products for criminal purposes.

The ROI and UK prepaid markets and their potential for ML or TF: A comparison

In many ways the provision of services in the ROI and UK are very similar. In both jurisdictions, cards can be obtained through retail outlets and provider websites, and can avail of full services once registered online. Additionally, untraceable mobile phones and email accounts are accepted, customers need only provide basic KYC information, while identification documents, usually certified copies, are normally only required for upgrades to higher limits. Cards can normally be funded by cash through numerous retail outlets, transfer from the customer's bank account and, occasionally, by transfers from other card holders. Monetary limits are almost identical given exchange rate fluctuations. However, there are some differences. Some UK cards can be used to receive wages/salaries, some offering direct debit

facilities, whereas ROI cards generally do not process such payments. Most importantly, UK providers use electronic searches to confirm a customer's KYC details before relying on the delivery of post if the search is unsuccessful. In the ROI, providers apparently rely on the delivery of post from the onset, routinely advising customers who have an outlet sourced card that a coded letter will be despatched.

But the main concerns are the commonality of some of the problems identified in the research findings. In both jurisdictions there appears to be very little monitoring for suspect behaviours, no meaningful verification of KYC details and few controls in place to prevent the issuance of multiple cards to a customer. Each of these facts makes the use of these products more attractive to those involved in ML or TF. In an age when the use of 'money mules' and identity theft continues to be major factors in financial crime these products, as they are administered at the moment, could be seen as tailor-made for abuse.

Online payment systems: ROI and UK

Many providers now offer online payment systems, sometimes in conjunction with online sales or auction sites, sometimes as an independent means of transferring funds between individuals or countries without the involvement of mainstream FSPs. A number of systems were sampled, accounts were opened and transactions conducted. Two examples of payment systems are examined here. Unlike prepaid cards there are few providers who operate in one country and not the other. Where there are differences in how the systems operate in the ROI and UK, these are detailed. Most services are only available via the internet, so the questions differ slightly from those applied to prepaid cards.

The two providers, dealt with in two case studies detailed hereafter, operate on virtually a worldwide basis. There are some differences in their provision of services. OPS1 concentrates on online payments only offering prepaid cards to valued clients. Upgrades are available to higher volume personal or business users, offering, for example, facilities for accepting subscriptions and recurring payments, payments through websites, and potentially, a prepaid card. OPS2, a provider of prepaid cards as well as payment systems, offers three types of account starting with a basic facility with restricted types of funding, and no withdrawals or transfers to other accounts. The other accounts offer more extensive facilities including expanded funding options, fund transfers to other account holders and a prepaid card for withdrawals.

The researcher was restricted to the use of his correct date of birth, and slight changes in the spelling of his name, in order to allow for the use of his identification document in an examination of upgrade processes.

Were any difficulties encountered in obtaining the product?

With both providers, applications for these services must be completed online. The basic process of applying for these services involved providing the normal KYC details, although OPS1 does not require a date of birth while OPS2 does. No documentary proof of identity or address was required, while anonymous phone numbers and email addresses were accepted. This initial account opening stage should provide no difficulties for those who would misuse the system.

What KYC checks were carried out when the service was applied for?

A number of applications with both providers were processed using UK addresses. Three accounts being opened with OPS1, using both real and fictitious addresses.

During the application process for the first account which used a real address, an automatic message advised that the KYC information could not be verified, requested that it was checked and warned that documents might be required. The documents could not be supplied and later attempts to log in were unsuccessful, triggering a contact request from the provider. A second account was opened using a fictitious address, was blocked when an enquiry was submitted soon afterwards, and a request received for KYC documents. The third account used the real address and remains active but has been used for only a few transactions and has not resulted in any requests for documentation or customer contact. Two UK applications were processed with OPS2. One application was blocked on completion when the provider was unable to trace the profile details provided and requested KYC documentation. In the second application, the provider immediately blocked the account and requested similar documentation due to the use of an outside ISP, as detailed in the section dealing with the monitoring of suspicious activities.

As KYC documents were not available, none of the blocked accounts could be reactivated.

Six applications were also processed for ROI accounts, three with each provider. Of the three accounts opened with OPS1, only the KYC details used for one would have been traceable. This account remains active but has only been used for a few small value transactions. A second account, which used the correct name but an untraceable address, also remains active but had not been used for any transactions. The third account which again used an untraceable address was used for a number of transactions totalling less than €150. However, this account was blocked and a request received for KYC documents. It is unclear why this occurred as a request for an explanation was not answered.

With the first OPS2 application the researcher's correct name and date of birth was used in conjunction with the address in the mid-west. This account was blocked, the provider later advising that it was for 'security measures'. The second account was opened some months later, using the correct KYC details with a slightly modified version of the researcher's home address. This account was blocked almost immediately on opening as a duplicate of the first account despite having a different address. This may also have resulted in the blocking being placed on the first account. The third account was opened with the correct KYC details of name and date of birth and a slightly modified version of the researcher's home address. This account remains active. Surprisingly, having been blocked, the first account is now active again. Having contacted the provider they advised that the block resulted from 'older security measures' and would now be removed. No further explanation was given.

Presumably in the hope of providing a direct link to a regulated entity, OPS1 actively encourages the customer to provide a link to another FSP during the application process. UK customers are asked for a link to their bank account while in the ROI they encourage a link to a bank account and/or a credit card. During one ROI application, a link to a prepaid card was accepted, despite the card being issued to a different address. Confirming a test transaction on this card led to the account achieving 'verified' status. OPS2 does not promote the link to a bank or credit card account as part of the account opening process.

Regarding OPS1, it is unclear why certain accounts were blocked and others left in place. The blocking that was implemented may have been triggered by the number of transactions rather than their total value. Unfortunately, despite a number of requests from the researcher for an interview, the provider did not reply. It is

therefore uncertain if the suspension of UK accounts relates to an inability to perform an electronic search or if the requests for documents on the ROI accounts were normal. However, it does appear to be a standard procedure on a global basis[94], and as such would be a major deterrence to those who wish to misuse the system. What is of concern was the granting of a verified status through the placing of a link to a prepaid card, a card which had been obtained with minimal KYC requirements and issued to a different address.

The findings relating to OPS2, the immediate blocking of a UK account when the KYC details could not be proven and the detection of suspected duplicate profile details with some ROI accounts, demonstrate a significant level of monitoring during the application process, and is a major deterrence to those trying to use the system for ML or TF. However the subsequent lifting on one blocking may indicate a softening of their regime.

How effective were controls over the receipt of documents/document numbers related to the confirmation of a customer's identity and address?

In order to upgrade to a higher level of account with either provider, the customer is required to provide two KYC documents. The researcher was therefore unable to apply for an upgrade on the UK accounts. To upgrade the ROI account, very poor copies of the researcher's driving licence and an address confirmation were uploaded to both provider websites. With OPS1 a letter from a prepaid card provider was initially advised in a phone call as being acceptable but rejected later. It is unclear why this occurred but the fact that the letter was undated would have

[94] Numerous comments on various online forums, from disgruntled account holders in different countries, refer to the provider suspending accounts and requiring KYC documents. Many of these requests are received at an early stage of the customer-provider relationship.

been unacceptable given their requirement for a document less than three months old. The unclear copies of the driving licence were rejected by both providers, as was the poor copy of a utility bill provided to OPS2. Given the quality of the copies these rejections were in line with normal compliance requirements, as was the rejection of the undated letter from a prepaid card provider by OPS1. Setting these standards for the receipt of documents will ensure compliance with AML and CFT requirements, and should aide in the detection of fake or fraudulently altered documents.

How stringently were controls preventing customers having more than one card or account, applied?

Ensuring that multiple accounts are not opened for the same customer is vital to a provider's compliance with the demands of e-money regulation. With OPS1, It is unclear how quickly multiple accounts would be detected in the normal course of events. For example, the researcher having contacted the provider with a query, triggered the discovery of a duplicate account. The researcher was advised of this and the second account closed off immediately. A UK account with similar profile information to another account but a different address, was blocked, without explanation, when the researcher submitted a query about the use of prepaid cards to withdraw funds. Unusually, two accounts were opened, one in each jurisdiction, using the same email address. This did not elicit any response from the provider, although one of the accounts was suspended at a later date for unknown reasons.

As set out in section (2) two OPS2 accounts in the ROI were set up using the same name and date of birth, but a different address. One of those accounts was blocked at the time of opening. As only two out of three of the principal profile details were the same, the name and date of birth, this indicates comprehensive monitoring for

duplicated KYC information. However, this decision has recently been rescinded. With UK accounts, similar profile details were used, but as one of the accounts was blocked on completion of the application it was not possible to assess if the OPS2 would have detected the second account.

This enhanced monitoring of accounts by OPS2 make the opening of multiple accounts difficult for those involved in ML or TF. With the lack of response to either the researcher's queries about account closures or to a request for an interview, this aspect of OPS1's AML/CFT regime remains unknown.

How easily could the product be funded?

Neither provider accepts cash lodgements, either directly or through such services as *Paypoint* or *Payzone.* Funding for transactions with both providers can be made through the customer's bank account or credit card, while OPS1 also offers the option of receiving funds from other OPS1 customers. As previously advised the option of using a bank account was not being used. OPS1 offers customers the option of using their services as a conduit for payments to others. As such a number of prepaid credit cards were used to fund transfers between a number of OPS1 accounts as well as to pay for a number of online transactions processed via OPS1.

With OPS2, two different prepaid cards were tried, one in the same name as the account and one not. However, both cards were refused. The provider subsequently advised that prepaid cards can only be accepted as a source of funds with upgraded accounts, with only mainstream issued credit or debit cards being accepted on the basic account. With the use of such cards reducing the possibilities of anonymous transactions taking place, this option was not utilised.

This lack of anonymous funding sources will render OPS2's basic account unpopular with those involved in ML or TF. However the same cannot be said of OPS1 whose acceptance of prepaid cards both as a funding source, via transfers between customer's accounts, as well as a payment source for online purchases, could make their services attractive for ML or TF.

What practical day-to-day needs, such as online fund transfers, retail purchases or ATM withdrawals, could be carried out with the product?

OPS1's system is primarily designed to allow for payments related to internet based sales and to transfer funds between friends or family. Therefore, a number of transactions in payment of online purchases were undertaken as was the transfer of funds between two of the accounts, one UK based, the other in the ROI. The purchase transactions were processed without difficulty or enquiry, only one being refused due to an unregistered card. However, one inter-account transfer was refused for security reasons[95]. The limitation on available funds meant that it was not possible to test the reaction of the provider to high value transfers. However, the fact that almost all of the accounts used for transactions received requests for KYC documents would indicate that this provider would certainly request the same of an account used for higher value transactions. The provision of such documents and links to regulated FSPs would deter those involved in ML or TF.

OPS2's entry level account is very limited in its functionality. The only transactions that can be processed are those payable to a merchant. The enhanced accounts do offer much greater facilities such as online fund transfers and ATM, but only after

[95] Details of this refused transfer are detailed in the section dealing with the monitoring of suspicious transactions by this provider.

KYC documents have been provided. This basic account would be of little use to those involved in ML or TF.

Would certain customer behaviours trigger an enquiry from the provider or the withdrawal of services?

In order to assess how these providers would react to unusual or suspect customer activities, a number of actions were implemented. During the application process an 'outside' ISP was used, potentially indicating that the customer was a non-resident. OPS2 blocked a UK account as soon as it was established, cited the use of the non-UK ISP and requested an explanation for its use. They also required the provision of KYC documents and a scanned copy of a credit card attached to the account. It should be noted that this was requested during an application for the basic level of account, a level at which they are not normally required. With OPS1 no queries were received for any of the account openings where outside ISPs were used.

A number of queries were submitted to both helpdesks. Queries were raised with OPS1 relating to a prepaid card from an independent provider who claimed that funds could be downloaded from OPS1's accounts. The immediate response was to block the account and request the provision of KYC documents, while not providing any response to either the original or subsequent queries. Similarly another query led to the discovery of a duplicate account which was quickly closed.

The queries submitted to OPS2 related to a change of address and login difficulties. The latter queries did not illicit any direct response, but the change of address query resulted in a blocked account and a requirement for KYC documents that exceeded

that normally required by mainstream providers[96]. It is possible that some factors, such as an inactive and unverified account while the submission of poorly scanned copies of KYC documents, detailed in section (3), may also have contributed to the blocking of the account. A query was submitted to the provider but the reply attributed the blocking to a now defunct 'security measure'.

With OPS1 the lack of monitoring for outside ISPs is a concern when compared to the response of OPS2. However, their reaction to any unusual query with a requirement for KYC documents, along with the proactive discovery and closure of a duplicate account point to an active monitoring for suspect activity which would deter those involved in ML or TF.

There can be no doubt that the level of monitoring of OPS2's accounts, evidenced by the detection of non-home state ISPs and the immediate requests for KYC documents when an online search failed, indicates that they supervise the account opening process closely and view any indications of nonconformity with the KYC information held, as a serious issue.

Does the provider monitor the product for suspicious transactions?

The inability to lodge funds to OPS2's accounts, apart from through a mainstream credit or debit card, and the restriction to transactions with merchants, made it impossible to conduct transactions in such a way as to test this aspect of their compliance regime. Similarly, the restrictions on the amounts involved made it difficult to replicate suspicious transactions, with smaller value transactions being

[96] Most mainstream providers only require a signed request from the customer to amend their address details.

the norm with OPS1. However, funds were transferred between a few of the accounts in an attempt to draw the attention of the provider to accounts with similar profiles. One of these transfers, from a UK account to a ROI account, was refused due to concerns that it portrayed a 'higher than normal risk'. However, OPS1 was unwilling to provide any further details. As previously advised, having declined a number of requests for an interview, it is therefore unclear what regime is in place for the monitoring of accounts for suspicious transactions.

Conclusion

Having opened a number of accounts it soon became evident that both providers were diligent in attempting to prevent misuse. OPS1 blocked duplicate accounts, suspended others and required KYC documentation whenever any sort of suspicious behaviour was exhibited by a customer, usually well before e-Money limits had been reached. Sometimes accounts were blocked and documents requested for no apparent reason. OPS2 required KYC documentation before full functionality would be made available and suspended an account due to a security protocol[97]. Both providers impose strict rules around the acceptance of KYC documents, refusing to accept substandard copies or unsuitable documentation.

However, there are differences. OPS2 actively monitors the application process, blocking one account when an online search did not confirm the KYC details provided and another when an outside ISP was used. Both accounts would require KYC documentation before being reactivated. OPS1 did not notice the use of an outside ISP during the application process. Given the global nature of the internet this could leave them vulnerable to the opening of supposedly EU resident accounts

[97] This protocol has since been removed and the account reactivated.

by non-EU residents. Additionally, OPS1 not only accepted prepaid credit cards as a funding source but allowed one to form part of a customer verification process. Conversely, OPS2 blocks the use of prepaid cards until the customer has provided KYC documents, only allowing funding from a standard, fully compliant credit card.

In conclusion, both providers appear determined to prevent the use of their systems by those wishing to remain anonymous. However, OPS1 has issues around its acceptance of prepaid cards as well as the lack of monitoring for the use of outside ISPs during the application process. However, its early and unpredictable demands for KYC documents compares favourably with OPS2's refusal to accept prepaid cards, monitoring for suspect applications and its early demands for KYC documents make misuse of their systems very unlikely.

However it should be noted that others in the industry operate in a manner very dissimilar to either provider. Many accept the receipt of post as proof of residency, only requiring KYC documentation when a customer requires higher limits. Most require similar levels of KYC information to Ops1 and OPS2 during account opening and accept prepaid cards as payment sources. However, unlike the providers in these two case studies, one provider accepted the central mail delivery address for an account and an attached prepaid card. This leaves this particular provider much more open to abuse that the two case studies detailed here.

There are few differences in the provision of services between the two jurisdictions. In the ROI there are some extra options for the linking of a credit card and/or a bank account, while the UK specifies only a bank account. Most providers in the UK can avail of online searches to confirm KYC information but in the ROI they normally require documentation to be provided as presumably the effectiveness of online

searches are limited. Unfortunately the researcher was unable to source information on the capabilities of those searches, in either the ROI or UK, as will be detailed in the next section.

CHAPTER 7

CONCLUSION

This thesis responds to the EU's call for research on the possible misuse of NPMs for TF. The research found that this call was warranted and that the potential for the misuse of NPMs, especially prepaid credit cards, for a variety of purposes including but not restricted to TF, is high. This is especially true for low-cost terrorist attacks such as those carried out in Madrid in April 2004 or the London bombings of 2005, the cost of each could easily have been transported using a few of these cards. Equally, the risk of their use for ML is also high.

The EU's call for research on the use of NPMs for TF is acknowledged in Chapter one, along with an expansion of this thesis to cover their potential use for ML. The first chapter continues with a review of the history and importance of AML and CFT and the concerns raised, not just by the EU, about the potential misuse of NPMs for ML or TF. A review of the literature dealing with NPMs and their misuse for ML or TF is detailed in Chapter two, before Chapter three reviews the regulations pertinent to NPMs. Chapter four examines various NPMs available in the ROI and UK, before detailing why prepaid cards and online payment systems were selected for an in-depth examination. The chapter concludes with detail of the methodology used in that examination. A review of the prepaid and online payment systems market in the ROI and UK is carried out in Chapter five, before a detailed breakdown and analysis of the research findings is provided in Chapter six.

Concerns and identified problems

Those findings highlight a number of concerns with both types of NPMs. Online payment systems appear to be administered with a view of erring on the side of caution: the researcher's experience was that KYC documents were being requested much earlier than necessary under regulation. However, there are issues around the use of prepaid cards as a verification source and the lack of monitoring of the use of outside ISPs with at least one provider. But it is with those prepaid cards that the greatest concerns have come to light. Both ROI providers had at least one serious issue each: the acceptance of a remote delivery service address by one, the lack of verification of identity documentation by the other. This concern extended to the UK where the same number was also accepted by a provider.

An additional, perhaps even greater shared concern is the ease with which multiple cards were obtained by the researcher. It soon became apparent that it was feasible to obtain numerous cards from various ROI and UK providers. Unfortunately, the refusal by providers and issuing banks for interviews means that it can only be speculated what their response would have been to the question of multiple card holdings. However, this is a core issue in preventing the abuse of a system which is meant to limit its usage to €2500 per person, per year. The numerous cards obtained in both jurisdictions, with the potential for many more, demonstrates that, as currently administered, these cards could be a useful tool for those involved in ML or TF.

There are also a number of other issues, some pertinent to all FSPs. Most NPMs, place great reliance on the provision of mobile phone and email contact details. However these would be valueless as they would be untraceable in the hands of a knowledgeable criminal or terrorist. While removing anonymous email addresses

would be almost impossible, compulsory registration of mobile phones has been imposed in some countries where their use for criminality was seen as a concern (Gow and Parisi, 2008, pp. 62-65). While the use of a link to a regulated FSP as part of a compliance regime is sanctioned under EC regulation (European Council, 2001a, *Article 1(3)(11*)), the worth of such a link has to be questioned. The researcher is aware of at least one mainstream provider currently accepting customer provided photo-copies of identification documents in a bid to update outstanding KYC issues. It is unclear how extensive this programme is or if it extends to other providers, but it does bring into question, the value of a link to such a provider. There have also been the concerns around poor compliance by mainstream FSPs referred to at the conference attended by staff from the Irish Central Bank[98].

Potential Solutions

Providers have a number of potential solutions using their current set-up. For example: enhanced monitoring for suspect behaviours such as the use of foreign ISPs, the use of foreign phone numbers as a contact detail, the purchase of other cards or the receipt of fee payments from foreign cards.

But in order to reduce misuse, providers must be able to confirm their customer's identity with confidence. Currently, this would entail extensive online profile searches. If those searches were unsuccessful, which could occur frequently dependent on their customer base, they would have to resort to the lengthy and expensive process of obtaining and verifying certified copies of KYC documents. The

[98] See Footnote 66.

cost to the provider of implementing such requirements would prohibit new entrants and may result in even more providers leaving the market[99].

As one solution, the researcher examined a system available in Germany. Where certified copies are required, a member of the public can visit a German Post Office and present their KYC documents for examination, copying and certification[100]. The copies are then forwarded directly to the provider by the post office. This is different to similar services in the UK and ROI. For example, in the UK the copy is then handed back to the customer who sends it on to the FSP[101]. However, this provides an opportunity for certified copies to be examined and fake certified copies produced[102]. The German system reduces the chances of this occurring.

Another measure, but one that some would balk at for reasons of personal privacy, would be the requirement for the customer to provide their personal social welfare number[103]. Unfortunately, the researcher could not verify exact system capabilities due to the lack of response from the FSP's support companies but is aware of similar systems being used. However, if on provision of that number to a FSP, customer's profile details were confirmed as matching, it would reduce the possibilities of identity fraud. This would have to be further confirmed by the use of the current postal code despatch system, and there would be some risk of theft of the customer's number and subsequent interception of post. However it would ensure

---

[99] Several providers left both markets during the course of this research, most noticeably Ruby cards in the ROI and O2 in the UK. The reason for these departures has not been confirmed.
[100] Deutsche Post Postident, see https://www.isbank.de/en/consumer-banking/services/account-opening-with-deutsche-post-postident-identity-verification/
[101] UK Post office, see http://www.postoffice.co.uk/sites/default/files/P6582.pdf
[102] The researcher is aware of issues around the use of fraudulent, certified copies of official documents.
[103] Personal Public Service number (PPSN) in the ROI, or National Insurance Number (NIN) in the UK.

profile details were correct and prevent the opening of multiple accounts with the same provider, once proper monitoring was in place. If the opening of the account was registered centrally it would also prevent the opening of accounts with different providers. This would also deal with an issue that the researcher has been aware of for a number of years: the ease with which genuine utility bills can be obtained for use as proof of a residential address[104]. During the course of this research, a number of utility providers in various EC member states, including the ROI and UK, confirmed that customer details can be amended by phone. This has implications for all FSPs, but would be solved by the use of the customer's PPSN/NIN.

For NPMs, both solutions would have to be accompanied by enhanced monitoring for multiple account holdings. The introduction of such schemes in the ROI and UK, perhaps at a reduced cost to encourage those with a low income, could have far reaching implications for the provision of financial services. If this scheme was extended to mainstream FSPs it would significantly reduce their compliance costs and perhaps open up the market for basic low-cost bank accounts.

However, these measures assume that there is a will or a need to prevent ML or TF of these values. Certainly, it would have been possible for the researcher to hold approximately €9,000 and £6,500 on payment systems, and €45,000 and £17,000 on prepaid cards. In all probably it would have been possible to continue obtaining cards using the methods described, there are very few restrictions given the infinite number of profile details that could be used. The question that can only be answered

[104] The researcher has personal experience of one joint Irish utility bill having at least one fake name on it.

by governments or transnational bodies, such as the EU or the FATF, is the value of preventing ML or TF at relatively low values.

Limitations

The research was limited by a number of factors. Firstly, the restricted amount of funds available during the process for the testing of AML/CFT/KYC responses from providers. Secondly, language difficulties prohibited the expansion of the research outside the ROI and UK. The third factor was the limited time available for experimentation in the UK. Fourth were the legal constraints placed on using fake or altered KYC documentation.

The final factor was the lack of response from many of those involved in the industry. Unfortunately, despite contacting approximately fourteen non-mainstream prepaid card providers and issuing banks along with four online payment system providers, none of those contacted were prepared to discuss their operations with the researcher. Some cited customer or client confidentiality while others did not reply at all. The sole successful contact was with some members of the Association of British Credit Unions Limited.

The researcher also contacted a number of support companies who provide KYC verification services for FSPs. Once again, despite numerous phone calls and emails, many of these companies did not reply and of those that did reply one agreed to call back but did not. Of particular disappointment was the reaction of one member of staff of a well-known support company whose name had been given to the researcher by a member of staff as a suitable contact. On making a call to this person, the researcher had to endure various insulting comments about his status as a student, before being told to send in an email to the general office email address,

which would be replied to. Despite that promise, and a reminder email being sent, no reply was forthcoming.

Future Research

There is considerable need for further research in a number of fields. Digital currencies such as Bitcoin have expanded in popularity over recent years and remain an unregulated means of fund transfer. As previously detailed there are some pending cases alleged cases of criminal misuse. There are also issues around the potential for those involved in ML or TF to set up their own digital currency. While research has been conducted in this field, the constant evolution of these currencies and their potential for misuse requires further research.

Business use of the internet ranges from sellers on internet auction sites to the largest commercial enterprises. However, during the course of this research a number of potential ML/TF have become apparent, including the ease with which companies can be registered using online resources, the potential use of various NPMs such as online payment systems in conjunction with fake businesses, the age-old use of 'phantom' trading[105] but now using online auctions and sales.

Finally there has been a considerable expansion in the involvement of non-traditional FSPs, such as supermarkets and department stores, who now offer credit cards, current and savings accounts on a non face-to-face basis. Additionally, there has also been a great increase in the provision of short term finance such as payday loans.

---

[105] This involves payments for goods which are never intended to be shipped, the funds transfer appearing to be legitimate.

Research to focus on all of these fields in relation to potential use for ML/TF, is warranted.

REFERENCES

Beasley, D. and Whitcomb, D (2009) 'Canada money launderer shows holes in Vegas casinos', *Reuters*, 17 November, [Online]. Available at: http://www.reuters.com/article/2009/11/17/us-insider-vegas-idUSTRE5AG5QH20091117

Bensted, G. (2012) 'Hi Terrorist Financing and the Internet: dot com danger.' *Information & Communications Technology Law,* 21(3), pp. 237-256. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/13600834.2012.744222?journalCode=cict20 (Accessed 15 December 2012)

Brezo, F. and Bringas, P.G. (2012) 'Issues and Risks Associated with Cryptocurrencies such as Bitcoin', *The Second International Conference on Social Eco-Informatics*, 21-26 October, Venice Italy. Available at: http://www.thinkmind.org/index.php?view=article&articleid=sotics_2012_1_40_30101 (Accessed: 10 January 2013)

Bronk, C., Monk. C. and Villasenor, J. (2012) 'The Dark Side of Cyber Finance', Survival: Global Politics and Strategy, 54(2), pp. 129-142. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/00396338.2012.672794 (Accessed 15 February 2013)

Brooks, G. (2012) 'Online Gambling and Money Laundering: "views from the inside" ', *Journal of Money Laundering Control*, 15(3), pp. 304-315. [Online]. Available at: http://www.emeraldinsight.com/journals.htm/journals.htm?issn=1368-5201&volume=15&issue=3&articleid=17041945&show=pdf (Accessed 31 August 2012)

Chambers, C. (2012) 'Can you ever Regulate the Virtual World against Economic Crime?', *Journal of International Commercial Law and Technology*, 7(4), pp. 339-349. [Online] Available at: http://www.jiclt.com/index.php/jiclt/article/view/168/166 (Accessed: 20 January 2013)

Chargualaf, J. (2008) *Terrorism and Cybercrime*, Unpublished dissertation. Air Command and Staff College Air University, Maxwell AFB, USA. [Online] Available at: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA489730 (Accessed 15 May 2010)

Choo, K.K.R. (2009) 'Money Laundering and Terrorism Financing Risks of Prepaid Cards Instruments', *Asian Criminology*, 4, pp. 11-30. doi : 10.1007/s11417-008-9051-6.(Accessed June 20, 2010).

Christin, N. (2012*) Travelling the Silk Road: A measurement analysis of a large anonymous online marketplace,* pp. 1-24, Unpublished paper. *Carnegie Mellon INI/CYLa.,* [Online]. Available at: http://arxiv.org/abs/1207.7139 (Accessed: 5 January 2013)

Council of the European Union (2009) '*The Stockholm Programme – An open and secure Europe serving and protecting the citizens.*', [Online]. Available at: http://ec.europa.eu/home-affairs/doc_centre/docs/stockholm_program_en.pdf (Accessed: 8 October 2010)

FATF (2001) 'FATF IX Special Recommendations', [Online]. Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf (Accessed: 18 September 2011)

FATF (2006) '*Report on New Payment Methods'*, [Online]. Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf (Accessed: 15 January 2011)

FATF (2010) '*Money Laundering using New Payment Methods'*, [Online]. Available at: http://www.gafisud.info/documentos/esp/doc_interes/tipologias/010-Money%20laundering%20using%20new%20Payment%20Methods%202010.pdf (Accessed: 23 April 2012)

FATF (2014)*'Virtual Currencies, Key Definitions and Potential AML/CFT Risks',* [Online]. Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (Accessed 4 July 2014)

Feldman, R. (2006) 'Fund Transfers-African Terrorists Blend Old and New: Hawala and Satellite Telecommunications', *Small Wars and Insurgencies,* 17(3), pp. 356-363. doi: 10.1080/09592310600672867. (Accessed: 1 June 2010)

Filipkowski, W. (2008) 'Cyber Laundering, An Analysis of Typology and Techniques', *International journal of Criminal Justice Sciences,* 3 (1), pp. 15-27. [Online]. Available at: http://www.sascv.org/ijcjs/Wojciechijcjsjan2008.pdf (Accessed: 1 June 2010)

Filipkowski, W. (2004) '*Internet as an Illegal Market Place'*, 6th Cross-border Crime Colloquium, Berlin. Available at: http://www.cross-border-crime.net/pdf/CCC-2004-Filipkowksi.pdf (Accessed: 16 December 2012)

FINCEN (2007) '*2007 National Money Laundering Strategy* ', [Online]. Available at: http://www.fincen.gov/news_room/rp/files/nmls_2007.pdf (Accessed: 7 July 2014)

Fossat, P., Kahla, S., Reyreaud, F. (2012) 'The Effectiveness of International Cooperation in the Fight against Money Laundering', *Themis Competition 2012,* Unpublished paper. [Online]. Available at; http://www.ejtn.eu/Documents/Themis%202012/THEMIS%202012%20ERFURT%20DOCUMENT/Written%20paper%20France_Team%201.pdf (Accessed: 15 January 2013)

Gonzalez, A.G. (2004) 'PayPal: the Legal Status of C2C Payment Systems', *Computer Law and Security Review***,** 20(4), pp. 293-299. [Online] Available at: http://www.era.lib.ed.ac.uk/bitstream/1842/2262/1/paypal.pdf (Accessed: 24 November 2011)

Gow, G.A., and Parisi, J. (2008) 'Pursuing the Anonymous User Privacy Rights and Mandatory registration', *Bulletin of Science Technology Society,* 28(1), pp. 60-68. [Online] Available at: http://bst.sagepub.com.remote.library.dcu.ie/content/28/1/60 (Accessed: 22 February 2013)

Grinberg, R. (2012)'Bitcoin: An Innovative Alternative Digital Currency', *Hastings Science & Technology Law Journal,* 4(1), pp. 159-208. [Online]. Available at: http://www.heinonline.org.remote.library.dcu.ie/HOL/Print?collection=usjournals&handle=hein.journals/hascietlj4&id=163 (Accessed: 18 February 2013).

Hals, T. (2014) 'Bitcoin traders settle class actions over failed Mt.Gox Exchange', *Reuters*, 29 April [Online]. Available at: http://www.reuters.com/article/2014/04/29/us-bitcoin-mtgox-settlement-idUSBREA3S02W20140429' (Accessed: 25 May 2013)

Hett, W. (2008) 'Digital Currencies and the Financing of Terrorism', *Richmond Journal of Law & Technology.* 15(2), pp. 1-43. [Online]. Available at: http://law.richmond.edu/jolt/v15i2/article4.pdf (Accessed: 5 July 2010).

Hinnen, T.M. (2004) 'The Cyber-front in the War on Terrorism: Curbing Terrorist use of the Internet', *The Columbia Science and Technology Law Review*, 5. [Online]. Available at: http://www.stlr.org/html/volume5/hinnen.txt (Accessed: 5 July 2010).

Horgan, J. and Taylor, M. (2003) 'Playing the 'green card'-financing the provisional IRA: Part 2', Terrorism and Political Violence, 15(2), pp.1-60. [Online]. Available at: http://www.tandfonline.com.remote.library.dcu.ie/doi/pdf/10.1080/09546550312331293027 (Accessed: 15 May 2011)

Hornle, J. (2011) 'Online Gambling in the European Union: a Tug of War without a Winner'*, Yearbook of European Law*, 30(1), pp. 255-297. [Online] Available at: http://yel.oxfordjournals.org/content/30/1/255.short (Accessed: 1 September 2012)

Hunt, J. (2011) 'The New Frontier of Money Laundering: how terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them', *Information & Communications Technology Law*, 20(2), pp. 133-152. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/13600834.2011.578933 (Accessed: 23 June 2011)

Irwin, A.S.M. and Slay, J. (2010) 'Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warfare', *1st International Cyber Resilience,* Edith Cowan University, Perth Western Australia, 23 August. Available at: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1004&context=icr (Accessed: 15 June 2011)

Irwin, A.S.M., Slay, J., Choo, K.K.R. and Liu, L. (2013) 'Are the Financial Transactions conducted inside Virtual Environments truly anonymous? : An experimental research from an Australian perspective', *Journal of Money Laundering Control*, 16(1), pp. 6-40. [Online] Available at: http://www.emeraldinsight.com/journals.htm?articleid=17068452&show=html (Accessed: 12 February 2013)

Jacobson, M. (2010) 'Terrorist Financing and the Internet', *Studies in Conflict & Terrorism*, 33(4), pp. 353-363. [Online]. [doi :10.1080/10576101003587184 (Accessed: 6 April 2010).

Kaplanov, N.M. (2012) 'Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against its Regulation', *Temple University Legal Studies Research Paper*, March. [Online]. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203 (Accessed: 10 February 2012)

Keene, S.D. (2012) 'Emerging Threats: financial crime in the virtual world', Journal of Money Laundering Control, 15(1), pp. 25-37. [Online] Available at: http://www.emeraldinsight.com/journals.htm?articleid=17004745 (Accessed: 26 June 2012)

King, D. (2013) 'Have Anti-Money Laundering Measures Kept Pace with the rapid growth of GPR Prepaid Cards?', *Retail Payments Risk Forum Working Paper*, Federal Bank of Atlanta. [Online] Available at: http://www.frbatlanta.org/documents/rprf/rprf_pubs/130117_wp.pdf

Landman, S.I. (2009) 'Funding Bin Laden's avatar, A Proposal for the Regulation of Virtual Hawala', *William Mitchell Law Review*, 35(5), pp. 5159-5186. [Online]. Available at: http://web.wmitchell.edu/national-security-forum/wp-content/uploads/2011/06/18-landman.formatted.proof_master.post_proof_2.final_for_managing-adine.pdf (Accessed: 25 November 2010).

Levi, M. (2009) 'E-gaming and Money Laundering Risks: A European Overview', *ERA Forum*, 10, pp. 533-546. [Online]. Available at: http://link.springer.com/article/10.1007%2Fs12027-009-0143-2?LI=true (Accessed Sept 15, 2010)

Linn, C.J. (2008) 'Regulating the Cross-border Movement of Prepaid Cards', *Journal of Money Laundering Control*, 11(2), pp. 146-171.[Online]. Available at: http://www.emeraldinsight.com/journals.htm?articleid=1724239&show=html (Accessed 9 May 2012)

Masciandaro, D.,_Takáts E. And Unger B. (2007) *Black Finance: The Economics of Money Laundering,* Cheltenham: Edward Elgar Publishing.

McMullan, J.L. and Rege, A. (2010) 'Online Crime and Internet Gambling', *Journal of Gambling Issues*, 24, pp. 54-85. [Online]. Available at: http://www.cbc.ca/news/pdf/online-gambling-crimestudy.pdf (Accessed 26 February 2012)

Melongi, G. (2010) 'Fighting Financial Crime in the Age of Electronic Money: opportunities and limitations', *Journal of Money Laundering Control*, 13(3), pp. 202-214. [Online]. Available at: http://www.emeraldinsight.com/journals.htm?articleid=1876040 (Accessed: 9May 2012)

Merritt, C. (2010) 'Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments', *Retail Payments Risk Form White Paper*, Federal Reserve Bank of Atlanta. [Online]. Available at: http://www.frbatlanta.org/documents/rprf/rprf_resources/wp_0810.pdf (Accessed: 11 January 2013)

Mills, J. (2001) 'Internet Casinos: A Sure Bet for Money Laundering', Journal of Financial Crime, 8(4), pp. 365-383. [Online] Available at: http://www.emeraldinsight.com/journals.htm?articleid=1650615 (Accessed: 18 February 2013)

Pagliery, J. (2014) 'Bitcoin exchange CEO arrested for money laundering', *CNN*, 28 January [Online] Available at: http://money.cnn.com/2014/01/27/technology/security/bitcoin-arrest/

Schneider, F. (2011) 'The Financial Flows of the Transnational Crime: Some Preliminary Empirical Results', *Economics of Security Working Paper,* 53. [Online] Available at: http://www.diw.de/documents/publikationen/73/diw_01.c.386647.de/diw_econsec0053.pdf (Accessed: 23 January 2012)

Shubber, K. (2014) 'Jeremy Allaire: Regulators, Wall Street and Bitcoin Hitting the Mainstream', *Coindesk*, 27 January [Online]. Available at: http://www.coindesk.com/bitcoin-abandons-anti-establishment-wall-street/ (Accessed 15 May 2014)

Sienkiewicz, S. (2007) 'Prepaid Cards: Vulnerable to Money Laundering?' , *Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper No. 07-02* , [Online]. Available at: http://www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/2007/D2007FebPrepaidCardsandMoneyLaundering.pdf (Accessed July 2, 2010).

Simser, J (2013) 'Money Laundering: Emerging threats and trends', Journal of Money Laundering Control, 16(1), pp. 41-54. [Online] Available at: http://www.emeraldinsight.com/journals.htm?articleid=17068453& (Accessed: 12 January 2013)

Smith, T.J.O. (2012) *Identification Requirements and Policy in Alternative Remittance: A Measure of Legislative Adherence*, Unpublished dissertation, Edith Cowan University Western Australia. [Online]. Available at: http://ro.ecu.edu.au/theses_hons/67/ (Accessed: 24 January 2012)

Stokes, R. (2012) 'Virtual Money Laundering: the case of Bitcoin and the Linden Dollar ', *Information and Communications Technology Law,* 21(3), pp. 221-236. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/13600834.2012.744225 (Accessed: 15 December 2012)

Stringer, K.D. (2011) 'Tackling Threat Finance: A Labor for Hercules or Sisyphus?', *Parameters*, 41(1), pp. 100-119. [Online]. Available at: http://www.carlisle.army.mil/USAWC/Parameters/Articles/2011spring/Stringer.pdf (Accessed: 3 November 2012)

The Guardian (2013) 'Liberty reserve founder arrested in Spain', 28 May [Online]. Available at: http://www.theguardian.com/world/2013/may/28/liberty-reserve-arthur-budovsky-arrested-spain (Accessed: 5 July 2013)

Tibbetts, P.S. (2002) *Terrorist Use of the Internet and Related Information Technologies*, Unpublished paper, School of Advanced Military Studies, United States Army command and General Staff College, Fort Leavenworth, USA. [Online]. Available at: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA403802&Location=U2&doc=GetTRDoc.pdf (Accessed: 25 November 2010).

U.S. Department of Justice, (2008) *Money Laundering in Digital Currencies*, [Online]. Available at: http://www.justice.gov/archive/ndic/pubs28/28675/28675p.pdf (Accessed: 23 May 2012)

van den Broek, M., (2011) 'The EU's preventative AML/CFT policy: asymmetrical harmonisation', *Journal of Money Laundering Control*, 14 (2), pp. 170-182.

Villasenor, J., Monk, C. and Bronk, C. (2011) *Shadowy Figures: Tracking Illicit Financial Transactions in the Murky World of Digital Currencies, Peer-to-Peer Networks, and Mobile Device Payments*, [Online] Available at: http://94.236.38.250/Finextra-downloads/featuredocs/Villasenor%20etal_tracking%20illicit%20transactions.pdf (Accessed: 15 May 2012)

Vlcek, W. (2011) 'Global Anti-Money Laundering Standards and Developing Economies: The Regulation of Mobile Money', Development Policy Review, 29(4), pp. 415-431. [Online] Available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1467-7679.2011.00540.x/abstract (Accessed: 15 February 2012)

Wilson, D. (2011) 'US makes arrests in major poker website crackdown', *the Inquirer*, 18 April [Online]. Available at: http://www.theinquirer.net/inquirer/news/2044291/makes-arrests-major-poker-website-crackdown (Accessed 15 October 2012)

Zerzan, A. (2010) 'New Technologies, New Risks? Innovation and Countering the Financing of Terrorism', *World Bank working Paper No. 174*, [Online] Available at: https://openknowledge.worldbank.org/bitstream/handle/10986/5918/518360PUB0REPL101Official0Use0Only1.pdf?sequence=1 (Accessed: 2 June 2010)

REGULATORY REFERENCES

European Commission 1987, Commission Recommendation 87/598/EEC, of 8 December 1987 on a European Code of Conduct relating to electronic payment (Relations between financial institutions, traders and service establishments, and consumers), [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1987:365:0072:0076:EN:PDF (Accessed: 11 October 2013)

European Council 1991, Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1991:166:0077:0082:EN:PDF (Accessed: 8 September 2013)

European Commission 1997, Commission Recommendation 97/489/EC, of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder, [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1997:208:0052:0058:EN:PDF (Accessed: 14 October 2013)

European Council 2000a, *Directive 2000/12/EC of the European Parliament and of the Council of 20 March 2000 relating to the taking up and pursuit of the business of credit institutions,* [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:126:0001:0059:EN:PDF (Accessed: 17 October 2013)

European Council 2000b, *Directive 2000/28/EC of the European Parliament and of the Council of 18 September 2000 amending Directive 2000/12/EC relating to the taking up and pursuit of the business of credit institutions,* [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0028:en:NOT (Accessed: 7 October 2013)

European Council 2000c, *Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions,* [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:275:0039:0043:EN:PDF (Accessed: 20 September 2013)

European Commission 2001, *Study on the implementation of Directive 97/489/EC concerning transactions carried out by electronic payment instruments and in particular the relationship between holder and issuer,* [Online]. Available at: http://ec.europa.eu/internal_market/payments/docs/study-recomm-97-489/study-part1-recomm-97-489_en.pdf (Accessed: 15 January 2013)

European Council 2001a, *Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering,* [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:344:0076:0081:EN:PDF (Accessed: 10 September 2013)

European Council 2001b, *Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures against certain persons and entities with a view to combating terrorism,* [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:344:0070:0075:EN:PDF (Accessed: 27 October 2013)

European Council 2002, *Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC,* [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:271:0016:0024:EN:PDF (Accessed: 21 September 2013)

European Council 2005, *Directive 2005/60/EC of the European Parliament and of the Council of 26 October2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*, [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:en:PDF (Accessed: 10 September 2013)

European Commission 2006a, *Evaluation of the E-Money Directive (2000/46/EC) Final Report.* Brussels, [Online]. Available at: http://ec.europa.eu/internal_market/bank/docs/e-money/evaluation_en.pdf (Accessed: 15 November 2013)

European Commission 2006b, *Commission Staff Working Document on the review of the E-Money Directive (2000/46/EC)*. Brussels, [Online]. Available at: http://ec.europa.eu/internal_market/bank/docs/e-money/working-document_en.pdf (Accessed: 15 November 2013)

European Commission 2006c, *Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis*, [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_214/l_21420060804en00290034.pdf (Accessed: 23 October 2013)

European Commission 2008, *Impact Assessment accompanying the Draft Proposal for a Directive of the European Parliament and of the Council amending Directives 2000/46/EC on the taking up, pursuit of and prudential supervision of the business of electronic money institutions*. Brussels, [Online]. Available at: http://ec.europa.eu/internal_market/payments/docs/emoney/sec-2008-2572-summary-en.pdf (Accessed: 1 November 2013)

European Commission 2011, *Final Study on the Application of the Anti-Money Laundering Directive,* [Online]. Available at: http://ec.europa.eu/internal_market/company/docs/financial-crime/20110124_study_amld_en.pdf (Accessed: 15 November 2013)

European Council 2006a, *Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (recast)*, [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:177:0001:0001:EN:PDF (Accessed: 30 October 2013)

European Council 2006b, *Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions (recast),* [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:177:0201:0201:EN:PDF (Accessed: 9 November 2013)

European Council 2006c, *Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds,* [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:345:0001:0009:EN:PDF (Accessed: 8 October 2013)

European Council 2007, *Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market mending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC,* [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0001:EN:PDF (Accessed: 20 October 2013)

European Council 2009, *Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC,* [Online]. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF (Accessed: 5 September 2013)

Ireland 2002, *Regulations entitled European Communities (Electronic Money) Regulations 2002 (S.I. No.221 of 2002)*, [Online]. Available at: http://ec.europa.eu/internal_market/finances/docs/actionplan/transposition/ireland/d1-ml-ie.pdf (Accessed: 26 October 2013)

Ireland 2003, *The Criminal Justice Act, 1994 (as amended), Money Laundering, Guidance Notes for Credit Institutions*, [Online]. Available at: http://www.centralbank.ie/regulation/processes/anti-money-laundering/Documents/Credit_Institutions_AML%20Guidance%20Notes%20CJA94%20Regime.pdf (Accessed: 29 September 2013)

Ireland 2010, *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Number 6 of 2010),* [Online]. Available at: http://www.irishstatutebook.ie/pdf/2010/en.act.2010.0006.pdf (Accessed: 14 October 2013)

Ireland 2011, *European Communities (Electronic Money) Regulations 2011 (S.I. No 183 of 2011),* [Online]. Available at: http://www.irishstatutebook.ie/pdf/2011/en.si.2011.0183.pdf (Accessed: 2 October 2013)

Ireland 2012, Department of Justice and Equality, *Government Publishes Proposed Amendments to Anti-Money-Laundering Law* [Press Release]. 6 June. Available at: http://www.inis.gov.ie/en/JELR/Pages/PR12000158 (Accessed: 14 November 2013)

Ireland 2013, *Criminal Justice Act 2013 (Number 19 of 2013)*, [Online]. Available at: http://www.irishstatutebook.ie/pdf/2013/en.act.2013.0019.pdf (Accessed: 29 November 2013)

United Kingdom 2002, *The Financial Services and Markets Act 2000 (Regulated Activities) (Amendment) Order 2002. (Statutory Instrument, 2002 No.682),* [Online]. Available at: http://www.legislation.gov.uk/uksi/2002/682/pdfs/uksi_20020682_en.pdf (Accessed: 24 October 2013)

United Kingdom 2007, *The Money Laundering Regulations 2007 (S.I. No 2157 of 2007),* [Online]. Available at: http://www.legislation.gov.uk/uksi/2007/2157/pdfs/uksi_20072157_en.pdf (Accessed: 16 October 2013)

United Kingdom 2011, *The Electronic Money Regulations 2011(S.I. 2011 No.99),* [Online]. Available at: http://www.legislation.gov.uk/uksi/2011/99/pdfs/uksi_20110099_en.pdf (Accessed: 22 October 2013)

United Kingdom 2012, *The Money Laundering (Amendment) Regulations 2012 (S.I. 2012 No. 2298)*, [Online]. Available at: http://www.legislation.gov.uk/uksi/2012/2298/pdfs/uksi_20122298_en.pdf (Accessed: 19 October 2013)

United States 1970, *Currency and Foreign Transactions Recording Act,* [Online]. Available at: http://uscode.house.gov/statutes/1970/1970-091-0508.pdf (Accessed: 29 July 2012)