An Roinn Airgeadais
Department of Finance

New Technologies Risk Assessment

Update of Ireland's National Risk Assessment

Prepared by the Anti-Money Laundering Section, Department of Finance
www.gov.ie/finance

Contents

Introduction **5**

Scope 5
Methodology 5

Virtual Currencies **7**

Nature and Scale 7
Risk scenarios and ML/TF Vulnerabilities 12
Established and Potential Mitigants 13
Residual Risk 14

Crowdfunding **15**

Nature and Scale 15
Established and potential mitigants 18
Residual risk 19

Electronic Money **20**

Nature 20
Scale 21
Risk Scenarios 21
Established and potential mitigants 23
Residual risk 25

Conclusions **26**

Acronyms

ML	Money-Laundering
AML	Anti-Money Laundering
TF	Terrorist Financing
CFT	Countering the Financing of Terrorism
NRA	National Risk Assessment
STR	Suspicious Transaction Report
CDD	Customer Due Diligence
SNRA	EU Supranational Risk Assessment
AMLSC	Anti-Money Laundering Steering Committee
4AMLD	EU 4th Anti-Money Laundering Directive
LEA	Law Enforcement Agency
OCG	Organised Crime Gang
ICO	Initial Coin Offering
DLT	Distributed Ledger Technolog

Introduction

This update of Ireland's national risk assessment, focusing on the AML/CFT risks of new and emerging technologies, has been undertaken in accordance with Recommendation 15 of the Financial Action Task Force (FATF).

Scope

The sectors assessed for the purposes of this 'new technologies' risk assessment are:

- virtual currencies/assets,
- electronic money
- crowdfunding.

Methodology

ML/TF risks are assessed under the following headings: Nature and Scale/Risk scenarios and ML/TF Vulnerabilities/ Established and Potential Mitigants/ Residual Risk.
The Methodology used in the EU's supra-national risk assessment (SNRA) was used to determine risk ratings for each sector.
For each sector, a rating was assigned for its threat level and vulnerability level. Those ratings were determined on a scale from 1 to 4 as follows:

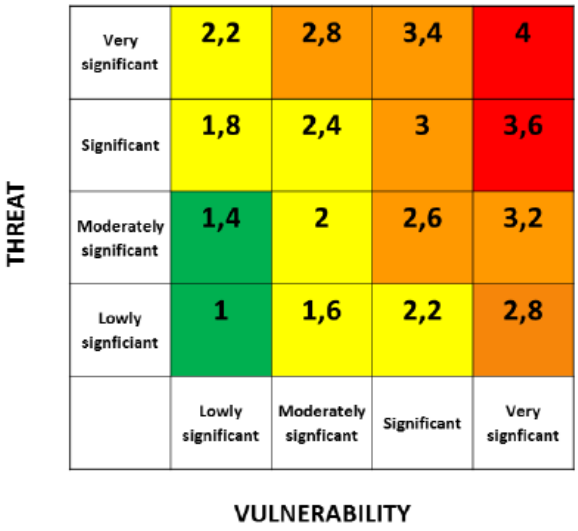
- Lowly significant (value: 1)
- Moderately significant (value: 2)
- Significant (value: 3)
- Very significant (value: 4)

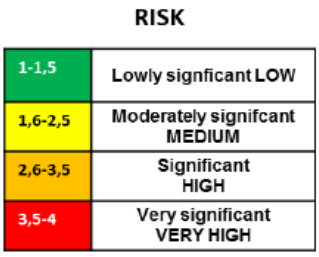
The SNRA methodology rated the level of residual risks by combination between the threat versus vulnerability. This risk level is based on a weighting of 40 % (threat)/ 60 % (vulnerability) – as it is assumed that the vulnerability component should be given more weight when determining the risk level[1].

1 European Commission 2017, Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, accessed 18 December 2018, https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF

The possible SNRA results are in the Table below:

SNRA Ratings scale





NRA Rating scale

Once a rating is calculated using the SNRA methodology, it is assigned a rating of low, medium-low, medium-high, or high as per Ireland's National Risk Assessment (NRA) ratings scale.

SNRA Rating Scale	NRA Rating Scale
Lowly significant (value: 1-1.5) LOW	Low
Moderately significant (value: 1.6-2.5) MEDIUM	Medium-Low
Significant (value: 2.6-3.5) HIGH	Medium-High
Very Significant – (value 3.5-4)VERY HIGH	High

Virtual Currencies

Nature and Scale

Of all 'new technologies', perhaps none has received the same degree of attention in recent years as virtual currencies, examples of which include Bitcoin, Ripple, ZCash, Monero, Dash and Ethyreum. In Ireland there has been an increasing level of attention brought to virtual currencies, or at least to blockchain technology, through a number of recent business and/or Government initiatives. These include the launch of a discussion paper by the Irish Department of Finance and the formation of a working group on the subject of blockchain/distributed ledger technology (DLT), the establishment by the Industrial Development Authority of Blockchain Ireland and the establishment in Dublin of new businesses such as ConSenSys, a company established by one of the founders of existing virtual currency Ethereum.

Yet the term itself is subject to dispute or confusion with other terms in use such as cryptocurrencies, digital currencies and virtual assets. With an absence of widely accepted definitions and regulation comes space for interpretations of them as currencies or assets, e.g. a number of authorities have determined that they should be dealt with as assets and this is also the approach currently taken to their taxation by the Irish Revenue Commissioners[2].

While the term 'currency' has been used to describe these items, the validity of its use in this context has been questioned. A paper by Professor Karl Whelan of University College Dublin[3] , commissioned by the European Parliament, makes interesting comparisons between 'virtual currencies' and standard defining criteria of a currency. A separate study produced by the Bank for International Settlements comes to a damning conclusion in this regard[4] . It also noted some forms of "privately issued "virtual currencies" – e.g. as used in massive multiplayer online games like World of Warcraft – predate cryptocurrencies by a decade"[5].

Detailed explanations of exactly how these assets/currencies work and the nature of the underlying technology are beyond the scope of this assessment and have been provided very well elsewhere. However, minor explanations may be necessary in the course of this document to explain what makes one product more or less of a risk than another.

Bitcoin, almost certainly the product which has gained the widest recognition in this field, consists of a verifiable 'block' of digital information, generated by solving complex mathematical problems ('Bitcoin mining'). The creation of a new Bitcoin and all transactions involving it must, by the nature of the product, be recorded on a 'blockchain', a form of distributed ledger technology, i.e. a digital ledger held in multiple locations. The nature of this makes their production and exchange highly consumptive of energy, e.g. reports in 2018 have suggested that the amount of energy used in mining virtual currencies in Iceland is set to overtake the country's electricity use for standard housing purposes. As every new bitcoin generated requires more energy to generate than any previous coin, this imposes a "rarity" factor for any given virtual currency akin to that for precious metals. However, many virtual

[2] https://www.revenue.ie/en/tax-professionals/tdm/income-tax-capital-gains-tax-corporation-tax/part-02/02-01-03.pdf
[3] http://www.europarl.europa.eu/cmsdata/149904/WHELAN_FINAL%20publication.pdf
[4] Annual Economic Report 2018, Bank for International Settlements
[5] Ibid.

currencies that have emerged since operate in a more efficient manner, consuming only a fraction of the energy associated with Bitcoin.

Bitcoin, and other non-state backed virtual currencies, are still not widely accepted as a means of payment[6]. The dramatic decline in the market valuation of Bitcoin from over $325 billion in December 2017 to less than $161 billon by May 2018, a decline of over 50%, may be evidence of their limited day to day use as a means of payment and may signify a decline in their popularity[7]. Most other virtual currencies have experienced similar declines in their value over this period. What virtual currencies have achieved, however, is to demonstrate that value can be transferred between individuals on a peer to peer basis without the need for centralised trusted intermediaries. This has led to the emergence of "tokenisation" whereby "virtual assets" can be used to securely and efficiently transact in traditional financial and non-financial assets such as equities or commodities (e.g. gold or diamonds). These "virtual assets" refer "to digital representations of value that can be digitally traded or transferred and can be used for payment or investment purposes[8]".

For example, a number of neighbourhoods in both the US and Australia have been able to use blockchain ledgers and tokens to manage peer-to-peer trading of renewable energy between participating households[9] , while banks can now partner with companies like Ripple to increase the speed of international payments by linking fiat currency transactions to tokens[10].

From the point of view of AML/CFT, in October 2018 the FATF agreed to amend its Recommendation 15 to extend AML obligations to what it terms 'virtual asset service providers', including not only those engaged in exchanges between fiat currencies and virtual currencies, as required by the 2018 package of amendments to the 4th AML Directive [11], but also those engaged in virtual-to-virtual exchange services. The new definition is as follows:

Virtual Asset	A *virtual asset* is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.
Virtual Asset Service Providers	Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more other forms of virtual assets; iii. transfer[1] of virtual assets; iv. safekeeping or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset. **Footnote 1:** In this context of virtual assets, *transfer* means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

[6] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf
[7] https://coinmarketcap.com/currencies/bitcoin/
[8] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html
[9] https://www.siliconrepublic.com/machines/brooklyn-microgrid-blockchain-energy-networks
[10] https://www.cnbc.com/2018/10/01/ripple-xrp-cryptocurrency-product-xrapid-goes-live-for-first-time.html
[11] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html

For the purposes of this risk assessment, we shall take 'virtual currencies' to include all products which could fall into the above FATF definition of virtual asset.

Scale

A number of research papers have been published examining the status of these products from different perspectives, including the risk of their misuse for criminal purposes. Perhaps inevitably the predominant product referred to or drawn upon for data is Bitcoin, the most recognisable of these products and the one which so far seems to have become in the public mind a byword for virtual currencies. The other products which fall into this category are numerous. However, it is considered that a dozen or so of these virtual currencies have attained a significant level of public awareness. The scale of the global virtual currencies market can be summarised by the following statistics:

As of April 2019, there were an estimated 2.160 different virtual currencies globally. Collectively, these had a total market value of roughly $182 billion (€162 billion). The market value of Bitcoin alone accounted for $93 billion, roughly half, of the total market value of all virtual currencies.[12]

The EU's 2017 Supra-national risk assessment provides the following picture of the scale of virtual currency use across the Union in comparison to globally:

Total VC wallets worldwide	**13 million**
VC wallets in the EU	About 3 million
VC users worldwide	From 1 to 4 million
VC users in the EU	About 500,000
VC miners worldwide	100,000
VC miners in the EU	10,000 (estimate)
VC software wallet providers worldwide	> 500 (estimate)
VC custodians worldwide	> 100(estimate)
VC custodians in the EU	> 20 (estimate)
Exchange platforms worldwide	> 100
Exchange platforms in the EU	> 28
ATMs worldwide	571
ATMs in the EU	> 100
Daily VC transactions	> 125,000 (Bitcoin only)
Merchants accepting bitcoins	110,000
Market capitalisation of VCs	**EUR 7 billion**

While the above mostly gives an indication of the numbers of people involved in this trade, the following table gives an indication of the value of major cryptocurrencies:

[12] https://coinmarketcap.com/

US Dollar value (as of April 2019)

Bitcoin USD 92.5 billion

Ethereum USD 19 billion

Ripple (XRP) USD 14.9 billion

Litecoin USD 5 billion

Bitcoin Cash USD 5 billion

EOS USD 5 billion

Binance Coin 2.6 billion

Stellar USD 2.4 billion

Cardano USD 2.3 billion

Tether 2.2 billion

TRON USD 2 billion

Bitcoin SV 1.4 billion

Monero USD 1.17 billion

Dash USD 1.16 billion

IOTA USD 981 million

NEO USD 812 million

Ethereum Classic USD 778 million

Zcash 451 million

Source: *CoinMarketCap*[13]

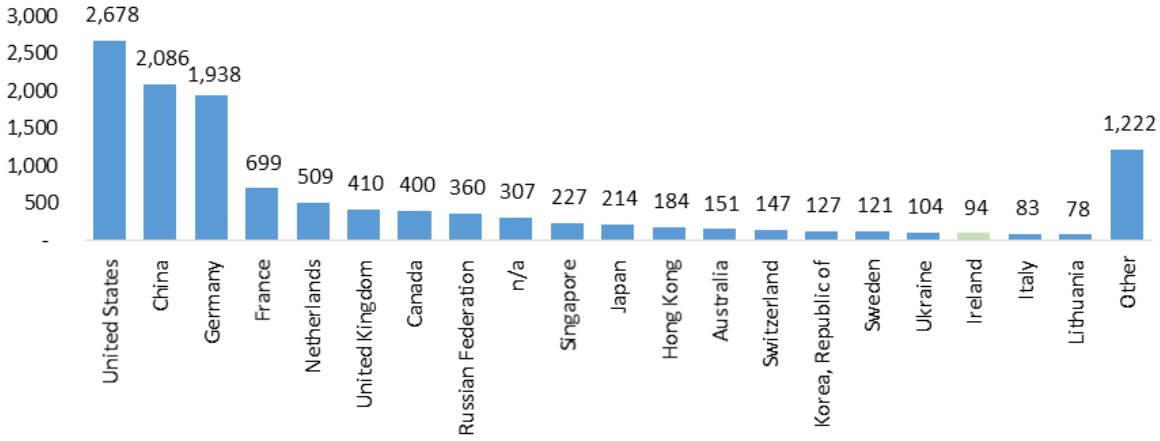
It can be seen from the above that despite the proliferation of different currencies, the market is dominated by a few and that Bitcoin in particular, at the time this table was compiled, was worth several times more than its nearest rival.

Unfortunately, there is a lack of data which would indicate the scale of this sector in Ireland specifically. Regulation which will follow the transposition of the 5th AML Directive will improve knowledge in this area. However, some sense of scale can be estimated.

The below chart[14] shows the number of Bitcoin 'nodes' by country. A Bitcoin node refers to the existence of a "full" client. A "full" client is a client that has access to the network and owns a copy of the blockchain ledger on which transactions are recorded. Although not very reliable as a measure, the number of nodes may help to determine the level of VC ownership that exists within a given country. According to this chart, Ireland ranks 18th in the world in terms of the number of nodes. Irish based nodes account for 0.8% of all nodes globally. However, this ranking has fluctuated over a period of months, e.g. from 17th to 23rd.

[13] Ibid.

[14] https://bitnodes.earn.com/# ttps://bitnodes.earn.com/#



A study carried out by communications agency Red Flag and research agency Amárach Research, which issued in June 2018, suggested that about 120,000 people in Ireland own cryptocurrencies.[15] The report also suggests that there has been a 300% increase in cryptocurrency ownership over the preceding four years.[16] Therefore, as in other jurisdictions, Ireland has seen an increase in the use of these assets over recent years which may only increase as encouragement is given to investment in them.

Scale of illegal activity

A recent study by a group of Australian academics[17] has determined, through a qualified analysis of transactions, that while the proportion of Bitcoin transactions associated with illegal activity has reduced since its earliest days, this is likely to be because of the wider adoption of the product and its use for legal activity as well. Therefore while the total number of transactions has increased significantly, illegal activity is still associated with a huge number of these transactions and with a huge number of Bitcoins in possession. The concomitant increase in legal activity only means that the proportional amount of illegal activity is less striking.

In detail, the study says:

> *We find that approximately one-quarter of bitcoin users and one-half of bitcoin transactions are associated with illegal activity. Around $72 billion of illegal activity per year involves bitcoin, which is close to the scale of the US and European markets for illegal drugs. The illegal share of bitcoin activity declines with mainstream interest in bitcoin and with the emergence of more opaque cryptocurrencies.*[18]

A 2018 FATF stocktake of trends in this area states:

[15] https://amarach.com/assets/files/cryptocurrency-research-may-2018.xlsx
[16] https://www.irishtimes.com/business/technology/irish-attitudes-to-cryptocurrencies-shifting-from-suspicion-to-curiosity-1.3525859
[17] Foley, Sean and Karlsen, Jonathan R. and Putnins, Talis J., "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?". Available at SSRN: https://ssrn.com/abstract=3102645 or http://dx.doi.org/10.2139/ssrn.3102645
[18] ibid, p. 14

> *Suspicious transaction reporting linked to crypto-currencies is rising. In Malaysia, there were 35x more STRs related to crypto-currencies reported to the FIU in 2017, than 2016. In Sweden the number of STRs filed doubled between 2016 and 2017. Spain has seen a 230% increase in the past year in crypto-currency STRs filed, and Japan received 669 STRs from exchangers between April 2017 and December 2017. In the Netherlands, the number of STRs received has increased from an average of 300 per annum (2013 – 2016) to 5,000 in 2017.*[19]

However, percentage increases are not a very useful measure of activity, and should be treated with some caution, as they are the result of the low initial numbers of reports. A number of arrests have been made across Europe relating to money laundering activities using virtual currencies.[20] Europol estimate up to £4.4 billion (€5bn) of criminal money is being laundered around Europe through bitcoin.[21] This equates to about 3-4% of the GBP 100 billion (€113bn) in illicit proceeds in Europe.[22]

Therefore it can be seen that Bitcoin, probably the most studied of virtual currencies, is certainly being used in connection with illegal activities. It seems reasonable to surmise that those currencies with enhanced privacy features are also being used to disguise the origin of funds.

In Ireland, law enforcement has stated that the most significant predicate crimes related to virtual currencies are drug related and fraud/cyber-crime related. The Financial Intelligence Unit of An Garda Síochána has received suspicious transaction reports related to virtual currencies but thus far none has by itself led to an investigation.

The Criminal Assets Bureau has taken a number of cases and actions involving virtual currencies that would put an estimated value of ML funds linked to virtual currencies in the tens of millions. However, it should be noted that this is based only on an extrapolation of the data to hand.

Risk scenarios and ML/TF Vulnerabilities

The risk from virtual currencies comes from their perceived 'anonymous' features. However, these could be more accurately described as 'pseudonymous'. The nature of distributed ledger technology means that every transaction carried out on a DLT-based system is recorded in multiple locations. Therefore transactions and owners can ultimately be tracked. The difficulty can then lie in identifying who it is carrying out transactions, particularly when multiple transactions are carried out to obscure a trail. Hence the use of 'mixers' or 'tumblers' which mix potentially identifiable currencies with others so as to make it more difficult to trace those engaged in illicit activities.

However, while the above description of a public record applies to DLT-based systems such as the most prominent, Bitcoin, as well as others such as Litecoin and Ethereum, new currencies have been developed specifically to provide greater anonymity, such as ZCash

[19] FATF RTMG June 2018 update, p. 2
[20] https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking
[21] https://www.em360tech.com/tech-news/technews/europol-arrests-11-ties-bitcoin-money-laundering-network/
[22] http://uk.businessinsider.com/europol-criminals-using-cryptocurrency-to-launder-55-billion-2018-2?r=US&IR=T

and Monero. The latter uses obfuscated ledger technology and 'ring signatures' so that each successive transaction becomes more difficult to track. It also uses 'stealth addresses' so that no-one other than the sender and receiver can determine the actual destination of a transaction. Obviously such a product is designed to protect the privacy of its users and even if the intent is not to facilitate illegal activity it thereby holds a greater risk of being used for ML or TF.

Therefore within the field of 'virtual currencies' lie several subgroups, some of which are dedicated to open shared information while others are focused on privacy and greater degrees of anonymity. While criminality may not be the aim of the latter products, this is obviously an aspect which makes them more appealing for use by criminal elements.

An aspect of virtual currencies which has also received much negative attention is that of Initial Coin Offerings (ICOs), the stage of inward investment at an early point in the life of a virtual currency, or other virtual asset. In 2017, it is believed that there were an estimated 552 ICOs with a combined value of just over USD$7.0 billion[23]. One study found that over 70% of ICOs by value went to what were believed to be "quality projects", but that over 80% of projects, by number, were identified as scams[24]. However, as this study demonstrates, the risk in ICOs is firstly as a means of fraud and/or Ponzi schemes. The Central Bank of Ireland has issued a number of consumer warnings in this regard. As these are financial crimes the proceeds of such fraudulent activity are likely to be laundered.

Regarding TF risks, these are considered as more likely to arise through the intersection of terrorism and criminality, with organised criminals being assessed as more likely to be aware of, and make use of, this sub-sector.

In light of this, the level of ML/TF threat related to virtual currencies is considered as **moderately significant.**

Established and Potential Mitigants

A number of jurisdictions, including Australia, Canada, Japan, and Spain, have already introduced regulation of virtual currencies, including for AML purposes.

Within the EU the amendments to the 4th AML Directive known as 5AMLD extend AML obligations to providers of exchange services between virtual and fiat currencies, as well as custodian wallet providers, and requires that all of these be registered. This will act as a mitigating factor within the EU as any movement between virtual currencies and the regular financial system will be subject to customer due diligence checks and exchanges shall be subject to supervision by state competent authorities.

The Central Bank of Ireland has issued consumer protection warnings on the fact that virtual currencies are not currently regulated in Ireland and on the dangers of ICOs. Further public

[23] https://www.pwc.ch/de/press-room/press-releases/pwc_mm_icoreport_de.pdf?utm_source=PwC%20CH%20Social%20Media https://cointelegraph.com/news/pwc-report-finds-that-2018-ico-volume-is-already-double-that-of-previous-year
[24] https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ

information is likely to be forthcoming when the 5th AML Directive is transposed and regulation takes effect in the world of virtual currencies.

Beyond these regulatory measures, the nature of those systems designed more for decentralisation than for anonymity acts as a mitigation of the risk of ML/TF as records of transactions are publicly accessible. Successes in using these records to trace criminals has been seen in Denmark[25] while in the USA, as part of an investigation of the use of virtual currencies by white supremacists, the American Southern Poverty Law Centre noted that *"Bitcoin purchases can be traced by a determined researcher."*[26]

The FATF's definition of virtual assets and virtual asset service providers, included at the beginning of this document, and its Recommendation that all such providers be licensed or registered and be regulated for AML/CFT purposes, will also serve as mitigating factors. Those changes go beyond the requirements of 5AMLD and its adoption by FATF members is likely to increase their ability to prevent the misuse of these assets and to better trace those using them for ML or TF.

While some of the above measures may make a significant difference, most of these regulatory measures have not yet taken effect. The level of ML/TF vulnerability related to virtual currencies is therefore considered to be **significant**.

Residual Risk

The findings of the EU SNRA, the urgency accorded to this sector by the FATF and the inclusion of measures to regulate the sector in the 5AMLD amendments all demonstrate the perception of a significant level of risk by authorities. This is reinforced by the findings of studies referred to in this report and accounts of law enforcement uncovering the use of virtual currencies in cases of both ML and TF. The nature of this technology, its decentralisation and cross-border use means that the initial risk is high in this jurisdiction as well.

The mitigating factors that Ireland benefits from are mostly to be introduced in the near future, in the extension of AML obligations included in 5AMLD and, as a FATF member, in the updated Recommendation 15. At present mitigating factors include the efforts of law enforcement to counter their use for ML and TF and the attendant publicity around such efforts.

While these measures are awaited, a mitigating factor existing now is the traceability of those transactions occurring on DLT-based systems. However, as outlined above, this takes dedication and resource while new techniques are being developed to make these transactions harder and harder to trace. Accordingly, while the strongest mitigating factors remain to be introduced in this jurisdiction, these assets are assessed as holding a residual risk of **medium-high,** for both ML and TF.

[25] https://www.coindesk.com/danish-police-claim-breakthrough-bitcoin-tracking/
[26] https://www.forbes.com/sites/janetwburns/2018/01/03/cut-off-from-big-fintech-white-supremacists-are-using-bitcoin-to-raise-funds/#9bde03733b36

Crowdfunding

Nature and Scale

Social media in the generally accepted sense, e.g. Facebook and Twitter, is primarily a means of communication rather than financing. The aspect of it which interests us here is the development of crowdfunding, where persons use social media to raise money, usually for a business venture or charitable cause, and usually in small amounts from multiple donors. Popular sites used for such include KickStarter, GoFundMe and IndieGoGo.

A good description is as follows:

Crowdfunding involves obtaining small amounts of individual funding from a large number of different sources through online platforms. These online platforms match lenders and investors with businesses or individuals seeking funding and arranges payments between them.

Crowdfunding falls into two general categories, non-financial and financial. Financial forms of crowdfunding involve the expectation of a financial return on behalf of the lender or investor. Non-financial crowdfunding is not considered to involve lending or investment type activity as there is no expectation of financial return[27].

As examples of scale, a 2018 US media report indicated that:

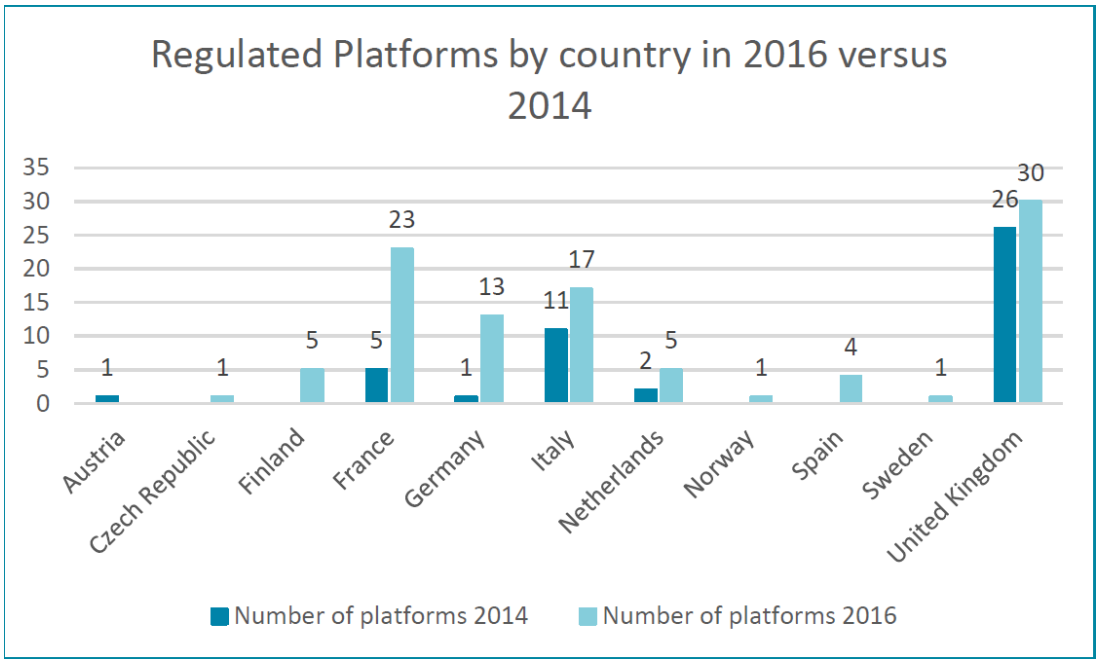
- Kickstarter has raised more than $3.6 billion for its users since it began in 2009 and Kickstarter projects that reached their funding totalled about $608 million in 2018 compared to $1.7 million in 2009. All these figures were provided by the company;
- Indiegogo has raised almost $1.5 billion for users since its 2008 debut. In 2017, Indiegogo's revenue rose 50% from 2016;
- By comparison, 'angel' investing in the USA totalled $6.65 billion in 2017, down from a peak of $8.55 billion in 2015 and up from $1.5 billion in 2008[28].

A study by the Irish Department of Finance in 2018 found that the crowdfunding market in Ireland is relatively small with only three crowdfunding platforms operating in the market, all of which provide peer-to-peer lending services, and no equity crowdfunding platforms operating in Ireland[29]. It found that crowdfunding constitutes approximately 0.33% - 0.4% of the SME finance market. As a comparison, this is 12% in the UK[30].

The average spend on, or investment through, crowdfunding in Ireland is $1 per capita; for comparison, this is $75 per capita in the UK. Linked Finance, which accounts for over 90% of the market share of peer-to-peer lending in Ireland, has more than 20,000 registered lenders and more than €75 million has been lent on this platform since its launch

[27] Dept. Finance Paper on the Regulation of Crowdfunding in Ireland , January 2018, p.4
[28] https://eu.usatoday.com/story/money/small-business/2018/04/30/crowdfunding-evolves-source-capital-test-market-startups/542978002/
[29] Linked Finance, GRID Finance and Flender
[30] Based on SME Credit Demand Survey & Linked Finance figures.

Chart 1: Regulated Platforms by country in 2016 as compared to 2014.



Source: ESMA

Chart 1 (above) indicates that the number of regulated platforms increased in the period 2014 – 2016 in a number of Member States.

Further figures from this study which can illustrate the scale of this sector are:

In 2013-2014, the European crowdfunding market successfully raised €2.3 billion[31].

Peer-to-peer consumer lending is the largest market segment of alternative finance, with €366m recorded for 2015 in Europe[32].

Between European member states, there are significant differences in terms of level of activity. The UK is the largest market for both loan and equity crowdfunding projects with €1.6 billion of funding raised through loan (peer-to-peer) crowdfunding projects and €89 million raised through equity crowdfunding projects in 2013-2014[33].

From the available information, one study has shown that the total European online alternative finance market grew by 41% to reach € 7671m in 2016. Excluding the United Kingdom, the industry grew 101% from € 1019m to € 2063m in 2016[34].

Risk Scenarios

The SNRA outlines the risks thus:

> *Crowdfunding platforms are set up under fictitious projects in order to allow collection of funds which are then withdrawn within the EU or transferred abroad. This could be*

[31] https://ec.europa.eu/info/system/files/crowdfunding-report-03052016_en.pdf
[32] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2016-european-alternative-finance-report-sustaining-momentum.pdf
[33] https://ec.europa.eu/info/system/files/crowdfunding-report-03052016_en.pdf
[34] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-ccaf-exp-horizons.pdf, p. 16

used either to collect funds from legitimate sources for the purpose of terrorist financing – or to collect illicit funds from criminal activities using anonymous products.

Social media misuses (the so called "crowdsourcing") are another kind of risk scenario. Terrorists groups in particular have made use of social media and other online and mobile platforms to obtain funds which are channelled afterwards through different means of payment. This type of crowdsourcing is not further analysed in this fiche. [35]

The SNRA goes on to clarify that the risks of TF and ML vary according to the nature of the specific product and type of crowdfunding and its interaction with other sectors, e.g. financial institutions, and their AML obligations or lack of same. It concluded that as it is not financially viable to raise or channel large amounts and as it may be insecure compared to other types of services, the TF threat related to crowdfunding is considered as moderately significant. For ML, the SNRA concluded that it requires some expertise to be profitable and there is little evidence that it has been used. In that context, the level of ML threat related to crowdfunding is considered as lowly - moderately significant.

It should be noted that the SNRA found that "…. competent authorities consider that controls and supervisory actions are weak in particular given the fact that many platforms are not established physically in the territory where they operate which hinders the efficiency of the controls."

Crowdfunding platforms can be used as a layering tool in money laundering, in advance of illegitimate funds being comingled with legitimate funds, prior to their withdrawal from the financial system. This could be achieved where illicit funds are invested in projects which may not successfully meet their fundraising target, with a view to the funds being returned to the investor. There could also be collusion between investors and crowdfunding platforms owners, or between the project owner and investors in order to launder money.

An example of this is where a criminal enterprise sets up a company to accept funding through a crowdfunding platform as payments for the sale of illegal items (e.g. drugs), disguised as a legitimate investment opportunity. Purchasers of such illegitimate items could then "invest" in this company through the crowdfunding platform.

Terrorist Financing has previously occurred through crowdfunding platforms where terrorist groups have solicited funds from unsuspecting backers by masking their campaign as legitimate charitable crowdfunding projects. While such activities can sometimes make it difficult to identity which humanitarian groups are legitimate and which have been created to finance terrorists, there have been more blatant examples of terrorist fundraising online, where websites or social media have been used to solicit funds from the public in order to overtly fund terrorism.

The potential for money laundering and terrorist financing is increased where there is limited or no due diligence undertaken on project owners or their projects. Although there is a lack of formal structured controls for CDD and other measures in the sector, which results in significant vulnerability, to date there has been little evidence of crowdfunding being used for TF in Ireland.

The Irish FIU has received STRs that show the use of crowd funding platforms to raise large amounts of funds. There is difficulty showing that the funds raised are being used for TF,

[35] EU SNRA Annex II, p. 54

however the submission of the STRs shows that designated bodies are monitoring the bank accounts of crowd funding platforms for potential TF.

The level of ML threat related to crowdfunding is considered as **moderately significant.**

The level of TF threat related to crowdfunding is considered as **significant.**

Established and potential mitigants

Crowdfunding is not currently a regulated activity in Ireland. Given this, there are no formal consumer protections available for those using crowdfunding platforms to provide funds. Consequently, the Central Bank of Ireland has issued an information notice alerting consumers to this fact, available at: https://www.centralbank.ie/consumer-hub/consumer-notices/consumernotice-on-crowdfunding-including-peer-to-peer-lending/

While some Member States have already applied their transpositions of the Payment Services Directive to cover crowdfunding, The European Commission in 2018 proposed a Directive to regulate crowdfunding.

The proposal is for a European label and for authorisation and regulation of crowdfunding service providers that operate on a cross-border basis in the EU. However, if a crowdfunding platform only operates in one member state it does not apply and authorisation is optional and not required. Ireland does not currently have a bespoke national crowdfunding regulatory regime.

In respect of AML the proposed new EU regulation states the following:

> *"….Article 9 requires that payments for crowdfunding transactions must take place via entities that are authorised under the Payment Service Directive (PSD) and, therefore, subject to the 4th Anti-Money Laundering Directive (AMLD), whether the payment is provided by the platform itself or by a third party. Article 9 also sets out that crowdfunding service providers must ensure that project owners accept funding of crowdfunding offers or any payment only via an entity authorised under the PSD. Article 10 introduces requirements for the 'good repute' of managers, which include the absence of any criminal record under anti-money laundering legislation. Article 13 requires National Competent Authorities (NCAs), including national competent authorities designated under the provisions of Directive (EU) 2015/849, to notify ESMA of any issue that is relevant under the AMLD and involving a crowdfunding platform. ESMA may subsequently withdraw the license based on this information. Article 38 provides that with a view to further ensuring financial stability by preventing risks of money laundering and terrorism financing, the Commission should assess the necessity and proportionality of subjecting crowdfunding service providers to obligations for compliance with the national provisions implementing Directive (EU) 2015/849 in respect of money laundering or terrorism financing and adding such crowdfunding service providers to the list of obliged entities for the purposes of Directive (EU) 2015/849."*

While such regulation will doubtless serve as a strong mitigating factor, it should be noted that the nature of crowdfunding as an open source tool also makes it that much easier to track both sources and destinations which criminals or terrorists may be attempting to obscure. As it stands, those crowdfunding efforts which overlap with the regulated financial system already encounter the AML/CFT requirements of obliged entities. Nonetheless, the lack of regulation of crowdfunding in Ireland at the moment means that:

The level of ML vulnerability related to crowdfunding is considered as **significant.**

The level of TF vulnerability related to crowdfunding is considered as **significant.**

Residual risk

As outlined above, the greater risk with crowdfunding comes from terrorist financing rather than money laundering. For the latter, it is far from the most attractive method. Added to this are the AML/CFT requirements of the regulated financial system where persons use this to contribute to crowdfunding. The EU's proposed Directive in this area will serve to further reduce this risk.

Accordingly, while strong mitigating factors remain to be introduced in this jurisdiction, it is assessed that the residual risk rating of crowdfunding is **medium-high**, for both ML and TF.

Electronic Money

Nature

The EU SNRA accessed the nature and Scale of the e-money money sector across the EU in 2017. The SNRA defined e-money according to the second E-Money Directive (EMD2, 2009/110/EC) as “electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer”[36].

An important characteristic of e-money is its pre-paid nature - an account, card, or a device needs to be credited with a monetary value in order for that value to constitute e-money. This can be stored on cards, money stored on mobile devices, and money stored in online accounts[37].

Prepaid cards (or pre-paid instruments) are a form of e-money which started developing at the end of the 1990s. These were seen as an alternative to debit cards (which require the existence of a payment account at a bank or a financial institution) and to credit cards (which require the card issuer to evaluate the cardholder's minimum level of creditworthiness)[38].

Prepaid cards can be categorised as “'closed-loop' prepaid cards, for purchases at a single merchant or among a limited network of merchants, and 'open-loop' / general purpose prepaid cards. General purpose prepaid cards are further divided into two sub-categories: reloadable cards and non-reloadable cards. Many cards need to be activated online to become operational”[39].

There is a clear increasing trend in the use of account based e-money products as compared to card based products. Growth can be expected in the area of digital wallets used for e-commerce payments as well as increased usage of NFC (Near Field Communication) technology allowing for contactless payments using mobile phones[40].

This assessment considers the overall assessment of the ML and TF risks posed by e-money sector in Ireland. It is acknowledged that there is a wide range of products in the electronic money sector and that certain e-money products will have higher and lower levels of ML and TF risks than the overall sector. 4 and 5 AMLD addressed this reality by providing the option of a specific derogation from CDD requirements for certain e-money products (Article 12 4/5AMLD). In the case of 5AMLD this followed an extensive examination of the

[36] European Commission 2017, Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, accessed 18 December 2018, https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF

[37] Ibid.

[38] European Commission 2016, Commission Staff Working Document Impact Assessment, Accompanying the document “Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC” ,https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A52016SC0223

[39] Ibid.

[40] European Commission 2017, Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, accessed 18 December 2018, https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF

options available to mitigate risk. Therefore for this category of products separate ratings of threat, vulnerability and residual risk are provided.

Scale

Available ECB statistics do not provide a full picture of the size of the e-money market, however they do provide some indications concerning the orders of magnitude related to the market size, as well as changes over time[41].

According to the ECB data analysed in the SNRA, over one year e-money payment transactions for the 22 Member States (that provided data) amounted to € 73 billion, corresponding to e-money payment transactions with e-money issued by EU resident payment service providers. This amount of € 73 billion includes € 57 billion in Luxembourg (which may be largely attributable to Pay-Pal and Amazon) and € 13 billion in Italy, which has a high usage of prepaid cards. As a comparison,the transaction value for debit and credit cards in the Union was €2,400 billion[42].

It should also be noted that the ECB datasets do not include several non-euro area markets and therefore underestimate the actual size of the EU market. The average transaction value on that basis was of € 35. E-money payments represented 3% of the total number of electronic payment transactions in the euro area (EU-18)[43].

The prepaid instrument market (i.e. excluding Paypal, Amazon, etc., but including UK figures) was estimated by the SNRA at € 19 billion, of which about €11 billion relates to anonymous prepaid cards[44].

Risk Scenarios

The SNRA identified two broad risk scenarios:

- Perpetrators use characteristics and features of some of new payment methods "directly" using truly anonymous products (i.e. without any customer identification) or “indirectly” by abusing non-anonymous products (i.e. circumvention of verification measures by using fake or stolen identities, or using straw men or nominees etc.)
- Perpetrators can load multiple cards under the anonymous prepaid card model. This multiple reloading could lead to substantial values which can then be carried out abroad with limited traceability[45].

The ESAs have provided guidance to E-money issuers on the range of factors that increase ML and TL risks. Products that allow high-value or unlimited-value payments, loading or

[41] Ibid.
[42] Ibid.
[43] European Commission 2017, Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, accessed 18 December 2018, https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF
[44] Ibid.
[45] Ibid.

redemption, or storage including cash withdrawal; which can be funded with cash, anonymous e-money, payments from unidentified third parties; or which allow person-to-person transfers, are designed specifically to be accepted as a means of payment by merchants, or can be used in cross-border transactions or in different jurisdictions; all contribute to that product having increased risk of being used for ML and TF[46].

The ESAs have also provided guidance on customer activities or characteristics which are indications of increased risk of ML or TF. Customers who purchase several e-money products from the same issuer, reloads the product or make several cash withdrawals in a short period of time and without an economic rationale; where a customer's transactions are always just below any value/transaction limits; when product appears to be used by several people whose identity is not known to the issuer (e.g. the product is used from several IP addresses at the same time); when there are frequent changes in the customer's identification data, such as home address or IP address, or linked bank accounts, are all such indicators[47].

Furthermore the ESAs have advised that where distributors (or agents acting as distributors) are obliged entities themselves, can increase the risk of ML or TF[48].

LEA Intelligence has found that prepaid cards are the most common forms of e-money to be used for criminal purposes[49]. Authorities (in the US and in Europe) have encountered misuse of prepaid cards in relation to "criminal activities (drug trafficking, human trafficking, prostitution etc.), illegal labour and tax evasion leveraging the anonymity offered by some of these cards"[50].

Prepaid cards are more traceable than cash in ex-post investigations, however they provide a number of investigative challenges. Prepaid cards are also less detectable physically than cash and where police or customs dogs are trained to detect bulks of bank notes, they cannot do so for plastic cards. Furthermore, for reloadable cards, where the money is not loaded on the card chip (i.e. in most cases), law enforcement authorities cannot know what amount of money is accessible via the card[51].

Intelligence suggests that the anonymity of prepaid cards is seen as an asset by criminals, all the more so as the acceptance of prepaid cards in the Union is relatively high and their spread is widening[52].

The SNRA found that e-money is attractive for criminal organisations and terrorist groups, especially when loaded onto prepaid cards, as it can easily allow money laundering and requires a low level of planning/expertise. The criminal intent to use e-money is quite high, while the capability of criminal organisations to use e-money is still higher for cash than for

[46] Joint Committee of the European Supervisory Authorities 2017, Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactionshttps://eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf

[47] Ibid.

[48] Ibid.

[49] European Commission 2016, Commission Staff Working Document Impact Assessment, Accompanying the document "Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC" https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A52016SC0223

[50] Ibid.

[51] Ibid.

[52] Ibid.

e-money. In light of this, the level of ML and TF threat related to e-money was considered as significant/very significant (level 3-4 on a scale of 4 as highest rating)[53].

In Ireland the first published examination of the ML/TF threat posed by e-Money in 2015 noted that there had been little indication from Irish law enforcement that e-money was being used for significant amounts of money laundering or terrorist financing, while acknowledging that the nature of such methods may make this hard to detect[54]. The Irish FIU has received a small number of STRs which make reference to e-money, however upon analysis none of these STRs have culminated in a ML or TF investigation.

There is significant correlation between the threat factors noted in the SNRA and those faced by Ireland. Therefore the level of ML and TF threat in relation to the e-money sector is considered as **significant.**

In the case of a product which complies with the provisions of the Section 33A of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended) the ML and TF threat is considered as **moderately significant.**

Established and potential mitigants

There are a range of mitigants which act together to reduce the threat of the ML and TF posed by e-money.

When the SNRA found that e-money had a moderately significant/ significant level (level 2/3) of vulnerability to ML and a significant/very significant vulnerability to TF (level 3-4 on a scale of 4 as highest rating), this assessment was based, in part, on the mitigants provided by the EU legal framework in place at that time[55]. This was the 3rd Anti Money Laundering Directive (3AMLD). 3AMLD allowed for e-money products to benefit from an exemption regime which allowed CDD not to be applied when specific conditions are fulfilled (EUR250 for non-reloadable e-money or EUR 2500 for reloadable e-money).

Since then 4AMLD and its subsequent amendment (known as 5AMLD), have both increased the mitigants provided by the EU legal framework against ML and TF.

Hence in Ireland exemptions from CDD measures now apply in more limited circumstances then were in place at the time of the SNRA assessment. Section 33A of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended) permits exemptions from CDD for certain forms of e-money/payment instruments that are:

[53] European Commission 2017, Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, accessed 18 December 2018, https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF

[54] The Department of Finance and the Department for Justice and Equality 2015, National Risk Assessment for Ireland Money Laundering and Terrorist Financinghttps://www.finance.gov.ie/wp-content/uploads/2017/05/NRA-FINAL-for-Publication.pdf

[55] European Commission 2017, Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, accessed 18 December 2018, https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF

- Non-reloadable
- Only usable within the state with a maximum monthly transaction limit of 250 euro
- Have a maximum storage value of 250 (500 euro if only usable in Ireland)
- exclusively used to purchase goods and services,
- unable to be funded with anonymous electronic money,
- subject to sufficient monitoring of the transactions or business relationship concerned to enable the detection of unusual or suspicious transactions, and transactions cannot be a redemption in cash or cash withdrawal of the monetary value of the electronic money of an amount exceeding €100.

These exemptions may not apply to customers resident in high-risk third countries or to customers who are politically exposed persons[56].

5AMLD will further limit the availability of anonymity when using e-money. Under 5AMLD anonymity will only be allowed for transactions up to €150 in person and up to €50 online.

Further, recent ESA guidance to firms stated that the exemption from CDD (under Article 12 of Directive (EU) 2015/849) does not extend to the obligation to conduct ongoing monitoring of transactions and the business relationship, nor does it exempt them from the obligation to identify and report suspicious transactions; this means that firms should ensure that they obtain sufficient information about their customers, or the types of customers their product will target, to be able to carry out meaningful ongoing monitoring of the business relationship[57].

The ESAs provided examples of the types of monitoring systems that firms should put in place to mitigate ML and TF risks[58]. These included transaction monitoring systems that detect anomalies or suspicious patterns of behaviour, including the unexpected use of the product in a way for which it was not designed; systems that identify discrepancies between submitted and detected information, for example, between submitted country of origin information and the electronically detected IP address; systems that compare data submitted with data held on other business relationships and that can identify patterns such as the same funding instrument or the same contact details; systems that identify whether the

[56] 33A. (1) Subject to section 33(1)(c) and (d) and subsection (2), a designated person is not required to apply the measures specified in subsection (2) or (2A) of section 33, or section 35, with respect to electronic money if—
(a) the payment instrument concerned—
(i) is not reloadable, or
(ii) cannot be used outside of the State and has a maximum monthly payment transactions limit not exceeding €250,
(b) the monetary value that may be stored electronically on the payment instrument concerned does not exceed— (i) €250, or
(ii) where the payment instrument cannot be used outside the State, €500,
(c) the payment instrument concerned is used exclusively to purchase goods and services,
(d) the payment instrument concerned cannot be funded with anonymous electronic money,
(e) the issuer of the payment instrument concerned carries out sufficient monitoring of the transactions or business relationship concerned to enable the detection of unusual or suspicious transactions, and
(f) the transaction concerned is not a redemption in cash or cash withdrawal of the monetary value of the electronic money of an amount exceeding €100.
(2) A designated person shall not apply the exemption provided for in subsection (1) if—
(a) the customer concerned is established, or resident in, a high-risk third country, or
(b) the designated person is required to apply measures, in relation to the customer or beneficial owner (if any) concerned, under section 37.".

[57] Joint Committee of the European Supervisory Authorities 2017, Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactionshttps://eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf

[58] Ibid.

product is used with merchants dealing in goods and services that are associated with a high risk of financial crime[59].

E-Money Institutions are designated persons under the Criminal Justice Act 2010 and the Central Bank monitors and supervises these entities for compliance with their AML/CFT obligations under the Act.

Given the mitigating measures in place, the vulnerability of the e-money sector to ML and TF is considered as **moderately significant.**

In the case of a product which complies with the provisions of the Section 33A of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended) the ML and TF threat is considered as **lowly significant.**

Residual risk

The SNRA methodology rated the level of residual risks by combination between the threat versus vulnerability. This risk level is based on a weighting of 40 % (threat)/ 60 % (vulnerability) – as it is assume that the vulnerability component should be given more weight when determining the risk level[60].

Using this methodology the residual money laundering risk of e-money was calculated as significant. The residual terrorist financing risk of e-money was calculated as very significant[61].

Since then the established legal controls have increased both across the EU and in Ireland which has have mitigated the risks identified in the SNRA. Furthermore the ESAs have published guidance to designated persons on both potential sources of ML/TF risks and means of mitigating those risks.

In 2015, the first Irish NRA concluded that e-money ML/TF risks are mitigated by the relatively low thresholds for exemption from CDD, the requirement to be licensed within the EU to issue e-money, and the necessity of creating a profile for the use of many larger online e-money services. These mitigating factors have been further strengthened by the entry into force of the Criminal Justice Act 2018.

It is therefore assessed that the residual risks of the e-money sector in Ireland are **medium-low**, for both ML and TF.

E-Money products which comply with the provisions of the Section 33A of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended) are determined to have a **low** residual risk of ML and TF.

[59] Ibid.
[60] European Commission 2017, Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, accessed 18 December 2018, https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF
[61] Ibid.

Conclusions

By the very nature of being ‘new technologies’, all of the sub-sectors assessed in this Risk Assessment are relatively recent adoptions whose nature and status are subject to a greater degree of change than more established sectors. In relation to crowdfunding and virtual currencies, which have been given risk ratings of medium-high, new regulations are being considered in order to mitigate the associated risks. For virtual currencies there has also been extensive work at an international level in order to develop satisfactory definitions of the terms involved and this work will also support further mitigation measures at the domestic level. It is expected that any new regulation and supervision introduced in these sectors will also have the benefit of providing greater quantitative information which will in turn be fed into revisions of the Risk Assessment of these activities.

With regard to Electronic money, this sector is more established, as reflected in existing regulation which has contributed to its lower residual risk than other sub-sectors.

Given the developing nature of many New Technologies, the residual risk ratings assigned in this assessment may well change when they are next reviewed, either due to changes in regulation or further developments of the technologies themselves. This assessment, however, must make its findings on the state of events at the time of writing. Even though new regulations may be put in place in the near future, the ratings arrived at here are based on the regulatory landscape as it is now.

An Roinn Airgeadais
Department of Finance

Tithe an Rialtas. Sráid Mhuirfean Uacht,
Baile Átha Cliath 2, D02 R583, Éire
Government Buildings, Upper Merrion Street,
Dublin 2, D02 R583, Ireland

T:+353 1 676 7571
@IRLDeptFinance
www.gov.ie/finance