Money Laundering and the FinTech Sector

Risks and Realities

White Paper

by the

FinTech Financial Crime Exchange

September 2017

FINTRAIL

RUSI
www.rusi.org

Abstract

The nature and extent of money laundering (ML) risk among the financial technology (FinTech) sector remains poorly understood. Attempts to describe the entire FinTech sector as posing uniformly "high" or "low" ML risks are often oversimplified and unhelpful. Rather, the FinTech sector is a diverse and complex one, where a true understanding of how ML risk manifests itself requires nuanced study.

This white paper aims to improve the understanding of factors that may influence ML risk exposure across the FinTech sector. It provides an initial, high-level view of some commonalities and divergences among the wide array of FinTechs that participate in the FinTech Financial Crime Exchange (FFE). Among its findings are:

- The self-identification of detailed ML typologies among FinTechs remains a significant challenge, owing to the often-limited view of financial activity FinTechs possess. FinTechs would benefit greatly from guidance and typologies studies from regulators and financial intelligence units (FIUs) that address risks related to specific product types and delivery methods in further detail.
- The nature of ML risk FinTechs encounter varies significantly based on the size of their customer base, geographical indicators, product features and operational factors, among others. In some cases, the ML risks will be genuinely low, in others higher. The level and nature of risk present, and the way typologies emerge, will differ greatly from company to company, and across market segments. Indeed, attempting to identify a single "FinTech typology" can prove unproductive.
- It is therefore important that FinTechs are not all stigmatised as "high risk" when there is no clear evidence that they pose higher ML risks than banks or other sectors. FinTechs and the public sector can play a role in clarifying this picture so that the FinTech sector is not broadly painted as "high risk" in instances where it is unwarranted. This is critical to avoid widespread "de-risking" of the sector.
- The non face-to-face nature of FinTech business means that fraud-related crimes predominate as the most commonly identified predicate offence to ML. Varieties of fraud encountered include stolen card fraud and identity theft, as well as more complex social engineering frauds.
- A limited range of other predicate offences and ML typologies were self-identified among FinTechs surveyed and warrant further study to determine their prevalence across certain product types and customer segments. These include elderly/vulnerable victim abuse, human trafficking/migrant smuggling, and drug-related crimes. However, this information is still anecdotal, and the FFE intends to undertake further study of these trends to understand their significance.
- Depending on their structure and product features, even UK-focused FinTechs can be vulnerable to "smurfing" or "money mule" activity that may be of low values in any single instance but can be frequent and widespread, and sometimes difficult to detect.
- Limits on product usage and the heavily UK/European Economic Area (EEA) customer base of most FinTechs surveyed in this report will tend to limit their utility for large-scale international ML; however, where FinTechs' products and services become more complex and extend in geographical reach, this may change.
- None of the FinTechs participating in this study has observed ML activity involving PEPs. Exposure to PEPs is low and the risk of laundering the proceeds of bribery and corruption is likely relatively small. The risks of laundering the proceeds of tax evasion are also perceived as relatively low.

Based on these observations, this white paper outlines recommendations for FinTechs, law enforcement, regulators and relevant international bodies. For example:

- FinTechs should undertake ongoing and robust assessments of their ML risk, and be willing to challenge commonly-held assumptions about the nature of that risk. They should look to harness their skill in leveraging data to build a more refined picture of ML typologies. By ensuring risks are identified, understood and controlled, FinTechs can help to change perceptions that the entire sector is uniformly "high risk."
- FIUs and law enforcement agencies should engage FinTechs in broader efforts to identify and develop more detailed ML typologies, and in advancing operational strategies for detecting and deterring ML.
- Regulatory bodies should aim to provide more detailed guidance on ML risks related to products and delivery methods with relevance to sub-components of the FinTech sector.
- International bodies such as the Financial Action Task Force (FATF) can play a role in fostering a detailed understanding of risks across the global FinTech sector, ensuring that FinTechs are included in global discussions about ML, and in developing consensus about appropriate responses.

About the FFE

The FFE was established in January 2017 as an intra-industry partnership. It was founded by the Centre for Financial Crime and Security Studies (CFCS) at the Royal United Services Institute (RUSI), a London-based defence and security think tank, and FINTRAIL, a UK financial crime risk management company. The FFE promotes an increased understanding of financial crime by the FinTech industry. It provides a collaborative forum for FinTechs to discuss financial crime typologies, risk management approaches and regulatory challenges. Its objective is to inform, debate and develop knowledge and best practices. Its members meet monthly to discuss these topics. As of September 2017, the FFE includes 30 participating members from the UK FinTech industry.

Enquiries about the FFE can be directed to the FFE Secretariat. For further information please contact Rebecca Marriott (rebecca.marriott@fintrail.co.uk) or Florence Keen (florencek@rusi.org).

About the Authors

David Carlisle is an Associate Fellow at CFCS, where he has written on topics including the regulation of cryptocurrencies. He is also an independent consultant whose work includes consulting with FINTRAIL to advise the FinTech sector on financial crime compliance issues. He previously worked with the US Department of the Treasury's Office of Terrorism and Financial Intelligence.

Florence Keen is a Research Analyst at CFCS, which she joined October 2015. Her work currently focuses on public/private responses to financial crime and terrorist finance, and she has researched the role of open-source and social media intelligence in tackling financial crime. She is also interested in the impact of illicit financial flows in the developing world, and drug trafficking.

Companies that are among the members of the FFE include:

bud.

Curve

Funding Circle

iwoca

LANDBAY®

lendable

liberis®

LOOT

marketinvoice

monzo

ozan

PAYBASE_

Pockit

Revolut

Rate%Setter®

satispay

stripe

TUNGSTEN NETWORK

Table of Contents

Introduction 1
Methodology 2
Money Laundering and the UK 3
Survey Results 6
Risk Perceptions, Risk Realities 16
Recommendations 18
Summary and Next Steps 19

Introduction

The extent to which the FinTech sector presents ML risks has been subject to much scrutiny in recent months. In many circles, FinTechs – as companies in the sector are known – are still somewhat of an unknown entity and thus perceived as "high risk." Governor of the Bank of England, Mark Carney, has spoken of the potential risks within the sector, not only in terms of financial stability, but of broader issues of ML, terrorism financing and data protection.[1] Whilst it is right to point out that there are elements and characteristics of the sector that carry ML risks, it is also important to acknowledge where the sector has proven itself to be extremely innovative in terms of detecting financial crime – as the FFE detailed in a white paper in May 2017.[2]

Indeed, many FinTech companies have demonstrated a deep awareness of their responsibility to prevent ML. As stated by the previous president of the Financial Action Task Force[3] (FATF), Juan Manuel Vega-Serrano, referring to the FATF's recent engagement with the sector, "there was a total understanding in the [FinTech] community about the dangers of money launderers. The industry understands that it's also in their interest [to combat illicit finance], and not just for societal reasons."[4]

However, despite high-level discussion, there is little concrete analysis available on the genuine ML risks the FinTech sector faces. Much of the discussion has simplified a complicated issue in what is an increasingly diverse sector, one that encompasses a broad array of products and services of all shapes and sizes, which naturally differ in the scope and nature of ML risk they encounter. In a sector that features pre-paid cards, current accounts, credit products, business banking products, P2P lenders, payment service providers, virtual currency platforms, service aggregators and a host of other niche products and services, the need for more detailed and clarifying analysis is critical but lacking.

This paper seeks to address this imbalance, based upon research conducted by the FFE. We have sought to provide some indications of where the key ML risks for the sector may lie, factoring in product type, size, geography and other indicators that impact the level and nature of risk present. In doing this, this report is designed to move away from the somewhat generic and arguably homogenous presentation of "FinTech risks" and provide a more nuanced picture – teasing out both the range of risks and typologies encountered, as well as noting where some commonalities exist.

On this basis, this paper will consider whether the ML risks are being truly assessed and understood, and what the implications are for the FinTech and public sectors. While this will primarily have a UK focus (due to the FFE's location and membership base), many of its conclusions have relevance more broadly.

The structure of this paper is as follows: it first provides background to the ML picture in the UK and its relevance for the FinTech sector. It then presents our research findings, offering an initial view of the ML risk landscape. Next it discusses some of the key considerations and implications of our results, such as if the risks have been fully assessed and understood, if any of commonly held assumptions are flawed, and what the broader consequences may be. This is followed by

[1] Jemima Kelly, "BoE's Carney sees systemic risk as fintech booms," *Reuters*, 25 January 2017.

[2] *Disrupting Financial Crime: Best Practices in Customer Due Diligence Among FinTechs* (FFE White Paper, May 2017), <https://www.fintrail.co.uk/news/2017/5/2/best-practice-in-customer-due-diligence-cdd-among-fintech-ffe-white-paper>.

[3] The FATF is the international standard-setter for money laundering, terrorist financing, proliferation finance and other financial crimes

[4] Samuel Rubenfeld, "FATF Wants to Use FinTech Against Money Laundering," *Dow Jones*, 20 June 2017.

recommendations for FinTechs and the public sector going forward. Finally, we draw some overarching conclusions, and consider where we may take this research in the future.

Methodology

The findings in this report are drawn from a survey conducted by the FFE Secretariat among its members, of which there were 20 participating FinTech companies when the survey was conducted. The respondents varied significantly in product type: half are either pre-paid card providers or P2P lenders, while other companies represented include a digital wallet provider, several money transfer services, a business-to-business (B2B) payment service, two dashboard service aggregators, a small business lender, a provider of mortgages and a crypto-currency exchange. The survey consisted of 20 questions, beginning with generic questions around participants' product type, services and customer size. We then sought to understand the respondents' experience in encountering ML risk at a more granular level by asking questions regarding:

- the frequency with which they observe possible ML activity;
- the ML typologies and related predicate offences they have identified; and
- the instances of ML activity they have encountered involving high-risk countries.

It is important to note some inherent challenges and limitations in this data collection and analysis.

Firstly, this is a relatively small sample drawn from voluntary participants based largely in the UK and with a wide array of service offerings, which makes firm conclusions difficult to draw. Secondly, due to the make-up of our survey, the findings will inherently be skewed towards certain product types that are over-represented within the group. To mitigate for this, we contextualise the results, acknowledging that what applies to one FinTech may not apply at all to another. Finally, the responses here point to ML risks that have been self-identified among survey participants, which naturally suggests some degree of observation bias, and implies that there may be risks present that have not been self-identified - a topic we address in this paper.

These caveats aside, we believe the results are an important step forward in contextualising the ML risk posed to such a diverse sector. It offers a starting point for further study as the FFE continues to facilitate discussion and information sharing among FinTechs.

Defining FinTech

The term "FinTech" is frequently used in a broad sense in public discussions, describing the increasing influence of technology in shaping finance, and the rapid adoption of technology by the financial sector. It is often used to refer to a wide range of activities, including: the use of new technology by major incumbent financial institutions; the provision of financial services by large, established technology and social media companies; and the establishment of new, start-up financial services firms that make technological innovation central to their product offerings and business models. This paper uses the term FinTech to refer to this last category – new financial services companies that specialise in the provision of products and services featuring online and mobile technology as a central component of their operations, and not as an incidental or merely adaptive feature.

Money Laundering and the UK

FinTechs have emerged as a prominent component of the UK financial sector just as tremendous scrutiny is being directed at the extent of ML activity occurring both globally, and locally in the UK.

Although precise figures are impossible to obtain, the IMF has estimated that the amount of money laundered worldwide equates to between 2% and 5% of global GDP annually,[5] or $800 billion and $2 trillion of funds that are illegally funnelled through the global financial system each year. The IMF describes ML as "the processing of assets generated by criminal activity to obscure the link between the funds and their illicit origins."[6]

London is frequently referred to as the "money laundering capital of the world,"[7] a feat which is difficult to prove – although it would be disingenuous not to acknowledge the vulnerabilities in the UK's financial system. Given the trillions of pounds of transactions made through the UK's financial institutions each year, it is one of the biggest financial sectors globally due to its perceived stability and widely used language. The UK's 2015 National Risk Assessment (NRA) of ML and terrorist financing noted that these characteristics make the UK particularly attractive to launder the proceeds of crime.[8] It is evident that substantial sums of money end up laundered through the UK, with the National Crime Agency (NCA) assessing that many hundreds of billions of pounds is laundered through UK banks, including their subsidiaries, every year.[9] Recent scandals such as the Panama Papers and the Russian and Azerbaijani Laundromats[10] indicate the scale of the problem – and these are likely to be just the tip of the iceberg.

Unsurprisingly, given their size relative to the rest of the UK financial sector, the UK's 2015 NRA identified banks as the country's greatest area of ML vulnerability when measured against 11 other financial products and services. The NRA notes that, "around 60% of current money laundering cases being investigated . . . have funds initially moved through banks, compared with 11% through [money service businesses]."[11]

However, the NRA noted areas of ML vulnerability among other components of the UK financial sector. Money service businesses and accountancy and legal service providers were noted as relatively high risk.[12] Estate agencies, which the NRA noted as posing moderate levels of ML risk, have come under significant public scrutiny in the two years since the NRA was published.[13] A 2016

[5] Michel Camdessus, "Money Laundering: The Importance of International Countermeasures", speech given at the IMF in Paris, 10 February 1998.

[6] International Monetary Fund, "The IMF and the Fight Against Money Laundering and the Financing of Terrorism," 31 May 2017, <https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/16/31/Fight-Against-Money-Laundering-the-Financing-of-Terrorism>, accessed 19 September 2017.

[7] Natasha Clark, "London is the 'money laundering centre of the world' says US businessman Bill Browder," *City AM*, 8 November 2016.

[8] HM Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (London: The Stationery Office, 2015).

[9] See National Crime Agency, "Money Laundering," <http://www.nationalcrimeagency.gov.uk/crime-threats/money-laundering>, accessed 19 September 2017.

[10] See, for example, Luke Harding, Caelainn Barr and Dina Nagapetyants, "UK at centre of secret $3bn Azerbaijani and global money laundering scheme," *The Guardian*, 4 September 2017.

[11] *UK National Risk Assessment of Money Laundering and Terrorist Financing*, p. 32.

[12] *Ibid*, p. 12

[13] See, for example, *Corruption On Your Doorstep: How Corrupt Capital is Used to Buy Property in the UK* (Transparency International UK, 2015).

UK government report noted that "recent high profile international corruption cases have demonstrated that criminal funds were used to obtain real estate in the UK."[14] While banks may pose the highest risk, other sectors also bear responsibility for ensuring that the UK financial sector is inhospitable for financial criminals.

As perceptions about ML risk have evolved, the UK has also emerged as a major hub – if not *the* global hub, as some would argue – for FinTech innovation and adoption internationally. One study from earlier this year suggested that the UK has one of the highest rates of FinTech adoption globally, with as much as 42% of the digitally active population using FinTech products or services.[15] A study commissioned by UK Trade & Investment notes "the UK has one of the highest levels of internet and mobile phone penetration globally, highest e-commerce spend in Europe and is a leader in online access to financial services."[16] That study also estimates that the UK FinTech sector is worth £20 billion in revenue annually.[17]

However, with opportunities also come risks. As the UK's Financial Conduct Authority (FCA) noted in its 2017/2018 business plan, "FinTech can sharpen competition and reduce overheads, potentially offering consumers better value for money and easier ways for firms and customers to engage with each other. But if not managed well, it can also introduce new risks into the financial system, or heighten existing ones."[18]

In this vein, law enforcement agencies have recently noted that the convergence of technology and finance may offer new opportunities for criminals while adding to the challenge of detecting ML activity. In its 2017 *National Strategic Assessment of Serious and Organised Crime*, the NCA noted that the expansion of FinTech "has seen new, highly accessible and technologically focused services provided to consumers. These exploit new technologies and are increasingly featured in crime with a wide array of offences being facilitated by these services."[19] Looking slightly further afield, in a study of organised crime activity across Europe, Europol noted earlier this year that new payment methods, "are significant obstacles in the identification of the beneficial owners of criminal proceeds."[20]

Where exactly does this leave the FinTech sector? What are the genuine ML risks? In the UK's 2015 NRA, five pages were devoted to the risks posed by new payments methods, including e-money products, pre-paid cards and digital currencies. The 2015 NRA assessed the overall level of risk posed by new payment methods as medium[21], suggesting a less significant vulnerability than banks and other high risk sectors noted above. However, the NRA also noted that with respect to new payment methods, "intelligence remains low-grade and needs to be further complemented."[22] With the second UK NRA due in the coming months, it is likely that a wider assessment of new payment

[14] Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance* (London: The Stationary Office, 2016), p. 28.
[15] EY, *EY FinTech Adoption Index 2017* (EYGM Limited, 2017), p. 8.
[16] *Ibid*, p. 3.
[17] EY (Commissioned by UK Trade and Investment), *Landscaping UK FinTech* (London: Ernst & Young LLP, 2014), p. 2.
[18] Financial Conduct Authority, *Business Plan 2017/18*, (London: FCA, 2017) p.42.
[19] National Crime Agency, *National Strategic Assessment of Serious and Organised Crime 2017* (London: The Stationery Office, 2017) p.24.
[20] Europol, *SOCTA 2017: EU Serious and Organised Crime Threat Assessment* (The Hague: European Police Office, 2017), p.19.
[21] HM Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing*, p. 12.
[22] *Ibid*, p. 82.

methods will be undertaken – perhaps with some clearer delineation between FinTech products, and a clearer picture of the risks.

With the UK also scheduled to undergo an evaluation by the FATF next year to assess the sufficiency of its national regime for combatting ML and terrorist financing, attention will almost certainly focus on how the UK is managing the ML risks posed by the new technology platforms transforming its financial sector. At the FATF itself, there appears to be a concerted effort to understand the FinTech sector, with regular meetings focusing specifically on the FinTech community. On the one hand, there is broad recognition that the engagement of the FinTech sector will be transformative in combatting ML, particularly should "RegTech" advancements prove fruitful in combatting ML risks – and yet on the other, there is still a sense that the ML risks posed by FinTech products have not been sufficiently addressed. What the FATF has yet to clarify is a more granular view of the risks the sector faces, and specific guidance on what it expects from the sector.

Perception is critical here. If the FinTech sector is viewed as broadly "high risk" for ML purposes without further context, this could have major ramifications, resulting in a loss of investment or banking access for the sector – a furtherance of the "de-risking" phenomenon that has seen whole sectors lose access to financial services in ways that are often crippling. A 2016 study conducted for the UK FCA described "start-ups in the FinTech sector with poorly understood business models" as particularly vulnerable to de-risking.[23]

To avoid this problem, FinTechs must take responsibility for identifying and managing the ML risks they face. The public sector must clearly articulate its view of those risks and its expectations for addressing them.

The purpose of this paper is therefore to provide greater clarification on what the ML risks for the sector might be, assess whether these risks are comprehensively understood, and offer considerations for further enquiry.

[23] David Artingstall, et al., *Drivers & Impacts of Derisking* (London: John Howell & Co. Ltd, 2016) p. 10.

Survey Results

I. ML Risk Landscape: A Varied Picture

Results from the FFE's survey suggest that there is an extremely wide range in the frequency, complexity and nature of ML risks encountered by different FinTechs.

When asked about their experiences in observing ML activity, several key factors influenced respondents' experiences and perception of those risks. These factors are outlined below.

Size of Customer Base

The size of FinTechs' customer bases can differ enormously. Respondents to this survey ranged from relatively new start-up companies with products still in testing phases and with as few as 150 active customers, to much larger businesses with upwards of several hundred thousand or nearly one million customers.

Unsurprisingly, there is noticeable correlation between the size of their customer base and the frequency with which they encounter suspected ML. Smaller-and medium-sized companies (e.g. those with 10,000 or fewer customers) indicated that they observe less than one instance of suspected ML activity per month to as many as 10 monthly, with an average of approximately 4 to 5 instances observed monthly. Larger companies (e.g. those with more than 10,000 customers) generally indicated that they observe approximately 10 – 20 instances of suspected ML per month.

However, there was not perfect correlation between the size of companies' customer bases and the frequency with which they observe suspected ML activity. Some points of variance exist. The highest number of instances of suspected ML activity observed monthly was noted as 200 by a company that was not the largest of the group, while one relatively smaller company noted that it sees several dozen cases monthly.

These numbers should be interpreted with caution. The frequency with which a company observes possible ML activity is not always a perfect measure of its relative success or failure in detecting financial crime activity; nor is it a clear measure of the level of genuine risk exposure. Other factors which may influence any given circumstance include:

- product type (about which more below);
- volumes of payments handled and the frequency of transactional activity;
- whether the company has recently come under concerted attack by criminal networks; and
- the maturity of ML systems and controls.

The point is this: FinTechs vary greatly in the size and scope of their services, which may be one indicator of the range and complexity of ML activity they are likely to encounter. Generally, there was some correlation between the size of FinTechs surveyed and the variety of ML typologies and range of associated predicate offences they had identified. Most smaller companies had never identified predicate offences other than first or third party fraud, while larger companies had in some instances self-identified typologies related to a dozen or more predicate offences they believe they have encountered. (A further detailed discussion of identified typologies and related predicate crimes is below in Section II).

One important consequence of this finding emerges for the sector: as they begin to scale and grow their customer bases, smaller and medium-sized FinTechs should be alert to the likelihood that their ML risks will grow in complexity and evolve concurrently.

FinTechs and PEPs

PEPs are regarded as a higher risk customers owing to their prominent public roles and access to public funds, which puts them at higher risk of engaging in bribery and corruption. While not all PEPs are involved in criminal activity, the 2015 UK NRA notes that corrupt PEPs have featured in international corruption cases and that related funds were likely processed through the UK banking sector (*UK National Risk Assessment of Money Laundering and Terrorist Financing*, p.36).

The general sentiment among FinTechs surveyed was that actual exposure to PEPs among FinTechs is relatively low. Where respondents do have PEP customers, they see these as legitimate customers warranting enhanced due diligence; however, none of the respondents has ever observed an instance of a PEP customer engaging in suspected ML activity. Many of the respondents have assessed that their product features are not attractive or conducive for laundering the proceeds of bribery and corruption at a large scale.

Geographic Factors

Another factor impacting the frequency, scope and complexity of self-identified ML risks among respondents relates to locational indicators.

Where respondents have encountered ML activity involving high-risk jurisdictions or other broad geographical risks, two primary factors appear to influence this.

- Firstly, whether the product is cross-border in nature, or is portable. Products that enable international payments and related services (such as money transfer services, foreign exchange products, or current accounts that feature the use of IBANs[24], etc.), or which may be carried during travel (such as card products), are more likely to be exposed to a range of geographical risks than are products and services which are more static and limited in range.

- Secondly, where customers are based. Nearly all respondents' customers are located overwhelmingly in the UK and EEA. Most of the participating companies will not offer their product to customers resident or, in the case of business customers, incorporated outside these jurisdictions. Several respondents, particularly lending products, service UK-resident customers only. This naturally limits their exposure to a broad range of geographical risks.

When asked if they have ever observed possible ML activity involving any of the 9 countries[25] that presently appear on the FATF's list of High-Risk and Non-Cooperative Jurisdictions, only one member had ever done so, that one instance involving Syria. Otherwise, none of the respondents

[24] IBANs are international bank account numbers, which allow customers to make or receive international payments.
[25] As of the time of this paper's publication, these where: Bosnia and Herzegovina, Democratic People's Republic of Korea (DPRK), Ethiopia, Iran, Iraq, Syria, Uganda, Vanuatu, and Yemen. See: http://www.fatf-gafi.org/countries/#high-risk

has observed ML activity involving the countries of greatest perceived systemic ML risk as indicated by the FATF.

The picture was more mixed when participants were asked if they have observed possible ML activity involving any of the countries that the UK government identified in its 2015 NRA as among the top 10 in terms of involvement with the laundering of UK criminal assets.[26] 8 of the 10 countries had featured in respondents' experiences of possible ML activity, with the number of respondents indicating as much noted in parentheses:

- Nigeria (4)
- Spain (3)
- Cyprus (3)
- UAE (2)
- Pakistan (2)
- Switzerland (2)
- British Virgin Islands (1)
- Hong Kong (1)

In addition to the above, other countries that respondents have seen associated with possible ML activity include India, Italy, Malta, Thailand, Latvia, Malaysia, Russia and Zimbabwe. It should be noted, however, that only 6 of 20 respondents indicated ever observing ML activity related to jurisdictions outside the UK. 14 respondents of 20 (70%) have never observed suspicious activity with any of the countries above. The bulk of ML activity observed by respondents focuses heavily on UK-based customers and transactions, as that is where their customers are overwhelmingly based and service offerings targeted. One respondent noted that because their product may only be serviced by payments to or from a UK bank account, any ML activity they are able to observe is exclusively UK-focused. This may suggest that direct exposure to large-scale international ML is not presently a major risk among UK FinTechs – though whether it suggests overall ML risk exposure could be characterised as "low" is another question explored further in Section II.

While products that are focused locally may face fewer obvious geographical risks, it would be unwise to assume that they are therefore immune to ML risk. As the NCA has noted, of more than 39,000 organised criminals based in the UK, 61% are UK nationals.[27] Additionally, one respondent noted that their company, which offers a UK-focused product, has repeatedly observed instances of possible ML activity involving certain nationalities, these being Danish, Dutch, Finnish, Hungarian, Romanian, Swedish and Zimbabwean nationals. This is not at all to suggest that suspicions should be immediately raised about customers from these countries; indeed, individuals from some of these countries are often the vulnerable *victims* of fraud. But the above factors suggest that products targeting only UK residents can face vulnerabilities as well.

Product Factors

As noted above, product features such as portability and cross-border transactions can have an impact on the varieties of ML risk that FinTechs encounter. Other key factors include:

[26] HM Treasury and Home Office*, UK National Risk Assessment of Money Laundering and Terrorist Financing*, p. 82

[27] National Crime Agency, *National Strategic Assessment of Serious and Organised Crime 2017*, p. 9.

- **Purpose.** The respondents to this survey provide a range of services to different market segments. This includes retail/consumer-focused products, business banking products, and B2B services. This has a noticeable impact on the nature of ML risk they encounter. For example, companies that offer both consumer and business services will naturally encounter a more diverse range of risks than those that offer only one or the other.
- **Transactional volume and velocity.** Another key factor influencing exposure to ML risks is whether limits have been placed around a product's use, and the nature of those limits. Most respondents' products feature relatively strict limits on the daily, monthly and annual levels of transactions which customers can access. The nature of these will impact the varieties of ML risk to which a product is exposed.
- **Functionality.** Other features may impact how ML risk manifests itself among FinTech products. For example:
  - **Card loading features.** Many of the respondents' products enable individuals to load with an external funding card. In some cases, respondents require that this must be a UK/EEA-issued debit or credit card. In others, there is an ability to load with a pre-paid card as well, which may present higher risks. Some respondents will not allow their customers to load with a pre-paid card for this reason.
  - **P2P payments.** In-app payments to other users can prove useful for criminal networks in "money mule"[28] schemes, and can allow linked individuals to move criminal proceeds internally across a single platform.
  - **Cash access.** Products that enable customers to fund their account with cash loading, and/or which permit customers to make ATM withdrawals, generally present higher ML risks than those that do not.
  - **Third party payments.** Whether the customer may obtain payments to or from third parties using facilities such as Faster Payments[29] raises the risk of exposure to high-risk third parties and enables transactions to be conducted swiftly.
  - **Ease of access to multiple devices.** Some FinTechs will only permit their customers to access their product using one mobile device. Others will permit customers to use multiple devices. Where multiple devices are used, this creates higher risks of impersonation fraud and other ML activity occurring, such as money muling.

Operational Factors

Another component that shapes how FinTechs experience ML risk is what might be referred to as operational factors – that is, their organisational structure and role in the broader financial and payments systems. FinTechs that responded to this survey have a wide range of operational structures. For example:

- **Directly licensed and supervised entities.** Some of the respondents to this survey are holders of electronic money issuer (EMI) licences or even banking licences. Such entities will have an obligation to file suspicious activity reports (SARs) directly to the FIU wherever they are regulated, as well as to adhere to other ML-related regulatory requirements, and cannot abdicate that responsibility where they use agents or distributors. Whether they are independently licenced and regulated will often also impact the range and nature of services these companies

[28] Money muling involves criminals using individuals – who are often unaware of the nature of the underlying criminal activity – to move illicit funds through their accounts.

[29] Faster Payments is an initiative of the UK banking sector to enable rapid domestic transfers.

can provide. These companies must go to significant lengths to demonstrate that they understand and are able to control the ML risks they face. Failure to do so can result in regulatory censure. Where they rely on the banking sector for certain services – such as currency clearing – these FinTechs risk losing access if their bank partners perceive their ML risks as uncontrolled.

- Agent/issuer relationships. Some respondents are not directly supervised entities but rather are products of another entity that holds an EMI licence, and are therefore agents of the regulated party, which acts as an issuer. As such, these agent entities will report their concerns about suspicious customer activity to their issuer, which then has ultimate responsibility for filing a SAR. This does not negate the requirement of the agent from having to escalate suspicions when it has them, but it does shift the emphasis of ultimate liability for failure to file a formal disclosure. FinTechs operating as agents will tend to offer a smaller range of products and services than will most fully-licenced entities. The UK government noted in the 2015 NRA that the segmentation of services that comes with agent/issuer relationships can add vulnerabilities and threats along the value chain.[30] While FinTechs that act as agents may not face the same legal liabilities as directly regulated entities, from an operational perspective their situation may be more fragile: if FinTech start-ups are viewed as unable to control their ML risks, the issuers they rely on may terminate those relationships. This underscores the need for even very small and new FinTechs to be thinking carefully about their ML risks from day one.
- Payment Service Providers (PSPs). Some FinTechs serve as PSPs that offer services related to funds transfers and sit between other entities in the payment chain. How they provide and deliver services will impact their ability to detect suspicious activity. Much of this will depend on the role of the company in a particular circumstance. However, as the UK Joint Money Laundering Steering Group (JMLSG) has noted, "As issuers of electronic money usually occupy the position of intermediaries in the payment process . . . they are often able to provide additional transaction information to law enforcement that compliments identity data provided by other financial institutions. This may be equally or more valuable evidence than a repetition of the verification of identity process."[31]
- Payee/payer. Most respondents provide a product that relies on PSPs or larger payment institutions to enable funds transfers. In such cases, their customers will be acting as a payee or payer at either end of a transaction that passes through numerous intermediaries. How these transactions are arranged will impact whether those companies at either end of the transaction chain can readily detect signs of ML activity.
- Service aggregators. One interesting development in the FinTech world is the emergence of service aggregators, companies that enable consumers to consolidate their financial apps from numerous providers onto a single visible and integrated platform. These firms will not own the relationship between the customer and any specific product or service, but rather enable the customer to have a holistic view of his or her financial activity across numerous accounts and products. Depending on the structure of their platform, the aggregator may not always be well positioned, or even able, to detect specific instances of illicit activity; however, they may be able to observe holistic patterns of activity across numerous products or services.

As some respondents noted, because of their organisational structure, FinTechs will usually feature in what is often described as the "layering" phase of ML activity. That is, rather than being the initial

[30] *UK National Risk Assessment of Money Laundering and Terrorist Financing*, p. 80.
[31] Joint Money Laundering Steering Group, *Prevention of Money Laundering/Combatting Terrorist Financing: Guidance for the UK Financial Sector Part II: Sectoral Guidance* (JMLSG: 2017), p. 38.

point of entry into the financial system, FinTechs will sit downstream in the payment chain. There are of course exceptions to this – for example, where cash loading facilities are allowed, or where the product or service itself is subject to theft or account takeover by fraudsters.

However, when it comes to laundering the proceeds of crime, certain structural factors can make the detection of ML activity, and associated indicators of underlying predicate offences and typologies, greatly challenging. This can be particularly true in the case of products such as P2P lending or prepaid card services with limited functionality. As one respondent noted, they find it "difficult to submit a SAR of real value" because often all they see is funds coming from or going to a customer's external bank account, and may lack useful data they feel they can provide about the broader context in which the activity is occurring.

II. ML Risk Landscape: Coming into Focus

Despite the divergences noted above, some common themes do exist across FinTechs when it comes to experiences of ML risk, even if not uniformly so.

Fraud is King

First of these is the overwhelming predominance of fraud-based crimes as the most commonly identified predicate offences to ML. Nearly all respondents indicated that they have observed first or third party fraud, and many respondents said that nearly every instance of suspected ML they observe – if not *every* instance – is fraud-related.

This emphasis on fraud is hardly surprising. FinTechs, like other financial institutions, can face direct and significant losses from fraud. They are naturally highly sensitive to fraud losses and view it as a tangible risk that requires urgent attention. Young start-up FinTech companies are particularly vulnerable and sensitive to fraud losses and will therefore place heavy emphasis on the deployment of fraud controls early in their development relative to the attention they may devote to ML controls.

What's more, fraud is more widespread than other crimes. As the NCA noted in its threat assessment earlier this year, "UK residents are more likely to be a victim of fraud than any other type of crime. The 2016 Annual Fraud Indicator, published by an academic/private sector partnership, estimated that annual UK fraud losses could be as much as GBP 193 billion. A significant proportion of this will require laundering within the UK or moving out of the UK."[32] As the most prevalent crime in the UK, it's only natural that fraud would predominate among FinTechs.

Additionally, as non face-to-face businesses that interact with customers and counterparties remotely and which enable relatively swift onboarding and access, FinTechs face obvious risks of impersonation fraud. FinTechs are taking critical and innovative steps to detect and deter fraud risks while also enabling a frictionless customer experience, as highlighted in the FFE's May 2017 white paper.[33] Several respondents to the current survey noted that they have seen discernible and marked reductions in both successful and attempted instances of fraud following the introduction of anti-fraud controls, such as sophisticated fraud detection systems. As one respondent noted, since the

[32] *National Strategic Assessment of Serious and Organised Crime 2017*, p. 22.
[33] *Disrupting Financial Crime: Best Practices in Customer Due Diligence Among FinTechs* (FFE White Paper, May 2017), <https://www.fintrail.co.uk/news/2017/5/2/best-practice-in-customer-due-diligence-cdd-among-fintech-ffe-white-paper>.

introduction of a new fraud detection system, they can "block [fraudsters] before they are fully active with a high level of accuracy."

Despite these successes, the nature of their remote access and ease of use can make FinTechs attractive targets for fraudsters. In its regular meetings, the FFE has observed that fraudsters sometimes deliberately target young FinTechs, looking to take advantage of companies with immature controls. This highlights the need for FinTech start-ups to think about ML risks and how to control them from the very early stages of company formation.

Participants encounter a wide variety of fraud typologies, from straightforward attempts by fraudsters to create accounts or obtain credit using false or stolen identities, to the use of stolen cards to fund or access an account. Several members noted instances of more sophisticated fraud typologies they have begun to encounter, such as complex social engineering frauds or instances of account takeover where 2-Factor Authentication was exploited.

In addition to impersonation frauds, two respondents have observed instances of advance fee fraud, or instances where customers are scammed into making payments to fraudsters.

Three respondents also noted instances of benefit fraud, while two reported observing instances of suspected VAT fraud.

Case Study: Social Engineering Fraud

One FFE member recently encountered cases of social engineering fraud. The fraudsters hacked various social media accounts and messaged the friends of the actual social media account holders with requests for money. The friends (victims in this case) were paying what they believed to be their friends, but were in fact fraudsters with accounts at the FinTech. The stolen funds were then spent using a prepaid card.

Other Offences

Another common theme emerged from the survey: respondents expressed that typologies and indicators of non-fraud predicate offences to ML can be extremely difficult to identify. Half of all respondents indicated that they have never filed SARs related to predicate offences other than standard first or third party fraud. Many suggested they can at best identify only generic behaviours and indicators of activities that raise ML red flags but which give little indication of what broader criminal activity may be occurring beneath.

8 of the 20 companies surveyed noted that they have observed instances of activity that bears the hallmarks of general money mule or "smurfing"[34] activity, but where they are unable to obtain any indication of what related criminal offences might be involved. For example, one respondent noted that it has observed frequent instances of customers engaging in debit card loading followed by rapid outbound Faster Payments, with no reasonable explanation for this activity.

[34] Smurfing involves engaging in small value transactions to evade detection and avoid triggering financial reporting requirements.

Again, this speaks to the potential utility of certain FinTech products as a method for layering criminal proceeds. While volumes and values of transactions may be relatively low, this activity may function as part of broader ML schemes, where what a FinTech observes may be only a piece of a much larger puzzle that also involves banks or other financial sector participants. As one respondent noted, they believe that owing to their product's "payment size thresholds our main risk is related to smurfing and money mule activities." While this underscores the challenge of identifying activity of concern, it also highlights the critical role FinTechs can play if they can submit SARs of intelligence value that assist law enforcement in connecting the financial dots. It also points to the importance of FinTechs receiving detailed typologies and risk indicators from the public sector so they can be better equipped to spot signs of ML.

It may be that the heavy incidence of fraud and money mule activity are directly related. Europol has noted its assessment that "more than 90% of money mule transactions are linked to cybercrime. The illegally obtained money often comes from phishing, malware attacks, on-line shopping/e-commerce fraud, payment card fraud (pcf), business e-mail compromise (bec) and on-line fraud, and others."[35]

Case Study: Money Mules

One FFE member observed a complex money mule typology. In that case, vulnerable individuals were used to open mule accounts via the company's app. These accounts were used to receive stolen funds from other victims of fraud campaigns. The stolen funds were then moved from the mule accounts onward to other members of the criminal network – for example, via electronic transfer, money service businesses or cash withdrawal at ATMs. Analysis of the customers' social media activity helped to identify other mule accounts associated with the criminal network.

In practice, identifying specific detailed typology indicators associated with money mule activity is challenging. However, when asked whether they have identified specific typologies related to a range of predicate offences, respondents offered answers which may hint at broader themes, albeit if drawn from a small sample size. Three that stand out are:

- Elder/vulnerable victim abuse. 6 of 20 respondents (30%) have identified instances of elderly or other vulnerable individuals being victimised. Others noted that while they have not seen specific instances of such abuse, they suspect it may be a risk for them owing to product features. For example, an exploiter could steal the identity information of an elder or vulnerable person to open an account or obtain credit products; or a family member may obtain access to or control over a vulnerable person's account and manipulate it. On the one hand, some FinTechs are well positioned to detect and report on instances of vulnerable customer abuse. Many FinTechs target their products at a relatively young customer base, so the mere fact that a new account has opened in the name of an older individual can be a red flag that might lead the FinTech to be alert to the risks of elder abuse. On the other, the general ability to engage in remote, non face-to-face business may be a factor that could make FinTechs attractive to individuals seeking to exploit the vulnerable, who are often used in money mule schemes. As one respondent noted, "family members are taking advantage of their less-tech savvy elder persons to install [the app]

[35] See, Europol, "Money Muling," <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-muling>, accessed 19 September 2017.

on their devices and set up SEPA[36] direct debit in order to access funds from grandparents' bank accounts." The FFE intends to make this an area of future research and study.

- **Drug trafficking.** 3 of 20 respondents have identified instances of suspected ML related to drug offences. Given the number of respondents who have witnessed instances of general money mule/smurfing activity, there is a significant likelihood that more than 3 respondents have in fact encountered drug-related ML, even if no clear indicators would have been present to alert them to as much. Money muling and smurfing are common techniques of organisations involved in drug offences, and insofar as FinTech products have features that put them at risk for those behaviours, they could be exposed.
- **Human Trafficking/Migrant Smuggling.** While only 2 of 20 respondents noted that they have observed instances of suspected ML related to human trafficking/migrant smuggling, other respondents suggested that while they have never with certainty encountered ML related to human trafficking/migrant smuggling, they believe it may be a risk they face. Several international organisations and law enforcement initiatives have published detailed typology studies of ML related to human trafficking and migrant smuggling.[37] These studies point to certain common features of human trafficking which may make some FinTech products useful to those criminal operations. For example, human trafficking organisations frequently need to make purchases for travel-related expenses, such as hotel payments at odd hours of the day, or frequent and unexplained purchases of transport services. Trafficked individuals have also been used to open accounts or obtain loans for organised crime groups.[38] FinTech products that are heavily geared toward a mobile, travel-heavy clientele may offer useful features in such typologies. As a subset of the risks around vulnerable persons, the FFE intends to study these potential risks in more detail.

In addition to the above, respondents noted general ML typologies related to several other predicate offences, though with only three or fewer respondents indicating they had observed each type. These included:

- theft, e.g. the laundering of the proceeds of the sale of stolen property (3)
- trade-based money laundering (2)
- proceeds from the sale of pirated content (1)
- illegal sale of prescription drugs (1)
- counterfeiting (1)

Notably, apart from a small number of possible VAT fraud issues, tax evasion was not identified as a meaningful risk. This is likely because the limits around many products make the laundering of large-scale tax evasion proceeds impractical. This may change where business rather than retail products are offered, but no significant instances were reported.

[36] SEPA refers to Singe Euro Payments Area, a European Union mechanism for enabling efficient cross-border euro transfers.

[37] See for example: Financial Transactions and Reports Analysis Centre of Canada, "Indicators: The laundering of proceeds from human trafficking for sexual exploitation," 15 December 2016, <http://www.fintrac.gc.ca/guidance-directives/overview-apercu/operation/oai-hts-eng.asp>, accessed 19 September 2017; FATF, *Money Laundering Risks Arising from Trafficking of Human Beings and Smuggling of Migrants* (Paris: FATF, 2011).

[38] HSBC, "Challenging the human traffickers," 18 July 2017, < http://www.hsbc.com/news-and-insight/insight-archive/2017/challenging-the-human-traffickers>, accessed 20 September 2017.

When asked to identify sectors and businesses they've encountered in instances of suspected ML activity, participants provided a wide range of responses. Examples of business types they have encountered, with the number of respondents noted in parenthesis, include:

- money service businesses (4)
- limited companies/limited liability partnerships (4)
- charities (4)
- dealers of precious metals and stones (4)
- dating services (3)
- virtual currency service providers (3)
- escort services (2)
- estate agents (2)
- casinos/betting shops (2)
- antiques or art dealers (2)
- online gaming (1)
- scrap metal wholesalers (1)

While there are certainly some typologies and businesses that feature among the experiences of several respondents, the above findings hardly point to a single consistent trend, and conclusions are difficult to draw. The above responses do not suggest that FinTechs are a magnet for illicit activity involving any particular business sector or economic activity. Further study will be required to understand how certain businesses or industries may feature in specific typologies encountered by FinTechs.

Risk Perceptions, Risk Realities

What to make of all the above findings? Several themes emerge.

For example, while there are some indicators of where ML risks lie, it remains incredibly difficult to generalise across the incredibly diverse FinTech world. The overall picture remains fragmented and contains many gaps. Outside of fraud-based activity, there are a few indicators that point to a conclusive picture or trends in typologies, apart from generic money mule activity and perhaps crimes related to vulnerable persons.

To a large degree, this is expected. FinTechs provide niche and limited financial services in such a manner that often they only see a very small snapshot of much broader financial activity. Whereas large banks may provide numerous products and services to their customers and may see a significant volumes and values of activity across customer accounts, allowing them to detect illicit patterns with relatively greater precision, FinTechs often only see a small series of activities that feature at one end of a much longer chain of events.

On the one hand, this is understandable and unavoidable. The nature of products and services – such as strict limits on spending – may indeed limit their utility for ML in many instances. On the other hand, certain product features could make them attractive for certain ends. While high-end ML activity via FinTechs may be difficult to achieve, certain FinTech products' features may provide additional avenues for money muling and smurfing. However, merely labelling the FinTech sector as uniformly "high risk" obscures this nuance as it manifests from company to company and product to product. A blanket approach to analysing the sector threatens to place unwarranted attention on risks that are minimal or do not exist, while also obscuring genuine risks that require more urgent attention and control in specific instances. What's more, it is critical to note that typologies identified in this report, such as money mule activity and the exploitation of vulnerable persons, are hardly unique to FinTechs but impact more traditional financial services firms as well.

The results of this study could also lead one to several potential conclusions that require further examination, and possibly challenge.

Among these is the conclusion one might draw that, because fraud predominates as the primary predicate offence observed, other crimes and typologies are of minimal importance. This conclusion faces two problems: (1) As suggested earlier, there is a likelihood that typologies related to non-fraud predicate offences are present even where they have not been self-identified (indeed, it is debatable whether they could be readily self-detected in many instances). In short, just because a ML typology hasn't been observed, doesn't mean it isn't there. (2) It may be that where fraud exists, other crimes lurk as well. Fraudsters can, for example, use stolen cards and stolen identities to commit other crimes, such as purchasing goods or services for use in human trafficking. After all, organised criminal networks that engage in fraud frequently perpetrate other crimes.

For example, in a study from earlier this year of organised crime across the EU, Europol highlighted that document fraud is used to facilitate a wide range of other illicit activities, such as drug trafficking and human trafficking/migrant smuggling. In the same study, Europol notes the case of an organised criminal gang that engaged in payment card fraud while also running a prostitution ring.[39] Europol also observes that, "Money launderers rely heavily on document fraud to facilitate their activities. Fraudulent documents . . . are used to conceal the origin of criminal cash, to open bank accounts or

[39] Europol, *SOCTA 2017: EU Serious and Organised Crime Threat Assessment*, p. 32.

to establish shell companies."[40] Thus, where a FinTech observes instances of fraudulent account opening using false ID documents or details, it would be prudent to ask whether other related ML activity might be at play among linked accounts or customers.

To this point, while detecting underlying offences is often impractical, more can almost certainly be done to identify indicators of specific ML typologies. As participants in a young sector, FinTechs are acquainting themselves with patterns of ML activity that incumbents have had years of experience encountering and observing. As awareness and understanding of typologies grows among FinTechs, it may be that more self-identified ML typologies emerge.

[40] *Ibid*, p. 18.

Recommendations

While challenging to decipher, the above exercise offers suggestions for stakeholders to take forward in building a more robust understanding of ML risk across the FinTech sector, and to enable a similarly robust response.

FinTechs. FinTechs should continue to work to understand the ML risks they face. Clarifying the true picture of ML risk, and ensuring risks are controlled, is essential if FinTechs wish to avoid the stigma that comes with being perceived as a "high-risk" monolith, and the debilitating consequences of de-risking that can follow.

The first key step in this for any FinTech company is undertaking a detailed and thorough risk assessment of its business. This requires challenging assumptions, testing vulnerabilities, and working in detail to understand the precise extent and nature of ML risks to which it could be exposed. FinTechs should leverage the skill they have in utilising data to decipher indicators of specific ML risks. In this endeavour, they should make use of available typologies studies related to certain offences to understand their potential exposure and assess whether any unknown risks do in fact exist. When conducting risk assessments, FinTechs should ask themselves:

- Has the risk assessment included a genuine attempt to understand all ML risk exposure?
- Have any assumptions to date been flawed?
- Will risks be manageable once companies scale up?
- What might be the unknown unknowns?

FIUs and Law Enforcement. FIUs and law enforcement agencies can benefit from an improved intelligence picture among FinTechs, while also helping to advance a more complete understanding of the risks faced across certain product types and delivery methods.

By engaging with the FinTech sector to discuss typologies, patterns of criminal activity and other related trends, FIUs and law enforcement can assist FinTechs in building a more complete understanding of risk indicators. Regular dialogue can clarify what information FinTechs require from the public sector in order to provide SARs of intelligence value.

Regulators. Regulatory bodies can facilitate the discussion as well, particularly by providing detailed guidance on product-specific risks and challenges. Of primary importance is ensuring that the FinTech sector is not viewed as a monolith – but rather as a sector with numerous diverse sub-components. This is not to suggest special treatment, but rather recognition that different sub-sectors of the FinTech world will face ML risks differently, and that operating from a set of broad assumptions may not always be helpful as they attempt to ensure they meet their regulatory obligations.

International Bodies. The FATF can advance an understanding of FinTech risks and solutions through further interaction with the sector globally. This can include providing fora for the sharing of typologies, facilitating discussion on what risks and requirements require emphasis and prioritisation, and clarifying definitions and terminology relevant to the FinTech sector.

Summary and Next Steps

FinTechs are working through the FFE to build a more complete understanding of ML risk. This will ensure that FinTechs take appropriate steps to address those risks, and that the public sector has an accurate perception of their true nature and severity.

The FFE plans to continue its study of ML typologies that carry potential consequences for FinTechs, particularly risks related to the exploitation of vulnerable persons. The FFE will continue its engagement with the public sector to foster dialogue on these topics.

Through further study and related outreach efforts, the FFE will continue building resiliency in the FinTech sector against ML activity.