Old Dogs New Tricks:

How existing money laundering typologies are impacting the emerging FinTech landscape.

November 2021

FINTECH FINCRIME EXCHANGE

FinTech FinCrime Exchange

ComplyAdvantage

In collaboration with ComplyAdvantage

FINTRAIL

Powered by FINTRAIL

Introduction

The way in which we interact with our banks has changed significantly over the past decade. Financial Technology firms (FinTechs) have enabled greater flexibility, not only in our choice of banking provider, but also in terms of how we access and control our money. Where once it was necessary to visit a bank branch during office hours to deposit a cheque, we can now upload a picture directly from our smartphones at any time of day; or, we can instruct international payments from our couch; make a virtual asset trade whilst taking a walk; or even apply for a loan on the bus.

Whilst banking has changed to better suit the needs of the law-abiding general public, so too have the opportunities for those that wish to abuse and exploit the financial system. Advancements that have been designed to increase ease of use and expediency have in turn been targeted by criminals for exactly these design characteristics.

Money laundering is not a risk unique to FinTechs. However, some characteristics of the FinTech sector may carry higher financial crime risks without proper controls in place.

This paper will explore how existing money laundering typologies might impact the developing FinTech landscape. In support of this paper, an anonymised survey was conducted amongst a number of FinTech financial crime experts from around the world to understand how they perceive the current and future threats facing the financial industry.

Current Money Laundering Environment

The environment in which money launderers now operate is hostile. Launderers could previously deposit suitcases full of cash over the counter into a bank account with minimal fear of exposure. Today, technological advancements have given anti-financial crime (AFC) professionals ever increasing abilities to detect, trace, and disrupt criminal entities like never before.

However, crime still pays and criminals still need to launder their money, regardless of the risks. To combat this, criminals have constantly evolved and adapted their methods to meet the challenges put forward by the ever-changing AFC landscape.

Cash-Based Money Laundering

There has been a surge in digital-banking adoption across all parts of society in recent years. However, the Bank of England's most recent quarterly bulletin on cash usage, *Cash in the time of Covid*[1], notes that whilst cash transactions dropped throughout the pandemic, the value of cash in circulation actually increased. This shows that, despite widespread adoption of digital banking solutions, cash remains a prominent part of our economy.

Cash poses unique challenges for FinTechs. One such challenge is how customers deposit cash into their accounts without a physical branch network. For years, the Money Service Business (MSB) sector has used third party cash deposit locations - such as bureaus based in small convenience stores, or Post Office locations - to accept and process cash on their behalf. The FinTech model has utilised the same network of third parties to process their cash transactions.

Cash is still king for the majority of criminal enterprises. As such, entry points for ill-gotten cash, such as the Post Office, represent a significant vulnerability for FinTechs who will look to exploit these third-party cash deposit locations.

Minutes for the most recent meeting of the UK's Economic Crime Strategic Board[2] (a government taskforce mandated to tackling economic crime in the UK) detailed specific actions aimed at addressing the cash-based money laundering (CBML) vulnerabilities, not just for bank branches, but also over the counter deposits at the Post Office locations. This suggests that whilst there may be controls in place, criminals are still finding ways to circumvent them, including through the use of coercion, complicity, or even intimidation.

The most recent UK National Risk Assessment[3] identified cash deposits via third parties as a major threat, citing the inability of third party organisations to access account details of where funds are being deposited, allowing greater anonymity and less scrutiny.

[1] Cash in the time of Covid

[2] Economic Crime Strategic Board 17 February 2021 agenda and minutes

[3] National risk assessment of money laundering and terrorist financing 2020

Control Spotlight: Cash Deposit Limits

A growing number of FinTechs do not offer cash deposit facilities and therefore will not be exposed to CBML directly. Nevertheless, those that provide products such as; business accounts, current accounts, travel cards, or money remittance services still operate within the cash economy and their customers will typically require cash deposit services.

In order for CBML to succeed, criminals must first successfully place typically large volumes of cash into a financial institution, before onward laundering the funds. Therefore, limiting the amount of cash a customer is able to deposit at any given time can help to deter criminals from exploiting a platform for CBML purposes.

Cash deposit limits in isolation may protect one institution. However, this approach is likely to push the criminal to another institution. As such, in addition to controls such as cash deposit limits, it is important that timely and accurate suspicious activity reporting is completed to successfully disrupt the criminal, rather than divert them to another institution.

From the survey...

From the firms that accepted cash, 50% of our survey respondents believed CBML to be a growing threat to their business. Interestingly, the other 50% held the contrary opinion that it was in fact not a growing threat. This polarised view could be the result of a number of different factors, including (but not limited to):

- Internal control effectiveness against CBML may vary between firms. For those with higher efficacy, the perceived impact of CBML may be skewed.
- Controls across different cash deposit locations may vary. Some cash deposit providers may employ stronger controls which in turn may deter criminal exploitation.
- FinTech may not offer transactional accounts, which would likely render them less attractive to money launderers operating in cash.

Money Mules

The term 'money mule' refers to an individual that moves illicit funds (either wittingly or unwittingly) on behalf of a criminal or organised criminal group (OCG). The overall aim of money muling is not only the placement of illicit funds into the financial system, but also to create distance between the criminals and their ill-gotten gains, before being reunited with their money, once they have been commingled with legitimate funds.

Money muling networks are often made up of large numbers of individuals, spread across one or more jurisdictions, that have access to basic transactional banking facilities (such as current accounts). Frequently, criminals target young people (such as students or the unemployed) who might not understand that the activity they are taking part in is illegal. Others might employ professional money mules to act on their behalf. A recent example of this is the reported increase in Chinese Underground Banking (CUB)[4], whereby professional money mules work alongside Chinese OCGs operating in the UK and abroad (often involved in narcotics and human trafficking) to launder their cash proceeds. This in turn facilitates shadow banking services for the Chinese and

[4] Chinese Underground Banking and 'Daigou'

South East Asian diaspora in the UK. This risk is not unique to the UK. In October 2021, a group of Chinese nationals based in Australia were accused of laundering at least AUD62 million through dormant bank accounts belonging to around 250 students who had returned to China after studying in Australia[5]. Similarly, in October 2021, a Singaporean woman admitted to laundering almost SDG700,000 through bank accounts belonging to her and her daughter[6].

Whilst these risks are not necessarily unique to FinTechs, the almost universal adoption of non face-to-face onboarding methods and the speed in which accounts can be opened makes FinTechs an attractive target for criminals. As a result, these criminals can treat their accounts as disposable utilities, enabling them to shut down any account they feel is compromised and move on to the next one with limited disruption to their laundering operation.

Control Spotlight: Customer Due Diligence and Ongoing Due Diligence

CDD ultimately refers to the process of taking steps to identify your customers and checking they are who they say they are. CDD should provide a picture of what is considered 'normal' behaviour for the customer, so that a firm can identify abnormal activity.

CDD consists of two core elements:

1. **Identification and Verification (ID&V):** the process of understanding who your customer is, including details such as their legal name, residential address, and date of birth (if they are a natural person), or - if dealing with a legal entity - their registered name, country of incorporation, date of incorporation, and company number.
2. **Know Your Customer (KYC):** KYC seeks to understand a little more about the customer and their background, including (but not limited to): their nature of business; their source of funds (and potentially their source of wealth); their geographical area of operations; beneficial ownership; delivery channel; and the expected use of any particular product or service requested by the customer.

From the survey…

92% of respondents believed that money mules are a growing problem. 60% of respondents noted that their business had been affected by money mules in some way, including having to put in place new policies and procedures to combat the problem, operational costs, either in time or money, to prevent mules using their platform or reputational damage following reports their platform had allowed money mules to operate on it.

[5] Three face court after police smash multimillion-dollar money laundering ring

[6] Woman admits to receiving more than $1m in ill-gotten gains in her bank accounts

Smurfing

Smurfing is the process of structuring a large sum of illicit money into smaller deposits and bill payments, with the ultimate aim of evading detection by law enforcement or in-house financial crime teams.

Criminals and OCGs will utilise money muling networks to 'smurf' sums of money on their behalf; the theory being that if a network of mules is large enough, the individual payments required by each mule can be small enough to slip under the radar of most detection scenarios or reporting thresholds.

FinTechs that offer transactional account facilities (such as current accounts) could be exposed to smurfing through a number of different vectors, including (but not limited to):

- Initial placement of cash into the account, typically via a third party cash deposit location
- Outbound structured transactions of illicit funds, i.e. onward laundering of proceeds of crime
- Accepting inbound funds derived from criminal activity from a third party
- Facilitating cash-out of funds; either through the purchase of goods and services, payment towards a credit card, or cash withdrawal via automated teller machines (ATM).

Control Spotlight: Transaction Monitoring

Transaction Monitoring (TM) refers to the practice of analysing a customer's transaction data in order to identify activity or behaviour indicative of crime. Firms are required to conduct ongoing monitoring of the business relationship with their customers, including the scrutiny of transactions undertaken throughout the course of the relationship.

By creating a strong TM framework, FinTechs can greatly increase their capacity to detect suspicious activity on their platform which in turn reduces the risks they and their customers face. TM systems can be rule-based, behavior-based, or more modern with the use of artificial intelligence and machine learning technologies.

An effective TM system should be specifically tailored to your business. It will be built around rules that take into account your customer base and their relationship to the product or services you provide.

A properly designed and implemented system will help identify potentially suspicious transactions by analysing patterns of payments. There are typically three categories of TM rules:

1. Value: the overall value of funds transferred over a specific time period
2. Volume: the overall number of transactions in a given time period amount of
3. Velocity: rules designed to identify rapid movement of funds, typically over a shorter period of time than the volume focussed rules.

Criminals will use any means possible to launder funds but by knowing the financial landscape that your company and your customers operate in, you will be able to build effective controls with which to identify suspicious activity and protect your business.

The primary purpose of smurfing is to circumvent detection mechanisms. However, this doesn't mean it is undetectable. By understanding the way in which criminals can exploit financial products to facilitate this type of activity, TM can be appropriately tuned and balanced to identify and alert against potential instances of money laundering.

From the survey...
77% of respondents believed that smurfing is a growing problem within the industry, and 31% found smurfing had increased on their platform over the past year.

However, when asked whether they feel confident in their businesses ability to identify and mitigate attempts at smurfing (with potential answers limited to: Yes - Completely; Yes - for the most part; or, No) 77% of respondents replied with Yes - for the most part, suggesting some a degree of uncertainty in their existing control framework.

Money Mule and Smurfing Example
I have £100,000 of illicit cash I need to move quickly. To help, I have a network of 50 individuals who are willing to act as mules. Each mule is given £2,000 in cash and told to keep 15% as commision. This means that each mule only has to move £1,700 to meet their quota. The mules are instructed to break that £1,700 into 4 separate transfers of £425 (smurfing), which will be sent to accounts owned and operated by the money launderer. Even if a further 10 - 15% of these transactions are frozen, lost, or intercepted, this means the launderer still receives £72,250 - £76,500 of illicit cash.

However, if the launderer chose to deposit and transfer the cash themself, the likelihood of detection would be significantly higher. The deposit location may request evidence proving the legitimacy of the funds - which of course doesn't exist - or a SAR could be raised alerting law enforcement authorities of the launderer's illicit activities, ultimately resulting in the complete loss of their £100,000.

Cross-border Payments

Cross-border payments are financial transactions where the payer and the recipient are based in separate countries. Millions of these transactions are made every day enabling individuals and businesses to operate anywhere in the world. Whilst there is no definitive figure for the amounts transferred on a daily basis, the value of cross border payments in 2017 was estimated to be $150 trillion and is expected to rise to $250 trillion by 2027[7].

Traditional methods of remitting funds abroad centred on either legacy banks using correspondent banking arrangements or MSBs. In recent years, the rise of technologically driven solutions has seen FinTechs take on the historic hegemony in this sector. A number of FinTechs now offer simple, rapid, and low cost ways to transfer funds abroad that have made them attractive alternatives to the traditional banks.

Threats such as the use of complex offshore structures to evade tax, organised crime groups using shell companies

[7] Bank of England 'Cross Border Payments' Overview, 15th June 2021

to launder funds and terrorist groups remitting funds to conflict zones in order to buy materiel, all require the means to move money quickly across international jurisdictions. Any FinTech company operating within this realm needs to be aware that they will be targeted by bad actors looking to abuse their platform.

The threat is not only from criminals. Fulfilling legal and regulatory obligations can be extremely difficult when operating in the multi-jurisdictional world of cross-border payments. Completing KYC on prospective clients whilst navigating local laws or researching adverse media written in a foreign language are all pitfalls that businesses need to be aware of and make provisions to mitigate.

Control Spotlight: Holistic Approach

In the previous sections we highlighted specific controls that could be applied to help mitigate different types of financial crime risk. However, the reality is that in order to successfully mitigate financial crime - be that cross-border payments, money muling, smurfing, CBML, or any other typology not discussed in this paper - a holistic approach to the control environment is required. A holistic control environment should include (but is not necessarily limited to): a robust CDD programme, suitably tuned TM systems, appropriate reporting mechanisms, and customer specific considerations (e.g. cash deposit limits).

From the survey...

The risk associated with cross-border payments was recognised by 100% of our survey respondents, International money laundering was also considered a clear threat, with almost 40% stating that their platform had seen an increase in attempts to transfer illicit funds from foreign jurisdictions. However, almost 70% of the survey respondents believe their business has, for the most part, adequate controls in place to mitigate the threat.

Emerging Financial Crime Risks

Criminals constantly adapt and evolve in order to stay one step ahead of the mechanisms designed to disrupt their illicit activities. As such, it is important to be aware of emerging risks that have not yet fully crystallised, but are likely to in the near future.

This section explores two high profile emerging money laundering risks to be aware of.

Deepfake Technology.

What does a viral video of Tom Cruise, Netflix's The Irishman, and a $35 million fraud all have in common? They were all executed through the use of deepfake technology. Deepfakes are, in essence, a digital mask that can be overlaid on someone's face so they look and sound almost unrecognizable from the person they are purporting to be.

Whilst this may seem like something derived from a SciFi film, the risk is, in fact, very real. Earlier this year, the FBI issued a statement noting their confidence that deepfake technology will be utilised by malicious actors in the near future[8]. In October 2021, it was reported that, by using a combination of a deepfaked voice and spoofed emails, criminals stole $35 million from a large UAE based bank[9]. In 2019, a similar case was reported in the UK whereby a fraudster was successful in deepfaking the voice of a company's CEO resulting in a scam worth €220,000[10].

Money muling to launder funds is dependent on having a network of natural persons that either receive and move money on behalf of a criminal, or hand over control of their account to the professional money launderer. However, what if the money launderer could open up hundreds of accounts without needing to recruit and manage a network of mules? All they would need to do is overlay someone's face on theirs, and use information obtained from a data leak to open accounts. Without the need to recruit numerous individuals to act on their behalf, the workload is significantly reduced. The risk for the criminal is also reduced as there is no chance that one of the mules will talk to law enforcement, as they don't exist in real life.

Ransomware

Ransomware is malicious software designed to block access to computer systems until a sum of money is paid. There has been a notable increase in ransomware attacks over the last year, with one expert estimating[11] that between 800 to 1,500 US based companies were impacted by ransomware in 2021. It was also reported that 98% of ransomware attacks request pay-out in the form of bitcoin[12]. In October 2021, the US Treasury[13] linked $5.2 billion in outgoing bitcoin transactions as potentially tied to ransomware payments since 2011.

Ransomware attacks aren't the only type of crime that utilises cryptocurrency as a cash-out mechanism.

[8] FBI Private Industry Notification, Synthetic Identities

[9] Bank Robbers Used Deepfake Voice for $35 Million Heist | AI-Enhanced Voice Simulation Used

[10] A Voice Deepfake Was Used To Scam A CEO Out Of $243,000

[11] Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says

[12] Ransomware: Paying Cyber Extortion Demands in Cryptocurrency

[13] US Treasury said it tied $5.2 billion in BTC transactions to ransomware payments

However, cryptocurrency as a means of monetising ransomware is a high profile typology that appears to be increasing. As such, FinTechs that offer native conversion services enabling users to exchange cryptocurrency for fiat currency may be particularly exposed to the subsequent movement and cash-out of funds derived from ransomware attacks.

From the survey...

15% of our survey respondents noted that one or more of their customers had fallen victim to a ransomware attack in the past year, with almost 70% stating that they did not think their business had the controls in place to identify and mitigate attempts at laundering funds using cryptocurrency.

FINTECH
FINCRIME
EXCHANGE

The FFE brings together a global network of FinTechs to collaborate on best practices in financial crime risk management. By sharing information on criminal typologies and controls, members help to strengthen the sector's ability to detect and counter the global threat of financial crime. The FFE was established in January 2017 by FINTRAIL and the Royal United Services Institute (RUSI), and its members meet regularly to discuss these topics and share information and insight on an ongoing basis. The global scope of financial crime and the shared threats faced by all major FinTech hubs particularly underscore the need for a global FFE network, which will give its members not only a trusted place to exchange information, but also access to an increasingly far-reaching network of resources and perspectives. Discover more at www.fintrail.com/ffe

Comply
Advantage

ComplyAdvantage is the financial industry's leading source of AI-driven financial crime risk data and detection technology. ComplyAdvantage's mission is to neutralize the risk of money laundering, terrorist financing, corruption, and other financial crime. More than 700 enterprises in 69 countries rely on ComplyAdvantage to understand the risk of who they're doing business with through the world's only global, real-time database of people and companies. The company actively identifies tens of thousands of risk events from millions of structured and unstructured data points every single day.

ComplyAdvantage has four global hubs located in New York, London, Singapore and Cluj-Napoca and is backed by Goldman Sachs, Ontario Teachers', Index Ventures and Balderton Capital. Learn more at https://complyadvantage.com/ or follow us on Twitter or LinkedIn.

FINTRAIL

At FINTRAIL we are passionate about combating financial crime. We are unique in that our team of experts are drawn from the industries we support and have deep hands-on experience in developing and deploying risk management controls from leadership roles with leading FinTechs, RegTechs and banks including Monzo, Stripe, Standard Chartered Bank, World First, Satispay, HSBC, Wells Fargo and Deutsche Bank. This experience grounds us, ensuring we offer our clients pragmatic solutions to the most complex challenges. The work we do in support of the global FinTech and financial service industry is intrinsic to our DNA but we are increasingly partnering with clients to apply that expertise and knowledge to wider regulated and non-regulated sectors. Our goal is to ensure our clients can thrive, free from the negative impacts of financial crime. Our approach is tailored to the unique circumstances of each client, is data and technology driven, and is focused on providing excellent customer outcomes. Discover more at www.fintrail.com

Thank you

www.fintrail.com/ffe

FINTECH FINCRIME EXCHANGE

FinTech FinCrime Exchange

Comply Advantage

In collaboration with ComplyAdvantage

FINTRAIL

Powered by FINTRAIL