Improved understanding of emerging technologies will facilitate more effective audit and supervision of the financial crime risks posed by Fintechs: A UK and US perspective

By Danielle Herndon

About the Author

As Head of Compliance and MLRO at Paybase, Danielle Herndon is responsible for enforcing the highest level of risk, regulatory and financial crime compliance standards throughout all aspects of the business. She works directly with partners, offering training and education on reducing financial crime, and has a pivotal role in the development of the Paybase Platform.

Apart from being a certified Anti-Money Laundering Specialist (CAMS), Danielle has great experience in bringing together compliance and tech - an ever-important skill for today's world and the future of payments. Before joining Paybase, she helped another Fintech develop their compliance framework and launch the business. Prior to this she worked in HSBC's Financial Crime Compliance team where she specialised in reviewing payments products for financial crime risk and high-risk commercial deals. She has vast international experience, having worked for global payments firms and FinTech start-ups in the USA, Europe and the UK.

Table of Contents

1. Executive Summary

It is well documented that the UK and the US are hubs for Fintech. Equally, there has been a recent focus on how these sophisticated economies have been exploited to launder illicitly gained funds.[1],[2] Fintechs' use of technology at their core has created new product types that are neither accounted for in regulation nor in standard supervisory and audit approaches. While clearly a source of new financial crime risk, this new technology can bring significant opportunities for the economies in which they are located. When creating a new supervisory and regulatory framework for Fintechs it is important to understand these new risks as well as the industry's potential.

Having this improved perspective and awareness will allow supervisors and auditors to more accurately review the riskiest segments of the industry, increasing efficiency overall. A balanced and informed approach will lead to a change in the supervisory process, which could reduce financial crime risk in the Fintech industry while also allowing the industry to flourish. This should not take the form of an update of specific points in a static auditory framework, but rather be the development of a framework than can be as dynamic as the industry it seeks to reflect. As consumers continue to demand faster and smarter financial tools,[3] the financial crime risk evolves, too. In order to ensure effective financial crime mitigation, it is essential that supervisors, auditors, and the financial intelligence unit (FIU) be given the resources to evolve with it.

Scope of This Paper

Fintech is a global phenomenon, and each jurisdiction is approaching its supervision of the industry differently. In this paper, the focus first will be on the relatively mature regulatory environments of the US and the UK. The focus will then turn to how supervisors, auditors, and the FIU can more effectively interact with these firms. This exploration will look at the areas of success as well as the improvements required to build a more effective assessment process of financial crime risks within Fintechs.

Specifically, this paper will delve into how an understanding of the technology and the products both used and offered by Fintechs creates new financial crime risks and new financial crime mitigation controls. The paper will explore this with a concrete focus on three areas of new risk: so-called cyptocurrencies, due diligence automation, and artificial intelligence coupled with machine learning. These are rapidly evolving areas

[1] Nationalcrimeagency.gov.uk. (2019). *National Crime Agency - Money laundering*. Retrieved from: https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-terrorist-financing?view=category&id=10 (accessed 1 February 2019).

[2] Fatf-gafi.org. (2019). Retrieved from: http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016-Executive-Summary.pdf

[3] Home.treasury.gov. (2019). Retrieved from: https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf

and the risk they pose is open to misinterpretation by regulators and lawmakers. This could ultimately hinder the growth of the Fintech industry.

2. What Is Fintech?

As a starting point, it is important to understand what is meant by the term "Fintech". A number of definitions are available which differ in focus, but for this paper a definition presented by EY is used as an initial guide: "In its broadest sense, we define Fintechs as high-growth organisations combining innovative business models and technology to enable, enhance and disrupt" financial services.[4]

It is also important to look at how the regulators in the UK and the US are looking to define Fintech in order to understand their perspectives on supervising and auditing these firms.

US Treasury

A US Treasury report reviewing "Non-bank Financial Institutions, Fintech and Innovation" recently defined Fintech simply as "financial technology"; however, the report does highlight the effect the industry has had and references the 3,000 new firms offering a financial services technology solution. The distinction between Non-Bank Financial Institution and Fintech is an important one, as not all non-bank financial institutions embrace technology in a way that makes them a Fintech. There are understandably a number of similarities in the operational and regulatory challenges faced by these firms.

UK Treasury

In the UK, HM Treasury has defined Fintech as a term used "to describe both technology driven innovation across financial services and to pick out a specific group of firms that combine innovative business models with technology to enable, enhance, and disrupt the financial services sector. Fintech delivers tangible benefits for customers of financial services right across the country, including lower prices, more choice, and better service."

The common theme across all definitions is that a Fintech must offer financial services through the use of technology and, when contrasted with traditional financial service organisations, is innovative in its approach. Therefore, the term "Fintech" in this paper shall refer to tech-focused and innovative financial service institutions.

[4] Fintechauscensus.ey.com. (2019). *Defining fintech.* Retrieved from: https://Fintechauscensus.ey.com/2016/Home/Defining-fintech (accessed 15 January 2019).

3. Current Challenges Faced by Fintech

3.1. Regulatory Landscape

The UK and the US governments have both recently performed studies into the various challenges faced by Fintechs as well as the opportunities they bring.[5,6] These reports highlight that one of the key issues faced by Fintechs is the regulatory environment. Fintechs must navigate a highly complex system not always conducive to innovation. This hinders growth and creates a disconnect, which opens the door to financial crime. This regulatory burden ultimately affects the consumer, who would benefit from the innovative and intelligent solutions available as they come to market.

There have been a number of examples in which the regulatory environment created complexities that disproportionately affected smaller financial institutions and emerging-types of financial institutions. This makes it challenging for firms to be compliant and for supervisors to ensure that regulatory and risk standards are met. A few examples of these challenges are outlined below:

- In the UK, different standards of due diligence need to be applied based on a customer's risk under the current Fourth Money Laundering Directive (4MLD). This can vary based on the type of financial institution, customer risk, and the firm's approach to risk, with some exemptions to due diligence. Prudent firms appropriately apply the risk-based approach in terms of simplified due diligence as it applies to their business, but the lack of an upper threshold can present enhanced financial crime risk. It may be better to standardise a baseline requirement, such as the Bank Secrecy Act (BSA) mandates in the US, or even introduce a threshold for reporting, as under the Third Money Laundering Directive.
- The new Fifth Money Laundering Directive (5MLD) definition of virtual currency is "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically."[7] This would appear to include all types of loyalty-point schemes. Curiously, it does not include initial coin

[5] Assets.publishing.service.gov.uk. (2019). Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692874/Fintech_Sector_Strategy_print.pdf

[6] Home.treasury.gov. (2019). Retrieved from: https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf

[7] Eur-lex.europa.eu. (2018). Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843 (accessed 1 February 2019).

offerings.[8] These discrepancies may present financial crime risks to consumers and could be a way to launder funds. It is expected that the UK will look to extend or amend the scope of the legislation to include initial coin offerings (ICOs), firms that cannot unilaterally exercise control over a customer's crypto assets (Non-Custodian), and software providers facilitating purchases on exchanges.[9]

- There is also an issue with the way regulatory changes have been introduced. The Second Payment Services Directive (PSD2), for example, is a highly complex piece of legislation that is being introduced and enforced in stages. It means that some firms reporting obligations are more stringent, and new firms are brought into the scope of the regulation. There is arguably too much guidance on the topic to the point of confusing the intended audience. What seems to be missing is using the opportunity to communicate the change in scope to the new types of firms impacted by the change. Fintechs servicing these firms are often using this as a competitive tool, but it really is ultimately not their responsibility to communicate these changes.[10] Many of the firms that are handling funds in a now non-compliant way are doing so naively, not out of malicious intent, because they are unaware of the changes in legislation.[11]

To say the regulatory environment is entirely inadequate, however, would be misleading. A number of progressive initiatives are being presented by UK and US regulatory bodies. In the US, the OCC proposal of a nationwide Fintech license for firms, while still in development, is a welcome opportunity for firms to grow without the significant burden and resources required to be individually licensed in each state. This approach would allow innovation to thrive in a controlled way; however, some states oppose it, such as New York.[12] The UK is also making a number of moves in a positive direction. Recently, the FCA released a number of "Dear CEO" letters to provide guidance in uncertain regulatory environments as well as the recognition of some emerging methods of CDD and controls for products like virtual currencies. This signals a number of forward-looking changes to the regulatory framework.

---

[8] Eversheds-sutherland.com. (2018). *Cracking the code A global guide to Initial Coin Offerings*. Retrieved from: https://www.eversheds-sutherland.com/documents/services/financial/ico-global-paper.pdf

[9] FCA. (2019). *CP19/3: Guidance on Cryptoassets*. Retrieved from: https://www.fca.org.uk/publications/consultation-papers/cp19-3-guidance-cryptoassets (accessed 3 February 2019).

[10] Cocoman, M., & Schreiber, D. (n.d.). *How PSD2 impacts marketplaces and platforms*. Stripe.com. Retrieved from: https://stripe.com/files/connect/guide/Connect-EU-guide.pdf (accessed 23 January 2019).

[11] Clifford Chance. (2017). *Clifford Chance | Impact of PSD2 on online marketplaces operating in Europe*. Retrieved from: https://www.cliffordchance.com/briefings/2017/11/impact_of_psd2_ononlinemarketplacesoperatin.html (accessed 1 February 2019).

[12] Reuters.com. (2018). *U.S. bank regulator allows fintech firms to seek federal charter*. Retrieved from: https://www.reuters.com/article/us-usa-treasury-fintech/u-s-bank-regulator-allows-fintech-firms-to-seek-federal-charter-idUSKBN1KL26N (accessed 2 February 2019).

3.2. Wider Financial Industry Acceptance

Fintechs are required to work with other financial institutions in order to provide their products. This could be, for example, an acquirer to accept card payments, a bank to protect client funds, or a payments firm to facilitate bank account withdrawals. This need to interact with other firms requires appropriate understanding of the risks associated with Fintech across the financial industry. Each of these institutions is required to perform due diligence on a prospective correspondent financial institution or customer. This could include an audit. Ensuring that the risks presented are accurately assessed on a case-by-case basis is critical, or it could lead to incorrectly declining an application. Declining a customer without appropriately applying the risk-based approach could amount to de-risking by the financial institution. Wholesale de-risking and the subsequent negative effects for the entire industry has been well documented in both the US and the UK.[13,14] A 2016 FCA report highlighted that Fintech was one of the most significantly impacted industries. US regulators have suggested that de-risking could even amount to a "public safety issue" because the exclusion of banking services to money service businesses (MSB) makes the enforcement of the BSA all the more challenging.[15]

It is difficult to determine whether wholesale de-risking is a conscious decision by these firms, given that each institution is entitled to its own risk-based approach. It should be appreciated, though, that any instances of de-risking have an adverse impact on the innovation and opportunities that Fintech can offer consumers. To combat the anti-competitive impact of de-risking, PSD2 has introduced a requirement for banks to notify their local regulators of every decision to decline an application for banking services. The bank is obliged to explain why and demonstrate that each case has been individually assessed on its merits.

3.3. FIU Reporting

In the UK, the process to file a SAR includes logging into an online portal, completing the mandatory fields, and then submitting the report. In the US this is an option, but firms can also submit SARs as a batch. This type of standardised reporting is beneficial for the regulator but lacks the flexibility for all types of firms to submit fully informative reports. Prior to submitting a SAR, the firm has usually performed an internal investigation to identify all customers connected to the suspicious or unusual activity. Condensing this information into the fields of a rigid form may save time for the FIU but makes it difficult to effectively extrapolate the financial crime risks, which constantly change. The information provided may not accurately reflect the depth of

---

13 Artingstall, D., Dove, N., Howell, J., & Levi, M. (2016). *Drivers & Impacts of Derisking.* FCA.org.uk. Retrieved from: https://www.fca.org.uk/publication/research/drivers-impacts-of-derisking.pdf
https://www.state.gov/e/eb/tfs/tfc/derisking/index.htm (accessed 28 January 2019).

14 State.gov. (n.d.). *De-risking*. Retrieved from: https://2009-2017.state.gov/e/eb/tfs/tfc/derisking/index.htm (accessed 21 January 2019).

15 Csbs.org. (2018). *Examining De-Risking and Its Effect on Access to Financial Services*. Retrieved from: https://www.csbs.org/examining-de-risking-and-its-effect-access-financial-services (accessed 1 February 2019).

the investigation done by the firm to safeguard itself against crime. The recent Financial Action Task Force (FATF) Mutual Evaluation of the UK assessed the technical compliance of the FIU as needing "significant improvements", with some of these issues being raised more than a decade ago by FATF.[16] The report raised the issue of technical systems being inadequate, further exacerbated by the lack of resources to review the SARs. It raises the concern that this was a UK policy decision to limit resourcing while systems were not adequate.[17]

Improving SAR data management, such as better data analytics, would allow for efficiencies to be achieved without significantly increasing the number of analysts required at the FIU. Some suggestions proposed during consultations on improvements to the UK SAR regime include real-time data reporting on customer details, centralised collection of transactions, and comprehensive analytics solutions to analyse and highlight financial crime risks on submitted transactions.[18] Improving the SAR reporting to allow for API submissions would allow Fintechs to submit their detailed internal SAR reviews in a seamless manner. The timeline for an effectiveness review of the changes not being scheduled until 2023 is also a significant problem in reducing the risks as outlined in the FATF report.[19] Technology is quickly evolving, and it would be wrong to say that what is agreed today as a cutting-edge and sophisticated solution will still be so in five years.

Another way to improve the UK FIU reporting is to introduce a de minimis reporting threshold. In the US, money services businesses (MSBs), which hold the same status as many Fintechs in the UK, are subject to a $2,000 reporting threshold.[20] This means that firms can dedicate more time and resources to investigations and submit even higher-quality SARs, while the FIU can focus its analysis on the riskiest cases. Although not a perfect solution, this would lead to a reduction in the sheer volume of reports and allow the FIU to prioritise highest-risk cases. There is no benefit to consumers, the public, or to firms in submitting huge quantities of information unless it will be reviewed.

---

16 FATF (2018), *Anti-money laundering and counter-terrorist financing measures – United Kingdom* Fourth Round Mutual Evaluation Report, FATF, Paris. http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf

17 FATF (2018), *Anti-money laundering and counter-terrorist financing measures – United Kingdom* Fourth Round Mutual Evaluation Report, FATF, Paris. http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf

18 S3-eu-west-2.amazonaws.com. (2018). *Anti-Money Laundering: the SARs Regime Consultation Paper*. Retrieved from: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/07/Anti-Money-Laundering-the-SARs-Regime-Consultation-paper.pdf (accessed 5 February 2019).

19 Lawsociety.org.uk. (2019). *UK performs well in its 2018 FATF assessment.* The Law Society. Retrieved from: https://www.lawsociety.org.uk/support-services/risk-compliance/anti-money-laundering/uk-performs-well-2018-fatf-assessment/ (accessed 2 February 2019).

20 Fincen.gov. (n.d.). *Money Services Business (MSB) Suspicious Activity Reporting.* FinCEN.gov. Retrieved from: https://www.fincen.gov/money-services-business-msb-suspicious-activity-reporting (accessed 25 January 2019).

4. Emerging Technology Trends—Fintech

Fintech spans a number of industries and types of technology. This paper will explore some current technology trends embraced by Fintechs that will have the most significant impact on the financial industry in the next few years. It is essential that the audit and supervisory framework reflects these advances. Crypto[21] is a particularly hot topic at the moment, with a number of Fintechs looking to support this type of product by providing fiat payments for the purchase or sale of Crypto, or even Crypto exchanges becoming regulated Fintechs. Although Crypto may be seen as driving risk, there have also been significant efforts dedicated to introducing controls to mitigate the associated financial crime risks. In particular, firms have been proactive in embracing strong customer verification and controls to mitigate the risk created by the lack of an in-person customer relationship. Fintechs more generally have been dedicating significant resources to create secure platforms that protect their customers and mitigate financial crime risk. In particular, the focus has been on incorporating artificial intelligence (AI) and machine learning into transaction- and customer-monitoring engines and risk assessments.

4.1. Crypto: What Is It and What Are the Risks?

In the UK, the phrase “crypto-asset” has begun to be used by the Bank of England. The justification is that virtual currencies are not like traditional currencies, in that they cannot be spent on the high street.[22] However, more broadly, the term “Crypto” refers to any type of virtual currency, crypto currency, or digital coin. These are often volatile investments that could drop in value to zero, creating significant conduct risk for consumers.[23] The regulatory status of each of the different types of firm supporting Crypto transactions still varies significantly depending on the specific functionality these offer. In the US, the CFTC, FinCEN, and the SEC have all released guidance as to what falls within their regulatory remit. Fintechs supporting any aspect of a Crypto firm’s business must have a clear understanding of when regulatory authorisation is required. Supervisors and auditors must also have this understanding to correctly remedy any firm supporting non-compliant Crypto activity that requires appropriate remediation. The following table defines a number of commonly used terms that should be considered when reviewing any Crypto firm.

[21] Defined to include virtual currencies, crypto currencies, crypto assets, and digital coins.

[22] Bankofengland.co.uk. (n.d.). *What are cryptoassets (cryptocurrencies)?* Retrieved from: https://www.bankofengland.co.uk/KnowledgeBank/what-are-cryptocurrencies (accessed 2 February 2019).

[23] Starks, M. (2018). *Blockchain: considering the risks to consumers and competition*. FCA. Retrieved from: https://www.fca.org.uk/news/speeches/blockchain-considering-risks-consumers-and-competition (accessed 2 February 2019).

- **Crypto Exchange:** In the 5MLD, the definition includes *"providers of exchange services between virtual currencies and fiat currencies."* Currently, Exchanges supporting exchange activity between virtual currencies are not captured by this legislation.
- **Custodian:** In the 5MLD, Custodians are defined as *"entities that provide services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies."* Quite often these firms are also Exchanges.
- **ICO:** According to Deloitte, this is *"a company, usually in early development stage,* [that] *provides a 'token' or 'coin' denominated in a cryptocurrency to investors in exchange for their capital investment. The business models of firms using ICOs are diverse and so is the basis on which the tokens are valued. Tokens may constitute a share in the company, a voucher for investors to benefit from the firm's project or product in the future or may not give any right or value at all.*"
- **Third Party Software Provider:** A firm that offers a user interface allowing customers to purchase Crypto from one or more Crypto Exchanges. These firms do not offer Crypto Exchange services themselves but are merely an interface for customers to access these services. They may or may not be a Custodian.

In order to understand the risks, it is important to understand the different types of firms that may support Crypto. Each of the types of firms outlined above will require a different compliance framework and cannot be bundled together in a one-size-fits-all approach.

Financial Crime Risk

Aside from the consumer conduct risk perspective, Crypto firms also present enhanced financial crime risk. The generally unregulated nature of Crypto firms means that a range of due diligence and risk management standards is being applied across the industry. The most reputable Crypto firms apply due diligence and monitoring standards in line with what is expected of regulated financial institutions. Some, such as Coinbase, have even been authorised themselves as an electronic money institution in the UK.[24] However, the ability to move a Crypto from a less strict Exchange or jurisdiction to one that is more reputable still remains a significant threat. While Exchanges are not yet regulated in the UK, they are subject to some US regulation. Firms should have regular legal reviews to ensure that they are only supporting Crypto firms that hold the appropriate regulatory authorisations and be prepared to cease operations with non-compliant firms.[25] Another recent impact on

[24]Register.fca.org.uk. (n.d.). *Financial Conduct Authority—CB Payments Ltd*. Retrieved from: https://register.fca.org.uk/ShPo_FirmDetailsPage?id=001b000003O1uMmAAJ (accessed 2 February 2019).

[25]Post, J., Hafter, M., & Smith, K. (n.d.). *Virtual currencies in the USA.* Lexology. Retrieved from: https://www.lexology.com/library/detail.aspx?g=71b4767c-3b6a-4f33-a2ba-0eda39aa1414 [Accessed 2 February 2019].

financial crime risk is the inclusion of two Bitcoin addresses in the OFAC list. Sanctions screening tools do not typically screen for Crypto addresses and this represents an emerging threat.[26] Privacy coins present another significant threat. Their activity is not visible on the public blockchain and could be attractive for financial crime, as it lends to anonymous transactions.

The anonymous or pseudo-anonymous nature of Crypto has been highlighted in notorious cases such as Liberty Reserve and Silk Road.[27] Europol just this year identified instances of Isis trying to crowdfund through Crypto.[28] Equally, however, it should be noted that in 2017, the UK national risk assessment highlighted the risk of money laundering in the UK by digital currencies as low.[29] Until regulation enforces standards on Crypto firms, it is largely up to the financial institutions that support fiat payments for these Crypto businesses to detect and prevent financial crime on their behalf.

Tax evasion and the responsibilities that financial institutions have in its prevention is another significant issue for Fintechs supporting Crypto more generally. The portability of Crypto means that it could be used as a vehicle to move funds undetected across borders. Fintechs working with these Crypto firms should ensure that this is appropriately factored into their risk assessment and prevention of tax evasion policies and controls.

4.1.1. What to Consider When Auditing Crypto Firms

As a general rule, the auditing and supervising of a Fintech supporting Crypto should be very similar to auditing any other type of financial institution. The supervisor or auditor should have an understanding of the expected controls, applicable regulations, and high-risk factors associated with the business type. With this understanding, supervisors and auditors will be able to set out their assessment framework and ask the appropriate questions. In return, firms supporting Crypto should have risk assessments prepared, documented controls in place, and policies and procedures to support the management of this element of their business.

A starting point for the supervisor or auditor is to identify the type of firm and Crypto activity being supported. Is this an Exchange, ICO, Custodian, or other Third-Party

---

[26] Home.treasury.gov. (2018). *Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses.* U.S. Department of the Treasury. Retrieved from: https://home.treasury.gov/news/press-releases/sm556 (accessed 2 February 2019).

[27] Fatf-gafi.org. (2014). *FATF Report: Virtual Currencies Key Definitions and Potential AML/CFT Risks*. Retrieved from: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (accessed 2 February 2019).

[28] Europol. (2018). *European Union Terrorism Situation and Trend Report 2018 (TESAT 2018)*. Retrieved from: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018 (accessed 2 February 2019).

[29] Assets.publishing.service.gov.uk. (2017). *National risk assessment of money laundering and terrorist financing 2017*. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf (accessed 2 February 2019).

Software Provider wishing to support Crypto? It is important to start here as the risks and expected controls will vary based on the type of business. It is also important that the customer risk assessment evaluate the specific product, not just the industry itself. Fintechs often have very streamlined resources, and it is imperative that risks are assessed according to their business models. In addition to the standard aspects of a risk assessment, it should be expected that firms draw out a few additional points—the types of Crypto supported, source of Crypto, supported jurisdictions and the regulatory landscape in each of these, the reputation of Exchange, and IT controls of the Custodian, among others. The main associated risks are explored in more detail below.

Privacy Coins

Some Crypto presents additional challenges given that the blockchain activity is private, such as Monero, ZCash, and Dash. The private nature of the blockchain makes it nearly impossible to monitor previous activity in relation to that Crypto, increasing the uncertainty and ultimately the risk. More and more, these coins are being used for sanctions evasion among other types of financial crime.[30] It should be expected that Fintechs have introduced controls to mitigate this enhanced risk. Some firms, in an effort to mitigate financial crime risk, have introduced more stringent due diligence in the form of customer identity verification, source of Crypto checks, customer device monitoring, or customer IP monitoring, while others may only support these Crypto in lower-value transactions. These controls offer some reduction in risk, but there remains residual uncertainty given the unknown source of funds.

Regulation

The regulatory framework is fragmented in the US and is only just being introduced in the UK. In the US, firms' Crypto activity may be captured by existing money transmission laws.[31] Some states, however, have gone above and beyond, like New York, and have introduced a dedicated "BitLicense."[32] In the UK, regulation will be introduced as part of 5MLD, but this does not capture all types of Crypto businesses or the conduct risks they present.

IT Controls

Firms acting as a Custodian should introduce controls to mitigate the risk of compromise. The splitting of keys where essentially two or three keys must be

[30] Fruth, J. (2018). *'Crypto-cleansing:' strategies to fight digital currency money laundering and sanctions evasion.* Reuters.com. Retrieved from: https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I (accessed 2 February 2019).

[31] Santori, M. (2016). *Bitcoin Law: Money transmission on the state level in the US*. CoinDesk. Retrieved from: https://www.coindesk.com/bitcoin-law-money-transmission-state-level-us (accessed 2 February 2019).

[32] Dfs.ny.gov. (n.d.). *NYSDFS: Final BitLicense Regulatory Framework*. Retrieved from: https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses (accessed 25 January 2019).

combined to facilitate a transaction can be likened to a strong customer authentication control. This is best practice, and failure to have appropriate security controls in place could result in all keys being stolen or compromised. Given the bearer nature of Crypto, it is important for users and platforms to mitigate the risk of assets becoming inaccessible. Supporting a business that has previously suffered a breach or that may suffer a breach could cause significant damage to the Fintech from a legal and reputational perspective.

Source of Crypto

For Exchanges, a very useful tool is the use of Elliptic or Chainalysis, which, in the briefest terms, provide a blockchain transaction monitoring service/source of Crypto check. At present, this type of solution is only available for certain types of Crypto, such as Bitcoin or Ethereum.

4.2. Customer Due Diligence and Risk Management

A number of innovations are being driven by Fintechs looking to introduce the best customer experience for their users. This includes offering the most secure solution possible. Increasingly, Fintechs are looking to use biometrics, machine learning and AI to offer a more secure and customised service to their customers. By building and managing this tech in-house, Fintechs can adapt the solution to their specific needs and thus reduce their overall financial crime exposure. In evaluating risk, it is vital that regulators be willing to see this new technology for what it is, rather than compare it against more established manual processes. To further explore the impact of these developments, it is important to consider some in more detail.

Selfie Video

This has been introduced as a control against the impersonation risk of onboarding a customer in a non-face-to-face environment. This check originally began as a “selfie” picture, but this has evolved to a more secure video check. Not only does it ensure that there is a real customer presenting information, but the facial images can be compared against identity documents that have been submitted. This verification gives an approval or rejection decision in near real-time, creating an efficient and customer-centric onboarding process. Monzo, Starling, and others are Fintechs that have introduced some version of this solution to customers. These tools can prevent the inconsistencies and mistakes resulting from human error.[33] The European Banking Authority (EBA) cites an impersonation fraud check as a means to reduce the overall customer risk.[34]

[33] GOV.UK. (2018). *Identification Document Validation Technology*. Retrieved from: https://www.gov.uk/government/publications/identity-document-validation-technology/identification-document-validation-technology (accessed 25 January 2019).

[34] Esas-joint-committee.europa.eu. (2018). *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 transactions*. Retrieved from: https://esas-

ID Chip Scan

This is one of the most accurate ways to verify an identity document's authenticity.[35] The customers themselves scan a document's chip in order to extract and upload their name, date of birth, photo, and a unique identifier to confirm its authenticity.[36] Some firms are using this in combination with the biometric check above, but it is only an emerging solution for due diligence given Android devices are the only ones capable of supporting this technology at the moment. Most recently, this control has been proposed by the UK government for EU citizens to formalise their residency status after Brexit.[37]

Machine Learning and AI

Machine learning is not a new concept; in fact, SAS says it used its first machine learning algorithm in 1979.[38] What is new, however, is the ability for smaller, tech-savvy firms to capitalise on this technology. Fintechs have built rules engines in-house that consider customer activity in a more holistic manner. This allows potential instances of risky behaviour or fraud to be viewed not only in isolation but rather in conjunction with other aspects of a customer's activity. The activity can also be compared with the accounts of the customer's peers to determine whether a single, non-risky action may actually be suspicious based on previous instances of suspicious activity by others.[39] This tool can be used to identify all customers involved in a fraud ring or organised crime group in an automated way, avoiding unnecessary time and resource from a team of analysts.[40]

AI allows this collated risk to have a decision taken on it much like that of a Level 1 compliance analyst. For now, it is being proposed that a human element needs to

jointcommittee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_EN_04-01-2018.pdf (accessed 25 January 2019).

[35] GOV.UK. (2018). *Identification Document Validation Technology*. Retrieved from: https://www.gov.uk/government/publications/identity-document-validation-technology/identification-document-validation-technology (accessed 25 January 2019).

[36] Fernandez, J. (n.d.). *Could the use of biometric data balance the e- money/customer due diligence equation?* Ppro.com. Retrieved from: https://www.ppro.com/wp-content/uploads/dlm_uploads/2016/04/Could-the-use-of-biometric-data-balance-the-e-moneycustomer-due-diligence-equation.pdf (accessed 2 February 2019).

[37] GOV.UK. (2019). *Using the 'EU Exit: ID Document Check' app*. Retrieved from: https://www.gov.uk/guidance/using-the-eu-exit-id-document-check-app (accessed 2 February 2019).

[38] Muezzinoglu, K., Suplee, C,. & Stewart, D. (n.d.). *Machine Learning Use Cases in Financial Crimes—Ten practical and achievable ways to put machine learning to work*. Aba.com. Retrieved from: https://www.aba.com/Tools/Offers/Documents/Machine%20Learning%20Use%20Cases%20in%20Financial%20Crimes.pdf (accessed 2 February 2019).

[39] Muezzinoglu, K., Suplee, C. and Stewart, D. (n.d.). *Machine Learning Use Cases in Financial Crimes—Ten practical and achievable ways to put machine learning to work*. Aba.com. Retrieved from: https://www.aba.com/Tools/Offers/Documents/Machine%20Learning%20Use%20Cases%20in%20Financial%20Crimes.pdf (accessed 2 February 2019).

[40] Breslow, S., Hagstroem, M., Mikkelsen, D., & Robu, K. (2017). *The new frontier in anti–money laundering*. McKinsey & Company. Retrieved from: https://www.mckinsey.com/business-functions/risk/our-insights/the-new-frontier-in-anti-money-laundering (accessed 25 January 2019).

remain even after the solution is sufficiently tested. Financial-crime alert reviews can shift towards being validated through a spot-check process.[41]

AI and machine learning not only are effective tools in identifying unusual transactions but also can be used for network mapping, dynamic customer and transaction risk assessments, adverse media analysis, and much more.[42]

4.2.1. What to Consider When Auditing These Tools

When auditing a Fintech, it is important to understand whether the firm has considered the risks and its required governance when introducing innovation into its products. Many of the cutting-edge solutions can offer important benefits, but this must always be balanced with a stringent approval and testing process. Automation can be a strength in the customer journey, but there are also limitations in terms of regulatory requirements when making an automated decision about a customer or the customer's activity. Article 22 of the General Data Protection Regulation (GDPR) makes clear that automating important due diligence and legal decisions about a customer without appropriate consent could be a violation.[43]

When auditing a Fintech, it is important to understand whether it has appropriate risk assessments in place as well as product governance processes. Stakeholders from all aspects of the business should regularly be consulted and sign off should equally come from these diverse perspectives. Otherwise, the automation could incorrectly allocate risk and bias.

With the use of AI and machine learning, or any other automated check, it is important that a quality review and oversight process is in place. This is crucial not only for escalations of instances that fall outside of the review policy programmed into the AI and machine learning system, but also to ensure that the alerted items are generated as expected. Without this oversight and regular review, firms could run into false positives being incorrectly escalated, suspicious patterns being missed, and inaccurate bias being introduced to the system. Google, for instance, recently identified an issue in using machine learning to inform its hiring process. By basing its decisions on the pooled data from hiring decisions made by humans, it integrated a bias against female candidates into its algorithm, according to a research report. [44]

---

[41] Zimiles, E., & Mueller, T. (2019). *How AI is transforming the fight against money laundering*. World Economic Forum. Retrieved from: https://www.weforum.org/agenda/2019/01/how-ai-can-knock-the-starch-out-of-money-laundering/ (accessed 2 February 2019).

[42] Zimiles, E., & Mueller, T. (2019). *How AI is transforming the fight against money laundering*. World Economic Forum. Retrieved from: https://www.weforum.org/agenda/2019/01/how-ai-can-knock-the-starch-out-of-money-laundering/ (accessed 2 February 2019).

[43] Ico.org.uk. (n.d.). *Rights related to automated decision making including profiling*. Retrieved from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/ (accessed 2 February 2019).

[44] Devlin, H. (2017). *AI programs exhibit racial and gender biases, research reveals*. The Guardian. Retrieved from: https://www.theguardian.com/technology/2017/apr/13/ai-programs-exhibit-racist-and-sexist-biases-research-reveals (accessed 2 February 2019).

5. Conclusion

While much progress and change are afoot in the Fintech industry, the financial crime risks are evolving at an equally fast pace. Supervisors and auditors are presented with a significant challenge in trying not only to understand the use of technology by Fintechs but also to consider the risks this brings. This white paper strives to introduce some of these emerging technologies and supervisory risk indicators while also offering insight into challenges faced from the perspective of a Fintech.

In order to ensure that supervision and audits are aligned to the risk posed by the fast-moving industry, it is important for both sides to continue to work together. Both the UK and the US have identified the complexities and opportunities offered by the Fintech industry. The UK's FCA sandbox and the US' proposal for a federal Fintech license look to support this growth. While these efforts are in keeping with the governments' recognition of the opportunities of the industry, significant obstacles remain for Fintechs to overcome. Regular supervisory engagement is key for success in making real progress. The FCA has begun offering events to payments and E-money firms, some of which are Fintechs, but there still are a number of firms that do not engage despite their regulatory status or authorisation type. Groups such as the Electronic Money Association and the Fintech FinCrime Exchange offer real insight into the way Fintechs operate and their risks. These groups regularly welcome the attendance and support of supervisors.

Beyond engagement there needs to be flexibility in the audit manuals for supervisors to ensure that the diversity of the industry and the new technology is not inaccurately assessed. New methods should be welcomed, provided that the Fintech can demonstrate due consideration has been given to potential risks and that clear governance structures are created for risk mitigation. Regulatory flexibility should thus be balanced with the traditional review of governance and policies and procedures. Ensuring that these audits and assessments are reflective of the financial crime risks of the entity will eventually lead to a broader acceptance across the wider financial industry. Until then, the regulator needs to ensure that there is no systemic de-risking or potentially misleading national risk assessments.

The Fintech industry is still emerging and experiencing growing pains, but having a strong and supportive supervisory framework in place will allow compliant firms to continue to expand and develop. This approach will improve consumer access to financial services and ultimately reduce the financial crime risks posed by the Fintech industry.