EGMONT GROUP

OF FINANCIAL INTELLIGENCE UNITS

Prepared by the Information Exchange Working Group (IEWG)

FIU – FinTech Cooperation and Associated Cybercrime Typologies and Risks

July 2022

Table of contents

Background

While preparing the concept note for this project, it became evident that the notion of FinTech could have different meanings. The priority given to information received from FinTech in connection with suspicions of money laundering and terrorist financing also seems to differ between FIUs. On the one hand, some FIUs encounter problems collecting information from FinTech operating in their jurisdiction; on the other hand, the information collected, including technical data, cannot be fully leveraged by all FIUs. These challenges are further accentuated with the emergence of new actors, such as Virtual Asset Service Providers (VASPs).

To obtain a better understanding of the FinTech environment, a questionnaire was circulated to Egmont Group member FIUs. The questionnaire sought to understand which types of FinTech are subject to regulation in each jurisdiction, how the legislation treats them, what information they report to authorities and how they report it, and how FIUs use the information received. The questionnaire was accompanied by a call for case studies featuring cyber-enabled financial crime and associated risks linked to FinTech.

A total of 41 FIUs responded to the call for information, including 13 case studies[1]. This report provides an overview of the outcomes of the project team's analysis of responses with observations regarding:

- The types of FinTech entities regulated across the globe.
- The nature of regulatory oversight of the FinTech industry.
- The level of FIU-FinTech cooperation, noting the transnational nature of many FinTech business models.
- How FIUs receive data from FinTech, including unique datasets held by FinTech and tools used to analyze such data.
- The quality and value of financial transaction data received from FinTech.

[1] Afghanistan, Australia, Belgium, Benin, Brunei Darussalam, Bulgaria, Cameroon, Chad, Congo, Ecuador, Finland, France, Germany, Gibraltar, Guatemala, Iceland, Isle of Man, Japan, Jordan, Kosovo, Lithuania, Malta, Moldova, Morocco, Netherlands, Nigeria, Peru, Philippines, South Africa, Senegal, Serbia, Singapore, Sudan, Sweden, Switzerland, Tajikistan, Tunisia, Turkey, Turkmenistan, Ukraine, United States.

1. What Is FinTech?

Key takeaways

- 'FinTech' is short for 'financial technology'.
- There is no commonly agreed definition of FinTech.
- FinTech aims to improve provision of financial services by using technology to enhance accessibility and increase profitability by driving down operating costs.
- FIUs may grapple with FinTech due to a lack of understanding of the mechanics behind technology-based innovations as well as the risks and vulnerabilities of new payment services and products.

FinTech is short for 'financial technology' and is part of our generation's global innovation boom. Several factors have contributed to the rapid growth of this technology-based innovation, such as increased access to the internet, the prevalence of mobile devices, the emergence of blockchain technology and growing digital storage capacity, amongst others.

There is no commonly agreed definition of FinTech. In the broader context, the term refers to computer programs and other technology used to support or enable access to banking and financial services.

For this project, FinTech refers to entities that enable payments or transfers of value by using new or emerging technologies. Egmont Group members were invited to indicate, by way of a survey, what entities they include under this definition.

Common examples of FinTech providing financial services include:

- Internet banking
- Mobile banking
- Digital or electronic money
- Money transfer platforms
- Non-face-to-face investments
- Crowdfunding platforms
- VASPs[2]

As it represents significant opportunities to streamline private sector operations through innovation, FinTech is promoted as the future of financial services. Yet, FinTech sees FIUs grappling with ways to engage with the sector and understand its product offerings and their associated money launderingand terrorist financing (ML/TF) risks and vulnerabilities. Noting this, FIUs need to better understand the mechanics behind technology-based innovations and the threats and vulnerabilities associated with new payment services and products. In addition, the environment in which FinTechs operate is, by its nature,

[2] Including, but not limited to, digital currency exchanges, cryptocurrency ATM operators, administrators of stablecoin arrangements, wallet custodians, hedge funds dealing in virtual assets such as cryptocurrencies. This also includes anything that is tokenized as an asset and transferred on a blockchain or other digital peer-to-peer format.

borderless. Therefore, FIUs must adequately harness more effective information-sharing mechanisms to address emerging challenges.

The FATF Recommendation 15 (New Technologies) requires jurisdictions to address risks arising from new and emerging technologies and to strengthen anti-money laundering and counter-terrorism financing (AML/CFT) systems and controls. In addition, the FATF recently amended this recommendation to require jurisdictions to regulate virtual asset service providers (VASPs) for AML/CFT purposes. This includes ensuring such entities have effective systems and controls to monitor and ensure compliance withthe AML/CFT measures contained within the FATF Recommendations.

Not all entities providing FinTech services are defined as reporting entities under international standards. Therefore, they may not be subject to AML/CFT regulatory oversight or required to report suspicious matters and/or other transactions to relevant authorities. This may present FIUs and their partners seeking to trace illicit fund flows with difficulties accessing information to build an intelligence picture and enhance law enforcement outcomes.

Noting the above, this project aims to:

- provide an understanding of how FinTech entities cooperate with FIUs in Egmont Group member jurisdictions,
- explore the regulatory environment in which they operate, and
- define potential best practices to engage with the FinTech sector, including identifying relevant risks and vulnerabilities.

For this purpose, Egmont Group members were invited to participate in a survey between March 2020 and June 2020. The project team received input from 41 members from North America, Europe, the Middle East, Africa, and the Asia-Pacific region.

2. Types of FinTech

Key takeaways

- FinTech is revolutionizing the way the world does business. With the emergence of faster, more streamlined transactions facilitated by blockchain and FinTech platforms, new opportunities for financial crime are presented.
- Although FIUs are familiar with most FinTech entities which provide traditional services albeit via new technology, others are relatively new and present FIUs with a significant challenge to understand how their services can facilitate financial crime.

Using survey responses from project participants and open-source research, the project team noted that FinTech commonly included entities that offered the following products/services:

- Internet payment services
- Mobile payment services
- Electronic money/e-money
- Peer-to-peer lending
- Crowdfunding platforms
- Neo banks or digital banks
- Advisory and Investment management platforms (e.g., Robo-advising apps)
- Trading platforms (e.g., stock-trading apps)
- Insurtechs
- "Buy now pay later" (BNPL)-platforms
- Trade finance and supply chain platforms (e.g., agribusiness, mining, manufacturing, etc.)
- Pay lending platforms
- VASPs

Several the financial services listed above are well known to FIUs. Some are considered emerging and, in turn, pose significant challenges for FIUs seeking to understand their product or service offerings.

For example, **internet-based payment service providers, mobile payment service providers and electronic money providers**[3] offer products or facilitate services considered more mainstream by design. Their use of technology is, for the most, easily understood by FIUs as they provide familiar products or services online or via mobile channels to provide flexibility and increase accessibility to the end user. Conversely, VASPs are considered relatively new, often providing services only beginning to be understood by some FIUs.

While the FATF definition of VASPs provides examples of specific financial activities and functions, it does not limit the definition to a particular kind of entity. Still, it considers how a person uses the virtual assets and for whose benefit. According to the FATF[4], if a person (natural or legal) is engaged as a business in any of the activities described below for or on behalf of another person, then they are, by definition, a VASP, regardless of the technology used to facilitate these activities:

- exchange between virtual assets and fiat currencies,

[3] The FATF defines electronic money as a record of funds or value available to a consumer stored on a payment device such as a chip on a prepaid card, mobile phones or computer systems as a non-traditional account with a banking or non-banking entity. It emphasizes that the definition of electronic money should remain flexible and can be further differentiated into network money, mobile money, electronic purse, and electronic wallet.

[4] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html.

- exchange between one or more forms of virtual assets,
- transfer[5] of virtual assets,
- safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets, and
- participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

The FATF definition extends to different types of cryptocurrency businesses, including digital currency exchanges, cryptocurrency ATM operators, wallet custodians, and hedge funds. Certain virtual asset entities, such as cryptocurrency miners, may or may not be captured by this definition, depending largely on their activities and functions. While the activities of an individual cryptocurrency miner may not be enough to classify them as a VASP, the activity of a cryptocurrency mining pool may well be captured if the group engages in any of the activities included in the FATF's definition.

Crowdfunding networks and peer-to-peer lending services enable users to receive and send money online via mobile apps. **Peer-to-peer lending**, known as 'marketplace lending,' directly matches borrowers with investors. These services provide direct competition to traditional financial institutions that rely onlarge complex systems to enable such transactions. Technology, in this instance, makes the process much cheaper and more efficient. However, it can also present challenges for regulators seeking to define which party has the AML/CFT obligation to undertake customer due diligence and report suspicious activity, particularly when the anonymity of the investor is promoted.

In its report on emerging terrorist financing risks[6], the FATF defined **crowdfunding** as an internet-enabled means for businesses, organizations, or individuals to raise money (via donations or investments) from multiple individuals. Crowdfunding websites allow people to easily set up a fundraising page and collect donations from various sources.

Neo-banks or digital banks operate exclusively online without traditional physical branch networks. They operate via mobile apps and offer most of the services a conventional bank does, except providing in-person services in physical branches. Some neo-banks partner with traditional financial institutions to deliver more tailored solutions for customers and may utilize technology such as artificial intelligence and machine learning.

Robo-advising and stock-trading apps use intelligent algorithms to provide intuitive asset recommendations to users. They also offer stock trading solutions to allow investors to easily trade stocks using their smartphones. Another FinTech entity, insurtechs, is working to optimize access to insurance products via apps. Entities in this field collaborate with conventional insurers to automate insurance procedures and extend coverage.

The retail credit market has evolved in recent years with the emergence of **buy-now-pay-later** providers. Most BNPL arrangements are marketed as a budgeting tool or a way to make more purchases.

[5] In this context of virtual assets, transfer means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

[6] FATF report on Emerging Terrorist Financing Risks, October 2015, https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

affordable and are generally facilitated via a mobile app. However, given that BNPL business models make

available both a factoring[7] service to the retailer and loans to the retail customer making the purchase, the products pose money laundering risks.

FinTech is also facilitating evolution in global **trade finance** using blockchain and distributed ledger technology. Improvements include speeding up trade finance lending processes and streamlining cross-border trade for buyers and sellers. Innovations include providing supply chain management and financing platforms, enabling businesses to manage and pay their local and international suppliers or facilitating settlements of agricultural commodities via a blockchain.

Use of electronic money providers by suspects

CASE STUDY 1:

In December 2018, a Financial Intelligence unit (FIU) opened a case on suspected drug money laundering based on a suspicious transaction report filed by a local bank.

The bank noticed three of its customers (the 'suspects') were receiving suspicious regular small transactions through automated teller machine (ATM) deposits. During the operational analysis of the case, the FIU received the customer due diligence information of the suspects, which helped to identify if they have opened accounts at other financial institutions. The analysis revealed that the suspects registered over a hundred accounts with electronic money providers (e-money accounts).

Further investigations revealed the e-money accounts were being used to receive funds from drug transactions. The illicit funds were then transferred to several other e-money accounts in different countries to conceal their origin.

[7] Factoring refers to a financial arrangement whereby the business sells its trade receivables to the factor (e.g. a BNPL provider or a bank) and receives the cash payment.

3. Legal Frameworks to Regulate FinTech

Key takeaways

- The legal status and regulation of FinTech varies across the globe.
- It is important FinTechs are captured by AML/CFT legislation to ensure active and passive cooperation with FIUs.
- In view of the online environment in which FinTechs operate, FIUs need a good understanding of the FinTechs that operate in their jurisdiction.

Many FinTechs simply provide financial services already subject to AML/CFT regulation, albeit via a new platform. In various jurisdictions, the majority of FinTech mentioned in the previous section are subject to national AML/CFT legislative requirements and regulatory oversight. However, in some circumstances, gaps exist for which a lack of regulatory oversightproves challenging for FIUs in their efforts to fight financial crime. This has been dubbed a 'sunrise-issue' in the latest FATF Recommendations about Virtual Assets[8].

3.1. Regulation

The project considered the current state of regulation of FinTechs and associated legal frameworks as reported by project participants. The FATF standards acknowledge that not all financial services face the sameML/TF risks, and there may be different approaches to the supervision of different financial sectors. It does not surprise that the questionnaire responses from project participants also illustrated a varied approach to classifying and regulating FinTechs. While some jurisdictions classify these reporting entities based on thetype of business, other AML/CFT legislative frameworks adopt a tech-neutral approach to capture the provision of specific services at risk of exploitation for ML/TF.

Given the nature of FinTechs and the pace at which previously non-existent technologies such as VASPs have entered the market, there will likely be certain FinTech industry subsets that many jurisdictions are yet to commence regulating.

Understanding jurisdictional differences and comparing key aspects of national AML/CFT regimes provides considerable value to FIUs seeking to follow international funds flows. It enables streamlined intelligence information exchange and supports law enforcement efforts and the progression of evidentiary requests.

Most survey respondents advised that **internet-based payment services** are regulated as payment service providers or payment institutions (with slightly different definitions, for example, 'operator of payment systems).' Some respondents noted that such entities are regulated as banking institutions in their jurisdiction. In contrast, others noted that these services are regulated when an entity commences offering the specific type of service rather than at the point of registration.

Interestingly, approximately 23% of respondents stated that internet-based payment services are currently not regulated in their jurisdictions, but such regulation is in preparation. A small minority of respondents(approximately 8%) indicated that internet-based payment services are not regulated.

[8] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf

As for **e-money institutions**, most respondents stated these were regulated as such. Some respondents indicated that these are regulated either as a non-financial bank/business/professional entity or as a bank or other traditional financial institution.

Regulation of the **mobile payment service (MPS) industry** differs significantly across the globe and largely depends on the interpretations of what constitutes an MPS. Approximately 30% of respondents confirmed that MPS entities are regulated collectively as MPS, while 60% of respondents advised that MPS are regulated as entities under different legal categories. In approximately 13% of jurisdictions, MPS were not subject to regulatory oversight.

Analysis of survey responses commonly found that MPS are regulated as payment service providers or payment institutions and less commonly as non-financial institutions. As was the case for internet-based payment services, some respondents advised that MPS are only subject to regulation when the entity commences offering a service captured under the national AML/CFT legislation and are classified according to this activity.

VASPs and the distributed-ledger technology that underpins these transactions are among the most recently emerged, complex and evolving types of FinTech, with regulation not yet in place in many jurisdictions to capture these products or services. In jurisdictions where the national legislation captures such entities, the regulatory environment varies widely from one jurisdiction to another. This is often due to different classifications of each service or product. Several jurisdictions indicated they had implemented legislation to supervise exchanges between fiat and cryptocurrencies (and vice-versa).

It should be noted that approximately 50% of the survey respondents advised that digital or virtual currency exchanges/operators are considered 'financial institutions' in their jurisdictions and, in turn, subject to regulatory oversight.

In jurisdictions where regulation is pending, most plan to regulate VASPs as digital or virtual currency exchanges or to simply include these entities within existing definitions of a "financial institution." An alternative approach considered by the remainder of respondents planning to regulate VASPs is to regulate them as a stand-alone cohort of reporting entities.

STRs from VASPs

CASE STUDY 2:

Several suspicious transaction reports were received by the FIU regarding a non-payment fraud scheme involving virtual assets.

A group of criminals promised the victims large financial gains through virtual assets. They promoted lucrative investments in Bitcoins. Appealing to people's appetite for high return investments, the main suspect managed to gather approximately EUR 120,000 per day.

Following national cooperation between the FIU and its competent authorities and international cooperation with foreign FIUs, the main suspect was arrested, and the criminal operation was shut down in July2019.

CASE STUDY 3:

Several kidnapping cases were reported where the perpetrators demanded a ransom to be paid in Bitcoin.

In May 2018, a 13-year-old minor was abducted while playing outside with his friends. Shortly after, the parents of the boy received a ransom note with instructions to send 15 Bitcoin to a specific Bitcoin address.

Based on the technical data linked to the Bitcoin address left on the ransom note, the local FIU was able to identify the users of the address. The investigation revealed it was a multi-signature Bitcoin address, requiring at least two out of three private keys to access the virtual assets.

The transaction analysis and the wallet clustering analytics helped identify the Digital Currency Exchanges involved. After receiving the ransom payment, the total amount was split into smaller units and transferred to several other Bitcoin addresses.

In the first layer, 0.5 BTC were exchanged for fiat currency in a European country. During the second and third layers, more units were exchanged at several other VASPs. The remaining amount was invested into "PlusToken," a Ponzi scheme in Asia.

The case and investigation resulted in the arrest of the two main suspects and the victim was reunited with his family.

CASE STUDY 4:

This case study shows an example of malware distributors demanding a ransom in virtual assets for the release of encrypted data.

An international group of cyber criminals targeted local governments and prominent business entities with the release of ransomware. The attacks consisted of the encryption of specific hard drives that would only be decrypted after the victims paid the ransom in Bitcoin.

Over the period of 2 years and 3 months, a total of 20.16165158 BTC were transferred to Bitcoin wallets linked to the suspects.

CASE STUDY 5:

The following case study presents an example of virtual assets laundering, using a VASP to conduct a sequence of transfers between different virtual assets prior to cashing out.

An individual requested the conversion of substantial Bitcoin holdings to fiat currency. In doing so, he requested the Bitcoin be sold for DASH, a privacy coin, and then sold back to Bitcoin prior to being converted to Euro. The individual claimed this transaction pattern was necessary due to tax reasons. The Digital Currency Exchange reported its suspicions to the local FIU, which in turn conducted an analysis of the client and related transactions. It was determined that the individual was known to law enforcement for drug convictions and had ties to organized crime groups.

The FIU shared its findings with the relevant law enforcement agencies and the taxation office for further action and investigation.

The survey revealed no specific regulation for **crowdfunding services/platforms** in many jurisdictions. A considerable number of respondents indicated that entities offering crowdfunding services/platforms are considered reporting entities in their jurisdiction, often as the products offered are consistent with existing definitions of designated services (i.e., making loans, allowing transactions, or even remittance services). Approximately 16% of respondents indicated that specific legislation on crowdfunding services/platforms is being considered or is currently pending in their jurisdiction.

Other FinTech entities, such as the **BNPL** sector, **peer-to-peer lending,** or **investment management platforms**, although not explicitly covered by the questionnaire, seem to be captured under existing definitions of traditional financial services in many jurisdictions. For example, FinTech entities offering lending and forfaiting/factoring services may be captured as entities offering consumer credit. If investments are packaged and marketed by FinTech entities, the latter could be considered an investment firm. In such instances, the technology is used to facilitate the service as opposed to being the service itself and, as such, captured under existing definitions of financial services underlying a regulatory oversight.

3.2. Identifying FinTech entities

Many FinTech entities offer their services online, which extends their reach globally. Therefore, a FinTech company providing services to entities in each jurisdiction is likely not domiciled or registeredin that same jurisdiction. Such circumstances may result in a lack of oversight of relevant transactions (i.e., STRs) by the FIU of the country where the entity conducts the transaction.

Based on survey responses, cooperation between AML/CFT supervisors and FIUs appears to be an approach commonly used to detect new FinTech products and service providers. Generally, the financial supervisor/regulator plays a major detection role in almost every responding jurisdiction.

In addition, some jurisdictions use open-source information, regular meetings with competent authorities/regulators, and engagement with the private sector, academia, industry associations or technology communities to gain awareness of new developments in the FinTech environment.

Although limited, some countries leverage Regulatory Sandbox Frameworks to test start-ups and new

products in a reduced regulation environment. This enables both parties to (i) identify ML/TF risks raised by FinTech products and services, (ii) gain an understanding of new technologies and (iii) adapt regulation to optimize integration into the economy as applicable.

In cases where FinTechs operate in a jurisdiction but are not subject to regulation, survey respondents (36%) most commonly rely on open-source information or regular monitoring by law enforcement agencies (LEAs) and regulators to remain informed of new developments in FinTech.

Further, whistleblowing by industry competitors or unsolicited disclosures by the public is also a means used by FIUs to identify FinTech entities operating in a jurisdiction and potentially circumvent AML/CFT requirements.

Importance of identifying FinTech entities: use of domestic e-money institutions in an international fraud scheme

CASE STUDY 6:

Six foreign companies from Country X opened accounts with a local e-money institution. All six companies were represented by Individual A, a resident of Country X. We hereby refer to the six companies as Company I – VI.

Over a period of two days, Company II and Company III received a total of EUR 154.460,36 in 8 separate transfers from the bank account of Company I held in Country X.

Some of the funds were immediately transferred to an Asian bank account, supposedly for the payment of invoices for electronic devices, clothes, shoes, and furniture. The remaining funds were transferred to the e-money account of Company IV, supposedly as payments of invoices for the organization of events and VIP meals and drinks. Company IV then wires the funds to the Asian bank account.

On the following day, the bank that approved the initial transfers to the e-money accounts of Company II and Company III requested a refund due to "fraudulent payments." The request also mentioned transfers executed a few days earlier in favour of the e-money accounts held by Companies II – V.

A few months later, another foreign company, Company VII, registered in Country Y, opened an account with the same e-money institution. This company was represented by Individual B, a Country X resident.

The account of company VII was credited with EUR 10.000 from two separate transfers, supposedly to cover invoices for advertising materials. The e-money institution noticed that the invoices looked identical to Company IV's previous ones.

Investigations of the local law enforcements revealed that the transactions were part of an international fraud scheme. The victims received phone calls by alleged financial brokers, persuading them to invest funds in fictitious financial instruments. The alleged brokers then provided the victims with the wire details of the e-money accounts.

3.3 Navigating legislative frameworks in other jurisdictions

New financial technologies are developing rapidly, and national approaches to regulation may not keep up with the evolving nature of FinTechs. The results from the survey responses noted that in many jurisdictions, new legislation is being drafted to address gaps in supervisory frameworks for FinTech products and services not yet captured by the existing legislation. As many legal frameworks are still pending or being implemented, international cooperation remains the key to understanding what information can be obtained from other jurisdictions to enhance law enforcement outcomes.

Unlike banking and other 'traditional' sectors, legal frameworks for FinTech may differ significantly across the globe. Analysts must consider this and know where to find information on regulatory regimes. While expertise in regulation is not necessary for analysts, a healthy appreciation of regulations in other jurisdictions is helpful, mainly to provide a qualitative international exchange of information upon request.

By establishing a baseline understanding of the legislative frameworks in place within a particular jurisdiction, information requests to foreign counterparts can be targeted on specific issues. Such a practice allows the request recipient to respond more promptly, easily, and efficiently.

In addition, several resources are available to FIUs to assist with the identification of FinTech entities/VASPs and may assist in building an intelligence overview:

- The Egmont Group's eCatalogue on VASPs.
- FATF/FSRB mutual evaluations or follow-up reports[9].
- Open-source rating websites list the top 100 cryptocurrency exchanges and their registration details.

There is still room for the Egmont Group to explore the opportunities for obtaining a better understanding of national regulatory approaches in practice. The Egmont Group's future work programs could consider progressing a project to consolidate national registries of FinTech entities.

[9] http://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate)

Importance of cooperation with FinTech

CASE STUDY 7:

The following case study shows how an illegal betting organization used online payment institution accounts and e-money transfers to launder the proceeds from its illegal activities.

An individual opened an account at an online payment service provider and transferred a small amount from his bank account to the newly opened e-money account on the same day. On the following two days, five individuals transferred a total of EUR 5,368,752 to the account. Following these incoming transactions, the owner of the e-money account attempted to transfer the funds back to his personal bank account. However, the e-money institution, suspecting the funds might be linked to illegal activities, delayed the transfer.

The local FIU conducted an analysis of the payments and links between the different counterparties. They concluded the newly opened e-money account was used as a pool account and the counterparties as liaison accounts for an illegal betting organization.

The investigation resulted in the seizure of EUR 5,368,752 by the public prosecutor's office.

Illustration of the AML/CFT risks posed by FinTechs

CASE STUDY 8:

This case study focuses on one of the largest investment frauds that ever took place in the concerned country. The perpetrators operated under the guise of a religious organization soliciting donations from the public in exchange for a lifetime of monthly 'blessings' equivalent to 30% of their donation.

Initially registered as non-stock cooperation, the organization was found to engage in unlicensed investment-taking activity, which eventually lead to the issuance of a Cease-and-Desist Order as well asa Freeze Order by the Court of Appeal in June 2019.

The Freeze Order secured almost EUR 1,750,000 in assets, including virtual asset holdings. Indeed, the financial intelligence report prepared by the AML/CFT regulator contained valuable information on the existence of one or more virtual asset wallets maintained within the platform of virtual currency exchange. According to the information available, the account owner held both Bitcoin and Ethereum wallets.

The investigation remains ongoing.

4. Reporting regimes and engagement with international counterparts

Key takeaways

- Reporting regimes differ between jurisdictions which creates a risk that unregulated FinTech entities' products or services are utilized by criminal organizations seeking to circumvent global reporting requirements.
- FIUs should agree on a common reporting format – including technical data – in partnership with FinTech entities to enable the collection of the broadest possible financial intelligence.
- STRs submitted by FinTechs involving other jurisdictions may warrant a spontaneous disclosure to the involved jurisdiction's FIUs. This assists in identifying suspicious activity linked to potential entities of interest and provides a greater understanding of national ML/TF risks.

FinTech services operate in a borderless world, in a multitude of jurisdictions offering products and services to consumers in a rapid manner. For example, consumers can utilize FinTech services to:

- Get a credit or debit card that can be used worldwide,
- Invest in virtual assets,
- Make payments via electronic money,
- Make mobile payments.

FIUs must be able to access information from FinTech entities offering products or services within their jurisdiction, regardless of whether the FinTech entity is domiciled/registered in its jurisdiction. This includes access to financial transactions reported to other FIUs.

Given the current global understanding of the sector and the ever-evolving nature of products and services being 'modernized' by FinTech – there is a real risk of criminal groups seeking services to circumvent global reporting requirements. This is particularly relevant where an emerging understanding of the products and services offered by FinTech entities and differences in national AML/CFT reporting regimes exist.

Ensuring that FinTech entities actively report suspicious matters and other relevant financial transactions carried out by their customers to one or more FIUs ensures they thoroughly address the risks of their products or services being misused for nefarious purposes.

Further, best practice examples provided by survey respondents highlighted results when FIUs looked to proactively share STR data received from FinTech entities with a nexus to other jurisdictions with their international counterparts. Such a practice enables other FIUs to identify entities in their jurisdiction potentially using foreign FinTech products or services to facilitate ML/TF or other serious crimes. It also allows those FIUs to strengthen operational outcomes by detecting and disrupting ML/TF at the national and international levels.

The spontaneous sharing of financial intelligence linked to FinTech entities with other FIUs allows jurisdictions to build upon their understanding of the risks and vulnerabilities posed by the products and services offered by regulated and non-regulated FinTech entities. This understanding can be fed into their national ML/TF risk assessments.

Depending on the applicable legislation, a FinTech entity may:

a) file all its reports with the FIU in the country of its incorporation
b) file its reports directly with the most relevant FIU (e.g., in the suspect's country of residence), or
c) file reports on the same suspicious activities or transactions in multiple jurisdictions (e.g., a report to the FIU of its country of incorporation and a report to the FIU of the suspect's country of residence).

While the latter option ensures effective STR reporting, it may also lead to parallel analyses by several FIUs. This duplication of effort risks disrupting ongoing investigations or, worse, inaction. A risk of non-reporting cannot be excluded either.

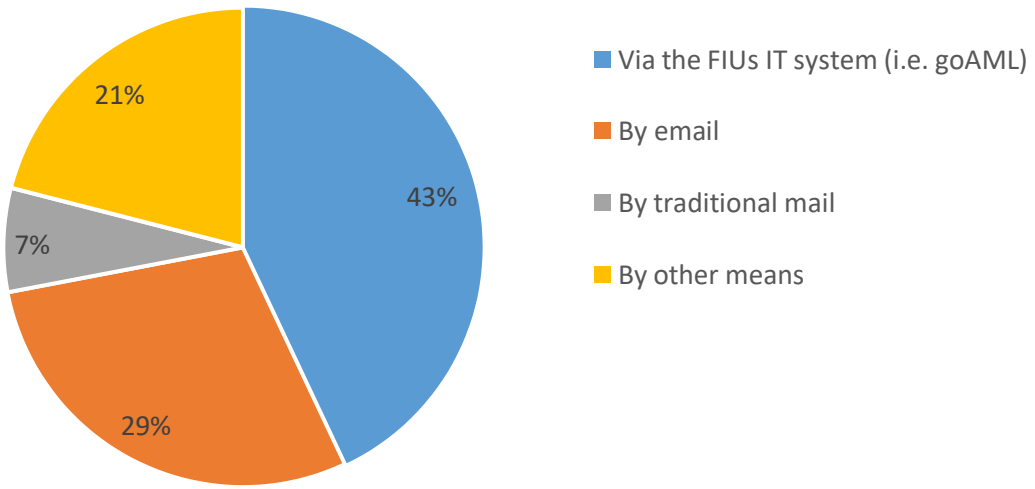
If a FinTech submits an STR involving another jurisdiction, it is recommended to consider international cooperation with the relevant FIU through spontaneous information exchange or a request for information. For Egmont Group member FIUs, the Egmont Secure Web provides a secure mechanism for this information exchange.

Reports received from FinTech are almost always electronic. This raises the issue of transmitting information in an appropriate format. The information received must not only be complete and intelligible to the receiving FIU but also be transmitted through secure communication channels. Difficulties may arise in this respect if the FinTech is not directly connected to the FIU's secure electronic reporting system.

Despite a general trend for receiving information via electronic means, a minority of survey respondents advised that they still receive reports via traditional mail and/or paper-based means.

Receiving data other than the FIU's electronic system may reduce the usability of reports received from FinTech entities, affecting the FIU's ability to harness the rich electronic data sourcescontained in STRs submitted by FinTech entities to inform their financial intelligence analysis (see Figure 1).

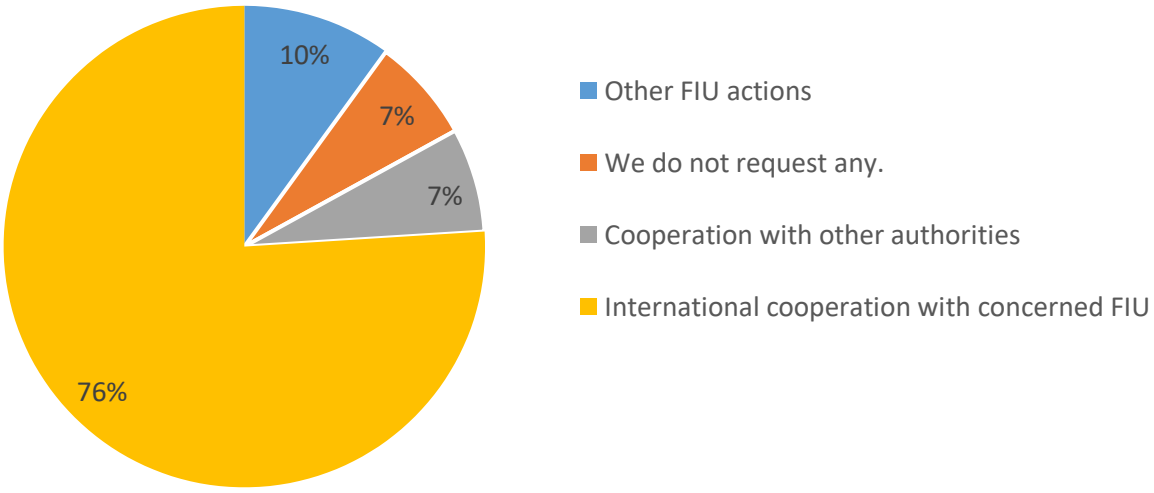
Figure 1: How do FinTechs report STRs to you?



In addition to the information in the STRs, the survey also considered the transmission of requests for information sent to a FinTech incorporated abroad. Most survey respondents (76%) indicated they rely on international cooperation between their FIU and the FIUwhere the FinTech is incorporated (see Figure 2) when seeking additional information about FinTech transactions linked to entities of interest. Other survey respondents indicated they cooperate with otherauthorities (e.g., law enforcement authorities or regulatory agencies) who can contact the overseas-based FinTech entity directly.

In the case of cross-border requests for information, it was reported that FinTech entities' transmissions are almost always undertaken via other means (i.e., through email)[10].

Figure 2: How do you obtain information concerning foreign FinTechs?



Please refer to *Section 6. International cooperation* for more information on this aspect.

[10] As reflected under figure 1.

5. Cooperation with FinTech entities

Key takeaways

- FIUs need to understand the services offered by FinTech entities.
- Financial intelligence received from FinTech entities will become more extensive and sophisticated as technological advances see FinTech products and services more widely used.
- To effectively analyze information reported by FinTech, financial intelligence analysts need to maintain a baseline understanding of the services offered by FinTechs and how to interpret the data submitted by these entities in financial intelligence reports.
- Public-private partnerships (PPPs) and regulatory sandboxes used in a number of jurisdictions, challenge traditional relationships to deliver innovative solutions jointly designed by private sector entities including FinTechs and a range of organisations involved in the fight against ML/TF and other serious crime.

Combatting modern-day financial crime requires cooperation across all entities within the global AML/CFT community of practice. Reporting entities, FIUs, AML/CFT regulators, LEAs and other competent authorities all have a role to play in fighting financial crime. Given the scale of financial crime globally and often limited public resources, it is crucial for FIUs and the private sector to cooperate more closely to respond to ML/TF threats.

In the case of FinTech entities, many are digital innovators, formed as start-ups bringing new services to the market. Such products often utilize new mobile payment solutions or provide services related to virtual assets.

To analyze the information reported by FinTechs, FIUs need to understand their services, how best to capture financial transaction data from them, their ML/TF risks and associated risk mitigation strategies. FIUs should, for example, be able to answer these questions about FinTech entities operating in their jurisdictions:

- How do they operate?
- What risks are inherent to the services offered?
- What are your customer (KYC) / customer due diligence (CDD) measures in place?
- How can transaction records be obtained in a format easily readable by the FIU's analysis tools?

In this context, there are many examples to illustrate the challenges FIUs face:

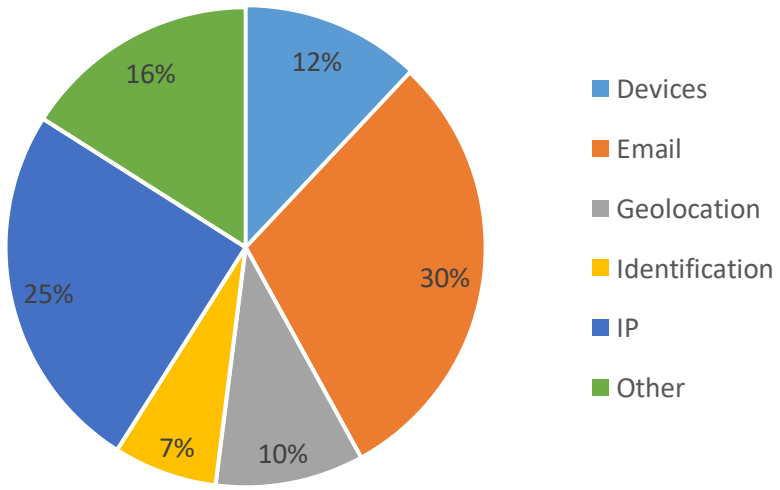
- For mobile phone-to-phone transactions, the transaction information must be completedwith the previously registered phone numbers.
- Virtual asset transactions must be reported accurately, and all elements provided (sending and receiving address, transaction ID) are useful from a financial intelligence perspective.

In addition to initial contact, FIUs and AML/CFT regulators should monitor the development of services offered by FinTechs. Regulatory sandboxes and public-private partnerships (PPPs) identified two good practices for responding to FIUs.

In the first case, the FIU was involved in the sandbox initiated by the regulator and contributed to the assessment of the risks presented by FinTech. In the second, the PPPs fostered dialogue between the participating FinTech entities by structuring operational and strategic exchanges.

Given the online activity of FinTechs (which goes hand in hand with remote KYC/CDD), the technical information available is crucial. An evaluation of the survey responses illustrates the breadth of information received from FinTech entities (see Figure 3).

Figure 3: What technical information do you receive from FinTech entities?



The customer's digital fingerprint is an essential element of the information received from FinTech entities and provides avenues for further FIU analysis. This includes the IP addresses from which the connections were made, the device identifiers and geolocation data. Technical information received from FinTech entities may include specific details on unique device identification numbers such as IMEI[11], IMSI[12] or SEID[13] numbers and MAC[14] addresses.

Other information received from FinTech, as reported by survey respondents, includes:

- Digital photo selfies (picture of the customer),
- Client identification data,
- Files related to voice or video identification,
- Detailed transaction communications,
- Economic origin of funds/wealth,
- Economic activity,

[11] The IMEI (International Mobile Station Equipment Identity) is an international 'serial number' for a mobile phone device to properly identify it on the carrier's network.
[12] The IMSI (International Mobile Subscriber Identity) is a code used by a phone company to identify the SIM on the mobile network.
[13] A SEID (Security Element Identifier) of the security element chip works together with the NFC (Near Field Communication) chip to support built-in payment functions on a smartphone.
[14] A media access control address (MAC address) is a unique identifier for an Ethernet or network adapter (e.g. Wi- Fi or Bluetooth) over a network.

- Purpose of the account,
- Expected amount and frequency of transactions,
- Associated entities,
- Entity structure charts.

Technical information is often challenging to bring together manually and can only be exploited with the helpof powerful IT tools. It is, therefore, crucial for FIUs to receive financial transaction reports from FinTechs in an electronic format and one that can be easily read and ingested by the FIU's software.

Risks posed by remote KYC/CDD

CASE STUDY 9:

To get a better understanding of electronic money schemes, an FIU conducted a study focusingon two different online payment service providers.

The first online payment institution offers services for both e-money and virtual assets and advertises quick and profitable deposits and withdrawals throughout the country. According to the website, all transactions are carried out in accordance with the applicable laws and confidential client information will not be shared with third parties.

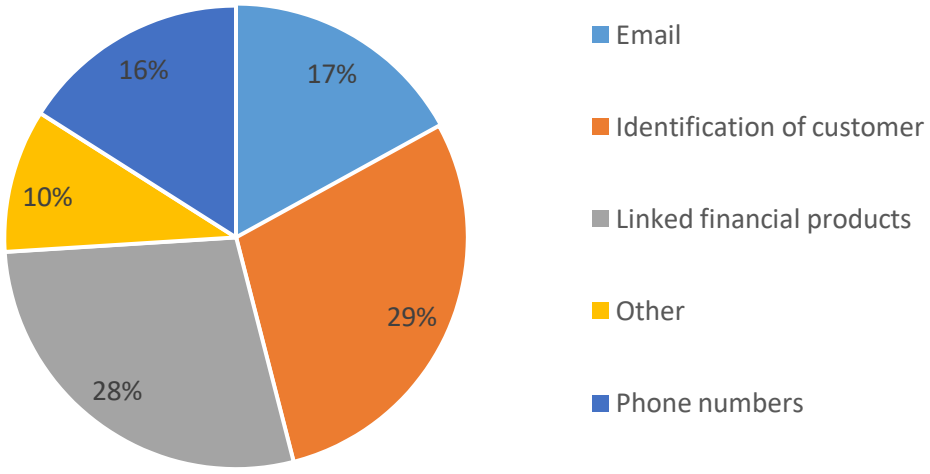
During the investigation the FIU contacted several clients of the online payment service provider to verify the legitimacy of the accounts. However, these individuals had no knowledgeof an electronic wallet having been opened in their name. One of the individuals had lost his passport a few years ago, while in a different case, the person had recently used his passport to register an account on a scientific website.

Regarding the second online payment service provider, the FIU discovered it was used to carry out international transfers bypassing banking charges usually applied to this type of transaction. Specifically, an individual in country "X" sells digital currency through the online payment service provider to a third party. The latter pays the former in fiat currency and proceeds to sell digital currency to a second individual in country "Y". For this service, the intermediary charges a fixed interest rate, lower than the bank interest rate.

These transaction patterns, being invisible to the banking institutions, make it difficult to identify the actual involved parties and therefore carry a high risk in terms of ML/TF and moving other criminal proceeds.

Survey respondents were asked to indicate the most helpful information from FinTech for theiranalysis (Figure 4).

Figure 4: What KYC/CDD information is most relevant for your analysis?



In addition to the above nominal data relating to customers, information about related financial products used by the customer was also considered helpful. For example, accounts opened with FinTechs are often linked to bank accounts or credit or debit cards (e.g., to top up an e-money account or to buy virtual currencies). These financial products allow FIUs to identify other avenues of financial analysis and link with the traditional financial sector.

Information request to FinTechs: importance of technical data and international cooperation

CASE STUDY 10:

In the following case study, a criminal group used FinTech entities to purchase equipment for their illicit activities.

An investigation was initiated based on information received from local law enforcement, that a group of six individuals, two nationals and four foreigners, had been linked to incoming money transfers from two FinTech entities registered in foreign jurisdictions.

The local FIU launched an international cooperation with the two foreign jurisdictions in which the involved FinTech entities were registered. This assisted in uncovering important information regarding the existing suspects as well as the possible involvement of other individuals.

International cooperation allowed the local FIU to uncover IP, email, and physical addresses, details about the goods in question, the devices used to purchase these goods, as well as other important information used to identify further related offences.

The case resulted in the arrest of the six prime suspects on the charges of organized crime, contract killings, and money laundering.

Cooperation with FinTechs – Importance of technical data

CASE STUDY 11:

This case study highlights the susceptibility of Internet payment accounts to spoofing and hacking.

In this case, a victim reported their Internet payment account was accessed by an unknown perpetrator who used the account to carry out payments to a second account held with the same Internet payment provider. The funds were then transferred from the second account to several other e-money accounts, for various services.

The analysis showed the victim's account was accessed from a spoofed IP address and the receiving account was set up using forged documents. Further, the receiving account shared the same IP address, computer cookies and similar account creation dates as various other accounts, involved in similar violations.

The ease of internet payment account creation has enabled criminals to set up multiple accounts using forged documents to layer criminal proceeds. However, with strong KYC/CDD policies in place and through the tracing of IP addresses and computer cookies, such cybercrime can be prevented.

Cooperation with FinTechs – Importance of transaction monitoring

CASE STUDY 12:

This case study focuses on a FinTech entity reporting a change in the spending behaviour of one of its clients, which eventually lead to the detection of a fraud scheme involving several millions.

The FinTech entity was alerted by the sudden and unusually high increase in spending by one of its clients. Over a few months the volume of outgoing transactions increased from less than a thousand Euro a month to several hundred thousand Euro a month.

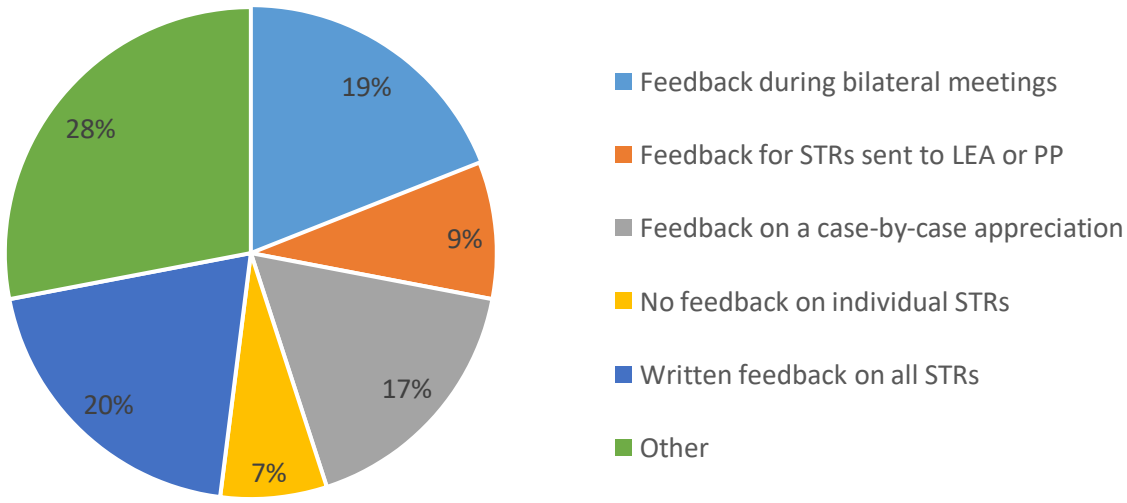
Based on this information, the FIU launched an investigation and discovered the individual's spending was way above his monthly income. In addition, the financial analysis revealed all the funds were used for gambling purposes. When investigating the source of funds, the FIU discovered the individualwas receiving two separate types of payments from his employer. In addition to the monthly salary, he regularly received payments tagged 'invoice' on a separate account.

The investigation revealed the individual, working in the finance department of a multi-billion revenue trade company, developed a scheme to defraud his employer. For over a year and a half, he re-activated several dormant credit accounts in the company system and placed them within the normal accounts payable process in such a way it went unnoticed, even by the external accountant responsible for reviewing the financial activities of the business at the end of the financial year.

The subject was subsequently arrested and sentenced to three years in prison.

In general, it appears that many FIUs provide feedback to FinTech entities either during bilateral meetings, in the form of written feedback on STRs received or by providing feedback on a case-by-case appreciation. Some FIUs, however, noted that feedback during bilateral meetings might only occur in limited circumstances, such as an onsite compliance visit, and likely only to address data quality issues (see Figure 5)[15].

Figure 5: What feedback do you provide on STRs submitted by FinTechs?



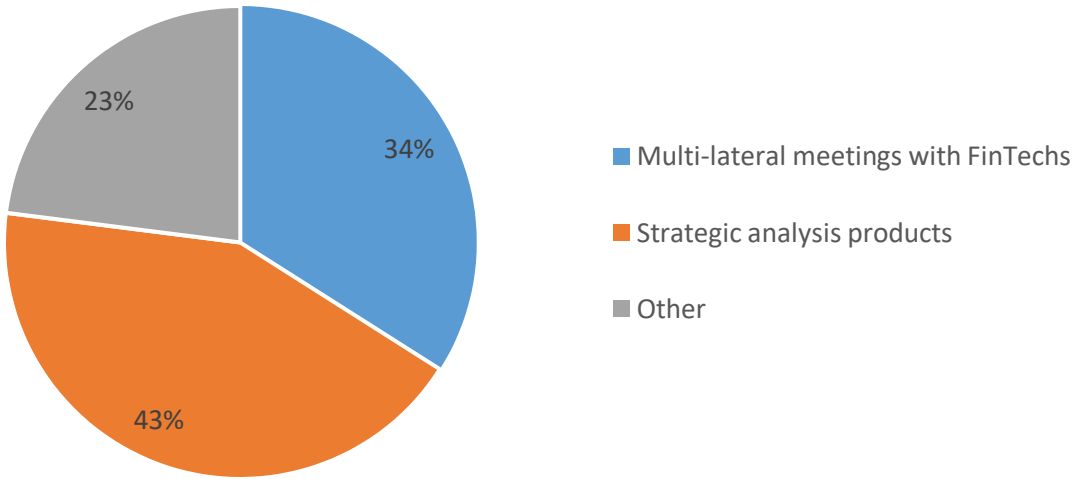
Some FIUs use an automatic reply system where reporting entities receive a confirmation that theirreport is accepted or has insufficient or problematic data. In the Netherlands, for example, reporting.

[15] In the figure, PP stands for public prosecutor.

entities receive a confirmation email in the unusual transaction report phase. Once it becomes an STR, they will receive an automatic reply.

The general feedback provided by FIUs includes reporting overviews, training, workshops, and multilateral meetings with FinTech representatives, published newsletters and strategic reviews with trends and typologies (see Figure 6).

Figure 6: What general feedback do you provide on FinTechs?



In the United States, the FIU, FinCEN, hosts FinCEN Exchange, the FIU's voluntary public-private information-sharing partnership among law enforcement and financial institutions. In addition, the Innovation Hours Program, an event hosted by FinCEN with private companies, offers a platform to showcase advances in certain fields of FinTech and furthers open dialogue between government and industry representatives. FinCEN also shares sanitized cyber indicator lists (CILs) extracted from their data with the financial sector, including FinTech entities.

In Australia, financial intelligence and AML/CFT regulatory teams utilize automated rules-based logic to triage reports submitted to identify high-priority matters and surface reports with questionable or problematic data. Reports are sometimes referred to the reporting entity for verification or correction. In addition, Australia's FIU, AUSTRAC, regularly presents to groups of reporting entities (including FinTech entities) to guide concerning what constitutes a good and useful STR. These efforts aim to uplift capability and explain how the different sectors can better contribute to effective law enforcement outcomes and disrupt financial and other crimes through their STR obligations.

Engagement with industry

CASE STUDY 13:

The AML/CFT Act in Australia requires reporting entities to submit an annual AML/CFT compliance report. This detailed information is analyzed in various ways to prioritize and inform compliance activities. This includes providing tailored feedback to entities to uplift theirability to detect ML/TF.

For example, one year, in response to the compliance report data received AUSTRAC's Monitoring and Triage teams engaged with certain entities, including digital currency exchange providers and FinTech entities, to provide tailored feedback regarding specific AML/CTF vulnerabilities and how they might improve responses to various ML/TF risks. Further, depending on the nature of an AML/CFT compliance assessment undertaken by the FIU, feedback may also be provided regarding the reports submitted by the entity to improve future data quality.

Another example is the Unregistered Remittance Campaign run by the FIU in 2019. In this example, various community town hall events were held across the country, with digital currency exchanges (DCEs) also in attendance. The campaign looked to educate interested parties within the community about the threats posed by unregistered remittance dealers, how to make informed choicesabout whom to do business with and how to report unregistered remitters to AUSTRAC. These events provided an important opportunity for sector members to meet in person with the AML/CTF regulator to ask questions and obtain feedback on the outcomes of reports made to the FIU.

6. International cooperation

Key takeaways

- FIUs should be aware FinTechs registered in their jurisdiction are likely to be offering their services in other jurisdictions.
- Spontaneous dissemination of information concerning FIUs in other jurisdictions is recommended.
- International cooperation between FIUs plays a fundamental role in gathering financial intelligence on online crime.
- FIUs should ensure they obtain conclusive information from FinTechs to ensure effective international cooperation.

Responses to questions pertaining to international cooperation suggested there are two aspects for FIUs to consider:

1) sharing of information received from FinTechs in STRs where the information concerns other jurisdictions, and
2) obtaining information from FinTechs incorporated in other jurisdictions.

Regardless of the type of international cooperation concerned, FIUs should ensure they receive and share information appropriately. In line with previous survey findings (see *5. Cooperation with FinTech entities*), the technical information provided by FinTechs can be complex, so transmission in an electronic format, at the very minimum, is recommended.

6.1. Sharing information received from FinTechs

Depending on the applicable legislation, some FinTechs may be required to submit all their reports to the FIU in the jurisdiction where they are incorporated, regardless of other territorial links (e.g., the suspect's residence). This is an example of a centralized reporting regime. This approach allows one FIU to assess the risks arising from FinTech's activity. FinTech, in this instance, cooperates with a single FIU and only needs to implement the technical solution for data transmission required by that FIU.

However, within the centralized model, while the reporting burden is reduced on the reporting entity, the receiving FIU carries the burden of the processing and analysis and needs to ensure that the information received is disseminated to its partners (both national and international) efficiently.

The FIU is responsible for ensuring information reaches the relevant partner FIU to enable timely identification of potential criminal activity within its jurisdiction. At the European level, this obligation is expressly provided for in the Fourth Directive, which states: *"when an FIU receives [an SAR or STR] which concerns another [EU] Member State, it shall promptly forward it to the FIU of that [EU] Member State"*[16].

In the *European context,* it is recommended that an FIU understands the breadth of the globaloperations of each FinTech registered in its jurisdiction to ensure all relevant transaction activity is reported. The FIU can actively work to prioritize sharing with its international counterparts.
Given the high volumes of reports received from some FinTechs, promptly disseminating this information to the relevant partner FIU can be challenging. It may also require substantial resources within the FIU to perform basic dissemination of information. For this reason, in jurisdictions where a centralized approach to reporting financial transactions is in place, it is recommended that an automated dissemination mechanism is set up, so information can be on-shared with relevant FIUs as required.

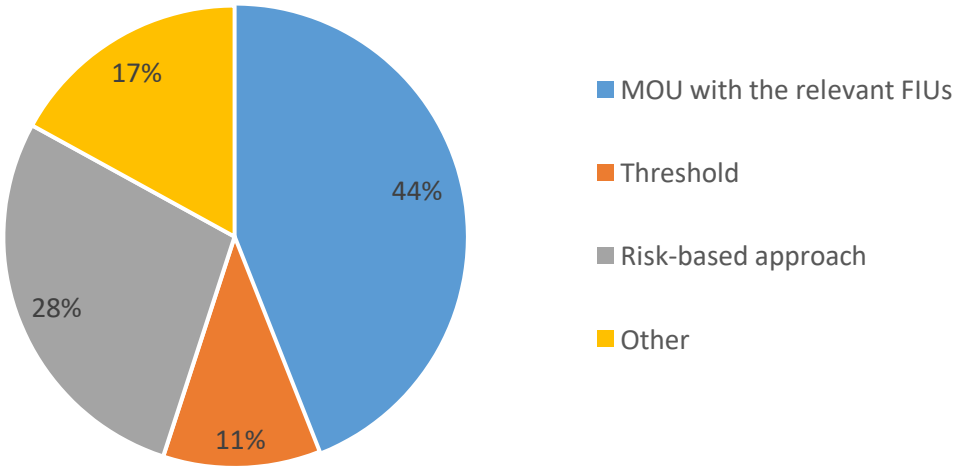
Some FIUs operating within such legislative regimes have tried to harness existing technical solutions available to make this process easier. For example, FIU.net provides opportunities for FIUs to share reports with their peers via the 'Cross Border Dissemination' and 'Cross Border Reporting' solutions, providing new opportunities for automated dissemination.

The analysis of survey responses indicated that most FIUs receive information from their counterparts regarding the activity of FinTech entities domiciled in other jurisdictions.
The majority (65%) of survey respondents advised that they received spontaneous dissemination of information about FinTech entities from other FIUs. These information flows among FIUs provide clear paths for the international community to gather relevant information to disrupt illegal money flows and support LEA investigations. Criminals can use various services offered by FinTechs, operating from different jurisdictions, to conduct their illicit activity. In such cases, FIUs need to work together to coordinate their action to achieve results.

[16] Article 53, §1, point 3 of the Directive (EU) 2015/849 of the European Parliament and the Council of 20 May 2015 on the prevention of the use of the financial system for money laundering or terrorist financing, https://eur-lex.europa.eu/eli/dir/2015/849/oj

Most survey respondents indicated that FIUs exchange information received from FinTech entities with other FIUs. The mechanisms underpinning such information sharing are listed below (Figure7).

Figure 7: Spontaneous dissemination based on certain criteria



While the criteria for dissemination varies across jurisdictions, most exchanges are underpinned by a Memorandum of Understanding (MOU) with the relevant FIU (44%).

Other criteria applied to spontaneous disclosures of STRs and other reports submitted by FinTech stem from a risk-based approach. Case reviews by analysts or the head of the FIU or monetary thresholds are also commonly used by FIUs to assess whether the reported financial activity may be of interest to another FIU.

Value of information exchanged spontaneously

CASE STUDY 14:

An FIU had been informed by a foreign FIU, about suspicious activity related to the turnover and use ofvirtual assets by one of their nationals. The local FIU managed to identify a personal account held by this individual at a VASP.

According to the information provided by the VASP, the individual had carried out several transactionsin favour of his personal bank account. The funds were used to purchase luxury cars and real estate.

During their analysis, the FIUs discovered the individual had only declared his yearly income from his activity as a private entrepreneur, while leaving out all the above. Thus, their initial suspicion was that the individual was engaged in tax evasion or evasion of the income declaration abroad.

However, further investigation into the individual's deposit addresses showed he had been receiving bitcoins from various Bitcoin wallets belonging to a group of unidentified individuals and from the high-risk VASP BTC-e (which is no longer in operation). The analysis revealed a link between these wallets and various fraudulent activities, ransomware attacks and the Darknet.

The FIUs worked together to communicate their findings to local law enforcement agencies, which were able to confirm the individual was a hacker involved in a range of illegal activities.

6.2. Obtaining information from FinTech

The digital world in which FinTechs operate contrasts with that of judicial cooperation, which often remains very formal and lengthy. Timely international cooperation between FIUs plays a fundamental role in collecting financial intelligence related to online financial transactions. It enables FIUs and their partners to build their intelligence picture more efficiently to better fight financial crime. Further, as more jurisdictions enact legislative change to capture all relevant FinTech entities as reporting entities, this increases the ability of the global network to harness the rich sources of data held by FinTech entities to detect and disrupt illicit fund flows facilitated by FinTech products and services – even if these are spread across multiple jurisdictions.

While some FIUs send requests for information directly to FinTechs not registered in their jurisdiction, most survey respondents indicated they regularly contact their foreign counterparts to obtain this information to assist with investigations (please refer to the graph presented under Section *4. Reporting regimes and engagement with international counterparts*). It is, therefore, imperative that FIUs, upon receiving a request for information from a counterpart FIU, have the authority to contact the relevant reporting entities (in our case FinTechs) to receive the requested information and share this with the requesting FIUs.

Importance of international cooperation – A "classic" case involving foreign FinTech

CASE STUDY 15:

A group of criminals set up and/or took over several businesses operating within the construction and cleaning sectors. These companies were used as a cover to employ non-declared workers and carryout transfers of illicit nature to offshore countries. The FIU conducted analysis of the financial activity ofthese companies and noticed they were part of a network of different entities with similar profiles and used for a limited time only. The FIU and its law enforcement partners noticed that over the past few years, these networks had started incorporating accounts held at foreign FinTech entities into their ML schemes, rendering them more and more complex.

In this case, a new construction company with no registered workers was set-up, showing all the characteristics of being part of the above-mentioned network. During the first few months following the incorporation, the company received payments related to invoices from other companies for a total amount of more than EUR 2,000,000. These funds were then transferred to a country in Asia as well as various private accounts held by the manager of the construction company. The manager opened accounts with ten overseas-based FinTechs, which were used to gather and withdraw funds fromthe company.

Since these FinTechs did not fall under remit of the national jurisdiction, the FIU could not directly address its requests to these entities and had to rely on international cooperation. The cooperation between the different FIUs turned out to be highly efficient and confirmed the company as well as the manager were part of a criminal organization laundering funds from illicit activities.

7. Tools for the job

Key takeaways

- Technology is evolving quickly, FIUs need to adapt swiftly to understand and address new risks.
- FIUs need to be agile, continuously looking to enhance their capabilities through digital transformation and fostering a culture that values and promotes continuous learning, sharing knowledge and experience.
- FIUs need to engage with FinTechs to better understand their product offerings, operations and what data is available upon request - partnerships are important.
- Despite technological advances calling for new knowledge and skills, traditional financial intelligence analysis methods continue to be of fundamental value to tackle FinTech-related crime.

FinTech provides the same financial services provided by traditional 'bricks and mortar' financial service providers – banking, value exchange and transfer, investment products and services, loans, forfeiting, trade, and gambling, etc., albeit via a new service delivery method.

Accordingly, criminals continue to use the same financial services and products to profit from crime, launder money, finance terrorism and proliferate weapons of mass destruction. Differences exist in the speed at which FinTech can facilitate transactions and the emergence of virtual assets as a funding mechanism. Analyzing activities undertaken and reported by FinTech need not be as daunting or specialized as perhaps it may initially appear. Financial intelligence analysts are still required to 'follow the money.' They may be able to paint a much broader and more accurate intelligence picture using data held by FinTech, provided, of course, they have the required tools to do so.

With an ever-evolving technological landscape, FIUs must, however, adapt their working methods and tools to better understand and address the new risks posed by FinTech. This necessitates a digital transformation of FIUs and adequate technological tools to assist FIU analysts in everyday work. However, while technology enables a quicker response to address criminality, and new commercial tools and knowledge are necessary to understand and analyze virtual assets' activities, these do not replace traditional analysis techniques to tackle FinTech-enabled crime.

The project team utilized the 41 questionnaire responses to gain insights into the current context in terms

of (1) what technical information is collected and processed by member FIUs, (2) what tools are used to process the information, and (3) what intelligence value such technical information provides. This also provides an 'as is' picture which will help inform the second phase of this IEWG project regarding the digital transformation of FIUs.

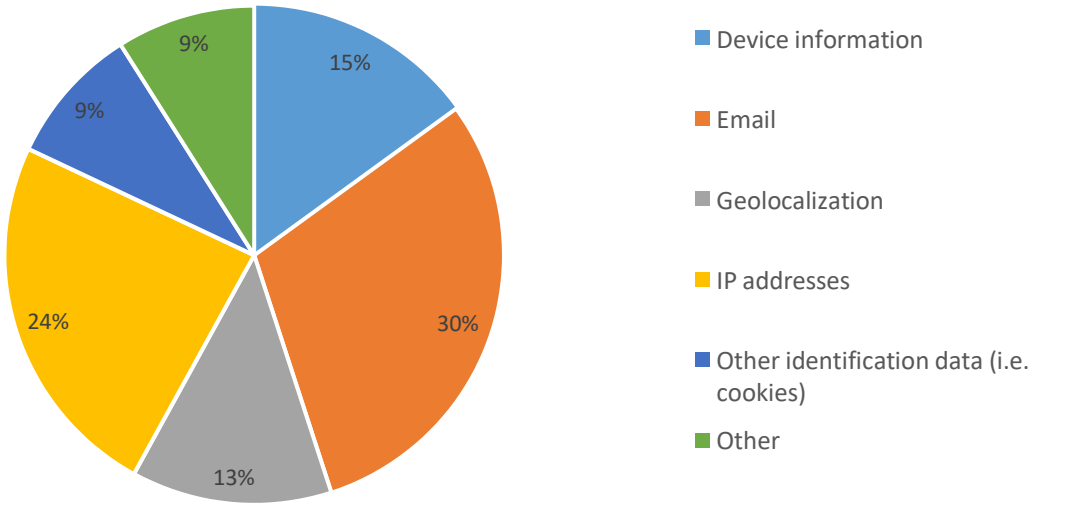
7.1. What technical information is available?

- If we consider the type of information reported by FinTech, we observe the typical KYC/CDD and transactional data reported by traditional reporting entities. FIUs are familiar with this information and can readily analyze and process it. Yet, the technological nature of FinTech products and services also presents opportunities to gather, collect and rely on new information, enabling FIUs to broaden the scope of their intelligence picture. The following is a non-exhaustive list of new data that can be incorporated into the analysis of FIUs: Cryptocurrency wallets/addresses and associated blockchain records
- Various identification numbers, including IMEI, IMSI or SEID numbers, as well as MACaddresses
- Login behaviour and IP data
- Geolocation data[17]
- Identification (e.g., authentication cookies) and information stored on devices.

The graph below illustrates the information survey respondents can currently process digitally. Given the commonality of email addresses in contemporary society, a notable observation is that less than one-third of project participants possess the digital capability to process email addresses and IP data.Perhaps not surprisingly, the ability to analyze geolocation or cookie data is less prevalent.

Figure 8: What type of information can be processed digitally by your FIU?

[17] Geolocation helps identify the actual geographic location of objects, such as mobile devices or any terminals connected to the internet. The term 'geolocation' represents both the process of geographical localization of objects and the actual identified geographic location.



FinTechs commonly record various technical data regarding customer activity, which may be useful for financial intelligence analysis. Yet interestingly, a recent report by the FinTech FinCrime Exchange (FFE) in partnership with the Royal United Services Institute (RUSI), Regulatory DataCorp (RDC) and leaders from 16 FinTech entities reveals that FinTech entities hold data not routinely requested by law enforcement or FIUs, including geolocation data, login behaviour, and device information (FFE, 2021)[18]. In cases where such data is not mandatorily reportable to FIUs under national AML/CFT legislation or is not available via open source, FIU analysts should consider engaging with the FinTech and making a formal request of information for the relevant data when there are sufficient legal grounds to do so.

7.2. What tools are currently in use?

Most FIUs use specific software to receive, integrate and analyze information digitally. However, survey respondents indicated they utilize a range of applications to conduct their analysis of FinTech transactions as their primary analytical tools cannot offer information such as:

- Network analysis and graphical depiction tools
- Blockchain analysis tools
- Domain analysis tools
- Commercial databases and threat feeds
- Open source and social media
- Programming tools for determining trends and extracting critical information from transactional data
- Geographical analysis tools.

As each application offers different functionalities, the survey responses indicate that analysts commonly

[18] FinTech FinCrime Exchange. (2021, February 2). *FinTechs and law enforcement partnerships.* https://static1.squarespace.com/static/57ea58d4cd0f685ecfe1a0c4/t/601d459f3d12c8463a534720/1612531139162/FinTechs+and+Law+Enforcement+partnerships.pdf

usea combination of commercial and open-source intelligence tools depending on case requirements.

Concerning VASPs, some FIU respondents indicated they could not analyze blockchain transactions at all. Over half of the respondents indicated they rely on open-source intelligence information as an alternative means to analyze VA transactions because their internal software does not currently possess the such capability.

The technology linked to virtual assets has moved exponentially, with legislation and regulatory oversight working to catch up. Further, as the uptake of VASP products and services increases,becoming increasingly mainstream, this will intensify international pressure on jurisdictions to legislate, regulate and monitor these in accordance with FATF standards. Consequently, the volume of reported data from the sector will grow.

The need for FIUs to accumulate knowledge, capability, and confidence in understanding how these products work can no longer be ignored. There is a real need for FIUs to actively work to build their understanding of these products and their vulnerabilities to enable them to effectively analyze, investigate and work with their partners to combat the crime. Digital transformation of FIUs is now an established priority, recognized by the Egmont Group and other international bodies such as the FATF[19].

The joint EG-FATF *Digital Transformation Report* recognizes that technology has immense potential to increase the efficiency of AML/CTF workflows and the effectiveness of efforts to combat serious crime. It also provides examples of how FIUs have incorporated different digital tools to assist their operational efforts. These tools range from automation to large datasets, big data, and advanced analytics such as artificial intelligence (AI) and machine learning. The increased capability of FIUs to fight financial crime following such technological uplifts cannot be underestimated, particularly regarding FinTech and virtual assets, where data underpins all financial activity.

7.3. Intelligence value-add of technical information

The project study positively found that most FIUs use email and IP addresses for network analysis. Such analysis allows FIUs to identify links between information in their databases (i.e., transaction reports) and extrinsic databases, including open-source databases and those held by LEAs. FIUs participating in public-private partnerships can further leverage private sector datasets to enrich the intelligence picture by identifying criminal activity that would otherwise have remainedundetected.

FIUs explained the value of virtual assets' addresses to assist analysts in identifying open-source information related to blacklisted wallets, scams, sanctions issues or ransomware cases, such as the Wannacry attack[20]. This enables the analyst to locate other accounts owned by POIs, leads to other victims, and provides opportunities for FIUs to cooperate with domestic and international counterparts to combat thesame criminal organization. Depending on the VA tools used, analysts can obtain information including:

- Name of the wallet's owner.
- First and last date a wallet/address was used.
- The number and value of transactions into and out of the wallet, including associated wallet addresses, for network analysis.
- Observe the time transactions occur, indicating a particular time zone and geolocation.

[19] https://www.egmontgroup.org/en/content/publication-joint-eg-fatf-digital-transformation-report
[20] FATF. (n.d.). How can criminals misuse virtual assets? *Virtual assets*. http://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate)

- Identify cashing in and out points.
- Risk rating associated with a wallet.

These examples provide several avenues for further investigation and analysis to build the intelligence picture.

Several FIUs indicated they also use IP data for geographical analysis. Visualizations can assist with analyzing scenarios spanning a local area, country, global region or worldwide. Though discrepancies inIP data may be considered somewhat unreliable because Internet service providers, VPNs, virtualmachines, and proxy servers can distort the true IP address, it can still prove useful for some purposes. However, survey respondents noted that if address (including IP address) information collected is not validated or geo-coded against any systems, manual conversion to latitude and longitude coordinates maybe required to conduct geographical analysis.

Analysis of information received from FinTech – technical data

CASE STUDY 16:

A suspicious transaction report was filed with the local FIU regarding 91 fraudulent transactions reported by foreign card owners. For each card, the frequency of the debit operations could be as little as a minute. All the transactions were executed using the e-commerce payment module of a company specialized in T-shirt printing.

For each fraudulent transaction, the FIU used the IP address to identity the country from which the transactions presumably took place. However, the analysis showed most of the transactions were executed locally. A total of 18 different credit cards from nine different countries were used.

The investigation revealed the website's owners used the e-commerce payment module to debit foreign bank accounts using stolen card data. Given the heterogeneity of the credit cards' issuing countries, the data was most likely acquired through the dark web.

8. Risks and offence types

Key takeaways

- Offences relating to fraud remain the most reported transactions from FinTech entities often due to their perceived anonymity and remaining inconsistencies around their regulation
- FinTech entities play an important role in detecting money laundering which utilizes virtual assets.
- Traditional criminal organisations may look to utilize FinTech products and services as an alternate to highly regulated sectors.
- Red flag or indicator reports are likely to assist new FinTech entities to establish their transaction monitoring process and programs – with education a key to ensuring the sector reduces the risks of its products and services being utilized for nefarious purposes.
- The sharing of intelligence and cooperation between international FIUs is vital in investigations where perpetrators from multiple jurisdictions are involved.

8.1. Common offence types reported

Offences reported by FinTech entities are wide-ranging, varying from fraud and tax crimes to extortion, illicit drugs, and arms trafficking. Although the sample of responses received is limited, some trends could stillbe observed from the responses.

Fraud is by far the most reported offence type, with some FIUs reporting that this encompasses 100% of STRs received from FinTech entities.

Tax-related offences also appear to be commonly reported, with some FIUs indicating these crimes makeup 45% to 75% of their total STRs received from FinTech entities.

Forgery was the third most common offence observed, with most FIUs reporting this offence type ranging between 10% and 36% of STRs received from the sector.

Illicit trafficking in narcotic drugs and psychotropic substances remains less commonly reported. Among the survey respondents, such STRs accounted for less than 5% of reports received fromthe sector.

Other commonly reported offences included the illegal sale of prohibited products, extortion, and cybercrime-related crimes such as denial-of-service (DoS) attacks and ransomware. The proportion of offences reported by the sector relating to terrorism accounted for 0.1% to 3% of all STRs received from the industry. However, it should be noted that only five FIUs indicated they had received such reports.

The most reported offence type for VASPs was like other FinTech entities, with most STRs relating to fraud. Many FIUs indicated such reports were also linked to identity theft,forgery or providing false ID, which was also reported as a common offence. Some examples of fraud reported to FIUs included Ponzi schemes, romance scams, and offences linked to stolen credit cards.

It appears tax crimes did not feature as prominently in STRS received from VASPs, with only a few jurisdictions reporting they had received tax-related STRs from VASPs compared to other FinTech entities.

One FIU wrote that murder and grievous bodily harm make up a significant proportion of their STRs received from VASPs – with theft and robbery also seeming to be common offences in this jurisdiction.

Conversely, the number of STRs reported by VASPs relating to terrorism financing was more common and ranged between 3% to 9% of the total number of STRs filed by the sector.

8.2. Common typologies/indicators

The most reported typologies appeared again to be fraud – with credit card fraud, identity fraud and scam-related activity being the number one typology reported.

Common typologies seen in reports by FinTech were:

- Use of e-wallets and issues concerning access and ownership of virtual asset wallets
- Transactions using virtual assets
- Involvement of shell companies and bank accounts opened by a third party
- Prominent use of fake IDs or stolen KYC data

The main reasons for suspicion reported by FinTech entities included transactional activity that was unexplained or inconsistent with the subject's known profile (e.g., money mules) and a lack of adequate supporting documentation.

Other red flags raised included requests for payments to be made to unrelated third parties or persons in high-risk jurisdictions, adverse open-source intelligence about the report and requests on the subject from law enforcement agencies.

9. Conclusion

FIUs may grapple with FinTech due to a lack of understanding of the mechanics behind these new technologies and the risks and vulnerabilities of the new payment services and systems.

FATF Recommendation 15 (New Technologies), recently amended to require jurisdictions to regulate VASPs for AML/CFT, requires jurisdictions to address risks arising from new and emerging technologies. The survey results illustrated a varied approach to classifying and regulating FinTechs globally. While some jurisdictions classify these reporting entities based on the type of business, other AML/CFT legislative frameworks adopt a tech-neutral approach to capture the provision of specific services at risk of exploitation for ML/TF. Despite the FATF's recommendations, VASPs and blockchain technology are examples where regulation is not yet in place in many jurisdictions to capture these complex and evolving types of FinTech. In the jurisdictions where such entities are captured by national legislation, the regulatory environment varies from one jurisdiction to another, mainly due to different classifications of each service or product.

Reporting entities, FIUs, AML/CFT regulators, LEAs, and other competent authorities all have a role to play in fighting financial crime. Given the scale of financial crime globally and often limited public resources, it is crucial for FIUs and the private sector to cooperate more closely to respond to ML/TF threats. This is especially important with the financial intelligence received from FinTech entities becoming more sophisticated as their technology becomes more widely used. Effectively analyzing information reported by FinTech requires financial intelligence analysts to maintain a baseline understanding of the services offered by reporting entities and how best to interpret the data submitted by FinTechs in financial intelligence reports. Two examples of best practice occurred via regulatory sandboxes and public-private-partnerships.

Understanding jurisdictional differences and comparing key aspects of national AML/CFT regimes is of considerable value to FIUs seeking to follow international funds flows. It enables a streamlined intelligence information exchange and supports law enforcement efforts.

To mitigate the risk of criminal organizations using unregulated FinTech entities' products or services to avoid global reporting requirements, FIUs must agree on a standard reporting format – including technical data – in partnership with FinTech entities. This allows the broadest possible range of financial information to be collected.

FIUs must ensure FinTech entities fully address the risks of their products and services being misused for criminal purposes by actively reporting suspicious matters and other relevant financialtransactions to one or more FIUs. STRs submitted involving other jurisdictions may require a spontaneousdisclosure to the jurisdiction's FIU. This assists in identifying suspicious activity linked to potential entities of interest and provides a greater understanding of national ML/TF risks.

FIUs should be aware that FinTechs registered in their jurisdiction are likely to be offering services in other jurisdictions, which criminals can use to conduct illicit activity, no matter where they're located. International cooperation between FIUs plays a fundamental role in gathering financial intelligence; therefore, it is recommended that the spontaneous dissemination of information concerning FIUs in other jurisdictions occur. FIUs should obtain conclusive information from FinTechs to ensure effective international cooperation.

Given the speed of the digital world, timely cooperation between FIUs is vital. In jurisdictions where FIUs take a centralized approach to reporting financial transactions, an automated dissemination mechanism is recommended to be set up, so information can be on-shared with relevant FIUs as required.

The technology that underpins FinTech's products and services is evolving at a rapid rate, and FIUs need to adapt swiftly to update and address new and emerging risks. Fostering a culture that values and promotes continuous learning, sharing knowledge and experience can be achieved through engaging with FinTechs to understand how they operate and enhancing capabilities through digital transformation.

Red flags or indicator reports can help newly established FinTech entities set up their transaction monitoring processes and programs, ensuring the sector reduces the risks of its products and services being used for criminal purposes.