Fintechs and Law Enforcement partnerships

FFE Expert Working Group

February 2021

POWERED BY

FINTRAIL

RUSI
www.rusi.org

rdc
Smarter Screening

FINTECH
FINCRIME
EXCHANGE

PSA

- public service announcement -

This working group made it clear that finding the right contact or information can be tricky.

Please do not hesitate to reach out to the FFE secretariat at ffe_admin@fintrail.co.uk if you need help making contact on an important law enforcement matter—this goes for law enforcement, FIUs and FinTechs.

We work hard to make sure our network is used to fight financial crime!

Introduction

How we all can best partner with law enforcement isn't always obvious, even though it's obviously important. As an industry, FinTechs still struggle for representation in public-private partnership forums. And we've heard from FFE members before that it's often not clear what they can share, and with who, or that—conversely—it's not clear to law enforcement how FinTech can help.

Leaders from 16 FinTechs joined the FFE, in partnership with RDC and RUSI, for a conversation on the industry's pain points—we hope you find the highlights and survey results useful in benchmarking your own approach.

Contributors include experts from Coinbase, Countingup, Gemini, Monzo, Paxos, RDC, Revolut, Starling Bank, Stripe, TransferWise, Varo Money and more—and, of course, each shared their own views as industry leaders and not those of their employers.

16
FinTechs

6
Industries

4
Regions

The FFE's expert working groups bring together senior leaders from across our industry to discuss common trends, challenges and best practices in a Chatham House Rule setting.

Benchmarking and best practices

Below are some common challenges and best practices highlighted by the roundtable's participating FinTechs, many of which mirror approaches taken by their more traditional peers.

Receiving requests

- Larger FinTechs may have a dedicated team or function for law enforcement engagement and responses
- Most felt that an MLRO was not the ideal PoC; investigations and reporting teams will have more detail in order to respond to law enforcement
- Security practices are common but not a constant: when you're contacted by someone claiming to be law enforcement, be sure your financial crime team adopts your company's protocols for validating a third party contact
- Also consider whether your customer service teams know how to handle inbound requests from law enforcement
- Few teams have 24/7 investigations and reporting coverage, but some may ensure more timely coverage in response to emergencies
- Court orders and other requests are often somewhat limited in what information they request–FinTechs often hold more data than what is requested

50%

hear from law enforcement several times a week

SARs

- Most FinTechs now include a brief summary of their product and business model at the beginning of their SAR narratives
- No FinTechs reported using SARs or STRs as a means of passing information to law enforcement without a money laundering suspicion

SAR Feedback

- This is not about a pat on the back, or cookie cutter training on how SARs are used
- The vast majority of FinTechs are versed in the fine art of SARs
- Participants felt that data points on SAR effectiveness would help us tweak our models, rules and processes
- Knowing how SARs are used also helps to tell a story for boards of directors (although FinTechs also realise that successful prosecution is rare)
- There's consistent confusion around what data is held by which institution
- Conversely, FinTechs hold data that isn't routinely requested: the most commonly reported were geolocation, login behaviour, and device information

40%

aren't always clear on what can be legally shared

Asset Freezing

- These can technically only be issued against a deposit account, so that excludes many FinTechs—instead, the order needs to be issued to the bank that holds funds on behalf of the FinTech's customers (some FinTechs have reported issues with freezing orders being served on them, rather than their deposit-holding partner, which can slow down the asset freezing and repatriation process)
- FinTechs often commingle customer funds in accounts (typically, by currency), so a new account specifically for the order is often necessary
- Balances often change, because of chargebacks or refunds, for example, from when a SAR was filed to the issuance of a freezing order
- If funds frozen need to be moved to a new account as part of an asset freezing order, include any law enforcement inquiry or account number information in the consent SAR

25%

cannot accept an asset freezing order

Stay Open Requests

- FinTechs felt more information on the reason for stay-open requests would allow them to apply appropriate controls to the account(s)
- Participants sometimes employ a proactive approach to keeping accounts open and gathering intel during high sensitivity investigations e.g. human trafficking
- Make sure a time period is set, and check back in with law enforcement for an update before it comes to a close

Training

- Some FinTechs are proactively offering training opportunities to law enforcement
- Training your FIU is not the same as training law enforcement—FinTechs should not assume there is a trickle-down effect
- Some participants provide "fact sheets" and guides on how to submit information requests to them—publicly available ones were reported to work reasonably well.

25%

have provided training for law enforcement

Information sharing forums

We all know that some combination of the Ps (public/private/partnership) is best. But, as one participant shared, it can feel like the best forums are those that are private or even a secret.

And most members shared concerns about exclusion if information-sharing on specific "bad actors" becomes a thing.

58%

struggle to get traction with industry groups

As one participant shared wryly, on the quality of information sharing forums:

"The more secretive, the better"

Our members participate in forums that include:

- Publicised law-enforcement led projects or networks (EMMA, CHS, Black Wallet)
- Closed-door law enforcement working groups(for ex., facilitated by the FBI)
- FIU-led groups (NCA's SAR Working Groups, the US BSAAG)
- Egmont Group's Information Exchange Working Groups (see the CSAE project as an example)
- Industry groups (EMA, UK Finance, ACAMS chapters, and more)

Many are invite-only and some are paid. But exclusivity does not help in the fight against financial crime.

We'd urge FinTechs to invite each other, or share what you're learning (within the confines of Chatham House rules, SAR confidentiality, etc., of course!)

And we'd urge information sharing to take place via industry groups and networks that can help law enforcement to distribute requests quickly.

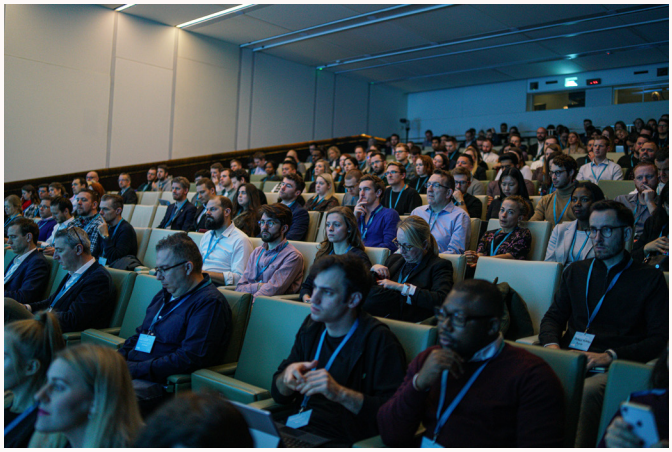
FINTECH
FINCRIME
EXCHANGE

The FFE brings together a global network of FinTechs to collaborate on best practices in financial crime risk management. By sharing information on criminal typologies and controls, members help to strengthen the sector's ability to detect and counter the global threat of financial crime.

The FFE was established in January 2017 by FINTRAIL and the Royal United Services Institute (RUSI), and its members meet monthly to discuss these topics and share information and insight on an ongoing basis. The FFE produces quarterly white papers on financial crime topics relevant to its members and stakeholders in law enforcement, the government and the financial services sector.

The global scope of financial crime and the shared threats faced by all major FinTech hubs particularly underscore the need for a global FFE network, which will give its members not only a trusted place to exchange information, but also access to an increasingly far-reaching network of resources and perspectives. www.fintrail.co.uk/ffe

RDC is proud sponsor of the FFE as part of efforts to help improve collaboration within the FinTech community and anti-financial crime space. www.rdc.com



Thank You

www.fintrail.com/FFE

FINTECH
FINCRIME
EXCHANGE