Crypto Industry Insights and Good Practice

FFE Expert Working Group

June 2021

FINTRAIL

ComplyAdvantage

jumio

FINTECH FINCRIME EXCHANGE

Introduction

Leaders from 16 crypto companies joined the FFE, in partnership with Comply Advantage and Jumio, for a conversation on the industry's pain points and common misconceptions—we hope you find the highlights and survey results useful in benchmarking your own approach.

Contributors include experts from Binance, Bitfinex, bitFlyer, bit2me, Coinbase, Coinmerce, DigitalMint, Elliptic, Luno, Paxful, Zumo, stealth-mode startups and more—and, of course, each shared their own views as industry leaders and not those of their employers.

16

Crypto companies

have worked in fincrime outside of the crypto industry.

16 members of the crypto industry across Europe + USA, but with global reach. Attendees included individuals from P2P marketplaces, bitcoin ATMs, and exchanges. Of our respondents, nearly 90% have worked in fincrime outside of the crypto industry.

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.

Areas for clarification

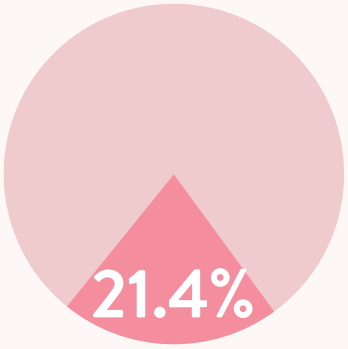
The largest area of clarification was, unsurprisingly, around implementing the Travel Rule. Discussion focused around whether the 'bigger' players in the industry would pave the way for this. Many attendees noted that there is unlikely to be one solution: instead, several software integrations will be needed to comply with the travel rule and serve a broad set of customers. It was noted that it is **crucial** that software solutions are interoperable amongst each other and other exchanges.

Benchmarking and best practices

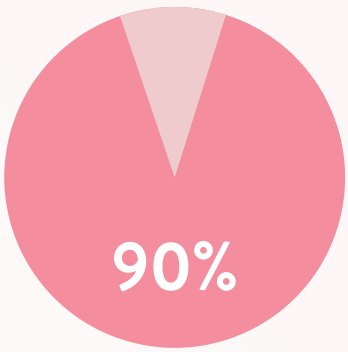
Below are some common challenges and best practices highlighted by the roundtable's participating crypto companies.

Hiring

- Many firms noted that they would prefer someone with experience in fincrime over crypto, if they had to choose.
- That said, regulators are challenging senior AFC hires on their crypto knowledge. Be ready to brush up fast!
- Most firms consider diversity and inclusion an important part of hiring. Several participating firms reported that 40-50% of their teams were female.
- The industry often looks to ex-law enforcement as a hiring pool—this may cause an inherited bias, with areas of law enforcement potentially less diverse.
- Senior AFC hires are expected to advocate for the firm and be active in the industry. Networks, existing connections (including with potential banking partners) and public speaking skills are especially important.
- The group largely felt they had more internal support, including from their board, for fincrime than teams at banks or even fintechs.



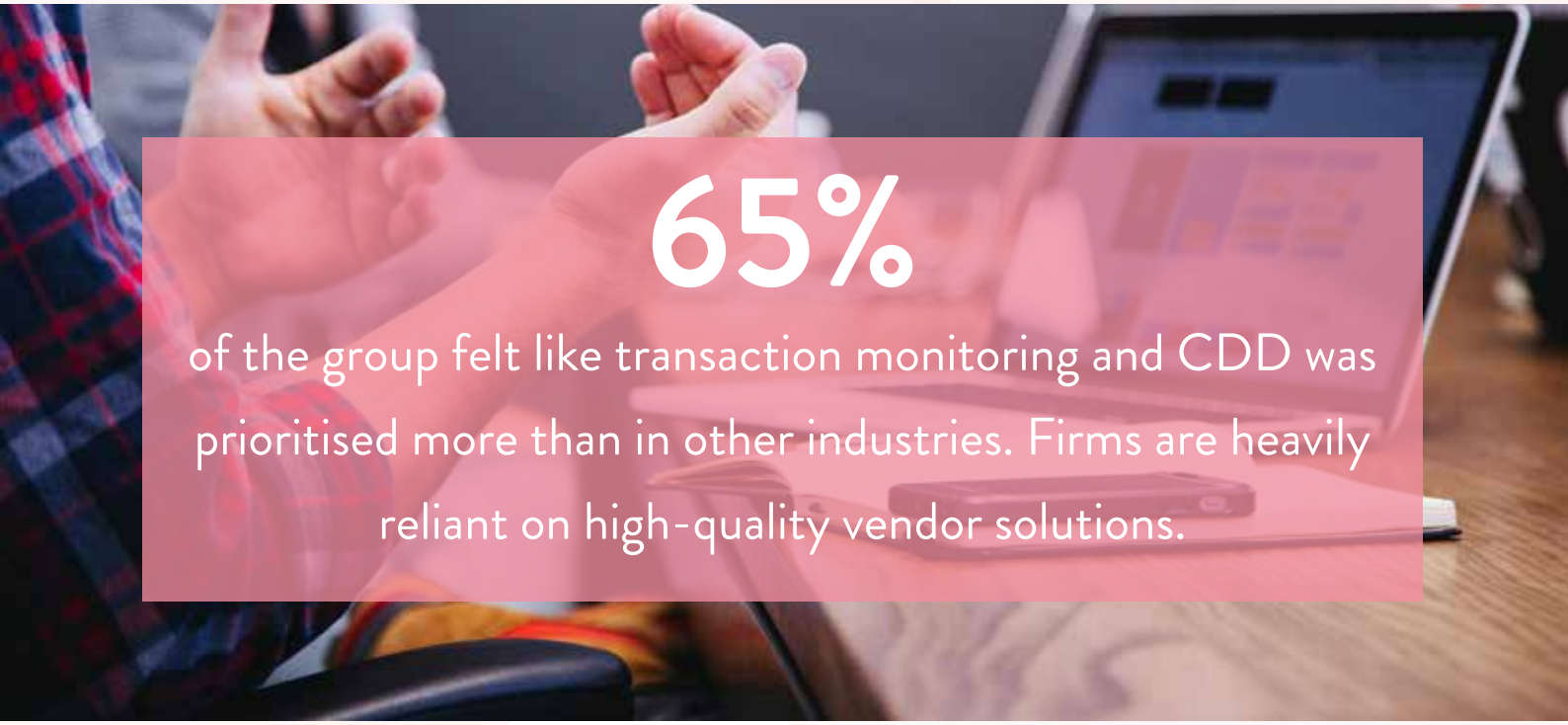
Do not feel crypto experience is required for Fincrime hires



Nearly 90% of Fincrime hires had previously worked in a Fincrime role outside of the crypto industry

Onboarding

- CDD and enhanced due diligence were the group's highest priority controls.
- In general, firms are applying more controls, not less—out of 25 controls, the group considered simplified due diligence to be the lowest priority.
- That said, firms feel that crypto customers expect a particularly friction-free onboarding experience.
- If onboarding takes too long, customers are quick to move their business to a competitor. Bitcoin ATM providers are particularly affected by this.
- Once onboarded, firms are struggling with how much to protect customers from themselves—for example, when they are interacting with bad addresses outside of the platform.



65%

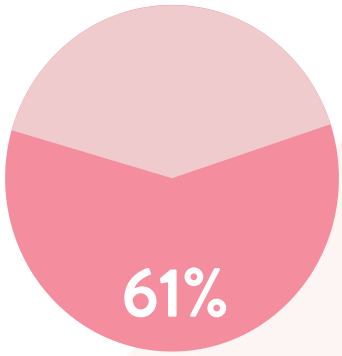
of the group felt like transaction monitoring and CDD was prioritised more than in other industries. Firms are heavily reliant on high-quality vendor solutions.

Travel rule

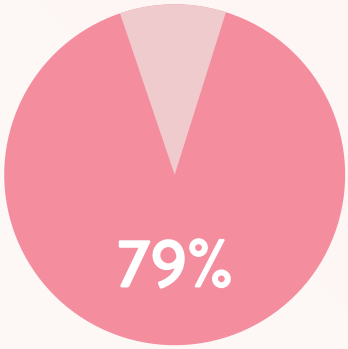
- Firms are concerned about the need for many vendor solutions—to send a payment, the firm will first need to be integrated with the vendor of the beneficiary institution.
- There may also be a possibility of using existing technologies to solve the problem (e.g. the use of digital identities). For global firms, that would still mean integrations with numerous digital identity systems.
- The group noted that the industry may wait for the larger firms to play their cards and show their solutions, with smaller players following suit.

Risk assessment & banking partner relationships

- Many, but not all, firms are assessing the risk of coins they support.
- FinCEN is increasingly critical of those that do not risk assess coins.
- This risk assessment is typically simple, considering whether:
  - the coin is traceable;
  - the firm's current transaction monitoring vendor(s) provide coverage for the coin.
- A risk-based approach is used where risks are higher—for example, exchanges that list privacy coins reported very tight controls on transaction limits and a thorough due diligence process for customers opting in.
- A platform's coin portfolio is usually available for all customers. In other words, a high risk customer isn't typically restricted to lower-risk coins.
- Incidents of financial crime were associated with the highest market-cap coins and rarely with privacy coins, according to the group's own experiences.
- Some financial partners restrict exchanges to a pre-approved list of coins, or won't service firms that deal in privacy coins.
- Some regulators expect updates on each new coin added (considered a new product or material product change).
- The industry would prefer a coin-neutral approach that made restrictions or recommendations based on risks vs. specific coins. The list of available assets changes more frequently than many banks would be able to keep up with.



Felt that scaling was a bigger challenge than the risk of their product

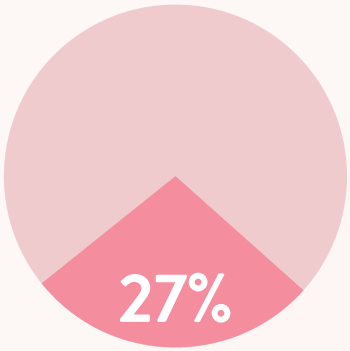


Felt that, relative to FinTechs, they had equal or better opportunities to engage with great financial partners

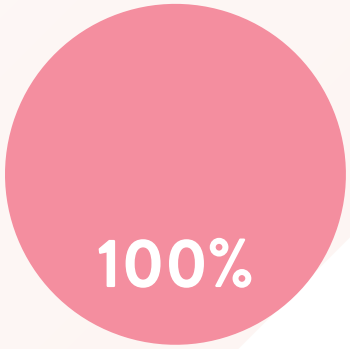
"Just because it works for traditional banking, doesn't mean it needs to work the same way for crypto companies"

"We are not all the same"

- Different types of crypto companies often get bunched together with each other.
- As an example, not all companies are exchanges, and P2P marketplaces and bitcoin ATM companies are not all as rogue as they're reputed to be.
- Crypto companies are also not necessarily FinTechs or even feel that they are disruptors: exchanges have been around for a long time, for example.
- The industry is keen to set best practices, even if that means going beyond regulatory requirements.
- Beyond differences in models and products, there are also increasingly mature players: 57% of respondents operate a 3LOD model, for example.



Felt that recent regulation does not effectively mitigate their product's risk.



Felt that increased regulation has boosted the industry's reputation

Regulator and LEA relationships

- Firms are spending a lot of time on education, especially with law enforcement and regulators.
- Working groups and committees are helpful, but there are lots.
- Firms often have to attend forums on AFC, on crypto, on crypto and AFC, and similar iterations focused on their specific product area within crypto.
- This is in addition to groups like the Crypto Defence Alliance, which helps firms share suspicious addresses with other crypto firms.
- While it's great news that crypto firms are given a seat at the table, and invited to events such as the FATF's Private Sector Consultative Forum, many would like to be included earlier in the regulatory drafting process. Consultation responses do not often feel effective.
- More guidance is also welcome, but generic guidance (as has been seen with FinTech) won't necessarily make sense across all crypto products.
- A specific control that could use revisiting is SAR/UTR/STR filing, with forms not appropriate for the information crypto companies need to report.

"We have to do it properly or we're out of business."

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.

Comply Advantage

ComplyAdvantage is the financial industry's leading source of AI-driven financial crime risk data and detection technology. ComplyAdvantage's mission is to neutralize the risk of money laundering, terrorist financing, corruption, and other financial crime. More than 500 enterprises in 75 countries rely on ComplyAdvantage to understand the risk of who they're doing business with through the world's only global, real-time database of people and companies. The company actively identifies tens of thousands of risk events from millions of structured and unstructured data points every single day. ComplyAdvantage has four global hubs located in New York, London, Singapore and Cluj-Napoca and is backed by Ontario Teachers', Index Ventures and Balderton Capital.

jumio

When identity matters, trust Jumio. Jumio's mission is to make the internet a safer place by protecting the ecosystems of businesses through a unified, end-to-end identity verification and eKYC platform. The Jumio KYX Platform offers a range of identity proofing and AML services to accurately establish, maintain and reassert trust from account opening to ongoing transaction monitoring.Leveraging advanced technology including AI, biometrics, machine learning, liveness detection and automation, Jumio helps organizations fight fraud and financial crime, onboard good customers faster and meet regulatory compliance including KYC, AML and GDPR. Jumio has verified more than 300 million identities issued by over 200 countries and territories from real-time web and mobile transactions. Jumio's solutions are used by leading companies in the financial services, sharing economy, digital currency, retail, travel and online gaming sectors. Based in Palo Alto, Jumio operates globally with offices in North America, Latin America, Europe and Asia Pacific and has been the recipient of numerous awards for innovation.

Thank You

www.fintrail.com/FFE

FINTRAIL

Comply Advantage

jumio

FINTECH FINCRIME EXCHANGE