FinTech approaches to sanctions regimes

FFE Expert Working Group

September 2020

POWERED BY

FINTRAIL

RUSI
www.rusi.org

rdc
Smarter Screening

FINTECH
FINCRIME
EXCHANGE

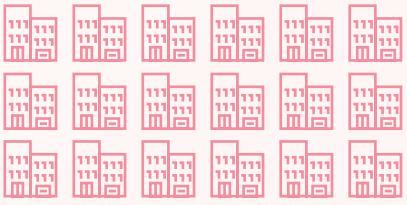
Introduction

In absence of guidance on what "good" looks like, we set out to benchmark the industry's approach to sanctions compliance and identify where FinTechs most want clarity—because, of course, one of the risks of a risk-based approach is that you may be the only one taking it.

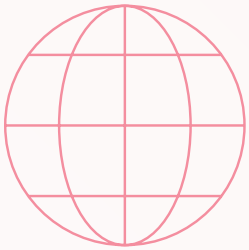
Leaders from 18 FinTechs joined the FFE, in partnership with RDC and RUSI, for a conversation on the industry's pain points—we hope you find the highlights and survey results useful in benchmarking your own approach.

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.

18 FinTechs



8 Industries



4 Regions

Contributors include experts from ClearBank, CountingUp, MarketFinance, Modulr, Revolut, Stripe, WorldRemit and more—and of course, each shared their own views as industry leaders and not those of their employers.

Areas for clarification

Although FinTechs broadly feel like they've been pointed in the right direction, there are still several areas where clarification on sanctions is needed—if not from regulators, then from peers.

60%

feel that governments provide sufficient guidance

Screening transactions, vs. customers

Roles and responsibilities

Examples of risk-based approach

MI and Board reporting expectations

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. In fact, the FinTechs we spoke with can be more risk averse than their peers (see List Screening section for more).

This *may* be because they're dependent on strategic relationships with global banking partners, investors, and regulators, and they're also typically not backed by capital that can sustain regulatory fines or reputational fallout.

Risk assessment

- Many firms are working to develop sanctions-specific risk assessments, while customer risk ratings still typically combine sanctions with other financial crimes risks
- FinTechs are focused on ensuring the risk assessment is nuanced enough to highlight sanctions-specific risk and controls and feel this is critical for employing a risk-based approach
- Payment methods used for transactions can provide some assurance to FinTechs, but only when backed by an assessment of the risk of each method (this is really time intensive, though)

60%

screen against lists of close associates or relatives of sanctioned persons

Governance

- Regulation and guidance doesn't explicitly outline what escalations to, or conversations with, the board are expected on the topic of the firm's sanctions program
- This is not necessarily problematic, but differs from AML regimes and can make getting an audience from board or C-suite trickier
- Reporting on the sanctions program is often limited to breaches, but FinTechs are encouraging increased engagement from their board and C-suite via reporting on customer impact, regulatory developments and efficiency gains
- FinTechs are also increasingly getting board approval for sanctions-specific policies, vs. just broader AML policies

29%

conduct a standalone sanctions risk assessment

... with a significant percentage working to produce one

Scale and the risk-based approach

- As FinTechs scale, and operational work increases, a risk-based approach becomes more critical
- Domestic transactions aren't automatically treated as lower risk by the FinTechs we spoke to
- Complex sanctions investigations require domain expertise--smaller teams struggle with supporting this cost, whether it's for an in-house expert or external counsel
- Even if a FinTech doesn't yet have two or three lines of defense, business and product teams should still be educated on sanctions risk

Scale and the risk-based approach, cont.

- Sanctions experts should be included in the product development process
- It's difficult to mitigate the risk of customers with complex ownership via automated controls, with some FinTechs reporting that many haven't built large enough portfolios of these customer types to invest in said automated controls
- Regulators are expecting to see breach reporting procedures in place long before a breach

0%

use exact matching when screening customers

List management

- Few FinTechs screen against all lists offered by their list providers
- FinTechs are using change logs and list maintenance documentation to evidence how they initially select lists and update them over time

List screening

- FinTechs have the ability to apply advanced, technology-enhanced risk based systems to screen customers and transactions but, due to lack of clarity on how to document and defend a risk-based approach, most opt for a risk-averse approach
- Match thresholds are set as low as 70%, more conservatively than industry standards closer to 85%-90%, and FinTechs we spoke with are more conservative with customer screening than transaction screening
- Exact matching may be used when screening transactions (specifically, for the payment reference field) but not when screening customers
- Real-time screening is enabled by time-zone distributed analyst teams to reduce impact on customers

Customer vs. transaction screening

- Incoming or outbound transactions are screened at a FinTech's discretion, with the majority opting for some level of controls on both
- These same transactions are typically also screened by several other institutions, although each institution may only have some of the key elements needed for efficient screening and reviews
- Some regulators have hinted at becoming more prescriptive by enforcing screening on certain types of transactions, a position this forum would not be in support of

Roles and responsibilities

It's often falling on FinTechs, vs. regulators, to provide clarification to their customers on the customer's own responsibilities under sanctions regimes. This highlights that sanctions compliance is poorly understood outside of regulated sectors.

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 underscores 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 prevents infiltration of the world's financial systems by providing intelligent, automated customer screening solutions to more than 1,000 financial institutions and FinTech companies around the world. RDC is proud sponsor of the FFE as part of its efforts to help improve collaboration within the FinTech community and anti-financial crime space. www.rdc.com.

Thank You

www.fintrail.com/FFE

RUSI
www.rusi.org

rdc
Smarter Screening

FINTECH
FINCRIME
EXCHANGE