The FinTech sector provides a broad set of financial services and has evolved significantly in a relatively short period of time. However, it has had less of a voice in influencing regulatory requirements and often, rules written for traditional retail banking are not always a good fit in the FinTech space. Exiger hosted its first roundtable event under Chatham House Rules for Heads of Financial Crime Compliance at a range of FinTech firms to discuss recent regulatory developments in this area and the key challenges they face in designing and implementing appropriate and sustainable Financial Crime Compliance Programmes.

Exiger outlined some important insights from the Financial Conduct Authority’s 2020 Sector Views illustrating the FCA’s concerns around safeguarding consumers and the sustainability of financial crime controls frameworks given the speed of innovation and fast-paced changes that occur in FinTech firms. Exiger shared their views and experiences from the advisory work we have carried out with FinTechs, helping to elucidate some key regulatory areas of concern:

1. Focus on customer experience & financial inclusion
2. Weak CDD/EDD and customer risk assessment that do not consider all risk factors
3. Inadequate transaction monitoring leading to increased risk of bad actors in customer base
4. Transaction monitoring scenarios that focus more on fraud detection and less on ML
5. Large FCC operational team in 1LOD with a less mature 2LOD oversight capability
6. Lack of adequate FCC resources / expertise
7. Ineffective policies and procedures
8. Insufficient QC/QA processes
9. No effective business-wide anti-money laundering risk assessment
10. Blurring of 1LOD and 2LOD
11. Lack of effective oversight of AML activities outsourced to third parties
12. Concerns over consumer harm if firms fail

Collapse of Wirecard sparked fears of challengers having less robust processes than incumbents

FOOD FOR THOUGHT

Are Financial Crime Compliance and customer experience mutually exclusive for Fintechs?

SCENE @ EXIGER’S FINTECH FINANCIAL CRIME ROUNDTABLE
HEARD @ VIRTUAL EVENT WITH HEADS OF FINANCIAL CRIME COMPLIANCE AT FINTECH FIRMS
Participants reflected on how these concerns could be addressed sharing where applicable examples of how they had approached these areas within the FCC programmes at their firms. Further roundtable discussion took place around the key challenges group members were facing and their top focus areas.

**Key Takeaways**

**Finding the Balance for Transaction Monitoring Systems.** Most FinTechs start out with an in-house built fraud detection system and build an anti-money laundering detection system on top as they evolve. However, achieving effective systems in both areas and system tuning has proven challenging.

- Because of the highly specific products and services provided by FinTechs, off-the-shelf products have not catered well to their needs, as they have tended to be more targeted towards traditional banking environments.
- In-house TM systems are often built by the same product teams which develop the customer experience platform. This can lead to a lack of expertise in the typologies and scenarios necessary to create effective Financial Crimes monitoring, in particular as it relates to money laundering. Further, this dynamic can lead to an inappropriate balance between creating a customer centric environment vs one which prevents or detects crime but could lead to poor customer experience.
- As the developers for internal financial crimes systems are often shared resources also working on business expansion tools, financial crime controls may be deprioritized. However, if done well there is value to be gained from building systems in-house as these can be tailored to relevant risks, but it requires bridging of intra-company silos and making best use of data in an effective way to be successful.
- One firm’s focus was to separate fraud and AML systems and develop a comprehensive TM coverage assessment across its jurisdictions. This resulted in a comprehensive AML typology library, leveraging public sources (such as regulatory publications) and creating a well-documented audit trail of the risks considered, how mitigated or risk accepted.
- Analysing historic SARs is also a great way to understand and update AML typologies.

**Improving Customer Risk Scoring.** Due to their fast international expansion, FinTechs tend to outgrow the risk scoring models original built for a smaller customer base in lower-risk jurisdictions. Models need to be updated to generate good insights and flag truly high-risk customers.

**Developing a Risk Appetite Statement.** A risk appetite statement is a powerful tool to help delineate how the second line of defence acts in accordance with the senior management of the firm’s risk appetite. Risk appetite statements can be particularly useful when faced with these challenges around the three lines of defence model:

- The first line of defence sees itself as a purely operational function Although they bring strong product and customer service experience, some senior executives at FinTechs did not previously operate in a regulated environment and can be slower to grasp the gravity of failing to implement an effective compliance framework.
- Unlike traditional FIs, FinTechs seem to “promote” into FCC roles with individuals from within the organization rather than selecting those with established financial crime experience. This results in many FinTechs having to react to regulatory scrutiny, only growing their FCC capabilities when facing some regulatory pressure (i.e. too late).
An Effective Governance Framework with committee representation across the first and second lines of defence can be a complementary tool for the practical application of the risk appetite statement on an ongoing basis.

Approaches to Account Freezing. While some FinTechs have different levels of account restrictions depending on the customer type and its responsiveness during a remediation or refresh process, other firms are able to use their business model to incentivise the customer to provide outstanding information. Although participating firms developed different ways of dealing with restrictions on accounts, they were in agreement on a couple of points.

- It’s important to find balance in terms of what is communicated to the customer during a temporary lock and to understand the basis of tipping off (participants discussed the topic of tipping off, with a general view that this risk was often over emphasized at the cost of taking other actions).
- Customer interaction occurs primarily through the CRM interface but other channels can be deployed if the customer is unresponsive.

Working through Covid-19. The pandemic presented a number of challenges, particularly around TM typologies and outsourcing.

- Firms had to be agile to create new scenarios for Covid-type typologies and work through alert spikes generated due to changes in the type of account activity, particularly for those clients in sectors significantly impacted by the lockdown rules.
- This was also an opportunity to test system resiliency, as in some instances, transaction volumes increased by over 80%.
- Teams handling customer data also faced challenges, particularly in relation to third party vendors in other jurisdictions that were required to work from home.