Payment Firms Under the Microscope – Do Your Financial Crime Controls Stand Up to Regulatory Scrutiny?

European and UK regulators are increasingly focusing on the financial crime risks within the payments sector. Recent activity aimed at payments institutions has included:

- the Financial Conduct Authority's ("FCA") "Dear CEO" Letter[1] published in March;
- the FCA's payments webinar;[2] and
- a European Banking Authority ("EBA") report on money laundering/terrorist financing ("ML/TF") risks published in June.[3]

All of these call on payments institutions, electronic money institutions ("EMIs") and registered account informational service providers to do more to protect customers' funds and the integrity of the financial system.

The regulators' recent publications and industry engagements suggest a shift in their supervisory approach, which is now more active and increasingly focussed on financial services players beyond banks (which have largely put their houses in order).

The FCA's message around the reduction and prevention of financial crime is consistent with their 2022-2025 strategy and the recently published 2023-2024 business plan.[4] They highlight the growing body of evidence that financial crime can be, and indeed is, perpetrated through the payments sector. The ability of payment firms ("PFs") to provide bank-like services, their willingness to service high-risk customers, and weaknesses in firms' systems and controls are making PFs a prime target for bad actors and criminals.

Recognising this, in its letter the FCA sets out two priorities for PFs:

Priority 1: Preventing Money Laundering and Sanction Evasion

Firms must have money laundering and sanctions controls in place that are effective and proportionate to the nature, type and scale of their business. A review of the Office of Financial Sanctions Implementation's fines from 2021 and 2022 highlights that too often PFs rely on other regulated institutions' sanctions and payment screening and do not independently screen inbound transactions. When establishing their sanctions controls, PFs must ensure that their systems and measures can effectively identify and manage the specific sanctions exposure and risks associated with their customers and business activities.

Priority 2: Preventing Fraud

The FCA is concerned that the current cost-of-living crisis will lead to an increase in fraudulent activities, similar to those seen during the Covid-19 pandemic. As such, the regulator expects firms to reassess their fraud risks and address these through adequate risk appetite statements, policies and procedures, and appropriate due diligence and monitoring measures that prevent fraudulent transactions.

Similarly, the EBA's report highlights ML/TF risks within the sector, including those aligned with:

— the high-risk customer base;

— the cross-border nature of executed transactions;

— new technologies, such as the use of remote onboarding, or the use of artificial intelligence for control measures;

— the use of agent networks and the lack of appropriate oversight; and

— the risks relating to outsourcing arrangements many PFs use to access specialised services.

In addition, new products such as the issuance of virtual International Bank Account Numbers ("virtual IBANs") are seen as an emerging risk to the sector. Virtual IBANs are used to reroute incoming payments to a regular IBAN linked to a physical bank account, therefore obscuring the geographical location of the underlying account.

The EBA also points to weaknesses identified in the authority's biennial risk assessment review, which highlighted poor anti-money laundering and countering the financing of terrorism ("AML/CFT") systems and controls across the sector. More notably, these included:

— poor understanding and management of ML/TF risks;

— weak governance procedures;

— insufficient suspicious activity monitoring and reporting; and

— poor controls, especially in relation to ongoing monitoring and screening of customers and transactions.

Drawing on FTI Consulting's experience of working across the payments sector, we regularly see firms having difficulties with:

Applying Proportionate Financial Crime Controls To Address Increased Risk

PFs' unique selling points are their speed, efficiency and enhanced processing capabilities. They typically process large numbers of lower-value payments and so many have a greater appetite for serving high-risk customers than do banks or other financial institutions. However, PFs' financial crime controls are often not calibrated to match their willingness to embrace riskier clients. They're driven by cost-efficiency pressures and often lack guidance on what a compliant anti-financial controls programme should look like. As a result, PFs often implement generic financial crime target operating models and "lift and shift" frameworks from institutions with very different business models and risk appetites.

PFs are highly digitally enabled, which is both an opportunity and a threat when it comes to defining financial crime controls. On the one hand, controls must be highly automated to deliver a positive customer experience aligned with user expectations. However, if not appropriately tailored, this digital advancement can be targeted by increasingly sophisticated bad actors. We have witnessed how some synthetic identity fraud techniques are more prevalent in the payments environment, where merchants frequently take the biggest hit.

For example, multiple accounts are opened under different, often made-up names, which are all controlled by one fraudster. This allows fraudsters to process more transactions than they would normally be able to do under one name, without triggering any transaction monitoring thresholds. Individuals whose identities or bank details have been used to commit the fraud may be able to obtain a refund, but the merchants processing those payments are left with unrecovered product and shipping costs. PFs that facilitate this activity ultimately take responsibility for the compromised controls environment and allowing fraudulent activities.

PFs should consider enhancing their controls with regard to merchants as opposed to the merchants' customers. With limited visibility of each merchant's customer characteristics, if the PF performs their due diligence directly on the merchants, they'll have a more detailed overview of what the underlying customer activity may look like. This will enable better financial crime detection. In the previous example, this could come down to enquiring whether the merchant uses a two-factor authentication process and/or checking whether one payment type is linked to multiple accounts instead of just one. This would help detect instances of account takeovers as well as synthetic identity fraud attempts where bad actors try to open new accounts with the PFs.

Scaling Up Businesses in a Safe Environment by Proactively Enhancing Existing Financial Crime Controls

In recent years, PFs have recorded more rapid growth than banks. For example, e-commerce boomed during the pandemic, as did digital payments and the firms that facilitate them. Suddenly finding themselves processing significantly higher volumes of transactions, many EMIs discovered their existing systems and controls were no longer fit for purpose and were unable to cope. This

resulted in backlogs, which were resolved by "waving through" Know Your Customer checks or batch closing alerts.

This growth comes not only from the volumes of customers and transactions but also through the expansion of merchants' business models, such as servicing end customers in high-risk jurisdictions or facilitating payments in more high-risk products like cryptocurrencies through a merchant's website. It is important for PFs to be aware of how their customers are changing and the resulting financial crime risks that they can be exposed to.

It is important that as they expand, PFs continue to regularly assess their business-wide risks, develop robust new product approval governance, and enhance their management information capabilities to identify shifts in customer behaviours and adjust their controls accordingly.

Enhancing Scrutiny of Third-Party Vendors To Ensure Effectiveness and Compliance

PFs often outsource customer due diligence processes (specifically identity and verification, politically exposed persons, sanctions, and adverse media screening) to third-party vendors. Therefore, vendors need to understand the underlying methodology used by the PF. For example, they should be able to explain fuzzy logic rules within a system they use regardless of the outsourcing arrangements and the rationale for discounting matches. If this doesn't happen, the firm's knowledge of their customers is weaker and their ability to provide the explanations required for any internal or external assurance reviews and regulatory inspections is undermined.

It is key that PFs assume full accountability for their customers, even when they operate in an environment full of third-party vendors and outsourcing arrangements. Both the FCA Handbook and the Joint Money Laundering Steering Group's guidelines are clear — a regulated firm cannot contract out of its regulatory responsibilities and is ultimately responsible for the controls undertaken on its behalf by a third-party vendor. To ensure accountability, firms must create robust reliance mechanisms that include regular effectiveness reviews to ensure the appropriateness of the controls operated on their behalf. This can sometimes result in firms requesting information directly from the outsourcer about the underlying customers' due diligence, and firms should also, at a minimum, fully understand third parties' policies and have a view of when and to what extent they change.

We work with several payment services firms and support them in developing and optimising their financial crime controls.

To find out more about our financial crime capabilities and how we may assist you in responding to individual business needs, please get in touch.

Endnotes

1 https://www.fca.org.uk/publication/correspondence/priorities-payments-firms-portfolio-letter-2023.pdf

2 https://webinars.fca.org.uk/webinars

3 https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2023/1056453/Report%20on%20ML%20TF%20risks%20associated%20with%20payment%20institutions.pdf

4 https://www.fca.org.uk/publications/business-plans/2023-24

CRAIG MCLEOD
Senior Managing Director
+44 20 3727 1000
craig.mcleod@fticonsulting.com

RICHARD GRINT
Senior Managing Director
+45 70 70 73 83
richard.grint@fticonsulting.com

BEA HRUBOSOVA
Director
+44 20 3077 0210
bea.hrubosova@fticonsulting.com