

Insights

FCA'S THINLY VEILED WARNING TO CHALLENGER AND TRADITIONAL RETAIL BANKS OVER FINANCIAL CRIME RISK

Apr 25, 2022

SUMMARY

On 22 April 2022, the FCA published the findings of its review of financial crime controls at six relatively new and primarily digital challenger banks that all offer similar products to traditional retail banks. These six banks represent over 50% of the relevant challenger firms and the FCA's review covered over 8 million customers. The scope is potentially much wider than this would suggest: the FCA expressed its view that *"there [are] limited differences in the inherent financial crime risks faced by challenger banks, compared with traditional retail banks."* This makes the review essential reading for anyone involved in mitigating the risk of financial crime in retail banking. Here are our key take away points.

The UK's 2020 National Risk Assessment of Money Laundering and Terrorist Financing (NRA) was the catalyst for the FCA's review. It highlighted the risk that criminals may be attracted to the fast on-boarding process advertised by challenger banks and that opening accounts very quickly could lead to insufficient information being gathered to identify high risk customers. The FCA wanted to make its own assessment of the financial crime risks involved. As such, the review provides useful guidance as to examples of good practice applicable not just to challenger banks but traditional banks as well. More importantly, it is clear the regulator expects more established banks to take note of what it has found.

It's important to bear in mind the prevailing context in which this report has been published. To that end, there are three preliminary points to bear in mind before delving into the detail of the report.

- A. The review was conducted before the situation in Ukraine crystallised and the subsequent expansion in sanctions in response. However, the FCA noted that *"the main financial crime and money laundering controls [it] assessed equally apply to firms' management of sanctions, specifically in respect of the risk that firms are utilised for sanctions evasion."*

- B. The FCA remains committed to prosecuting money laundering and fraud offences where it can as part of its financial crime strategy for the coming years. According to its three-year strategy published on 7 April 2022, the area in which it feels it can be most impactful is in tackling authorised push payment fraud and investment frauds.
- C. Finally, according to a recent FOI response by the regulator, the FCA is conducting upward of 40 investigations into potential AML failings, which include at least one case set for criminal disposal and 8 dual-track investigations. There is clearly an ongoing appetite for tackling money laundering by focusing on the preventative regime and penalising those tasked with keeping dirty money out of UK Plc.

TAKE AWAY 1 – SMFS MUST BE RESPONSIBLE FOR FINANCIAL CRIME CHANGE PROGRAMMES

Financial crime risks change rapidly and financial services firms must keep up. In its review, the FCA has made it abundantly clear that it expects senior managers to be accountable for implementing necessary changes to anti-financial crime programmes. Specifically, it *“expects firms to have clear project plans for control enhancements outlining key milestones, accountable executives and delivery dates. Senior management should also be tracking projects and ensuring that key deadlines are being met.”* In other words, financial crime change programmes cannot be hit into the long grass. The importance of the FCA’s resolve in this regard should not be underestimated given the recent fine against a well-known retail bank that did just this.

TAKE AWAY 2 – DIGITAL INNOVATION IS WELCOMED

The FCA positively recognised evidence of a number of good practices. These included challenger banks harnessing technology to identify, verify and monitor customers in a way that was both innovative and effective. The use of video selfies, mobile phone geolocation data and photo images of a customer’s passport were all welcomed by the FCA as means to mitigate risks. Regulators are increasingly embracing and encouraging the use of technology in financial services, particularly in the compliance and monitoring space. This can pose its own challenges, however, when it comes to the duties to ensure compliance with data protection and security requirements.

TAKE AWAY 3 – A TAILORED APPROACH IS ALWAYS BEST

Echoing findings made in recent final notices against established retail banks, the FCA emphasised the need for tailored policies and procedures that are updated regularly to mitigate against financial crime. It welcomed the use of additional risk monitoring that is tailored to known fraud typologies at the on-boarding stage and as part of account monitoring. It also commended those challenger banks that had in place specific financial crime policies and procedures tailored to the particular financial crime risks of their business.

This reinforces the point that policies and procedures cannot simply be taken off the shelf. They must be bespoke to the business if they are to not only be effective in protecting the bank and its customers but also give the former a defence against strict liability corporate offences (failure to prevent bribery and the criminal facilitation of tax evasion). Such policies and procedures need to be informed by appropriate financial crime risk assessments, including having in place sufficiently detailed and well-developed customer due diligence systems and processes.

TAKE AWAY 4 – ANTI-FINANCIAL CRIME PROCESSES MUST BE CONSISTENT AND THOROUGH

The FCA identified serious lacunas in some of the firms' on-boarding processes. It was critical of firms that failed to obtain full customer information to determine their customers' risk profile. It also criticised those banks that failed to implement required CDD procedures at the customer on-boarding stage and stressed that, *"No matter how good a transaction monitoring system is, firms must still comply with the relevant CDD requirements."* Criticism was levelled, too, at banks that failed to consistently apply EDD and failed to document it as a formal procedure. Failures in transaction monitoring were also highlighted, including: inconsistent and inadequate rationale for discounting alerts by alert handlers; lack of basic information being recorded in investigation notes; and a lack of holistic reviews of the alerts.

These gaps may go some way to explain the failings the FCA noted in respect of SARs. Of significant concern was its finding that *"firms have sent a significant number of reports to the UKFIU when exiting customers that do not fit their documented risk appetite [which] indicated that these customers shouldn't have been onboarded and that better controls and risk assessment may have identified them sooner."*

CONCLUSIONS

In short, firms should consider themselves put on notice that they must have adequate resources in place to ensure they satisfy regulatory requirements and the FCA will take notice if their CDD, EDD and transaction monitoring practices are applied inconsistently or superficially. Being a new entry to the financial services market doth butter no parsnips.

BCLP's financial crime lawyers remain on hand to advise you on your financial crime risk including providing training and reviewing your internal policies and procedures. Please do feel free to get in touch.

RELATED CAPABILITIES

- White Collar

- Anti-Bribery & Corruption
- Anti-Money Laundering Compliance
- Finance
- Financial Regulation Compliance & Investigations
- Financial Services Corporate & Regulatory Team

MEET THE TEAM



Polly James

London

polly.james@bclplaw.com

[+44 \(0\) 20 3400 3158](tel:+442034003158)

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.