CUSTOMER RISK ASSESSMENT: AN ALL-TOO-COMMON FAILING IN CHALLENGER BANKS' FINANCIAL CRIME CONTROLS

Despite the effective use of technology to identify and verify customers at speed, Challenger Banks and FinTech's in the UK must prioritise the implementation of a regulatory compliant Financial Crime Customer Risk Assessment.

The UK Financial Crime Authority (FCA) recently published their findings following a review of Financial crime controls at Challenger Banks. The review focused on six challenger banks, in response to the risks raised in the UK's 2020 National Risk Assessment (NRA) of Money Laundering and Terrorist Financing. The NRA noted the potential for criminals to "be attracted to the fast on-boarding process that challenger banks advertise, particularly when setting up money mule networks". The FCA also highlights a risk that challenger banks may consequently promote the ability to open accounts quickly to attract customers, without sufficient information gathered to identify high risk customers.

Balancing Technology and Customer Experience with Regulatory Obligations

While the FCA has praised Challenger Banks' use of technology to innovatively identify and verify customers at speed, they also highlight the potential for regulatory failings. Although challenger banks target rapid onboarding and customer growth, the FCA stresses that this "must not come at the detriment of complying with Customer Due Diligence (CDD) obligations as set out in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017".

Ⓣ +44 (0)203 102 9526
Ⓔ enquiries@plenitudeconsulting.com
Ⓦ www.plenitudeconsulting.com

Plenitude Consulting Limited, 30th Floor,
40 Bank Street, Canary Wharf, London E14 5NR

> Without a customer risk assessment, a firm can't ensure that due diligence measures and ongoing monitoring are effective and proportionate to the risks posed by its individual clients.

Among the key financial crime control areas that require improvement, the Customer Risk Assessment (CRA) was highlighted as a critical weakness. The FCA found that the CRA framework was not well developed in some challenger banks and "lacked sufficient detail", with some challenger banks failing to even implement a basic CRA in the first place.

CRA allows a firm to determine the level of CDD/KYC that needs to be performed, and the level and frequency of ongoing monitoring, including periodic and event driven CDD/KYC reviews, transaction monitoring and alert prioritisation. As indicated by the FCA, without a CRA, "a firm can't ensure that due diligence measures and ongoing monitoring are effective and proportionate to the risks posed by its individual clients[1]".

Ensuring CRA compliance

Effective design and implementation of a CRA requires deep subject matter expertise and practical experience in order to fully comply with regulatory requirements and avoid the typical pitfalls of designing a CRA in-house. Based on Plenitude's proven experience, the following steps are critical for a robust CRA:

- **Comprehensive Regulatory Analysis** – the design, implementation, and maintenance of an effective CRA presents a significant challenge due to the requirement to undertake comprehensive regulatory analysis across multiple sources and the jurisdictions the Bank operates. Regulatory analysis ensures the bank accurately identifies the applicable obligations and guidance which in turn inform the design of the CRA methodology. There is also a requirement to horizon scan for future changes to laws, regulations and guidance to ensure the CRA remains compliant on an ongoing basis.

- **CRA Methodology** – the methodology should cover the required quantitative risk factors (Country, Entity, Industry, Product and Channel risk), alongside qualitative 'Special Risk Factors', such as the presence of Politically Exposed Persons (PEPs), sanctions exposure, negative news and complex structures. In addition, there is a requirement to define and maintain supporting risk lists with appropriate risk classification across the five risk factors. This requires a systematic approach for determining the risk rating of each country, industry sector, and the firm's products and channels.

[1] https://www.handbook.fca.org.uk/handbook/FCG.pdf

- **Testing & Calibration** – prior to implementation, the CRA methodology needs to be appropriately tested and calibrated to understand the overall portfolio risk distribution. Banks must also ensure that the risk classification is appropriate and does not present a significant operational impact which should be considered part of a risk-based approach. Without this step, a Bank may inadvertently apply insufficient or indeed too much weight to a risk factor(s), which inappropriately skews the results. All too often institution's fail in this regard and implement a deficient or suboptimal CRA control.

Challenger banks can develop and implement a custom CRA in-house, however this option is typically costly to develop and maintain in the long run and may present ongoing challenges to ensure compliance with evolving regulations, especially in firms with a rapidly growing geographic footprint or product offering. If the design of the methodology or its calibration is not appropriate, it presents a risk exposure to the bank. It may also present obstacles to enabling accelerated international expansion of challenger banks. This is especially pertinent when entering emerging markets with potentially higher inherent financial crime risks.

Alternatively, challenger banks can adopt an off-the-shelf solution such as ClientSight, which can be adapted to the challenger bank's business, products and services. More effective customer risk classification drives better risk management and ultimately risk mitigation outcomes, reducing your exposure to potential enforcement actions or fines.

The leading CRA solution: Plenitude ClientSight

Plenitude offers a cloud based CRA tool, **Plenitude ClientSight**, which allows challenger banks and other financial institutions to assess the inherent financial crime risks of its natural persons (individuals) or legal persons (entities).

It is grounded in Financial Crime Compliance (FCC) regulation and the guidance of UK and key global markets.

ClientSight provides full coverage of a wide spectrum of financial crime risk themes, including:

- Money Laundering
- Terrorist Financing
- Sanctions Evasion
- Proliferation Financing
- Bribery & Corruption
- Tax Offences

Plenitude ClientSight offers an API and can be integrated with your existing KYC, onboarding applications or transaction monitoring system, to assist with a seamless onboarding process and ongoing monitoring without additional complexity for your organisation.

If you would like more information regarding ClientSight or to schedule a product demo, please contact Plenitude.

CONTACTS

Pedro Arevalo
Senior Executive
E-mail: pedro.arevalo@plenitudeconsulting.com