REFINITIV EXPERT TALK

How digital banks can turn AML/KYC challenges into opportunities

Authors

Christopher Stringham
Solutions Consulting Manager Director, Customer and Third-Party Risk, EMEA, Refinitiv

Aravind Narayan
Global Director – Sales Strategy & Execution, C3PRS, Data & Analytics, Refinitiv

As our lives become more digitally connected, the financial sector has significant opportunities to deliver engaging 24/7/365 banking services. But at the same time digital banks face rapidly escalating threats as technological developments in cybercrime make it easier than ever for financial criminals to commit fraud. Against this backdrop, how can digital banks build resilient, robust and customer-centric compliance frameworks to stay ahead of the regulatory curve?

The benefits of embracing digital transformation in the banking industry – including lower costs, decreased risk, and constant connectivity – are undeniable, but 135 years after the American science fiction writer Edward Bellamy first wrote about credit cards, this narrative has begun to accelerate[1].

Digital banks have continually been improving their banking solutions by offering customers easy, engaging and cost-effective experiences. Many traditional banks – with paper-based, old-school banking processes – are scrambling to keep up.

The Covid-19 pandemic has further highlighted the urgent need for banks to focus on implementing digital transformation and embrace new digital banking opportunities.

Money laundering and other illicit activity

As hyper-digitalisation advances, financial criminals are exploiting new, technology-enabled opportunities for illicit activity.

The estimated cost of money laundered across the globe every year is a breathtaking 6.7% of global GDP, equivalent to $5.8 trillion – and crime on this scale has far-reaching economic and humanitarian consequences, eroding the fabric of society and causing untold human suffering.

Both digital and traditional banks are on the front line in the fight to combat financial crime and money laundering. However, despite a record $50 billion spent on sanctions compliance in 2021[2], shortcomings in anti-money laundering (AML) processes resulted in fines totalling $10.4 billion in the same year, an increase of more than 80% over 2019[3].

The scale of these fines highlights that many banks focused on digitalisation are struggling to keep up with their KYC (know your customer) and AML obligations, especially where their onboarding and monitoring processes are unable to trigger the right checks and send the right signals to back-office systems.

Technology is stepping up to help though – Refinitiv research reveals that 86% of respondents in our 2021 survey[4] agree that innovative digital technologies have helped them to identify financial crime within their operations.

1 https://en.wikipedia.org/wiki/Looking_Backward
2 economist.com/finance-and-economics/2021/04/12/the-war-against-money-laundering-is-being-lost
3 complianceweek.com/surveys-and-benchmarking/report-fines-against-financial-institutions-hit-104b-in-2020/29869.article
4 refinitiv.com/content/dam/marketing/en_us/documents/gated/reports/global-risk-and-compliance-report.pdf

Join the conversation to #FightFinancialCrime

REFINITIV®

An LSEG Business

Regulating digital banking

The regulatory landscape governing digital banking is dynamic, but there are notable relevant developments:

Worldwide

The Financial Action Task Force (FATF) – the global AML industry watchdog – updated its 2019 risk-based guidance on cryptocurrencies in 2021, and specifically highlighted that the financial system suffers from insufficient safeguards relating to the misuse of virtual currency.[5]

The FATF extended its AML and CFT (Combating the Financing of Terrorism) obligations to Virtual Asset Service Providers (VASPs) via the Travel Rule. This rule requires VASPs to identify the originators and beneficiaries of transfers above a certain threshold and transmit this information to VASP counterparties[6].

In the US

In the US, FinCEN (Financial Crimes Enforcement Network) defines virtual assets as a "preferred form of payment" for illegal activities[7] and the Office of Foreign Assets Control (OFAC) has increased its focus on the cryptocurrency space, targeting both individuals and entities using cryptocurrency to advance illicit activities. Financial services firms and VASPs that knowingly or unintentionally enable illicit activity are also on the radar. Also, a Bank Secrecy Act (BSA) Travel Rule requires all FIs (financial institutions) to pass on certain information to the next FI under certain circumstances[8].

In the EU

Across the European Union, regulators have also been scrutinising the digital space, with the Crypto Travel Rule mandated within the EU from mid-2021[9]. The European Commission is promoting consistency with the FATF Travel Rule and has released a proposal around the information accompanying transfers of funds and certain crypto assets.

More broadly, the European Commission has set out a digital finance package to "further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks"[10].

Building compliant, customer-centric processes

Given this backdrop, how can digital banks build solutions to ensure AML compliance and focus on the all-important aspect of customer-centricity?

Best-practice solutions begin with ensuring access to the right data and technology – both of which play a pivotal role in reducing risk and improving customer experiences. For example, automation reduces time employees spend on manual, low-value tasks that are often error-prone, saving money, reducing risk and allowing those same employees to focus on value-added areas of the compliance function.

Drilling down, five focus areas for digital banks to consider:

1. Customer onboarding
2. Ongoing monitoring
3. Transaction screening and monitoring
4. Change of circumstance alerts
5. Risk scoring

During the **customer onboarding** process, it is essential that institutions understand who their clients are, but this is also the first opportunity to ensure favourable customer engagement. Effective customer screening, KYC and enhanced due diligence when required are the key pillars of successful customer onboarding. This must be completed in an efficient manner that does not comprise the customer relationship from the outset.

Digital documents must be verified to ensure that they are not fraudulent, but further elements to consider include:

- Are the customers screened sanctions, other watchlists, PEPs, as per the risk appetite?
- Are they screened against adverse media?
- Does the solution generate a transparent risk score for each customer?
- Are the checks being completed in real time and is there a review workflow?
- Are liveness and facial matching checks conducted?
- Is the data available in machine-readable format for backend systems to consume?

After a customer has been successfully onboarded, the next crucial step is **ongoing monitoring**, since risk changes over time with clear implications for risk-based assessments of ongoing relationships. Screening datasets should generate meaningful alerts, which can be incorporated into each overall customer record.

5 Documents – Financial Action Task Force (FATF) (fatf-gafi.org)
6 fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf
7 AML/CFT Priorities (June 30, 2021) (fincen.gov)
8 sec.gov/about/offices/ocie/aml2007/fincen-advissu7.pdf
9 https://notabene.id/world/eu#:~:text=Is%20the%20Crypto%20Travel%20Rule,as%20of%20June%2020%2C%202021
10 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

Transactions should be monitored for any red flags. For example, is a customer sending payments to an entity that is either directly or indirectly sanctioned by a regime? Has a customer fallen prey to a financial criminal? Are any accounts showing warning signs of account takeover?

Change of circumstance alerts are another important element of a robust compliance framework. Banks must remain mindful of which data points trigger a KYC process. There are various factors to consider here, including the weighting given to specific data points and the initial risk score generated. If an address change is triggered, for example, does that automatically schedule a set of additional activities as per a set of predefined rulesets?

There are several factors that contribute to a customer **risk score**. It is important to ensure that all information captured is collated and that each system used has a machine-consumable result set that can be fed into the risk engine on a continuous basis, helping to ensure that the customer experience is consistent with any possible risk tagged against them.

Partnering for future success

While digital banking faces a range of regulatory and financial crime-related challenges, there is enormous opportunity to harness the power of data and technology to manage these issues and deliver digital experiences that will deliver future success.

Carefully executed digital strategies can win customers and fight financial crime, while doing so in an operationally efficient way. The right data and technology are helping digital banks meet their regulatory obligations and win market share, partnering with the right providers remains critical: digital banks need ongoing support and trusted relationships to flourish in a dynamic industry.

Join the conversation to #FightFinancialCrime

Visit **refinitiv.com** | @Refinitiv Refinitiv

REFINITIV®

An LSEG Business

RE1627991/7-22