Regulatory and compliance

AML compliance steadily progressing

Saudi Arabia is approaching its two-year anniversary of its acceptance into the Financial Action Task Force (FATF). The Kingdom continues to make progress in anti-money laundering (AML) and counter-terrorism financing (CTF) initiatives.

Evaluating progress

FATF's mutual evaluation report (MER) is the primary publicly-available tool to track the Kingdom's progress in addressing its previous shortcomings in preventing money laundering and terrorism financing. FATF's expectation is for member countries to have addressed "most if not all technical compliance deficiencies" three years after adoption of their MER, which in Saudi Arabia's case was mid-2018.

In January of last year, Saudi Arabia received its first (and only, to date) follow-up report from FATF on its progress. In two areas – targeted financial sanctions related to terrorism and terrorist financing and targeted financial sanctions related to proliferation – the Kingdom's rating was upgraded from "partially compliant" to "largely compliant". However, the follow-up report also re-rated Saudi Arabia's measures against FATF recommendations that have changed since the 2018 mutual evaluation. For the three changed recommendations, FATF maintained one rating and downgraded two recommendations. In all, Saudi Arabia is currently compliant on 17, largely compliant on 21, and partially compliant on 2 of the 40 recommendations. With a year having passed since this assessment, these ratings may not reflect the current position.

FATF road ahead

For its part, SAMA has been moving quickly to address remaining issues with the AML/CTF environment in Saudi Arabia, and to help bring banks into compliance with new standards. SAMA is likely to provide further focus around standards, monitoring and risk oversight regarding AML/CTF issues. This is likely to encompass:

- Enhanced supervision and monitoring, in so far as it relates to existing AML regulations and standards;
- A more hands-on focus on key areas of risk and risk assessment, including likely enhancement of enforcement actions; and
- New standards and developments, for example in the context of SAMA's focus on e-banking and digital banking platforms.

Covid-19 AML/CTF challenges and responses

The Covid-19 pandemic has changed the way many organizations operate – particularly their use of office space and remote working arrangements. While this has yielded some new potential efficiencies for organizations, it also opens up new risks in the AML/CTF area.

Key challenges faced

- The risk of non-face-to-face identification due to digital on-boarding
- Increased activities of non-profit organizations in countries with a higher risk of money laundering or terrorist financing
- Controls may be weakened by disjointed processes and remote handovers
- Businesses that are suffering from the crisis may be targeted for money laundering
- New (emerging) risks are not timely and adequately identified, assessed and, where necessary, mitigated

How to respond

- Design and implement controls with respect to on-boarding in the time of social distancing, and take maximum advantage of other digital channels available to corroborate identity, source of wealth, etc.
- Communicate clear compliance processes which enable employees that work from home to maintain full compliance
- Stay focused on ongoing client monitoring to identify unusual activity, including development of new typologies relevant

> Banks gather more data points than most other consumer services – as required by law and by virtue of a client's interactions.

to increased online activity. Expected client activity volumes and behaviors should also be reconsidered to reflect the Covid-19 impact on particular business sectors
- Businesses benefiting from government support schemes in response to Covid-19 should be subject to additional screening to ensure compliance with the qualifying criteria
- Update your AML/CTF risk assessment to take into account new (emerging) risks, and changes in channel activity by clients

KYC in a digital, dispersed world

Even prior to the pandemic, banks had developed non-face-to-face customer on-boarding processes that paired improved customer experience with maintaining "know your customer" (KYC) controls. Now, with social distancing restrictions and bank branch closures further shaping the on-boarding process, these efforts have been put under the microscope. Though remote on-boarding presents challenges, there are a number of benefits – both to the KYC process and to data quality and cost savings – that a savvy bank can realize.

Banks gather more data points than most other consumer / business services – as required by law, and by virtue of a client's interactions and established "footprint". This data, if well organized and smartly analyzed, can improve a bank's AML (and anti-fraud) practices by allowing for consistency checks, statistical anomaly flagging, and suspicious pattern identification.[3]

Data is only as valuable as it is useful, and without using effective data analysis tools and employing capable data engineers, troves of customer data can be wasted. Using the right technology can allow a bank to better on-board customers and more efficiently handle regulatory cases. Additionally, using the right tech can lead to cost savings of over 90%, according to Fourthline.[4]

KYC/CDD challenges

Globally, financial institutions spend an average of USD 150 million a year on KYC and customer due diligence (CDD) operations, yet many struggle with inefficient and ineffective delivery centers, and face long KYC remediation projects. Major financial institutions have increased their focus on reducing the cost of compliance by designing customer-centric changes and re-engineering processes to simplify and standardize CDD processes.

Financial institutions continue to face a number of regulatory and operational challenges with CDD frameworks. These include:

Process inefficiencies: Globally inconsistent, fragmented and non-standardized KYC/CDD processes with limited end-to-end automation, resulting in lower staff productivity and significant rework.

Fragmented data: Siloed, duplicative and inconsistent data (structured and un-structured) offers limited ability to search and access internal and/or public sources to meet compliance needs.

Unfocussed technology investments: Increased suspicious activity case volumes call for continuous investments in technical capabilities (e.g. case management, AI and machine learning) to adequately scale operations and maximize the efficiency of investments in human capital.

Negative customer experience: Cumbersome and disjointed on-boarding and periodic customer refresh processes, resulting in redundant, inconsistent and repetitive customer outreach to collect and verify KYC/CDD data.

Labour-intensive operations: Significant manual processing creates an unattractive workplace, with redundant activities and weak controls resulting in sub-optimal quality and higher rework, along with higher staff attrition and re-training requirements.

Fragmented controls: The response to increasing AML/KYC requirements is often to layer with additional controls, without taking a holistic approach to the control environment to ensure manual and systems controls are operating in sync – and appropriately driven by the institution's risk assessment process – to efficiently meet compliance needs.

Phil Knowles
Senior Director, Financial Services
KPMG in Saudi Arabia

Phil Knowles has extensive financial services sector experience, gained through his work in the assurance and advisory practices of KPMG in Sydney, London, Dubai and East Africa prior to joining KPMG in Saudi Arabia. He has also held senior regional compliance roles in the banking industry.

[3]https://www.fourthline.com/download-kyc-remediation-white-paper
[4]Ibidem