The Business Case for Digitalizing Anti Money Laundering (AML) and Why AI & RPA Are Critical

Summary *- Money laundering is a billion-dollar problem, but AML efforts impact less than 1% of criminal activities. Banks and financial services providers must urgently implement digital technologies (specifically artificial intelligence and robotic process automation) to curb this trend. This article discusses five ways digitalization can aid AML and steps for getting started.*

Introduction

In just one year, the penalty imposed on financial services providers related to money laundering increased by a massive $262 million to reach $706 million in 2020. Not only does this place enormous pressure on banks, lending institutions, and other service providers, but it also fosters a risk-averse attitude that deters innovation and growth. It is critical that this sector adopts digitalization, specifically purpose-built AML solutions powered by AI & RPA, to reduce the risk of money laundering, optimized manual efforts needed for AML activities, and strengthen the foundations for future growth.

The State of AML and Why Digital Intervention is Necessary

There are several reasons why banks and financial services providers struggle to keep up with the proliferation of money laundering cases worldwide.

- 55% say that their current staff isn't sufficiently trained in AML
- 13% cite the lack of senior management buy-in as a hurdle
- Increased regulatory expectations are the No.1 challenge faced by 62%
- 51% find it challenging to manage the requirements of multiple jurisdictions

The intelligent application of technology can reduce dependence on human efforts, using automations to overcome AML-specific skill gaps among the BFSI workforce. Also, these solutions would be better attuned for ROI, thereby encouraging timely buy-in from senior management.

A technology-driven solution would be dynamic, adapting, and scaling in response to the needs of the regulatory environment at hand. In this context, artificial intelligence (AI) and robotic process automation (RPA) have a major role. AI can ingest voluminous data in real/near-real-time to make smart, almost “human” discretionary judgments on money laundering risks. RPA could funnel these insights into an actionable process-flow, leading to a more streamlined AML roadmap across the entire assessment, detection, reporting, and redressal value chain.

However, most institutions are yet to realize this potential.

AML fines were on a downward decline between 2018 and 2019 but rose again in 2020. In some cases, banks are too focused on simple transactional behaviors, causing an overwhelming number of false positives and unnecessary investigation costs. Also, regulatory agencies try to identify the threat actor after a money-laundering event, instead of proactively identifying vulnerabilities that facilitated them. This retrospective approach piles up the penalties without necessarily preventing future incidents.

To ensure that investments in AML do not turn into sunk costs, banks must incorporate the power of technology at critical moments of truth, both in the prevention and response phases.

5 Examples of How Digital Technology Can Augment AML Capabilities

Digitalization can reduce the risk of money laundering and optimize AML processes by:

1. Detecting anomalies in transactions

While essential tools are in place to monitor simple transactional behaviors, banks can go the extra mile by adopting advanced AML technologies like AI. AI systems can collect and curate behavioral data from a variety of sources to "learn" the most common patterns, potential red flags, and exceptions to the rule -- highlighting anomalies in transactions with minimal false positives. For instance, NASDAQ has developed an in-house AI tool called the Automated Investigator, that ingests data, analyzes it, and replicates the human decision-making process to generate an auditable justification for all the flagged transactions within seconds. It goes beyond the flagging of anomalies to classify them in an actionable manner, making response mechanisms simpler during investigations.

2. Streamlining regulatory investigations

AML compliance costs are over $25 billion a year, and ongoing investigations comprise a significant portion of this amount. Frequent false positives coupled with an inefficient investigation process means there is a massive workload waiting for already-stretched AML staff at any given point of time. As mentioned, AI can filter datasets so that investigators consider only what's most relevant, streamlining regulatory investigations. RPA could automatically generate comprehensive reports that reduce manual labor and speed up investigation timelines. One North American bank was able to reduce its average case handling time from 340 seconds to 86 seconds by switching from a manual to an automated workflow.

3. Automating KYC and customer onboarding

Regular Know Your Customer (KYC) checks – both at the time of onboarding and throughout the customer relationship – can flag high-risk and potentially suspicious clients. Under the Patriot Act, US financial services providers have several obligations around AML-KYC processes, as this is the first step in ensuring that customer validity and due diligence. AI techniques like optical character recognition (OCR) can extract key customer data from unstructured sources/documents and, coupled with RPA, it would populate electronic forms at scale and in an error-free manner. This would allow banks to scale customer onboarding activities without compromising on security or risk management.

4. Adopting sophisticated customer segmentation based on risk

Traditional AML is built on fixed business rules, segmenting customers, transactions, and behavioral triggers into rigid (often inaccurate) buckets. Instead, a risk-based approach would assess each flagged instance's risk level individually to place them in customs segments and prioritize action. Risk-based customer segmentation monitors a massive breadth of customer transactions to surface thousands of possible risks, passing them through multiple layers and parameters, and finally unraveling a handful that merits further investigation and investments. Customers can be segmented based on KYC, behavioral patterns as well as transaction monitoring, feeding the data generated from these into an AI engine. The AI would assign a projected risk score to each red flag, aiding prioritization based on detailed and accurately labeled segments.

5. Screening customers in real-time as per dynamically updated watchlists

Monitoring transaction value alone cannot reveal all of the indicators that might suggest a money laundering risk. Banks also need to look at behavioral triggers such as access frequency, destination accounts, etc. to obtain an accurate picture of the customer's financial intentions. Two things can help here: automated real-time screening of KYC details and AI-based analysis of behavioral footprints. The global AML watchlist is updated rigorously and dynamically as per sanctions. RPA can assemble all of this data into a consolidated source of truth and scan customer profiles in near-real-time as part of every KYC cycle, finding politically exposed persons (PEPs) and other risk vectors. AI adds another layer of screening by analyzing high-risk individuals' behavioral traits.

How to Adopt AI and RPA for Anti-Money Laundering

All of the examples we discussed rely on various forms of AI and varying degrees of automation to sieve through massive volumes of data, unlock actionable insights, and initiate an executable process roadmap with minimal human dependencies. To gain from these technologies, financial institutions must:

1. Conduct a rigorous analysis of the as-is landscape

This applies to greenfield and brownfield implementations alike. The first step is to take stock of the existing technology infrastructure, its gaps, as well as possibilities. For example, a bank could be leveraging a technology vendor who also has AI expertise and product offerings. A rigorous analysis will furnish a detailed map of current technology artifacts, technology/process owners, efficiencies/inefficiencies, and the distance to be covered before reaching the desired outcomes.

2. Planning for the initial pilot(s), mid-term milestones, and long-term directions

Once the foundational landscape assessment is in place, AML stakeholders can explore either point solutions or end-to-end digital transformation to reach their target. There are three options to consider, and the final decisions would depend on the scale, available resources, and dependencies involved in the implementation:

- **In-house development** - Banks (particularly super-large organizations with custom requirements) could build AI models, deployment interfaces, and automated workflows from scratch. This could involve acquiring additional domain knowledge, such as NASDAQ's minority stake investment in the Fintech firm, Caspian.

- **Off the shelf purchase** - Smaller banks could opt for ready to use solutions, like Jumio (for KYX), SAS Anti-Money Laundering, Oracle Financial Services Express Edition, etc. These are point solutions, targeting only a few of the use cases we discussed, and offer limited configurability.

- **Managed development and implementation** - Organizations could partner with service providers who intersect domain expertise with technical competencies to build a managed solution. The service provider must be backed by fintech partnerships to provide ongoing support in a dynamic marketplace. This strategy optimizes AML workflows while ensuring uninterrupted compliance.

3. Enforcing robust governance monitoring and upgrade for sustainability

Given the BFSI industry’s highly dynamic nature, banks need AML solutions that upgrade seamlessly and are easy to govern. This means regular SLA adherence checks to reduce the possibility of AML penalties, compliance violations, and unprecedented effort overheads in the short-term. In the medium-term, banks must keep up with changing regulatory requirements either by updating systems in-house (and provisioning the necessary investments for the same) or by working with a vendor/managed partner to bring about ongoing transformation. The long-term roadmap will include integrating the latest AI techniques and RPA technologies as they pass testing and become ready for adoption at scale.

What Are the Benefits of Digitalizing AML Programs?

The case for digitalizing AML operations by embracing AI and RPA has never been clearer. It can help to unlock benefits such as:

- **More data-informed operations in a hyper-connected world** - Today, there is a vast expanse of publicly available, third-party and first-party data with which banks can better segment customers and spot AML risks on time. Digital solutions help to maximize this opportunity.

- **Increased agility for a volatile business environment** - Banks and financial institutions must be highly agile to unprecedented challenges and come out on the winning side. Digital AML programs are adaptable, quickly responding to crisis events like a pandemic or an economic downturn. Banks can extend their KYC operations to remote platforms, scale back initiatives to ensure profitability, and can optimize AML operations in an agile manner to ensure ROI.

- **Optimize effort utilization and freed-up resources** - Automated and AI-powered AML programs will reduce human dependencies to a great extent, freeing up a bank's resources for value-generating efforts like new product development or customer experience management.

- **Readiness for a digital-only banking ecosystem** - The last few years have seen payment activities move to digital platforms, and AML must keep up. As today's digital-first transforms into a digital-only model, AI and RPA will ensure banks' readiness for this tectonic shift.

Conclusion

Today, there is a degree of complacency around AML, and banks often over-estimate their ability to prevent/counter money laundering. A report found that over 50% of the financial services providers are confident about their prevention capabilities. In comparison, traditional AML processes have less than 1% impact on crime. It is critical that banks immediately conduct a rigorous assessment of where they stand, their exposure to money-laundering threats, and inefficiencies that could be costing them financially or in terms of non-compliance. Fortunately, digital solutions powered by AI and RPA can help to curb this challenge, building on a bank's existing digital bulwark to prepare for the road ahead.