Automating Anti-Money Laundering (AML)

A plethora of inefficiency still exists across the financial crimes compliance industry landscape, both domestically and internationally. Based on interactions and experience with industry participants, compliance costs are so out of control and so burdensome that, in some cases, they can have a lasting impact on the success and growth of the institution. Annually, billions of dollars are spent on troves of analysts performing repetitive triage and investigative functions that could have been automated and saved much-needed funding for investments in technology, marketing, and other ways to improve the business. So why are many still reluctant to invest in automating components of AML?

One answer is that many risk management functions fear the possibility of noncompliance with regulations and, therefore, discount possible high-impact automation opportunities, overpowering decisions to invest in opportunities that can pay back handsomely on an annual basis. In addition, in many cases, sunk costs in technology infrastructure dissuade stakeholders from changing the technology environment and processes, as technology teams and operations teams are barely able to stay on top of many tasks at hand and remain compliant using the technology that they just spent millions on implementing.

Our perspective is that the fear of doing nothing for the above reasons is eventually more costly than breaking the status quo, and those who invest in automation will end-up with a competitive advantage over others who do not. Without greater investments in automation, higher costs reduce the ability to invest in higher-priority initiatives, trap otherwise available resources, and result in customer friction that drives market share to other competitors, that are more agile, more forward-thinking, and more able to meet the needs of today's customers. Separately, in an age of technology disruption within the banking community, proactive leaders who procure tech, analytics, and automation are more likely be the major contributors to businesses that succeed in today's hypercompetitive landscape.

What are three fundamental reasons to invest in financial crime automation strategies?

1 Cost Takeout

- Institutions can save an average of 25 percent of annual compliance costs through automation—on average, based on what our clients save every year after conducting time-study analyses and cost measurement activities.
- The cost savings are rewarded to financial institutions that drive change by building and implementing a plan. Strategic roadmaps, robust cost-benefit analysis, reward-versus-complexity projections, and micropilots prove out highest-impact area targets—and form the basis for a path forward.
- Cost-takeout plays in the Financial Crimes space can include areas such as false-positive hibernation models, alert-overflow demand/supply functions, all-lines-of-defense control automation, and Know Your Customer (KYC) automation.

2 Customer Experience

- Customers no longer tolerate waiting on the phone to contact a representative for their fraud case or dispute status, waiting days after onboarding to begin transacting, or being contacted for KYC information.
- They need answers on their mobile phones within seconds, with clear status and knowledge of actions taken.
- They appreciate streamlined onboarding and KYC experiences that leverage AI-based identity verification services.
- They don’t want to pay fees to cover compliance costs.

3 Risk Aversion

- Automated controls can significantly reduce human error and therefore reduce risk. Empowering lines of defense (Operations, Financial Crimes Compliance, and Audit) with the right tools is paramount. Artificial intelligence (AI) platforms, natural language processing techniques, graph technologies, and entity resolution capabilities can lay the groundwork for that control framework.
- Many use cases exist to enable control automation and advanced control analytics. The control inventory constantly evolves and becomes smarter to avoid recurring pitfalls that many institutions experience.

Today's leaders seek opportunities in their organization to gather information and to prove that automation benefits significantly outweigh the costs (and risks) to the firm. The following are examples of Financial Crimes automation and technology where we help clients on their journey in this regard.

Client Onboarding and KYC

- **Streamlined Onboarding**
  Streamlined and consistent onboarding platforms across products serve as the entry-point for customers
- **Autonomous Identity Verification**
  Identity verification via biometrics, deep learning, ID document scanning, and third-party tools
- **Evergreen KYC Requirements**
  Real-time KYC requirements are integrated into onboarding workflows as quickly as regulations or policies change
- **Quant-based Customer Risk Models**
  Supervised machine learning models empirically support groups of subject matter professional judgment
- **Perpetual KYC**
  Eliminate manually intensive "periodic reviews"

Key Impacts

- Significantly faster compliance handling times over traditional methods for improved customer experience
- Identity-based fraud loss (via onboarding) eliminated
- Reduction in Customer Due Diligence (CDD) operating costs through the elimination of back-office and support needs
- Increased consistency in the customer risk assignment and review process

Transaction Monitoring and Screening

- **False Positive Hibernation**
  New models predict whether an alert generated is a false positive with 99 percent accuracy
- **Machine Learning**
  Supervised learning detection models integrated into the core AML and fraud transaction monitoring engines, outperforming legacy pattern detection
- **Generative AI**
  Alert narrative generation using natural language processing as an analyst
- **End-to-end Automation**
  Automate structuring, which based on public estimates contributes to largest percentage of the industry's Suspicious Activity Reports
- **Graph Entity and Network Analytics**
  Visually depict networks associated with customer, leveraging internal and third-party data sources

Key Impacts

- Large reduction in operating costs
- Significant decrease in false positives and Level 1 Alert review needs
- Elimination of an average of thousands of hours per month via robotic process automation and process engineering
- Fraud losses reduced
- Reduced regulatory exposure through elimination of prone-to-error processes

Investigations and Reporting

- **Robotic Process Automation**
  Bots and scheduled jobs that are adaptable and controlled to automate tasks
- **Customer 360**
  View consolidated historical investigations and reporting across AML, fraud, cyber, sanctions, and anti-bribery and corruption
- **Agile Workflows**
  Workflow systems that quickly adapt to changing and evolving processes
- **Predictive Capacity Planning**
  Ability to predict resourcing needs months ahead of alert drops and new initiatives
- **Integrated Quality Assurance Control** technology
- **Optimized Metrics**
  Simplify metrics processes through a streamlined hub

Key Impacts

- Reduction in team workloads via more efficient investigations
- Enhanced decision-making capabilities and control of operations
- Avoidance of hundreds of thousands in overages due to imprecise planning and mismanagement of resources
- Streamlined and risk-based quality reviews

How KPMG Can Help

KPMG can help you free up resources, reduces costs, and position you for strategic growth by creating and executing a transformation plan that incorporates automation. KPMG continues to receive recognition from a number of industry sources in recent years based on our collective experiences in demonstrating that we operate and drive results for organizations in this area of specialization. KPMG offers extensive experience and leadership across the industry in a multitude of Financial Crimes Compliance offerings.

AML Technology Suite

- Transaction Monitoring Alert Classifier
- Sanctions Alert Classifier
- SmartCDD
- Suite of Bots
- Entity Resolution and Graph
- Integrity Due Diligence
- Automated Screening
- Identity Verification
- Automated Due Diligence
- Reporting and Dashboards
- Model Validations (including ATL, BTL testing and rule/scenario tuning)
- Sanctions Entity Analytics (50 Percent Rule)

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.