genpact

POINT OF VIEW

When it comes to anti-money laundering and anti-fraud, together is better

Fraud, or any scheme to defraud, is a predicate crime for money laundering. Conversely, many money launderers commit fraud. So, the bottom line is where there is fraud there is money laundering – and, often, vice versa. For this reason, the Financial Crimes Enforcement Network (FinCEN) has issued advisories and guidance on various fraud-related activities, such as mortgage fraud, identify theft, tax-refund fraud, healthcare fraud, and elder abuse. Even when there is no known connection between a fraudulent transaction and money laundering, financial institutions have an obligation to file a suspicious activity report (SAR) relating to the fraud, assuming that the transaction meets a minimal threshold.

A historical division between the anti-money laundering (AML) compliance area, which naturally rolls up to the Chief Compliance Officer, and the anti-fraud department, which typically is housed in the Chief Risk Officer's domain, has morphed into divided cultures and mindsets. As a result, these units view their missions as separate, despite the fact that they are carrying out similar work. This work is centered around discerning patterns that may indicate a problem, investigating system-generated alerts, and identifying bad players. But the perceived uniqueness of their missions can lead to unnecessary disconnects and the creation of data silos. These divisions can also appear in financial institutions where both units report up the same management chain. A historical division between AML and anti-fraud has morphed into a cultural and mindset split leading to disconnects and data silos.

Ensuring that money is not lost through fraud, which requires real-time solutions, has typically been seen as a key component of the core business process. Identifying a case as fraudulent is easier, since the victim or customer is likely to report or verify it. In this light, fraud can be viewed as operational loss, with significant public relations risks. In attempting to navigate the obstacle course of customer experience, dollars lost, and operational costs, financial institutions need to determine a path and develop a mitigation roadmap.

In contrast, AML has been considered a regulatory-driven cost-center in which identifying suspicious activity can be difficult, so maintaining proper audit trails and documentation is critical. This imbalance between voluntary and regulated costs frequently has led to advances in fraud analytics. This gap can be reduced through advances in training and digital interventions.

AML and anti-fraud departments often do not communicate, work together, or share case management or monitoring systems. Further compounding the divide, the two units frequently compete for budget, resources, and the attention of senior management. Thus, anti-fraud investigators often do not know that a person is under investigation by AML teams, and vice versa.

A historical division between AML and anti-fraud has morphed into a cultural and mindset split leading to disconnects and data silos.

Even when there is no known connection between a fraudulent transaction and money laundering, financial institutions have an obligation to file a suspicious activity report relating to the fraud

In recent years, there has been a healthy trend toward combining the two functions (along with cybersecurity) under an enterprise-wide "anti-financial crime" umbrella. Indeed, third-party providers that traditionally had distinct AML and anti-fraud solutions are increasingly offering platforms, monitoring systems, and case management tools that readily integrate with fraud prevention. This trend has been encouraged by regulators, including FinCEN, which expects financial institutions to promote "communication and collaboration among internal AML, business, fraud prevention, and cybersecurity units."

Building upon common ground

Merging the AML and anti-fraud functions takes advantage of several synergies. A key one is that much of the data required to detect money laundering is the same as that needed to prevent fraud. For example, similar products types, such as international wire transfers and stored-value cards, are typically considered high risk and monitored more closely. Delivery channels, such as online and remote access, are also higher risk for both money laundering and fraud. AML and anti-fraud leverage the same transactional parameters, account and customer information, peer-group definitions, watch lists, and certain scenarios or detection models. From the standpoint of both business

Combining AML and anti-fraud functions has been encouraged by regulators as they expects financial institutions to promote "communication and collaboration among internal AML, business, fraud prevention, and cyber-security units.

and compliance, then, there is great value in a united database that provides a holistic view of a customer's total relationship with the bank, increases visibility into products, transactions, and accounts in different lines of business – and investigates any concerns that arise.

AML know-your-customer (KYC) procedures and documentation of expected activity for customers can serve as important fraud tools. AML and anti-fraud programs share many policies and procedures, including referral of information to law enforcement, termination of customers for inappropriate activity, and due diligence monitoring. Both teams use similar tools and protocols for completing workflows and resolving cases; when it comes to alerts and case analysis, as well as investigations, they leverage many of same skill sets. AML and anti-fraud professionals tend to be knowledgeable about similar laws and adept at conducting research and complex analytics, interviewing people, and writing comprehensive reports.

The potential benefits of eliminating redundancies by combining AML and anti-fraud efforts are clear. Consolidation can lead to more targeted and actionable

Merging the AML and anti-fraud functions takes advantage of several synergies. A key one is that much of the data required to detect money laundering is the same as that needed to prevent fraud.

Consolidation of AML and anti-fraud functions can help achieve:

- More targeted alerts, actionable investigations, and quick resolution
- Potential cost savings through efficient use of resources
- Elimination of duplicate alert reviews and case investigations
- Fewer duplicate SARs and more thorough SAR filings
- Greater visibility for management through aggregated reporting, and a more holistic enterprise-wide view.
- Mitigate the risk of inadequate coverage,
- Opportunities to cross-train, and develop more well-rounded analysts and investigators
- A more balanced load across individual units

alerts for investigations, with all alerts for the same subject being displayed to analysts. With more information available, investigators are able to reach resolution more quickly. In addition, fraud detection rates improve, and investigators are better able to identify sophisticated schemes. For example, while multiple low-value events may not be registered as frauds, an enterprise-wide system can aggregate exposure and help detect patterns.

Furthermore, potential cost savings can be realized through more efficient use of resources, including system enhancements, data management and audit consolidation, IT staffing costs and software maintenance fee reductions, and the elimination of duplicate alert reviews and case investigations.

AML and anti-fraud units working in a coordinated fashion facilitates easier hand-offs of alerts, cases, and investigations, together with greater sharing of leads and information. This can result in, among other things, fewer duplicate SARs and more thorough SAR filings. Breaking down silos can also lead to better identification of fraud and money laundering schemes across channels, products, and lines of business. The result is greater visibility for management through aggregated reporting, which provides a more holistic enterprise-wide view.

In addition, there are opportunities to cross-train, mitigate the risk of inadequate coverage, and facilitate load balancing across individual units. Consolidation enhances the ability to develop more well-rounded analysts and investigators, as well as to improve employee morale and retention by providing more opportunities for learning and advancement. For example, the institution would have "financial crime analysts" responsible for reviewing both money laundering and fraud alerts, rather than siloed AML or anti-fraud analysts.

Overcoming resistance to change

Of course, challenges exist. One might be described as "cultural." Individuals in an AML group tend to have legal and compliance backgrounds, while those on the fraud side are generally more operational. Nomenclature and sense of identity differ, too. Leadership from one discipline may lack the knowledge and experience to manage the other area effectively. And management may see one program as more important than the other, leading to insufficient allocation of resources. An AML leader might well worry that AML could be overshadowed by an urgency to reduce fraud losses.

The list of challenges extends to the need to merge and redesign processes, recognizing and accommodating necessary differences (for example, differences in investigatory workflows), and understanding that for AML compliance regulatory reporting requirements are the main driver. Combined AML and fraud management systems require renewed integration with host systems (for instance, core banking, credit cards, and more). And the institution's case management system must support an integrated approach, while still providing the specific workflows vital for AML and fraud analysts to be effective.

The list of challenges extends to the need to merge and redesign processes, and recognizing and accommodating necessary differences. Combined AML and fraud management systems require renewed integration with host systems, a case management system that supports an integrated approach, while still providing the specific workflows vital for AML and fraud analysts.

Moreover, the financial institution must leverage technology across disciplines. In this regard, institutions continue to ramp up their efforts to use artificial intelligence and digital tools for a myriad of purposes, including reducing false positives, rendering customer segmentation and alerts generation smarter, and automating manual investigative processes. This move to more real-time and intelligent decisioning and workflows should be coordinated between AML and anti-fraud to best take advantage of available synergies.

Finding a way forward

So, how can an institution maximize the benefits of AML and anti-fraud consolidation, while minimizing cost, burden, and inefficiency? The answer is to proceed slowly and methodically. A move to combine the two groups may not be the right answer initially. It would require, among other things, creating a single alert monitoring system, which would observe and notify unit supervisors of common touch points between an alert subject or alert subjects. A combined monitoring system, running both AML and fraud rules together with an entire new set of policies, procedures, and processes, could be further enhanced by a holistic case management platform. Consolidating AML and anti-fraud would require creating a combined monitoring system, running both AML and fraud rules, coupled with an entire new set of policies, procedures, and processes. Financial institutions must proceed slowly and methodically to maximize the benefits of consolidation.

Consolidating AML and anti-fraud would require creating a combined monitoring system, running both AML and fraud rules, coupled with an entire new set of policies, procedures, and processes. Financial institutions must proceed slowly and methodically to maximize the benefits of consolidation.

A better tactic might be to keep the groups separate, but formalize the relationship, with both areas reporting to the same senior executive. There would be regular meetings between the two groups to discuss strategies, provide feedback for improvement, and share information about cases. The institution would maintain separate databases and transaction-monitoring systems, but now AML and fraud staff would be specially trained to look out for, understand, and share information and red flags for the benefit of both departments. Even when an AML alert does not turn out to be positive when investigated by the anti-fraud team, it still could indicate the presence of fraud, and vice versa.

This approach would also allow for the gradual development of a unified case management system that facilitates appropriate file hand-offs between analysts and investigators. Such a reimagined case management solution, which might incorporate intelligent optical character recognition, natural language processing, and computational linguistics for meaningful extraction and analysis of unstructured information, would allow for faster and more accurate decisioning and improved agent and customer experience.

In the Financial Crime Compliance programs where the AML/fraud divide is severe, there may be a preponderance of data misalignment. RPA can alleviate this issue by quickly and accurately formatting data into a single, standardized system

Other useful steps for maximizing the benefits of this transformation include:

- Conducting a data assessment to ascertain quality, identify underutilized sources, and determine how to close any gaps
- Evaluating the alert remediation process to fully understand the workflow architecture and identify additional opportunities to embed artificial intelligence and other digital tools
- Developing additional management information system (MIS) and other performance-tracking tools around key performance indicators (KPIs) in order to create enterprise-wide measures of success and improve benchmarking
- Creating a centralized rules engine that is more dynamic and real-time, with existing rules optimized and new rules introduced to cover all current vulnerabilities
- Introducing a more intelligent workflow to manage alerts and optimize triaging

Consolidating an institution's AML and anti-fraud areas is the current trend. It meets regulatory expectations more effectively, and offers the opportunity to achieve a number of significant synergies. But it must be approached carefully and thoughtfully, incorporating modern digital tools as appropriate.

Utilizing digital interventions

In assisting the convergence between AML and fraud units, digital solutions – such as robotic process automation (RPA), machine learning (ML) and artificial intelligence (AI) – can help with data conditioning and consolidation. In Financial Crime Compliance (FCC) programs where the AML/fraud divide is severe, data misalignment may be a persistent issue. But RPA can help by quickly and accurately formatting data into a single, standardized system. In the Financial Crime Compliance programs where the AML/fraud divide is severe, there may be a preponderance of data misalignment. RPA can alleviate this issue by quickly and accurately formatting data into a single, standardized system.

Data conditioning can be further improved by implementing AI to fill in missing information, a problem which continues to plague both AML and fraud units. Whether these gaps are found in internal forms, transaction details, or third party subscriptions, they can be confounding to lower-level investigators. Utilizing AI to enrich client data and subject profiles can reduce false positives, shorten cycle time, and alleviate repetitive work, which drains morale and causes investigator burn-out.

Furthermore, by creating a single stream and more accurate alert flow, investigators and managers will be better able to approach their workflows in a risk-weighted or risk-segmented manner. In addition, through modern digital interventions, AML and fraud case management can be intelligently augmented, allowing for streamlined case allocation, tracking, and cross-unit communication. That, in turn, will result in decreased information silos, shorter cycle times, and the potential to intelligently automate the dreaded "task trackers," which plague managers and team-leads alike. These efforts can further inform thematic or key risk indicator reports, thereby helping senior management quickly understand the burdens and successes of their various units.

Modern digital interventions can intelligently augment AML and fraud case management, allowing for streamlined case allocation, tracking, and suggested cross-unit communication.

If this modernization is implemented in a way that allows for the underlying principles to be easily understood, key stakeholders will be able to onboard and offboard new vendors, third-party data subscriptions, and more – and do so with the confidence that these back-end systems can be adjusted with minimal disruption to BAU. Moreover, transparent AML allows for quickly understood detection scenario tuning and operation in a post-detection-scenario world.

As banks continue to intensify their compliance efforts, money laundering and fraud schemes will only get more sophisticated. There is no simple way to develop a state-of-the-art compliance program. However, by moving away from a counteractive approach, converging AML and fraud, developing agile risk management frameworks, and adapting digital technologies to develop the ability to anticipate and act at speed, banks are likely to achieve greater compliance in a highly susceptible global banking environment and generate benefits for their business.

How can Genpact help?

Genpact helps banks consolidate AML and anti-fraud functions into a single, enterprise-wide program with platforms, monitoring systems, and case management tools that bring together data and talent with modern digital technology. We can apply either an integrated, end-to-end solution or individual modular offerings for banks across the value chain – from strategy to transaction detection, alert triage, investigation, case management, and SAR filing – to help drive targeted AML and anti-fraud outcomes. These include Smart Investigator, our case management offering, which can reduce cycle time while eliminating backlog, as well as Smart Data Aggregator & Modeler, our data engineering and model development solution, which can reduce data aggregation time and cut false positives without losing critical data. To learn more, contact us today at banking.solutions@genpact.com.

About Genpact

Genpact (NYSE: G) is a global professional services firm that makes business transformation real. We drive digital-led innovation and digitally-enabled intelligent operations for our clients, guided by our experience running thousands of processes for hundreds of Global Fortune 500 companies. We think with design, dream in digital, and solve problems with data and analytics. We obsess over operations and focus on the details - all 78,000+ of us. From New York to New Delhi and more than 20 countries in between, Genpact has the end-to-end expertise to connect every dot, reimagine every process, and reinvent companies' ways of working. We know that rethinking each step from start to finish will create better business outcomes. Whatever it is, we'll be there with you - putting data and digital to work to create bold, lasting results - because transformation happens here, at Genpact.com.

For additional information contact, cfo.services@genpact.com and visit www.genpact.com/finance-accounting/enterprise-performance-management

Follow Genpact on Twitter, Facebook, LinkedIn, and YouTube.

Transformation Happens Here

genpact