genpact
Transformation Happens Here

POINT OF VIEW

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

Aligning teams, backed by artificial intelligence, to fight financial crime

Where there's fraud, there's often money laundering. Where there's money laundering, there's often fraud. For this reason, the Financial Crimes Enforcement Network (FinCEN) has issued advisories 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), assuming the transaction meets a minimal threshold.

Anti-money laundering (AML) is often overseen by a chief compliance officer and anti-fraud is often overseen by a chief risk officer. Historically, they view their missions as separate, despite the fact that they perform similar work centered around discerning patterns that may indicate a problem, investigating system-generated alerts, and identifying bad behavior. Ensuring that money is not lost through fraud – which requires real-time data solutions – was typically seen as a key component of the core business process. Identifying a case as fraudulent is easier, as the customer will usually report or verify it.

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

Conversely, the AML cost center is often driven by regulation, where identification of suspicious activity might be difficult and audit trails and documentation were critical. The two areas often did not communicate, work together, or share case management or monitoring systems, and competed for budget, resources, and senior management attention. This meant anti-fraud investigators would be unlikely to know that a person was also being investigated for money laundering, and vice versa.

In recent years, there has been a tendency to combine the two functions 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 more 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."

Combining AML and anti-fraud functions has been encouraged by regulators as they expect financial institutions to promote communication and collaboration internally

Working better together

Merging the two functions has many advantages. A key one is that much of the data required to detect money laundering is the same data that's needed to prevent fraud. For example, similar product types, such as international wire transfers and stored-value cards, are typically considered high risk and monitored more closely. Also, delivery channels, such as online and remote access, are at higher risk for both money laundering and fraud. AML and anti-fraud also leverage the same transactional parameters, account and customer information, peer group definitions, watch lists, and detection models. From both business and compliance perspectives, there's value in a united database that provides a holistic view of a customer's relationship with the bank and any concerns that the relationship raises.

AML know-your-customer procedures and documentation of customer's expected activity can serve as an important fraud tool. Moreover, 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, and alert and case analysis and investigations leverage many of the 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.

There's also potential to eliminate redundancies by combining AML and anti-fraud efforts. Moreover, consolidation can lead to more targeted and actionable alerts and investigations, with all alerts for the same subject being displayed to the analyst. With more information available, investigators can reach resolutions more quickly. Fraud detection rates also improve, as well as the ability to better identify sophisticated schemes. For example, multiple low-value events may not be registered as frauds, while an enterprise-wide system that aggregates data can detect previously hidden patterns.

Consolidation of AML and anti-fraud efforts can lead to more actionable alerts and thorough investigations, with all alerts for the same subject being displayed to the analyst

Moreover, there are potential cost savings realized through more efficient use of resources, including systems, data management, audit consolidation, reduction of IT staffing costs and software maintenance fees, and elimination of duplicate alert reviews and case investigations.

AML and anti-fraud units working together also makes the handing off of alerts, cases, and investigations easier. This should result in fewer duplicate SARs and more thorough SAR filings. The breaking down of silos can also lead to better identification of fraud and money laundering schemes that cross channels, products, and lines of business, and therefore greater visibility for management through aggregated data reporting, providing a more holistic enterprise-wide view.

Additionally, 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, businesses could have financial crime analysts responsible for reviewing both AML and fraud alerts rather than AML or anti-fraud analysts.

Challenges

Of course, challenges exist, one of which might be described as cultural. Individuals in an AML group tend to have a legal and compliance background, while those on the fraud side are generally more operational. Nomenclature is different. 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, recognize differences and integrate systems. The institution's case management system must support an integrated approach, while still providing the specific workflows vital for AML and fraud analysts

Moreover, institutions must leverage technology across disciplines. In this regard, financial institutions continue to ramp up their efforts to use artificial intelligence and digital tools for myriad 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 decision-making and workflow should be coordinated between AML and anti-fraud to best take advantage of available synergies.

The 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 - proceed slowly and methodically. A move to combine the two groups may not be right initially. It would require, among other things, creating a single transaction monitoring system running both fraud and AML rules and an entire new set of policies, procedures, and processes.

A better tactic might be to keep the groups separate but formalize the relationship with both areas reporting to the same executive. There should be regular meetings between the groups to discuss strategies, provide feedback, 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. If an AML alert does not turn out to be positive, it could still indicate the presence of fraud, and vice versa.

This approach would gradually develop a unified case management system that facilitates the appropriate handing off of files between analysts and investigators.

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

- Conducting a data assessment to ascertain quality, identify underutilized sources, and determine how to close any gaps
- Assessing the alert remediation process to fully understand the workflow architecture and identify additional opportunities to embed artificial intelligence, machine learning, automation and other digital tools
- Developing additional management information systems and other performance tracking key performance indicators to create enterprise-wide managerial measures of success and enable improved benchmarking
- Creating a centralized rule-based engine that is more dynamic and real-time, with existing rules optimized and new rules introduced to cover all current vulnerabilities

Crucially, technology can make compliance resilient, responsive, and sustainable. For example, digital solutions such as robotic process automation (RPA), machine learning, and artificial intelligence, can assist in data conditioning and consolidation. In financial crime compliance programs where the AML and anti-fraud divide is severe, there is typically significant data misalignment. RPA can alleviate this issue by quickly and accurately formatting data for use in a single, standardized system.

When it comes to better ways of working, the future for many institutions will be augmented intelligence - combining machine intelligence with human judgment. When it comes to financial crime detection, you can use artificial intelligence to analyze large volumes of multidimensional, real-time data to generate intelligent recommendations. These recommendations can be combined with years of human knowledge, experience, and technological expertise to determine when and how to act from a single source of truth. Only when artificial intelligence is used in this way can institutions expect to uncover financial crime where employees previously hadn't thought to look.

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

Data conditioning can be further improved by artificial intelligence as it can be used to fill in missing information, a problem which plagues both AML and anti-fraud units. These gaps, whether they are found in internal forms, transaction details, or third-party subscriptions, can be

confounding to lower-level investigators. Utilizing artificial intelligence to enrich client data and subject profiles will result in fewer false positives, reduced cycle time, and the alleviation of repetitive work that drains morale and causes investigator burnout.

In the financial crime compliance programs there may be a data misalignment. RPA can alleviate this issue by quickly and accurately formatting data into a single, standardized system

Moreover, by creating a single stream or more accurate alerts, investigators and managers will be able to approach their workflow in a properly risk-weighted or risk-segmented manner. A new case management solution, which incorporates 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 decision-making and improved agent and customer experience. Additionally, through modern digital interventions, AML and fraud case management can be intelligently augmented, allowing for streamlined case allocation, tracking, and suggested cross-unit communication. This would result in decreased information silos, further reduced 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, helping senior management to quickly understand the burdens and successes of their various units.

Furthermore, if these innovations are implemented in a way that allows for their underlying principles to be easily understood, key stakeholders can opt to bring in or release vendors and third-party data subscriptions with the confidence that these backend systems can be adjusted with minimal disruption to BAU.

The bottom line is that consolidation of an institution's AML and anti-fraud areas is an industry trend that meets regulatory expectations in a better fashion and offers the opportunity to achieve several benefits. But it must be approached carefully and thoughtfully, incorporating modern digital tools - especially artificial intelligence - and developing agile risk management frameworks that allow the ability to anticipate and act at speed and achieve greater compliance in an increasingly complex global banking environment.

The future is augmented intelligence – combining machine intelligence with human judgment. Use AI to analyze data to generate intelligent recommendations before applying human knowledge, experience, and technological expertise

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 to take full advantage of 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, and SAR filings - to help drive targeted AML and anti-fraud outcomes. These offerings include Smart Investigator, our case management solution, which can reduce cycle time while eliminating backlogs, and Smart Data Aggregator and Modeler, our data engineering and model development solution, which can reduce data aggregation times and cut false positives without losing critical data.

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 primarily for Global Fortune 500 companies. We think with design, dream in digital, and solve problems with data and analytics. Combining our expertise in end-to-end operations and our AI-based platform, Genpact Cora, we focus on the details - all 87,000+ of us. From New York to New Delhi and more than 25 countries in between, we connect every dot, reimagine every process, and reinvent companies' ways of working. We know that reimagining each step from start to finish creates better business outcomes. Whatever it is, we'll be there with you - accelerating digital transformation to create bold, lasting results - because transformation happens here.

For additional information visit, https://www.genpact.com/risk-compliance/fraud-and-disputes

Get to know us at Genpact.com and on LinkedIn, Twitter, YouTube, and Facebook.

genpact
Transformation
Happens Here