

The great divide:

**Getting convergence
right this time**



As the world becomes increasingly interconnected and digital, so too has the threat of financial crime. Traditionally, siloed methods of combating financial crime, such as anti-money laundering (AML) and fraud detection, must adapt to the changing landscape and find ways to effectively mitigate the risks posed by increasingly sophisticated cybercriminals. At the same time, the field of cybersecurity is also evolving due to increased threats, such as phishing schemes and business email compromise, which can lead to the redirection of payments by transnational criminal organizations.

The convergence of AML, fraud and cyber presents both challenges and opportunities for financial institutions (FIs) and law enforcement agencies. On the one hand, it requires the development of new technologies and approaches to identify and prevent financial crime. On the other hand, it also creates the opportunity for greater collaboration and information sharing among stakeholders, allowing for a more comprehensive view of risks posed to the institution.

This article will explore the convergence of AML, fraud and cyber and discuss the challenges and opportunities it presents. It will also examine the role of people, processes and technology in combating financial crime and consider the future of financial crime prevention in the digital age.

Similar, yet different

There is a clear overlap between fraud, AML and cybersecurity, as all three are concerned with protecting clients and the institution against financial crime and other illicit activity. For example, cybercriminals may commit fraud to steal sensitive financial information or launder money to obscure the origin of their funds. Similarly, individuals or organizations involved in money laundering may use cyberattacks to gain access to financial systems or to cover their tracks. Fraud was named as the largest driver of money laundering, generating billions of dollars annually, according to the U.S. Department of the Treasury National Money Laundering Risk Assessment, further highlighting the interconnection.¹

Despite the similarities between fraud, AML and cybersecurity, many previous attempts at convergence have failed. Some of the reasons are found in deep-rooted silos that have developed over the years, creating barriers to transformation. While there is general agreement that convergence drives many benefits, the hurdles can feel overwhelming to overcome.

HURDLES:	BENEFITS:
<ul style="list-style-type: none">• Siloed data and applications• Required buy-in from organizations with distinct leadership, budgets and operations• Satisfaction with the status quo• Short-term budget restrictions	<ul style="list-style-type: none">• Enhanced ability to identify complex financial crimes schemes• Equal access to technologies across domains• Alignment with regulatory expectations• Long-term cost savings

The benefits of the convergence of AML, fraud and cyber

Enhanced ability to identify complex financial crime schemes

As the financial sector becomes increasingly digital, so too does the risk of financial crime. Cybercriminals are constantly finding new ways to exploit vulnerabilities in the system, whether through phishing scams, ransomware attacks or other forms of cybercrime. At the same time, traditional methods of combating financial crime in money laundering and fraud are struggling to keep up with increasingly sophisticated threats that require broader data features and greater collaboration. Criminals exploit these intelligence gaps within FIs for their benefit.

Equal access to technologies and information across domains

Combining resources means that technology investments can be amortized across teams. Access to powerful and automated technology to handle tasks across the intelligence life cycle, from data engineering to model development, visualization and deployment to ongoing monitoring and optimization, is shared by the team. Illicit actors are always looking for the weakest link and will capitalize on it once found. Convergence raises the bar across the board for better defense.

Alignment with regulatory expectations

While regulators have not explicitly mandated convergence, there has been guidance that demonstrates an expectation of information sharing and collaboration. In the U.S., the suspicious activity reporting requirements have expanded in recent years to include mandatory suspicious activity report (SAR) submissions of cyber-events, and the Financial Crime Enforcement Network list of National Priorities emphasizes comprehensive risk management. Greater collaboration across teams also ensures standardized business processes and improved governance for meeting regulatory filing requirements.

Long-term cost savings

There is the redundancy of data, technology and workforce across silos that is increasing the cost of compliance. However, convergence brings long-term cost savings through integration. In a recent survey, LexisNexis found that institutions that invest more in technology transformation have experienced lower costs and fewer compliance operations challenges.²

The hurdles to the convergence of AML, fraud and cyber

Siloed data and applications

Overhauling deeply siloed data and applications can feel overwhelming and requires multi-phased projects to unravel. When embarking on enterprise-scale projects, leaders often struggle with where to start. Creating an inventory of technology and business processes in the current state and a strategy of what the target state will look like is a great start. Convergence is an evolution, so start with applications that have an overlap of data to deliver quick wins to stakeholders.

There are many unknowns when embarking on the convergence journey, but the payoff will improve the ability to manage both risk and operations

Required buy-in from organizations with distinct leadership, budgets and operations

Cooperation across organizations is often harder than it looks. Leadership has different charters, budgets and distinct operations, which require changing deeply entrenched processes. Fraud leaders are concerned with losses and the bottom line. AML leaders are worried about meeting regulatory expectations and mitigating reputation risk. Cyber leaders often have oversight that goes far beyond financial crime into areas such as conduct and physical security. It is essential to have executive sponsorship at a program level as strategies will evolve based on innovations in technology and the threat landscape.

Satisfaction with the status quo

Some leaders pay homage to the old saying, "if it is not broken, do not fix it." Change is disruptive and can evoke fear regarding goals not being aligned, not being able to balance workloads through the technology integration process and/or the impacts it will have on morale. There are many unknowns when embarking on the convergence journey, but the payoff will improve the ability to manage both risk and operations. Ideally, convergence will make investigators' work more impactful by providing them with greater intelligence and context.

Short-term budget restrictions

The World Bank has cited that the global economy will come "perilously close" to a recession due to a slowdown in mature markets such as the U.S., Europe and China.³ In response to this and other economist predictions, FIs are signaling tightened budgets. However, there are steps that can be taken to augment current operations working toward convergence.

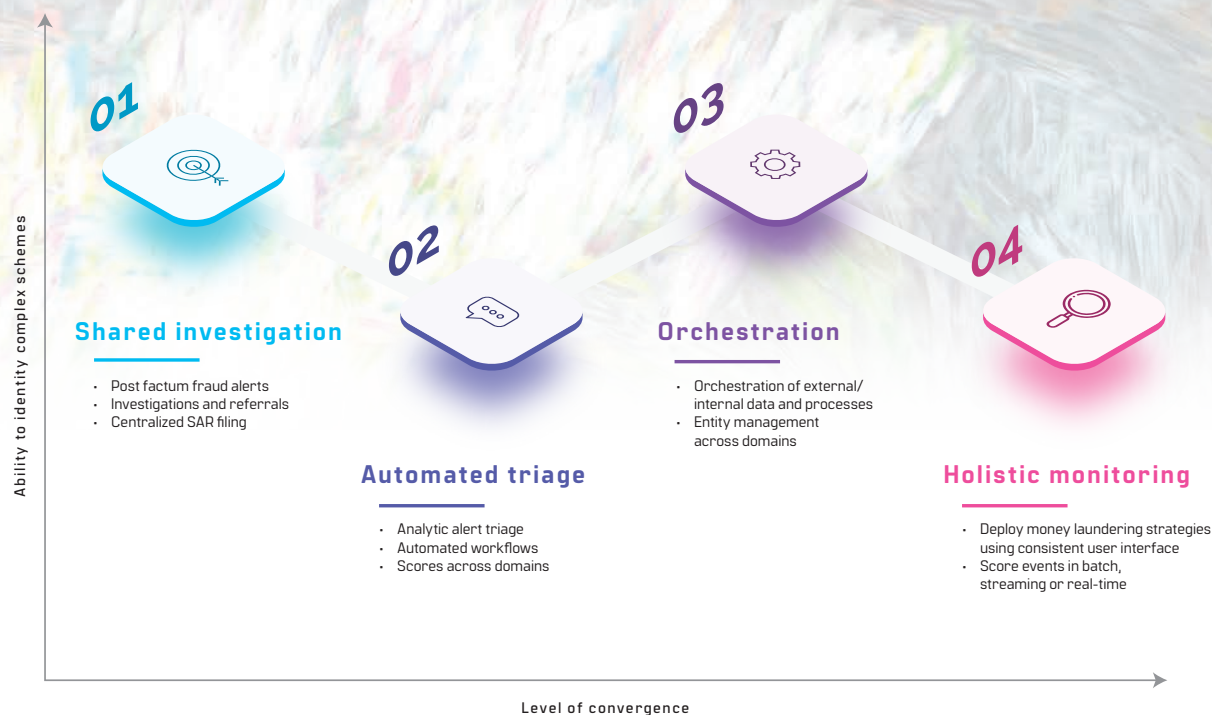
What modern convergence looks like

There are many misconceptions about what convergence looks like, so perhaps the best place to start is to define what convergence is not. Convergence does not look like the following:

- Elimination of specialized experts in fraud, AML and cyber
- Single business process and workflow for all domains
- Common service-level agreements
- One detection engine

Convergence is about bringing people and data together using technology while embracing what each needs to reach quality decisions. This is best illustrated in Graphic 1 by reviewing different operating models that are found in the industry:

Graphic 1: The levels of convergence




Source: SAS

- 1. Shared investigation:** Known fraud events, automated system alerts and manual referrals are collated into a common case management system. If entity management of common party identifiers is lacking, advanced search is a critical requirement. Typically, SARs/suspicious transaction reports (STRs) are filed following centrally governed processes.
- 2. Automated triage:** Discrete detection events are consolidated into a common scoring and prioritization methodology. The ability to score at a party or external party dimension is desirable. Common policies and operating models are governed through automated workflows that improve sharing of information across teams.
- 3. Orchestration:** Through industry-standard application programming interfaces (APIs), external data (adverse media, device reputation, biometrics, etc.) is ingested to supplement profiles and historical data to derive a more complete view of risk exposure. For AML investigators, this can reduce the time it takes to complete an investigation. In fraud operations, orchestration may be used to push step-up authentication or deposit holds based on a series of conditions.
- 4. Holistic monitoring:** As model governance becomes more critical to deploying machine-learning strategies, providing common user experience and methodology is essential. In some cases, the features and algorithms may be designed to identify productive investigations without bias to traditional typologies.

In a 2021 survey, Aite Novarica cited that 42% of FI compliance executives had information and data sharing as well as enterprise policies and processes in place. Furthermore, 27% had fully consolidated case management and staff, while only 23% had integrated detection technology.⁴

Conclusion

The convergence between fraud, AML and cybersecurity is a major challenge for organizations and governments around the world. The lines between financial crime disciplines have blurred due to the sophistication and coordination of transnational criminal organizations. To effectively address these challenges, it is necessary to adopt a comprehensive approach that combines strong technical controls with effective risk management and compliance processes. By working together, we can create a safer and more secure financial system for all. 

Beth Herron, manager, Americas Fraud and Security Intelligence Practice, Beth.Herron@sas.com

David Stewart, director, Financial Services Vertical, Global Security Intelligence Practice, David.Stewart@sas.com

Rob Goldfinger, CAMS, senior SME, Fraud Security and Intelligence Business Development, Rob.Goldfinger@sas.com

¹ "National Money Laundering Risk Assessment," *U.S. Department of the Treasury*, February 2022, <https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf>

² "2022 True Cost of Compliance Study Global Summary," *LexisNexis Risk Solutions*, June 2022, <https://risk.lexisnexis.com/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report>

³ "Global Economic Prospects," *The World Bank Group*, January 2023, <https://openknowledge.worldbank.org/bitstream/handle/10986/38030/GEP-January-2023.pdf>

⁴ "Key Trends Driving AML Compliance Transformation in 2022 and Beyond," *Aite Novarica*, February 2022, <https://aite-novarica.com/report/key-trends-driving-aml-compliance-transformation-2022-and-beyond>