protiviti®
Global Business Consulting

COMPLIANCE INSIGHTS

Where fraud meets compliance: Building a stronger line of defence

By Carol Beaumier and Bernadine Reese

Efforts by the financial services industry to merge the management of fraud and compliance risk — particularly, but not exclusively, anti-money laundering (AML) risk — have been evolving over the last quarter century. There are examples, frequently unsuccessful, from the early 2000s of financial institutions — from traditional banks to insurance companies — that sought to integrate their fraud and AML risk management functions (often referred to as "FRAML"). For the industry at large, however, Fraud and Compliance remained distinct disciplines with little mainstream focus on formal convergence.

Traditional description of fraud and compliance disciplines

- **Fraud**: detection, prevention and response to malicious behaviour resulting in financial loss or other form of enterprise harm.
- **Compliance**: adherence to jurisdictional laws, regulations and policies.

The slow journey toward integrated fraud and compliance risk management

By the mid-2010s, the impetus for at least a better alignment between Fraud and Compliance functions increased, driven in part by:

- The recognition that Fraud and AML teams were increasingly investigating the same bad actors and using the same, or at least similar, threat/risk typologies.
- Regulators, such as the UK Financial Conduct Authority (UK FCA) and the U.S. Financial Crimes Enforcement Network (FinCEN), encouraging greater collaboration among AML, Fraud and Cybersecurity functions.

- Technology vendors of all sizes — from fintech firms to established providers — beginning to offer integrated detection platforms.

Even still, convergence remained mostly an aspirational concept, not a reality, save for a handful of larger financial institutions that did seek to gain some operational efficiencies.

In the last three or four years, the convergence of fraud and compliance risk management has moved beyond a "nice to have" efficiency play to a strategic imperative. Why? Moody's in a 2025 study cites three compelling reasons:

- Instant payments allow fraud and money laundering to occur nearly simultaneously.
- Fraud is increasingly a predicate offense that directly feeds AML investigations.
- Institutions using separate systems lose visibility and experience slow response times.

Taken together, these developments signal a clear inflection point. What began as sporadic attempts at organisational efficiency have accelerated into widespread recognition that fraud and AML risks are now deeply intertwined — operationally, technologically and strategically.

The shifting landscape

Regulatory drivers and government focus

In addition to the realities identified by Moody's, there is continued regulatory emphasis on the need for coordination. For example, the EU Anti-Money Laundering Authority (AMLA), which launched in 2025, was formed to integrate supervisory oversight and intelligence sharing across financial-crime domains and explicitly to close the loopholes exploited by complex schemes that involve both fraud and money laundering. Similarly, FinCEN's February 2026 launch of its whistleblower tip program encourages the reporting of known or suspected money laundering violations and fraud schemes.

At the same time, jurisdictions such as Singapore and the UK are tightening consumer-protection rules, with particular attention to fraud reimbursement. In Singapore, the Shared Responsibility Framework mandates losses from certain types of phishing scams be equitably shared among scam victims, financial institutions and mobile telephone operators.

Under the UK fraud payment reimbursement rules, all payment service providers, including banks and electronic payment firms, must reimburse eligible victims of Authorised Push Payment (APP) fraud made via Faster Payments or CHAPS. In addition to the "liability shift," this mandate provides additional safeguards for vulnerable customers. The rapid growth of fraud perpetrated on consumers means that an increasing regulatory focus on consumer protection and reimbursement is likely.

Beyond the actions of the regulators, the proliferation of fraud has gained attention at the highest levels of government. On March 6, President Trump signed an Executive Order titled "Combating Cybercrime and Fraud," instructing various government agencies to coordinate and do more to identify tools to combat fraud and cyberattacks. The signing of the order followed a hearing of the House Financial Services Committee in which financial services industry executives voiced their support for more government assistance in fighting these crimes.

In the UK, the government announced in March a new fraud strategy and launched the Online Crime Centre to bring together specialists from government departments, intelligence agencies, the police, banks, mobile phone networks and technology firms. The intention is to share data, deploy AI and work together in coalescence to build a single picture of global fraud networks. Greater alignment by UK authorities is expected to enable deeper coordination across both fraud and compliance matters.

These governmental efforts emphasise that fragmented approaches to identifying and addressing fraud risks are no longer sufficient — a message that should resonate with financial institutions.

Fraud trends and modus operandi

As long as financial institutions have existed, fraudsters have been trying to exploit them and their customers. Modern fraud challenges include an array of tactics such as social engineering, account takeover, mule networks, real-time payments fraud and deepfakes. These methods not only exploit vulnerabilities in existing systems but also capitalise on the increasing reliance on digital transactions and the rapid advancement of technologies such as AI. For example, social engineering techniques, which manipulate individuals into divulging confidential information, have become alarmingly prevalent.

Similarly, account takeover schemes involve fraudsters gaining unauthorised access to legitimate accounts and often lead to significant financial losses for consumers and institutions alike. Both threat vectors may use data harvested from cyberattacks (or other forms of data compromises/leaks). The convergence of these fraud trends highlights the inadequacy of siloed approaches to compliance and fraud prevention.

As fraudulent activities become more intricate and intertwined with legitimate transactions, financial institutions must adopt a holistic view that encompasses both compliance and fraud detection.

Technological disruption

Digital identity technologies, artificial intelligence and machine learning (AI/ML), behavioural analytics and modern data architecture are allowing financial institutions to unify the historically fragmented worlds of compliance and fraud risk management. Digital identity and access management technologies, including device intelligence, biometrics and identity-proofing platforms, add another critical layer of detection: Verify who a customer *actually is* and detect synthetic or manipulated identities before they enter the ecosystem, closing a key gap exploited by both fraudsters and money launderers.

AI/ML models can analyse vast amounts of structured and unstructured data in real time, allowing financial institutions to identify suspicious behaviours earlier and with greater accuracy. When coupled with behavioural analytics, financial institutions can move beyond simple rule-based alerts to recognise subtle anomalies in customer behaviour. This more targeted approach dramatically reduces false positives — a major inefficiency in both AML and fraud operations — and creates shared insights that benefit both Fraud and Compliance.

Types of fraud affecting financial institutions and their customers

- APP fraud, social engineering scams
- Check fraud
- Loan fraud
- Phishing, smishing, vishing including business e-mail compromise (BEC)
- Account takeover fraud
- First party and synthetic identity fraud
- P2P payment fraud
- Real-time, instant payment fraud
- Deepfake-enabled fraud
- Mule activity
- Internal fraud

Data lakes serve as the connective tissue that makes these capabilities work holistically. Instead of siloed datasets scattered across compliance, fraud, operations, credit and customer channels, data lakes consolidate relevant information into a single environment with consistent governance and schema flexibility. This unified data foundation allows AI and analytics tools to run across customer journeys, transactional flows and risk indicators simultaneously — something older architectures simply cannot support.

As a result, financial institutions can deploy enterprisewide risk scoring, shared alerting and cross-functional dashboards. The outcome is a more integrated, intelligence-led approach that reduces duplicative reviews and accelerates the investigation process. Ultimately, these technologies enable financial institutions to move from reactive, siloed controls to proactive and coordinated risk management — bridging Compliance and Fraud in a way that reduces inefficiency and improves overall program effectiveness.

Cyber risk

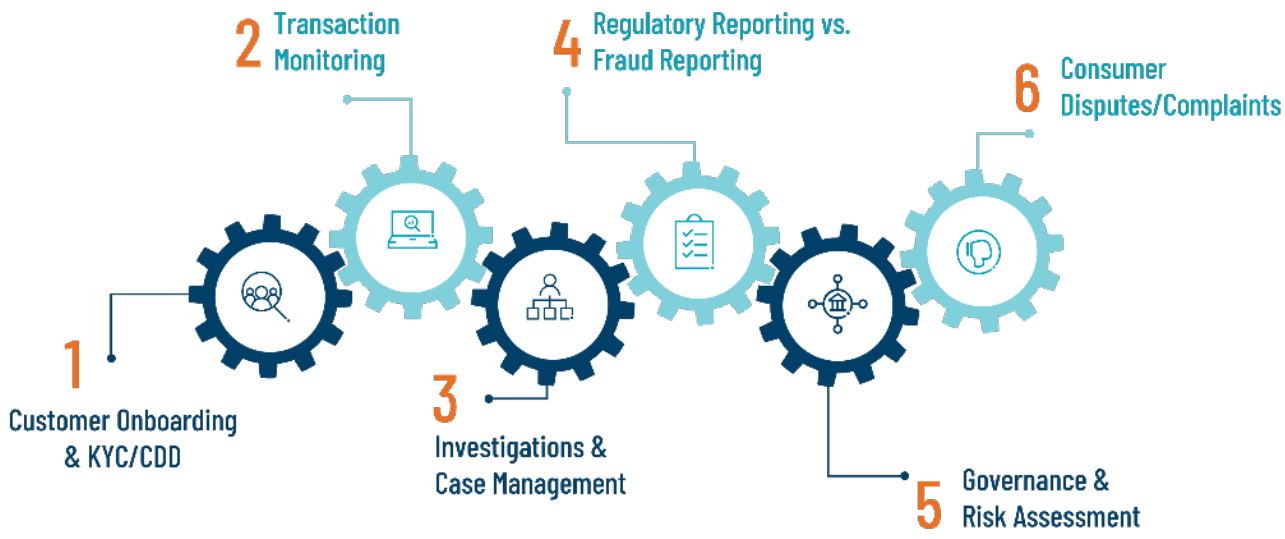
Closely related to technological disruption is the escalation of cyberattacks. Cyberattacks at financial institutions, including orchestrated automated-electronic threats (e.g., "bot" attacks), provide threat actors the access and data they need to execute fraudulent transactions. Data breaches and system intrusions expose sensitive customer information criminals use to take over accounts or authorise illicit transfers. Increasingly, AI-enabled cyberattacks amplify the problem: Bad actors use deepfakes, AI-enhanced social engineering and realistic impersonation to trick employees or customers into approving fraudulent payments or bypassing basic know-your-customer (KYC) controls.

Cyberattacks on third-party service providers also create systemic openings for fraud by disrupting core platforms, degrading controls and exposing multiple institutions simultaneously. These vulnerabilities, when exploited, can enable large-scale fraud campaigns that move quickly across interconnected systems.

The bottom line: Criminals — whose sophistication is steadily rising with the "democratisation" and "weaponisation" of AI for nefarious activity — do not distinguish between fraud and compliance; the regulators do not distinguish; therefore, financial institutions should not distinguish either. The enterprises that prosper will be those that create a unified framework that recognises and supports the shared mission of fraud and compliance risk management: To protect the integrity of the financial institution.

Where the intersections occur: Six critical touchpoints

The convergence of Compliance and Fraud functions is most palpable at six critical touchpoints within the financial institution's operating model. These intersections represent both the challenges and opportunities for building a stronger, unified line of defence.



Six Critical Touchpoints

Customer onboarding is the first line of defence against both financial crime compliance breaches and fraudulent activity. A thorough and integrated identity assurance/verification and document authentication that

includes both advanced document authentication and biometric checks not only satisfies KYC/CDD (know your customer/customer due diligence) requirements but can also identify and prevent synthetic identity fraud. Similarly, shared data models for risk scoring enable institutions to flag high-risk customers early, supporting both compliance and fraud prevention objectives. By integrating fraud detection logic into KYC/CDD workflows, financial institutions can help reduce fraudulent activity upon entry and minimise the risk of money laundering at the same time.

Transaction monitoring is another key area where Fraud and Compliance overlap and could be aligned to much greater effect. Both disciplines analyse transaction patterns for suspicious/anomalous activity, often using similar typologies and alerting logic but distinct monitoring tools and platforms. This can result in duplicative alerts for transactions or activities that trigger for both fraud and AML purposes. However, leveraging shared data and behavioural analysis allows for more accurate detection of both compliance violations and fraud schemes — particularly as real-time payments and cross-border transactions grow in complexity. Unified transaction monitoring systems enable more intelligent risk detection via a faster triage process and reduction of alert fatigue, thus ensuring that critical threats are not overlooked.

Once suspicious activity is detected**, investigations and case management** become the focal point for resolving both compliance and fraud issues. Traditionally, cases are managed in separate platforms, leading to duplicated customer outreach, inconsistent findings, incomplete information and reconciliation challenges. Integrated case management platforms facilitate coordinated investigations, centralise documentation and support collaborative triage models, with an added benefit of reduced operational costs due to process synergies. This approach not only enhances operational efficiency but also ensures consistent and comprehensive decisions are made to cover all aspects of a given scenario.

Reporting obligations are another area where the boundaries blur between AML compliance and fraud. For example, Suspicious Transaction Reports (STRs)/Suspicious Activity Reports (SARs) and fraud reporting must be made and often handled by separate teams — although this varies by country and financial institution — to differing processes and standards**.** The information reviewed tends to be specific to the issue raised and there is limited scrutiny of the wider activity or previous decisions. Unified reporting frameworks can help reduce duplication; improve accuracy, headcount and operational effectiveness; and result in more comprehensive and insightful reports.

Duplication of fraud and **AML governance and risk assessments** can result in less effective outcomes. Unified governance structures foster cross-functional collaboration and drive accountability, a more detailed understanding of the issue and consistency of decision-making. By combining fraud and other financial crime risks into a single risk taxonomy, financial institutions can gain a better understanding of the risk environment and are better able to assess and prioritise responses. Similarly, joint enterprisewide risk assessments and customer risk assessments covering both fraud and wider financial crime ensure that emerging risks are identified, measured and mitigated across all relevant risk factors.

Customer disputes and complaints often reveal hidden risks and vulnerabilities that are valuable to both fraud and money laundering compliance. Both Compliance and Fraud teams benefit from analysing dispute and complaint data, which can signal systemic issues or new fraud trends. Furthermore, integrated handling of complaints ensures reduced customer friction via more timely and consistent resolutions while also enabling institutions to identify root causes and strengthen controls.

The historical barriers

Despite the growing recognition of the need for convergence between Compliance and Fraud functions, several historical barriers have hindered progress. Among these, cultural and regulatory challenges have been particularly significant, creating silos that limit collaboration and efficiency.

A significant obstacle to integration is the cultural divide between Fraud and Compliance enterprise teams. Fraud prevention often is established as a first-line business operations function, focused on minimising losses and ensuring customer satisfaction, whereas Compliance is typically a second-line function**,** dedicated to adhering to legal and regulatory standards. This difference fosters competing missions: Fraud teams prioritise operational responsiveness, while Compliance teams emphasise governance and risk management. In some instances, these barriers are a smokescreen to mask turf battles — the unwillingness to cede authority or autonomy in an integration. Misaligned performance metrics can further exacerbate the divide. Fraud teams are evaluated on loss reduction and efficiency, while Compliance teams are judged on regulatory adherence. This friction can lead to isolated operations rather than collaborative efforts.

Regulatory expectations, which continually morph and vary across jurisdictions, also pose a challenge, particularly the requirement for maintaining appropriate second-line independence. Compliance functions must operate independently from first-line activities to ensure impartial oversight. While essential for governance, this independence can hinder collaboration with Fraud teams. None of these barriers is insurmountable, but they do require careful and considered design of the framework, roles and responsibilities and appropriate governance.

For many institutions, though, the barrier to integration is centred on the need for technology modernisation, including upgrading systems, migrating to the cloud to support the use of AI/ML, tackling data siloing and data deficiencies, and involving additional internal

The legacy mindset holding back integration

- Fraud and Compliance have different missions: Fraud's principal role is to protect the organisation and its customers from financial harm. Compliance's remit is to comply with laws and regulations.
- Compliance looks at activity after the fact and needs to provide a clear audit trail to support its conclusions. Fraud needs to act immediately and in real-time or near-real time to stop the bad actors and prevent financial loss and would never be able to satisfy Compliance's documentation standards.
- Compliance needs a lot of background on customers, counterparties and historical activities to reach its conclusion. Fraud is focused on device IDs, velocity, geolocation and authentication failures — *threats in the moment*.
- Fraud is about stopping losses. Compliance is about reporting and regulatory adherence.
- Compliance's independence mandate prevents it from merging with Fraud.
- Fraud and Compliance face off to different authorities who have separate and specific processes and expectations.
- Fraud and Compliance investigators need different skillsets.
- Integrating Fraud and Compliance investigations would slow down the process.

stakeholders (e.g., the Chief Data Officer, Chief Technology Officer, Chief Information Officer). Technology plays a pivotal role in enabling convergence, offering financial institutions unified data architecture and shared analytics platforms leveraging AI/ML and behavioural analytics across both Compliance and Fraud functions, and enabling advanced tools such as real-time payment protection to reduce the time to detect and mitigate threats.

The importance of addressing these issues extends well beyond their impact on Fraud and Compliance integration efforts. Technology modernisation and fixing data silos/data deficiencies, though, are foundational to the future viability of financial institutions. Financial institutions that fail to modernise both technology stacks and data access and capabilities will face rising costs, shrinking competitiveness and heightened risk.

The benefits of convergence

Converging Compliance and Fraud functions offers financial institutions the opportunity to build a stronger, more cohesive holistic defence against financial crime. By breaking down silos, institutions can unlock significant benefits including:

- **Enhanced risk detection.** Convergence empowers financial institutions to detect risks more accurately and earlier in the lifecycle of financial crime through sharing intelligence and improved insight generation of red flags using advanced analytics. In addition, early detection of suspicious activity is facilitated by integrated transaction monitoring and behavioural analytics, helping financial institutions stay ahead of evolving risks. This enhanced capability is particularly critical in combating sophisticated fraud techniques such as synthetic identities and real-time payment fraud, which have been on the rise because of perpetrator erudition coupled with increased weaponisation of AI.

- **Operational efficiency and cost reduction.** One of the most immediate advantages of convergence is the reduction of duplication in processes, data management, talent cadre optimisation and streamlining of investigative processes. Consolidating these functions enables efficient workflows, eliminating inefficiencies such as duplicate alerts or parallel investigations, as well as resource optimisation through shared data, technology and headcount.

- **Improved customer experience.** Reduced duplication or friction during onboarding allows for fewer false positives enabled by shared intelligence and analytics and greater accuracy of risk assessments and potentially faster resolution through coordinated investigations and case management.

- **Regulatory resilience.** A converged model strengthens an institution's ability and dexterity to meet current and evolving regulatory requirements, allowing consistent and accurate recordkeeping and providing clear oversight and accountability, all while demonstrating compliance with regulations and guidelines.

- **Lower enterprise risk.** A more resilient, measurable and sustainable financial crimes program reduces the likelihood of major fraud losses as well as regulatory and reputational risk.

The desired end state … and the journey to reach it

The desired end state for a unified financial crime and compliance risk management framework — let's call it an Enterprise Threat, Financial Crime & Customer Integrity Framework — is one where shared governance, standardised procedures, and a consolidated data and technology ecosystem support an integrated, not siloed, approach to managing cyber risk, financial crime (including fraud, AML and sanctions) and any resulting customer harm.

Threefold mission of integrated framework

Recognise	Respond	Report
• Horizon scanning (new and emerging typologies, threat intelligence) • Customer due diligence and verification, with appropriate countermeasures to protect against identity fraud • Unified, risk-scored transaction monitoring and converged case management so reviewers and investigators see everything at once — KYC and identity attributes, transaction monitoring results, fraud intelligence, geolocation anomalies, patterns across channels	• Real-time intervention (e.g., blocking transaction, holding transaction for additional review, alerting customers, activating countermeasures)	• Integrated management reporting • Suspicious activity reporting • Coordination with law enforcement

This function is led by a Chief Financial Crimes Officer and is staffed with a cross-disciplined team with diverse backgrounds and skillsets, including data scientists and AI/ML domain experts, threat intelligence analysts, behavioural analytics, scam specialists, sanctions experts, typology designers, skilled investigators and red

teamers. In some organisations, this will require both upskilling and investing in additional talent, but in many institutions these roles already exist but operate in silos. The integrated team has a three-fold mission — recognise, respond and report suspicious activity across all domains.

At its core, the integrated framework provides a holistic view of customer and counterparty behaviour — supported by a common data lake, advanced entity resolution and responsible AI-driven analytics — that enables real-time recognition and response to suspicious activity. The integrated framework also supports internal and external reporting that aids in continuous learning that serves to enhance an institution's program and better protects it and its customers. The move from the traditional siloed approach to an integrated framework will present challenges for some organisations. Typically, the journey will include five stages:

1. **Minimum cooperation stage.** Organisations in this stage coordinate to a limited extent (e.g., on SAR/STR filing) but remain unconvinced of the real benefits of aligning activities further.

2. **Acknowledgement stage.** Organisations in this stage recognise that fraud, AML, sanctions, cyber and customer protection risks increasingly share common data, common actors and common attack surfaces, while also benefiting from common detection approaches and analytical methodologies. Here, organisations often have formed cross-functional working groups and share information on identified suspicious activity and, in some cases, conduct joint investigations at least on an *ad hoc* basis.

3. **Alignment stage.** At this stage, organisations have begun coordinating processes, data and analytics but without updating their organisational structures. To reach the alignment stage, organisations need to be able to consolidate — or at a minimum link — alerting and case management platforms and be at least in the early stages of using AI/ML to inform their efforts.

4. **Integration stage.** At this stage, organisations formally adopt a unified framework that is centrally managed by a Chief Financial Crimes Officer. Here, intelligence sharing, identity and AML checks, transaction monitoring, case disposition, and reporting are all fully integrated.

5. **Optimisation stage.** At this final stage, organisations operate using a unified platform that seamlessly monitors customers, counterparties, identities, devices and behaviours. Here, monitoring is real-time, AI/ML models are used for autonomous detection, customer onboarding is digitally supported, customer risk scoring is dynamic, and customer complaints and cyber events are added to traditional AML, sanction and fraud indicators to create a holistic view of the risks.

For many institutions, the progress toward convergence will need to be incremental as they determine the best way to tackle the existing barriers. With cost optimisation an ongoing focus for financial institutions broadly, efficiency improvement and reduction in financial losses remain compelling arguments to advance integration.

Conclusion

Ultimately, the shift toward integrated Fraud and Compliance functions is about more than structure. It is about leadership choosing collaboration over fragmentation, shared intelligence over siloed information and customer protection over organisational turf battles. Institutions that embrace this mindset will define what credible, modern financial crime risk management looks like in the years to come.

Protiviti Managing Directors Constantine Boyadjiev and Tom Giltrow contributed to this article.

About the authors

Carol Beaumier is a senior managing director in Protiviti's Risk and Compliance practice. She has more than 30 years of experience in a wide range of regulatory issues across multiple industries. Before joining Protiviti, Beaumier was a partner in Arthur Andersen's Regulatory Risk Services practice and a managing director and founding partner of The Secura Group, where she headed the Risk Management practice. Before consulting, Beaumier spent 11 years with the U.S. Office of the Comptroller of the Currency (OCC), where she was an examiner with a focus on multinational and international banks. She also served as executive assistant to the comptroller, as a member of the OCC's senior management team and as liaison for the comptroller inside and outside of the agency. Beaumier is a frequent author and speaker on regulatory and other risk issues.

Bernadine Reese is a managing director in Protiviti's Risk and Compliance practice. Based in London, Reese joined Protiviti in 2007 from KPMG's Regulatory Services practice. Reese has more than 30 years' experience working with a variety of financial services clients to enhance their business performance by successfully implementing risk, compliance and governance change and optimising their risk and compliance arrangements. She is a Certified Climate Risk Professional.

About Protiviti's Compliance Risk Management practice

There's a better way to manage the burden of regulatory compliance. Imagine if functions were aligned to business objectives, processes were optimised, and procedures were automated and enabled by data and technology. Regulatory requirements would be met with efficiency. Controls become predictive instead of reactive. Employees derive more value from their roles. The business can take comfort that their reputation is protected, allowing for greater focus on growth and innovation.

Protiviti helps organisations integrate compliance into agile risk management teams, leverage analytics for forward-looking and predictive controls, apply regulatory compliance expertise and utilise automated workflow tools for more efficient remediation of compliance enforcement actions or issues, translate customer and compliance needs into design requirements for new products or services, and establish routines for monitoring regulatory compliance performance.