PARTNER
WHITE
PAPER

Enterprise Fraud and Financial Crimes Compliance: How Banks Need to Adapt

sas | Capgemini

Contents

Introduction

In the digital age, the implications of fraud and financial crimes against financial services institutions and their customers have become ever more significant. These risks now represent one of the biggest areas of concern for the industry and one of the largest drivers of IT expenditure and compliance costs.

Fraud

Typical organizations **lose 5% of revenues to fraud each year**. The most frequent victims are the banking and financial services, government, and manufacturing industries. The digital economy and the rise of cybercrime create an even greater level of vulnerability for banks and other financial institutions.

The European Central Bank **published statistics in 2020** that showed the total value of transactions using cards issued in SEPA countries amounted to EUR 4.84 trillion in 2018, of which EUR 1.8 billion was fraudulent. Card fraud volume increased by 25.1% compared with 2017, while the total number of card transactions increased by 11.3%. The same report highlights that 79% of the value of card fraud in 2018 resulted from card-not-present (CNP) payments (i.e., payments via the internet, mail or phone); 15% from transactions at point-of-sale (POS) terminals, such as face-to-face payments at retailers or restaurants; and 6% from transactions at ATMs.

The Federal Trade Commission has announced that in 2020, **people filed more reports about identity theft (29.4% of all reports), in all its various forms, than any other type of complaint**. Impostor scams, a subset of fraud reports, followed with 498,278 reports from consumers in 2020 (10.6% of all reports). Online shopping and negative reviews (7.5% of all reports) rounded out the top three reports to FTC's Consumer Sentinel.

While direct losses due to fraud are staggering, the actual cost is much higher when you consider lost productivity, customer confidence and attrition, and undetected fraud. Fraudsters keep getting more sophisticated, changing their mechanisms and making transactions and money movements more complex. They are also becoming more digitized, taking advantage of synthetic identities, data breaches, the dark web and faster payments movement.

Financial crime compliance

The cost of compliance has been on an upward trend for some time, increasing by double-digit percentages. The projected global cost of financial crime compliance is $180.9 billion, led by the UK and Germany, followed by the US, France and Italy, **according to a recent study**.

Labor costs are a significant driver of spending for Know Your Customer, anti-money laundering and sanctions programs. This is also now being acknowledged as a growing problem for fraud prevention. Due to rising alert volumes, high false positive rates and manual tasks, financial institutions have seen a sharp climb in head count to manage both regulatory and operational compliance risks. Additionally, siloed operations for fraud and financial crime compliance have created gaps in understanding holistic customer risk and created inefficiencies in both detection and investigation. As a result, there is accelerating innovation in the financial crimes compliance field to improve the identification of illicit actors and reduce inefficiencies.

Convergent attacks blur distinctions among cyber breaches, fraud, financial crimes

Fraud & insider threats

- Internal & external threats.
- Retail & nonretail threats.
- Insider threats.
- Market abuse & misbehavior.

Cyber breaches

- Confidentiality.
- Integrity.
- Systems availability.

Financial Crimes

- Money laundering.
- Bribery & corruption.
- Tax evasion & fraud.

Example: Cyberattack on central bank

- Employee SWIFT* credentials stolen with insider help.
- Malware installed to prevent discovery.
- Funds routed from bank's account at a branch of another country's central bank to a third bank (on a weekend to ensure staff absence).
- Withdrawals made at third bank through multiple transactions not blocked in time.
- Attacks may have been linked to a known sanctioned entity.

* Society for Worldwide Interbank Financial Telecommunication

Fraud, to some degree, has an easier route to efficiency. Most third-party fraud, except ATO and synthetic identities, can be confidently resolved by automated customer contact, such as SMS and push notifications. In fact, consumers are expecting these zero-touch interactions. This just leaves first party and internal fraud, along with corporate customers, needing a higher investment of effort through alert investigations.

Where is fraud and financial crime compliance falling short?

The increasing significance of fraud and financial crime is taxing first generation fraud management solutions and placing pressure on many banks' financial crime management capabilities. As financial institutions have grown larger, managing many portfolios and related business lines across multiple channels has made fraud and suspicious activity detection more difficult. Many solutions are focused on only one channel or type of crime. Disparate, multiple systems of record make detection of suspicious activity across the enterprise extremely difficult. Current systems and processes are reactive to fraud once it has occurred and fall short of taking proactive steps to combat cross-channel behavior.

With the level of sophistication of fraudsters increasing, many fraud and money laundering detection systems are no longer effective enough. While rules-based systems are good at spotting recurring and known financial crime patterns, they can also flag too many legitimate customers, and fraudsters can use targeted methods to circumvent the system. Rules-based systems are unable to detect emerging patterns of fraud and money laundering and can miss crimes concealed in complex layers of transactions across channels, products and accounts.

Financial institutions must carefully balance risk identification and loss prevention against the customer satisfaction that comes from faster transaction processing. They should also rethink and accelerate their processes so they can react quickly to changing industry requirements. Furthermore, too many false positives, inefficient investigative processes and lack of accuracy in transaction authentication all drive up operational costs as financial institutions must increase spending on financial crime risk management against sophisticated attacks.

The combination of money laundering, organized crime, global terrorism and new types of fraud – plus banking industry drivers and increased regulatory requirements – has led financial services organizations to pursue new techniques for preventing and detecting illegal activity.

> "In today's digital and mobile banking environment, banks should be looking to manage fraud across channels and lines of business from a single view of fraud risk. A platform that can integrate legacy channel fraud applications and point solutions to create a unified fraud risk score for any entity in real time is a strategic goal that banks should be striving to achieve."
>
> **IDC MarketScape:** Worldwide Enterprise Fraud Management in Banking 2020 Vendor Assessment

5 emerging trends driving the next generation of fraud and financial crime management

Forward-thinking banks are evolving their fraud and financial crime management systems from a level of standalone rules-based detection to one of enterprise predictive risk assessment. They are integrating more data, machine learning provided by advanced analytics and real-time functionality with customer experience. These new solutions capitalize on five emerging trends in fraud and financial crime management.

1. A centralized approach to fighting financial crime

To both increase efficiency and improve the effectiveness of fraud detection and prevention, an increasing number of financial institutions are implementing solutions that cover a broad spectrum of financial crimes, including cybersecurity, fraud and anti-money laundering. Integrated solutions enable firms to leverage information more easily and more efficiently comply with numerous evolving regulatory requirements while driving down costs. Centralized operations help to break down silos across business units and channels for a holistic view of risk. Furthermore, maintaining data and infrastructure security and updating fraud management systems with new rules, statistical models and acquired knowledge becomes easier and more efficient with centralized systems.

Several leading banks are now coordinating AML to provide efficient implementation and tangible business value.

For one large North American bank, combining fraud and AML paid dividends in transaction monitoring. An independent assessment of the value of fraud prevention estimated that for every dollar invested in the bank's enhanced AML fraud capabilities (including implementing a leading vendor solution), $27 in fraud was prevented. Currently, the bank prevents 97% of attempted fraud.

A large French bank rolled out AML/CTF across 17 European countries via a centralized program. A central team conducts investigations on behalf of subsidiaries across Europe and feeds back only those cases requiring hands-on investigation by local AML officers. In this way, the bank was able to continuously improve its processes and standardize its risk-based approach at a group level.

As centralized AML controls mature, banks and their regulators can be confident they can actively detect money laundering and quickly modify their systems as new threats emerge.

2. More third-party data for real-time monitoring

Financial services institutions are no longer content with just using internal transactional data to fight fraud and financial crimes. They are also looking at external information obtained from third-party vendors and integrating that intelligence to improve their detection capabilities. They are further enhancing information by integrating disparate data sources, regardless of format (including unstructured text fields). By using data across all a customer's accounts, transactions and profiles, they can better monitor the behavior of individuals to incrementally detect fraud, enhance Know Your Customer data and reduce false positives. The solution can be integrated or on-demand, providing 100% real-time scoring across all data to give clients full coverage and provide insight into information that was previously not accessible.

3. Use of machine learning techniques

Modern fraud and financial crime solutions incorporate a hybrid of advanced analytics to score every action. They can uncover hidden relationships, detect subtle patterns of behavior, prioritize suspicious actions and predict future risks. Each technique is powerful when used in isolation, but when combined in a hybrid approach they enable fraud and AML analysts to identify targeted transactions, entities and potentially fraudulent networks through complex money movement. Some of these techniques include:

- Machine learning models combine internal and external data to detect complex risks that are not easily identified using traditional if-then logic. A wide variety of models are available, from traditional machine learning algorithms to deep learning models.
- Out-of-pattern analysis, which compares customer activity with peer group behavior and the customer's past behavior to identify unexpected changes.
- Network analytics resolves entities, identifies hidden risks and identifies patterns of illicit behavior across the institution.
- Rule development, which involves creating and applying rules for known behaviors, as well as specialized rules for specific scenarios.
- Robotic process automation (RPA) for automating low-value activities to free up valuable personnel for more important investigations. Where possible, organizations can use straight-through processing (STP) for work that doesn't need human attention.

4. Next-generation identity verification

Identity theft, including creating synthetic identities, is used to open new accounts to commit various types of financial fraud and money laundering. Financial institutions are improving their ability to combat financial crime through a new generation of identity verification technologies. This can improve security while creating competitive advantage by meeting consumers' expectations for products that are both simple and secure. These technologies also enable financial institutions to de-risk customer onboarding with Know Your Customer identity verification and follow the Customer Due Diligence (CDD) Rule to ascertain and verify ultimate beneficial ownership.

5. Protection against new fraud and financial crime risks

New fraud and financial crime risks are constantly evolving. For example, a proliferation of malware has accompanied the increased adoption of mobile devices. It is imperative that next-generation solutions include proactive approaches to fraud detection analytics to protect against unforeseen risks. Unsupervised learning techniques can help institutions monitor for emerging risks and put in controls before it's too late.

Why banks must adapt

Together, these five trends outline the capabilities that will define the next generation of enterprise fraud and financial crime management. By adopting more modern, sophisticated fraud and financial crime management, financial institutions can combat the evolving financial crime landscape while reaping numerous benefits for the organization. New solutions provide faster and more effective fraud and money laundering detection and higher visibility of exposure across channels while providing a single view of the customer. Companies have achieved increases in detection rates

Fraud detection with a rapid return

One large bank that took a single platform approach to address all financial crime benefited by being able to analyze transactions and customer activity, develop new models and tune existing models to improve fraud detection efficiency and create reports. The bank has detected twice the level of check fraud than it did with its legacy system, increased internet banking fraud alerts by 60%, and improved check and internet fraud loss-to-turnover ratios by 50% and 80%, respectively, compared with five years ago.

from 50% to 90% while reducing overall alerts from tens of thousands to under 100. This increased effectiveness and efficiency results in improved compliance, reduced fraud losses and increased ROI.

A new approach to fraud and financial crime management also protects a firm's brand and reputation, leading to greater trust among customers. Faster response times and a reduction in false positives – with some companies experiencing up to 95% improvement in false positive rates – improve operational/investigation efficiency and drive down the costs. With "stickier" customers, firms have a greater opportunity to cross-sell and expand the customer relationship.

Criminals will always be working to find new schemes to commit fraud and other financial violations. In this digital age, the importance of fraud and financial crime prevention and detection will only increase in significance. As they consider new processes and solutions to fight financial crimes, financial institutions that adapt to capitalize on these emerging trends will be ready to better mitigate risks and generate a more substantial return on their investments.

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Since 1967, Capgemini has been building on its strong heritage and deep industry-specific expertise, enabling organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 270,000 team members in almost 50 countries. **Learn more about Fraud management for banking and capital markets.**

About SAS

Curiosity is our code. SAS analytics solutions transform data into intelligence, inspiring customers around the world to make bold discoveries that drive progress. SAS delivers better fraud and financial crimes compliance with enhanced fraud detection; efficient, effective investigations; consolidated monitoring and reporting; and proactive protection through advanced analytics, AI and machine learning technologies.
sas.com/bankcrimes

Learn more about the SAS and Capgemini partnership at sas.com/capgemini.

POWER OF THE PARTNER

At SAS, we love bold questions. And when we combine our analytics leadership with the innovative technology and expertise of our partners, we help our customers turn data into answers. That's the kind of curiosity that moves the world forward. That's the **Power of the Partner**.