What is Fraud Prevention, and Why is it Important?

What is Fraud Prevention?

Fraud prevention refers to a firm's policies, functions, and processes that keep fraud from occurring. No fraud prevention strategy is foolproof, but firms can focus on preventing the types of fraud they're most at risk for. This will ensure they use their resources most effectively. To do this well, they can implement regular risk assessments to ensure their framework is based on realistic risks.

The Difference Between Fraud Prevention and Detection

Fraud prevention and detection are complementary strategies to reduce fraudulent activity and losses. **Fraud detection identifies fraudulent activity** that has occurred or been attempted. It responds to an existing threat. With fraud prevention, firms implement policies and safeguards that make it harder for criminals to commit fraud. Examples include:

- Employee and customer screening.
- Customer education.
- Customers can activate card freezing and similar protections if their account is compromised.
- Transaction screening.

5 Tips on How to Prevent Fraud

Even though a thorough fraud prevention strategy must be tailored to a firm's unique risks, there are several facets that every firm should consider.

1. Conduct an Enterprise-Wide Risk Assessment (EWRA)

Effective fraud prevention programs must be risk-based. This entails performing **regularly-updated EWRAs** that analyze fraud risks based on a firm's unique context. An up-to-date EWRA will help a firm focus on the **fraud risks relevant to its operations** and avoid wasted resources on low-risk typologies for their business and sector. Armed with a comprehensive understanding of its true risk, the firm can consider its risk appetite. Since risk can never be completely eliminated, a risk appetite considers a realistic and effective level of risk control that enables reasonable business to continue.

To effectively apply its individualized risk assessment, a firm should create controls addressing its residual risk – what lies beyond the firm's risk appetite. Specifically, fraud risks should be controlled in light of the overall risk profile, including other risky behaviors and typologies. Traditionally, firms have viewed fraud prevention as part of a process primarily aimed at reducing loss to the company and maintaining positive customer service. While these are important fraud detection and prevention aspects, they are not the whole picture. As a predicate offense to money laundering, fraud is often tied to broader criminal activity, from other predicate crimes such as **wildlife** and **drug trafficking** to money laundering and terrorist financing. To effectively combat fraud, firms must understand it in its entire context rather than viewing fraud events as isolated incidents.

All too often, fraud and AML teams operate in siloes. Yet both departments have access to information that could significantly improve the firm's overall understanding and mitigation of its risks. For example, **money laundering patterns could lead back to fraud as their source**, alerting a firm to risks they may not have adequately prevented. This, in turn, could lead to better fraud prevention – and detection should activity slip through the cracks.

2. Strengthen Internal Controls

Firms should take stock of their business operations in light of their updated EWRA and risk appetite. Because the risk a firm faces depends on its unique activities and structure, it is impossible to give a universally exhaustive list of necessary controls and policies. The firm must ultimately determine this as appropriate to its own operations and obligations. That said, risk-based controls and policies will share several features in common.

Internal Fraud Prevention

Employees can use their access to fraudulently benefit themselves or others. In more serious scenarios, those higher up in a firm can use it as a front to perpetuate their own illegal activity, which could include theft, money laundering, bribery, and terrorist financing.

In dealing with sensitive financial information, firms should ensure they understand which duties are incompatible, meaning different people should hold them and have strictly controlled access to relevant information. This is a basic necessity for the prevention of internal fraud. According to accountants **Alexander Aronson Finning CPAs**, four categories should never be held by the same personnel:

- Authorization or approval.
- Custody of assets.
- Recording transactions.
- Reconciliation/control activity.

External Fraud Prevention

Firms must ensure customers are protected from exploitation by fraudsters and that fraudsters do not open and use their accounts to perpetrate fraud. This latter scenario can cross into anti-money laundering (AML), as the two can easily overlap when the fraudster is the account owner. Policies should include processes and roles that help to mitigate this risk in line with a firm’s most recent EWRA.

Thorough documentation of processes and roles is essential to ensure the fraud prevention program aligns with risks, strategizes for the right functions and resources, and complies with any applicable laws, such as those regulating the handling of sensitive information. It’s also necessary for proper segregation of duties. Finally, it will provide a clear baseline to measure against when auditing a fraud prevention program for effectiveness.

3. Create a Fraud Prevention Culture

No fraud prevention program will be effective if it does not permeate the firm. This means everyone should be aware of the risks associated with internal fraud and trained in basic security measures to prevent it.

Training

Knowledgeable, well-trained staff are crucial to a **well-designed fraud prevention program**. Aside from hiring capable individuals, the individualized nature of each firm’s risk requires regular training. Even veteran fraud professionals will not be familiar with a firm’s unique risk landscape without continual updates. Training should be updated to align with a firm’s most recent EWRA and provide a holistic picture of fraud risks and compliance requirements.

Avoiding generic or rote programs can also help with retention and compliance. Effective training goes beyond imparting static knowledge or testing short-term memory. Instead, it practically orients fraud professionals and gives them a concrete understanding of how policies practically apply daily. Staff will then be better able to carry out more effective fraud prevention.

Anyone dealing with customer information – even if their role is not explicitly related to fraud – should be thoroughly trained to understand when customers may be at risk of exploitation. They should have a reliable chain of command to turn to when they suspect a customer may be especially vulnerable or getting scammed.

Sound Governance

General awareness also needs to be supported by sound governance. To ensure fraud prevention policies, procedures, and roles are properly implemented, it’s important to soundly structure roles, from upper leadership to each team and its members. Although each governance model will be tailored to a firm’s **unique risks**, there are core features most programs should entail.

The three-lines-of-defense model is an industry-validated approach to governance in risk management. It provides a sound framework for firms as they determine the roles needed to respond to the risks uncovered by their tailored EWRA. PwC provides a **helpful outline** of what each line entails.

1. **First line** – These are the people in charge of the front-facing fraud prevention strategy and its associated processes. A well-developed first line should include an autonomous senior executive assigned to coordinate the strategy and processes for all first-line risk management, especially:
   - **Fraud strategy development and implementation.**
   - **Fraud analysis, investigation, recovery, and reporting.**
   - **Coordination between fraud prevention and related functions**, especially cyber security, authentication, customer service, and broader financial crime risk management (including AML).

   This executive oversight should keep the fraud prevention and risk management function running smoothly. It should ensure all teams are working at their best with appropriate equipment and that the whole process is risk-based and **integrates with wider risk management functions**.

2. **Second line** – Those involved in the second line are responsible for establishing an objective, holistic, and well-structured picture of the company’s fraud risks. This is most reliably established through regularly updated EWRAs, which will look at financial crime risks within the context of the firm’s activities and regulatory requirements. Based on the risk profile established, this line of defense will also ensure adequate policies and procedures are in place.

The second line of defense for fraud prevention will include the compliance team, overseeing the fraud prevention program's compliance with company policy and, as applicable, any regulations such as privacy protection laws and any overlapping AML obligations.

3. **Third line** – Independent assessment and accountability are crucial to any effective risk management program. As such, the third line of defense helps hold both the first and second lines accountable by assessing the adequacy and effectiveness of their policies, procedures, and processes. This is done through internal auditing.

Firms are also well-advised to undertake third-party reviews of their risk management processes to ensure all three lines of defense are held accountable.

4. Implement Strong Cybersecurity Measures

Cybersecurity is key to ensuring a company's sensitive data is not compromised, falling into the wrong hands and violating regulatory requirements. Every firm's tech must have built-in cybersecurity measures. Firms should also train employees in basic cyber hygiene. This can prevent internal attacks such as unauthorized account access or spear phishing, where a fraudster poses as a trusted person to obtain money or sensitive information to be used in a fraudulent scheme.

Digital-native firms not operating **bug bounty programs** – incentive-based programs designed to stress test platforms for potential flaws – should also consider implementing them alongside frequently-scheduled **pen testing exercises**.

A dedicated information security team is key to effective cybersecurity. This team should be well-trained and knowledgeable in how their function can help prevent internal fraud. A firm's fraud prevention governance policies should delineate their roles and responsibilities.

5. Establish a Process for Response in Case of an Incident

When an internal fraud incident occurs, it may be argued that the time for prevention is past. However, a swift and adequate response can help ensure the incident does not blow out of proportion. In line with their most recent risk assessment, firms should consider fraud scenarios for which they may be especially at risk. A response strategy can be outlined for each scenario and validated against industry practice. Such scenarios might include:

- Strategies for responding to an information security breach or hack.
- A chain of command and process to follow if an employee believes they've discovered evidence a colleague is committing fraud.

Using Advanced Tech: Emerging Technologies for Fraud Prevention

The support of proper technology is increasingly vital to reliable risk management. For example, **machine learning and artificial intelligence enable the detection of otherwise hidden risks**. Firms can use this for fraud prevention in customer due diligence, deploying tools that implement natural language processing (NLP) for more effective adverse media checks at onboarding.

ComplyAdvantage's **AI-powered transaction screening** and monitoring solution, for example, can adapt to evolving fraud typologies, which can, in turn, help firms update their fraud prevention strategy to reflect the latest risks. Similarly, with **Fraud Detection by ComplyAdvantage**, firms can enhance their fraud prevention strategies as they leverage one of the most powerful machine learning models that not only detects fraud but also explains the reason why each alert was created.

Firms may consider how technology might empower anti-fraud teams to use their time and analytical capabilities better by reducing false positives and offering better insights. Even firms not yet ready for a technological overhaul can benefit from AI overlays that offer intelligent risk detection and alert prioritization to legacy platforms. Firms can also audit their existing tools to ensure they support a risk-based approach.

By Company Advantage