Integrating fraud detection and prevention into a GRC framework

As financial services firms face a number of challenges in the prevention of fraud, they are eliminating weaknesses by implementing robust governance, risk and compliance programmes. Karen Van Ness, Oracle Mantas, outlines the most common types of fraud, the challenges in addressing them with traditional systems and how a holistic approach can strengthen a firm's defences

In an environment characterised by growing regulatory complexity and increased reputational risk, financial services firms are focusing like never before on implementing effective governance, risk and compliance (GRC) programmes. GRC is essential to eliminating organisational weaknesses that can lead to significant operational risk, financial losses, regulatory censure or fines. Many financial institutions, however, face a shared challenge – bridging specific areas of risk or compliance into an enterprise-wide approach.

Fraud detection and prevention is one area in which an organisation can get significant value for its investment dollar by pursuing an enterprise approach. Fraud is considered a key operational risk to profitability and reputation. Fraud has always been a problem for financial services firms and, in recent years, many have made fraud detection, prevention and security systems a critical part of their ability to control operational risk. Integrating fraud detection and prevention into a firm's overall GRC framework can provide substantial benefits, including a comprehensive understanding of the impact of financial crime on the institution, improved return on risk and compliance investments, enhanced reputation and higher levels of customer trust.

An escalating war

Fighting fraud has become an escalating war. Even those firms with the most advanced tools and processes to detect and prevent fraud feel like they are falling behind. The technical advancement and globalisation of fraud activity will continue to provide new challenges to a firm's ability to manage fraud. Key trends include the following:

- Greater professionalisation of fraud practices. Smarter attacks, especially online, result in bigger payoffs, which in turn attract more talented thieves.
- Increased 'sharing' of fraud practices from fraudster to fraudster.
- More fraud perpetrated from offshore locations and by organised crime cartels.
- An increase in technical fraud (for example, hacking and other internet-related skills coupled with a more traditional fraud skill set).
- More brazen initiatives as fraudsters take over the bank accounts of legitimate customers or go to the bank branch in person to open their own fraudulent accounts.
- More collusion between merchants, fraudsters and firm insiders.

Regulatory drivers also have an impact on financial institutions' efforts to better detect and prevent fraud, especially in the areas of identity theft and account takeover. As such, regulations and guidelines require increasingly tougher fraud prevention measures. For example:

- The Federal Financial Institutions Council guidance dictates that customer data security and authentication measures must be improved, especially for online activity. Strong authentication should be combined with risk monitoring and analysis.
- Industry groups, such the UK Association for Payment Clearing Services and the Payment Card Industry Security Standards Council, are pushing financial institutions towards better compliance with customer and firm data security guidelines and best practices.
- The US Federal Deposit Insurance Corporation (FDIC), the UK Financial Services Authority, other financial services regulators and external governing entities such as the EU's Anti-Fraud Office are pushing financial institutions to implement stronger measures against fraudulent activity, with an emphasis on identity theft and account takeover.

While many institutions use solutions to detect and evaluate fraud, few are using technology to look across their corporate systems. As a result, fraud detection solutions and disparate data streams are isolated in silos, creating substantial challenges to detecting and preventing fraud.

The current approach to fraud management is inadequate

Most financial institutions have invested in products and processes to identify and prevent fraud on a product or channel-specific basis. Traditionally, firms have focused on employing point solutions, which can be an effective measure for each product (for example, cheque kiting or credit card fraud), but do not support the ability to share and consolidate critical information between fraud detection silos, leaving the institution and its customers vulnerable to more sophisticated fraud schemes.

The major areas of fraudulent activity that create the most challenges for firms in terms of losses, customer service issues and reputation typically involve more than one type of mechanism, channel or product. Let us look at some of the types of fraud in financial services and the challenges encountered in addressing them.

Access vulnerabilities

Customer data and accounts are becoming increasingly vulnerable to sophisticated hacking, phishing and social engineering techniques employed by fraudsters. Of particular concern are account openings and transactions initiated by phone or over the internet. This situation is forcing financial institutions to upgrade their security and authentication measures, as well as real-time or near-real-time monitoring of account access and transactions.

Real-time detection and interdiction capabilities are necessary to detect and prevent fraud involving online and electronic channels and products. Typically, the fraudster starts by gaining access to the enterprise through the web portals put into place for legitimate customers only. An effective fraud solution must, therefore, provide real-time capabilities to either directly monitor transactions or to apply higher-level analytics to the output of other real-time point solutions. The solution must also be able to collect access alert events and apply analytics to determine if fraudulent activity is occurring. Tying together external access, geographical information, authentication, client and account behaviours help to expose real-fraud events and more effectively protect customers from identity theft and account takeover schemes.

Identity theft

Identity theft is a fast-growing type of consumer fraud and is considered to be the leading threat against deposit accounts. It is perpetrated through account takeover or account hijacking (a fraudster gains control of a customer's account), true-name fraud or identification fraud (a fraudster assumes the identity of a real person to open a phony account) and collusion between fraudsters and customers or between fraudsters and employees of a firm.

In its oversight of regulated institutions, the FDIC is pushing banks to incorporate the following into their fraud surveillance systems:

- A layered approach that combines scanning software with other monitoring tools to proactively identify and defend against identity theft.
- Improved authentication procedures, including layers and token or biometric authentication devices and procedures.
- Implementation of fraud detection software to identify account takeover.

The confluence of identity theft and insider fraud is an important trend for financial firms to recognise and protect against in their fraud tools.

Insider fraud

Insider fraud is endemic in the financial services industry. As a result of the direct access that certain employees have to financial resources and customer data, there are opportunities for them to carry out fraud. Indeed, a high proportion of fraud within the financial services industry is perpetrated by employees conducting fraudulent activities or providing sensitive information to fraudsters outside of the firm.

Internal fraud is increasingly connected to organised crime rings. An emerging trend is the placement of gang members or accomplices into teller and other sensitive positions at banks with the intent of committing fraud. In 2002, the US Office of the Comptroller of the Currency alerted financial firms to fraud schemes involving newly hired bank tellers. Organised crime rings were aggressively recruiting bank tellers to cash forged savings account withdrawals from customer accounts and to cash stolen or forged cheques.

According to informal research and customer surveys, existing solutions do not adequately address employee and insider fraud. This threat is typically handled through internally developed methods that are becoming increasingly ill-suited to the task.

Since up to 70% of identity theft cases involve an employee or insider, the confluence of identity theft and insider fraud is an important trend to watch.

New account fraud

New accounts are particularly susceptible to fraud. Recent statistics show that 23% of cheque fraud cases and 26% of fraud losses are linked to new accounts. These percentages continue to increase year over year. Forty-one per cent of new fraud cases occur within 30 days of account opening; 21% within 31–60 days; 13% take place within 61–90 days and 25% happen within 91–180 days. At regional banks, new account fraud appears to occur even earlier in the account life cycle: 87% occur within 90 days of account opening.[1] New account fraud is a growing problem and has become a main conduit for identity theft and cheque fraud.

Payments fraud

Another area of concern is related to the greater variety of electronic payment products and channels that financial services firms offer to their customers. Payments fraud creates special challenges. The tremendous growth in electronic payments, coupled with the electronic presentment of cheques, shortens the window for detection. Thus, fraud attacks on payment activities are occurring at a greater frequency. Complex, higher-dollar fraud events occur across multiple channels and payment types. And funds are often moved offshore where recovery is less likely.

Financial crime and compliance management – the call for a more holistic approach

Given the challenges in fighting fraud, it is no surprise that financial services firms are recognising the need to take an enterprise approach to fraud management. While point solutions offer extensive capabilities within specific areas of fraud, they can generate high

levels of false-positive alerts and, typically, are not well-integrated within the overall fraud and risk management regime of the firm. Financial institutions and regulators now have higher expectations. Firms want a single, integrated view of fraud across accounts, customers and business lines.

Financial institutions, especially larger ones, are establishing financial crimes units or financial intelligence units as a first step towards targeting fraud with a holistic approach. However, the effectiveness of this approach is dependent on the ability to bring together existing fraud detection point solutions under a single umbrella.

Financial institutions require integrated, layered technologies that seamlessly

financial crime areas, such as anti-money laundering (AML). Given the synergies and commonalities between AML and fraud, this approach can significantly reduce implementation costs, as well as increase speed to deployment of an enterprise fraud management platform.

Committing to an enterprise approach to managing financial crime and compliance is the pivotal step to better integrating fraud detection and prevention into a firm's overall GRC framework – and can deliver real value and efficiency.

Following are recommendations for implementing an enterprise-wide fraud management platform in the most effective and results-producing manner possible.

trader identification or name, and so on, within a certain window of time. Further, the alert correlation engine also:

- scores this association of alerts to prioritise the analysis and subsequent actions to be taken;
- assigns the alerts to the appropriate analyst or group of analysts for action based on a set of configurable business rules;
- sends out an e-mail or asynchronous notification to the analysts if they are unavailable; and
- in addition, the alert correlation engine automatically feeds this association of alerts to a case management system to either create new cases for analysis and action or to augment existing cases already under review for analysis and action.

> Committing to an enterprise approach to managing financial crime and compliance is the pivotal step to better integrating fraud detection and prevention into a firm's overall GRC framework – and can deliver real value and efficiency

incorporate point fraud prevention and detection applications into cross-channel fraud management systems, allowing financial institutions to address complex and evolving fraud patterns and correlate data from multiple systems. An effective fraud solution enables fraud analysts and investigators to view transactions, accounts and relationships holistically. A centralised 'hub' approach, combining real-time or near-real-time fraud detection capabilities with sophisticated analytics, facilitates earlier detection of fraud schemes and rings, and enhances loss prevention and mitigation. Regulators are increasingly encouraging this type of holistic approach.

In addition, firms should consider other investments in risk and compliance software and how they can be integrated with fraud management to improve detection and prevention. For example, firms should consider leveraging data, scenarios and risk models already applied against other

Alert correlation

Identifying potential fraudulent activity emanating from event and transaction streams – for example, the capability provided by point fraud applications – is only half the solution. The other half involves the ability to correlate the reported alerts or exceptions in real-time to provide a complete and consolidated view of fraudulent activity. Not all events are fraudulent or identifiable as fraudulent activity. But, by correlating these alerts in real-time over a specified window of time, a firm can gain a more complete picture and can conduct further analysis to determine whether a concerted effort is under way to perpetrate fraud. In other words, any one of the individual alerts might not appear significant but, when analysed together, they could become significant enough to require action.

In an anti-fraud software solution, an alert correlation engine associates alerts using a common attribute, such as login identification, account number, customer name, employee identification or name,

After financial firms aggregate all alerts of suspicious behaviour and correlate the alerts to identify related activities, related customers or entities and related accounts, they must be able to share the information within the organisation. The value of a fraud system that pulls together all alerts of suspicious behaviour is its ability to distribute that information in a timely manner to the appropriate personnel within the financial firm. Armed with this information, a fraud officer can investigate the alerts and possibly prevent the loss of additional funds from related accounts.

Sophisticated behaviour detection

Additionally, a firm needs to implement a system that will supplement individual incidents of suspicious behaviour with a sophisticated behaviour engine that can identify more complex patterns of activities, such as:

- current and historical behaviours of the individual account and all related household accounts;
- entities transacting with the identified suspicious account; and
- any other networks of related suspicious behaviours.

[1] Statistics taken from the American Bankers Association Deposit Fraud Survey

Unified financial intelligence

Anti-money laundering

Know your customer/
customer due diligence

Fraud detection

Access management
solutions

Employee onboarding

Others

Enterprise
financial crime
detection
engine

Enterprise
financial crime
investigations

Enterprise
financial crime
resolution and
reporting

Collection management
solutions

Liability risk and
management systems

Operational risk solutions

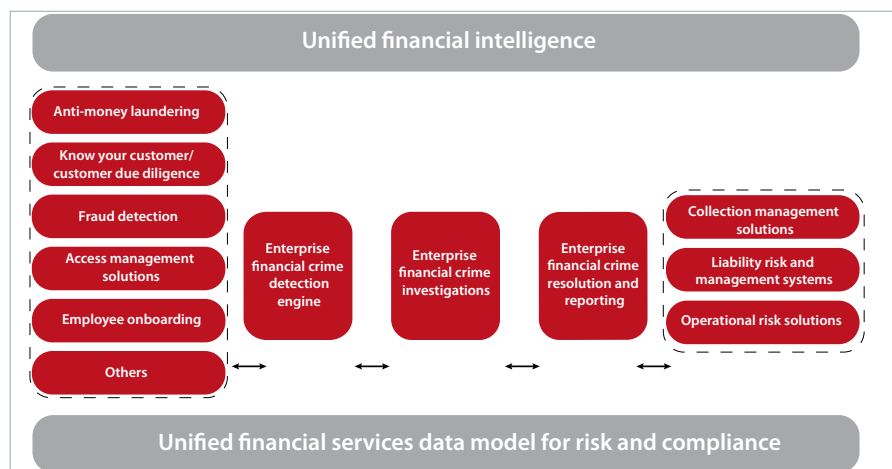**Unified financial services data model for risk and compliance**

Figure 1: Financial crime and compliance platform

An advanced set of analytics, which far exceeds the basic rules engine capabilities of many point solutions, can be applied to more accurately identify fraudulent activity. Advanced analytics include techniques that can detect outlier patterns, identify complex sequences, discover and analyse links and perform complex event processing.

With this additional overview of suspicious or potentially fraudulent activity, the firm will have a detailed picture of existing and potential areas of concern. This provides a significant advantage: the firm can proactively identify which accounts to monitor for potential behaviours and can be ready to stop anything that is even slightly suspicious.

Enterprise case management

Comprehensive alert and case management can automate processes and reduce the cost of investigations. Enterprise case management built specifically for financial crime investigators provides a single view of fraud, risk and compliance status. It can help prevent and reduce fraud losses by automatically uncovering and intelligently focusing investigations on the most urgent and actionable alerts.

A key attribute is open architecture for simple integration with legacy systems, from payments to point solutions to general ledger

reconciliation. Such a system improves the efficiency and effectiveness of investigators by focusing on actionable, higher exposure activities, resulting in better protection for the firm's customers and fewer account and service interruptions.

In their efforts to more successfully manage financial crime and compliance, financial services firms are recognising the need to take an enterprise-wide approach to fraud management. A comprehensive fraud solution must not only provide a single point of analysis for account and customer activity, but it must also monitor and detect complex behaviours and patterns that could indicate broader issues. Exposing events, particularly the more complex, cross-channel fraud schemes, as they are happening – and taking action before assets have left the institution – is critical to minimising losses and the challenging task of recoveries.

Establishing an enterprise fraud management platform is a key step in better integrating fraud detection and prevention into a firm's overall GRC framework – which, in turn, can provide substantial benefit, including fully understanding the impact of financial crime on the institution, improving return on risk and compliance investments, enhancing the institution's reputation and cultivating customer trust.

About the Author
Karen Van Ness is senior manager for product management at Oracle Mantas, a part of Oracle Financial Services Software. She has 20 years of experience in the information technology and financial services industries. At Mantas, she has helped bring to market Mantas solutions targeted at AML and fraud, and supported implementations at top-tier banking and brokerage firms in the US and internationally. Prior to joining Mantas, Ms Van Ness was a vice president at Citigroup and Chevy Chase Bank.

Ms Van Ness holds a bachelor's degree from Dartmouth College and a master's degree from The Johns Hopkins University.