An Oracle White Paper
November 2012

Fraud Fight:
Enterprise-wide Strategy Sets the Stage for Victory
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Overview</td>
<td>2</td>
</tr>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>Schemes Become More Complex</td>
<td>5</td>
</tr>
<tr>
<td>The Need for Speed…and Cross-Channel Visibility</td>
<td>6</td>
</tr>
<tr>
<td>Part of the Compliance Ecosystem</td>
<td>7</td>
</tr>
<tr>
<td>New Requirements for New Era</td>
<td>8</td>
</tr>
<tr>
<td>Self-Assessment</td>
<td>10</td>
</tr>
<tr>
<td>Conclusion</td>
<td>11</td>
</tr>
</tbody>
</table>
Executive Overview

The adage, “there’s nothing new under the sun,” does not ring true when it comes to financial crime. The media warns us almost weekly of new threats and schemes, and financial institutions and businesses continue to take a hit…both to their bottom lines and reputations. Financial institutions are on the front lines of this battle and seek new approaches and solutions for fraud that not only enable more rapid detection across all products and channels to reduce losses, but also can set the stage for prevention and better overall risk management.

Introduction

The number of financial fraud incidents is growing dramatically. According to the 2011 ABA Deposit Account Fraud Survey Report, 100% of super-regional/money center institutions participating in the survey reported debit card, check, and automated clearing house (ACH) fraud in 2010. (See Figure 1.)

![Figure 1 – Types of Fraud Reported by Various Types of Financial Institutions](image)

Source: American Bankers Association Deposit Account Fraud Survey 2011
In the same biennial survey, respondents rated the level of threat posed by various risks to the industry in the next 12 months on a scale of 0 to 5 (with 0 being “none” and 5 being “extremely high”). The leading threats identified were: signature debit card fraud, customer victimization scams, cross channel fraud, and automated clearing house (ACH) fraud – originations.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Perceived Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACH fraud, originations</td>
<td>77%</td>
</tr>
<tr>
<td>Online Banking</td>
<td>51%</td>
</tr>
<tr>
<td>Wire fraud, receiving</td>
<td>43%</td>
</tr>
<tr>
<td>Wire fraud, originations</td>
<td>41%</td>
</tr>
<tr>
<td>ACH fraud, receiving</td>
<td>39%</td>
</tr>
<tr>
<td>Debit card (PIN based)</td>
<td>36%</td>
</tr>
<tr>
<td>Organized ring attempts</td>
<td>29%</td>
</tr>
<tr>
<td>Remote deposit risk</td>
<td>26%</td>
</tr>
<tr>
<td>Identity theft</td>
<td>6%</td>
</tr>
<tr>
<td>New account fraud</td>
<td>4%</td>
</tr>
<tr>
<td>Debit card (signature based)</td>
<td>4%</td>
</tr>
<tr>
<td>Check fraud (paper based), deposit</td>
<td>-17%</td>
</tr>
<tr>
<td>Check fraud (paper based), withdrawal</td>
<td>-19%</td>
</tr>
<tr>
<td>Customer victimization scams</td>
<td>-33%</td>
</tr>
</tbody>
</table>

Figure 2 – Change in Perceived Fraud Threat Levels Between 2009 and 2011
Source: American Bankers Association Deposit Account Fraud Survey 2011

What is more revealing is how the perceived threat levels have changed when compared to the same survey from 2009. (See Figure 2.) The risks that gained most in perceived threat were fraudulent ACH originations, online banking fraud, fraudulent wire receiving and originations, fraudulent ACH receiving, and PIN based debit card fraud – all the transaction types that have gone through significant innovation in terms of processing times and moved into remote channels.
Financial crime is big business that contributes to an estimated $20 billion in direct losses annually. Industry experts suspect that this figure is much higher, as many firms cannot accurately identify and measure losses due to fraud. The impact on a bank’s bottom line tells only a small part of the story, however, as financial crimes of all types – including fraud – can deal a powerful blow to a financial institution’s reputation and to consumer confidence. In addition, as financial crime continues to grow in frequency and sophistication, firms must spend a larger portion of their time and greater resources detecting and investigating incidents, preventing future events and recovering funds. Regulatory oversight also has increased, bringing with it new costs and requirements.

Many firms have adopted a risk-based approach to managing fraud detection and rely on inflexible, disparate rules-based risk and compliance point solutions that detect specific anomalies within large data sets. This approach does not yield the enterprise view of customer activities across channels and products required to effectively identify all threats. More importantly, it does not provide real-time detection capabilities. Organizations, therefore, are left to identify and investigate fraud well after it happens, as opposed to while it is happening, which would allow them to stop incidents immediately and even prevent future attacks. Further, many legacy systems do not provide the flexibility needed to quickly and effectively meet changing regulatory requirements – instead, they require customizations that are expensive and time consuming to build and maintain, and they still do not yield enterprise-wide visibility.
Schemes Become More Complex

In recent years, the financial services community has focused efforts on reducing latency, accelerating transaction speed to handle increasingly high volumes, and delivering the immediate service capabilities that today’s customers require. Automation and the push for straight-through transaction processing—which can be completed without any human intervention—has been the goal and is, increasingly, a reality. Today, consumers can open accounts online without ever stepping foot in a brick-and-mortar financial institution; bank-to-bank transfers are de rigueur; auto bill pay is bringing new levels of convenience to millions of individuals and businesses; and consumers are intrigued by and quickly moving to adopt remote deposit capture of checks using smart phones and other devices.

While straight-through-transaction processing has afforded new levels of efficiency for financial institutions and greater convenience for consumers, it also is creating new opportunities for fraud, as transactions are faster, do not require any human intervention, and are often “anonymous.”

Channel proliferation also is creating new opportunities for fraud and making it more difficult for financial services organizations to identify schemes and stop them in their tracks. Traditionally, firms have adopted a point-solution approach for financial management focused on each specific channel, such as wire transfers or automated clearing house (ACH).

Fraudsters, having done their research, know that banks typically do not monitor and analyze customer behavior across multiple accounts, channels, and systems. As a result, we are seeing a proliferation in cross-channel fraud, in which criminals are able to “fly under the radar” and gain access to a customer’s account and use that information to commit fraud that spans multiple channels. For example, fraudsters might siphon off funds from a commercial account via a series of small ACH debits after they know, based on knowledge gained from malware placed in a computer, that the account holder might have received a larger wire transfer. This crime would span two channels, and the small ACH

transfers, which might look to the bank like payroll transfers, would avoid detection because the bank monitors each channel separately and the transactions take place at different times.

Many firms appear to trail far behind the fraudsters when it comes to this emerging type of fraud. Only 26% of the 230 financial services executives participating in a 2010 Information Security Media Group study\(^2\) said that their organizations have a team assigned to detect cross-channel fraud.

The Need for Speed… and Cross-Channel Visibility

Straight-through-transaction processing and channel proliferation are changing the game for fraud detection and prevention. Stated simply, today’s financial institutions require an enterprise-wide approach to fraud management – one that includes real-time, cross-channel monitoring and investigation capabilities coupled with powerful analytical and reporting tools.

Most financial services institutions today, however, have a series of point solutions for specific lines of business or channels. These solutions fall short on several fronts. First, many rely on batch technology, which does not enable real-time visibility, even into a single channel. In an era of automated transactions, speed is of the essence. Real-time monitoring is essential to protect customers and the bank from losses, as well as preserve a firm’s reputation. According to a March 2008 TowerGroup report, “Surrounded by the Enemy: The Case for Enterprise Fraud Management,” victims who detect fraud within 24 hours are defrauded for an average of $428 per incident. Those who took up to five months to report fraud lost nearly $1,207, almost three times as much as victims who detected the fraud within one day. When one multiplies these figures by the tens of thousands of accounts affected annually, the impact becomes apparent and acute.

While some firms are making progress on the real-time monitoring front, these capabilities often are limited to specific lines of business or channels and still do not enable an institution to “connect the dots” across channels or the enterprise to identify and combat complex fraud schemes. In addition, independent point solutions – which the enterprise does not manage centrally – can deliver a high number of false-positive alerts that are not readily recognizable as such and, therefore, require follow-up investigation. Further, the point-solution approach requires an institution to purchase and maintain multiple systems, which brings additional direct and indirect expenses and can lead to inconsistent data.

Part of the Compliance Ecosystem

Financial institutions are finding that their legacy fraud management systems are falling short on another front – as part of their broader governance, risk, and compliance (GRC) program. In the wake of the financial crisis, financial institutions – faced with higher compliance thresholds – are taking a harder look at operational risk, of which fraud is an important part.

Specifically, recent reports by New York’s Department of Financial Services (DFS) and the U.S. Senate Permanent Subcommittee on Investigations called out several deficiencies in the status of financial crime compliance operations at two global financial institutions. These reports turned the spotlight on the status of compliance in financial organizations driven by deal makers, fast-growing and global institutions, and institutions linked to banks based in or operating in countries blacklisted by the United States Office of Foreign Assets Control.

Taking to heart these reports and others as a bellwether of things to come for the industry, forward-looking financial services organizations are beginning to evaluate their fraud management operations from the top down in terms of processes, systems, and checks and balances – and the overall effectiveness of their efforts. In addition, they are quickly realizing the importance of linking their fraud management initiatives to their broader GRC operations. At the same time, financial institutions are determining that many of their fraud case management solutions stop at reporting fraud losses and act more as data entry tools as opposed to analytical tools – limiting their ability to support broader GRC initiatives.

Today, some organizations can track operational losses related to fraud. In many more cases, however, firms cannot accurately calculate the extent of fraud losses across the enterprise, as they are often misrepresented as accounts that are “bad” due to unforeseen circumstances. More importantly, financial institutions have no way of determining how well their surveillance solutions are actually performing. Both of these metrics are increasingly important to firms’ chief compliance and risk officers.
New Requirements for a New Era

As firms today take a harder look at fraud as part of overall operational risk, they are rethinking their fraud detection and case management solutions – and with good reason. Experts confirm that investment in fraud management solutions can pay off in a big way. TowerGroup calculates that for every dollar spent on fraud management, the enterprise gains back as much as $8\textsuperscript{3}.

Three concepts define the shift toward more effective fraud management initiatives – cross-channel, real-time, and enterprise-wide. In addition, the approach must encompass monitoring, investigative/case management, and reporting capabilities. (See Figure 3.)

Financial institutions require an integrated platform that leverages a single data model to enable a holistic and accurate view of accounts, customers, transactions, channels, and entities across the enterprise. The platform must enable real-time monitoring and interdiction capabilities, including online access and authentication for increased productivity and earlier identification of potential fraud schemes.

---

Additional requirements include the following:

- A comprehensive set of fraud scenarios, sophisticated behavior detection and profiling techniques, and advanced risk scoring that drives more targeted and effective fraud detection for current and future schemes
- Comprehensive case management capabilities built specifically for financial crime investigations, including robust workflows, documentation, loss and recovery data, and an audit trail
- Robust information enrichment from external and other internal systems, as well as network analysis capabilities
- Advanced analytical capabilities that enable event identification and correlation across the enterprise, including intelligent aggregation and correlation of alerts and exceptions from point fraud solutions to ensure the detection of more complex, sophisticated fraud, case management and analysis across all channels and lines of business
- The ability to evolve quickly and keep pace with new criminal trends
- Robust reporting capabilities
- Flexibility to integrate with a firm’s enterprise GRC solutions and initiatives to support company-wide compliance and risk management programs – ideally giving decision makers a snapshot of total risk through an intuitive dashboard approach

Many financial services organizations have made a significant investment in their risk management environments. As such, it is essential to identify a platform that will enable them to leverage existing technology investments – including point solutions, where appropriate – as part of their new approach to financial crime management. The new platform should enable real-time integration with point systems and provide standard integration APIs for the bank’s source systems and payment gateways. (See Figure 4.)
Figure 4

Self-Assessment

After defining a vision for the firm’s approach to fraud management moving forward, organizations must take stock of where they are today. As part of this formal evaluation process, fraud, risk, and compliance teams should consider the following:

1. **Can we create an enterprise-wide view of patterns and perpetrators?** As part of this question, does the organization have a knowledge base that incorporates data from operational/transactional system across separate business units, from human resources and audit records, even from external data sources, such as fraud consortium databases?

2. **Can we detect all types of financial crime, such as wire fraud, ACH fraud, phishing schemes, money laundering, and more?**

3. **Can we prevent and detect fraud in an enterprise context?** Do we pass each transaction – such as account openings, ATM access, online banking transactions, wire transfers, ACH transactions, call center encounters, and more – through a set of rules and predictive models? Can our systems check transaction activity in real time, against enterprise-wide intelligence about the customer and identify potentially suspicious behaviors?

4. **Can we investigate and resolve fraud in an integrated environment?** Can we aggregate and prioritize alerts from the bank’s various fraud detection and money laundering tools and correlate them to provide a full picture of the risk associated with an account or relationship? Can it automatically assign suspicious cases to an investigator?

5. **Do our systems integrate with and help to support broader GRC initiatives and reporting?** Can the solution effectively track the impact of fraud and fraud trends across the enterprise? Are our fraud case management and loss reporting practices standardized throughout the enterprise? Equally as important, is fraud loss reporting methodology
consistent across channels? For example one silo might report a loss as an initial loss, while another channel might report a related loss as a write off, which obscures the true fraud picture. Can our solution measure productivity and report on other efficiency and success metrics to help risk management to direct the fraud management function more effectively?

For each of these questions to which the organization answers “no,” it must dig deeper and understand the extent of the requirements moving forward.

Conclusion

The time has come for financial services organizations to pursue a more strategic approach to fraud management within their organizations. Firms can no longer ignore a powerful convergence of events – more sophisticated schemes and complex organizations coupled with a proliferation of automated channels and transactions – that puts their organizations at increased risk for serious financial losses and reputational damage. Organizations require a comprehensive, enterprise-wide approach to fraud management that supports broader organizational compliance and risk management. The path to this approach includes an IT infrastructure that enables enterprise-wide, real-time, and cross-channel monitoring and management capabilities.