April 2016

Financial crimes observer

A publication of PwC's Financial Crimes Unit

Bank fraud: Old defenses won't stop new threats

Fraud schemes continue to pose an increasing threat to the financial services (FS) industry. In 2015, fraud attacks (i.e., misrepresentation of the truth in order to commit crime) increased overall by approximately 20%, with rapidly-growing attacks such as account takeover fraud[1] and card-not-present fraud[2] increasing twofold.

The integration of technology into the financial services industry is a major factor in this increasing prevalence of fraud. As new payment services, digital products, and connected devices[3] become available, FS firms have been slow to adjust their controls and detection systems. Additionally, the increasing amount of information shared on social media provides fraudsters with new access to data that can be used to perpetrate attacks.

Meanwhile, FS firms have adjusted their fraud programs to prevent well known types of attacks, but fraudsters have adapted quickly. Instead of targeting a broad audience through mass phishing emails, attackers are refining their approach to target particularly high-reward or vulnerable people, from high-profile customers to customers who primarily transact digitally and have limited in-person or phone interactions with FS firms.

Despite the increasing threat of fraud, we have seen that only approximately half of FS firms perform annual fraud risk assessments and, as a result, lack the information necessary to identify vulnerabilities and adjust controls accordingly. Additionally, many FS firms operate with decentralized fraud programs where departments do not coordinate or share information with each other, and as a result often miss red flags and use resources inefficiently.

To proactively prevent fraud and more quickly respond to fraud attacks, FS firms should conduct robust risk assessments, centralize their fraud program, enhance controls, implement a data analytics program, and increase fraud awareness and training.

This **Financial crimes observer** provides ten key steps that FS firms can start taking now.

---

[1] For additional information regarding account takeover fraud, see PwC's *Financial crimes observer, Fraud: Email compromise on the rise* (February 2016).

[2] Card-not-present fraud is the unauthorized use of credit card information to purchase goods or services in a non-face-to-face setting (e.g., internet, phone, postal mail).

[3] For our perspective on managing the security challenges presented by connected devices, see PwC's *Financial crimes observer, Cyber: Securing your Internet of Things* (December 2015).

pwc

What should FS firms be doing?

While there is no one-size-fits-all model for fraud programs, we recommend the following ten steps to improve the detection and prevention of fraud attacks.

1. *Establish a fraud operating model*

Centralization

We have observed that many FS firms' fraud programs are not integrated into the firm's broader risk management framework. For example, FS firms often fail to incorporate fraud into their overall risk assessments, and instead only conduct one-off fraud risk assessments that are inconsistent with the firm's overall risk management strategy. As a result, the business is not provided with the big picture view of the overall risk landscape that is necessary to make decisions about the fraud program. FS firms must integrate fraud into their overall risk management programs – including risk assessments, governance, monitoring, and training.

Additionally, many FS firms have a fragmented approach for reviewing alerts, using multiple teams (e.g., fraud, cyber, AML) that do not coordinate or share information with each other. As a result, such firms struggle to manage data with the accuracy and speed necessary to identify and stop fraud attacks, and use resources and technology inefficiently. By pooling data, FS firms can efficiently analyze overlaps and linkages from formerly siloed departments. Firms can use this centralized data to build predictive models that estimate the probability of future fraud attacks, allowing the firm to combat such attacks proactively.

Leadership

FS firms should formally appoint a fraud leader responsible for managing fraud risk and for communicating related issues with senior management and the board. The fraud leader should be the owner of the firm's fraud risk, and should be given the autonomy to execute policy, set the tone at the top, and coordinate with other departments.

Defined roles and responsibilities

It is essential for FS firms to clearly define roles and responsibilities for key fraud detection and prevention functions, as well as ensure that all three lines of defense are working together effectively and not duplicating roles. Roles and responsibilities should cover fraud incident escalation, investigations, and mitigation.

2. *Implement multi-factor authentication controls*

As the sophistication of fraud increases and more information becomes available on social networking websites for attackers to use, FS firms need robust authentication controls to verify the identity of customers and employees. We have seen that many FS firms lack such controls, relying instead on knowledge-based authentication (e.g., password, date of birth, social security number).

The rapid increase of account takeover attacks highlights the need for enhanced authentication controls. In this type of attack, fraudsters sift through FS firms' websites and social media networks to gather information, and then gain access to accounts by impersonating a customer or employee. The attacker can then transfer funds to an external account. By requiring multiple layers of authentication and implementing more robust authentication controls such as biometrics (e.g., fingerprint, voice recognition) or telephone call backs, FS firms can make it very difficult for fraudsters to impersonate the rightful account holder.

As a baseline, we recommend that FS firms implement multi-factor authentication for most transactions. For higher risk transactions, FS firms should implement additional controls such as out-of-band authentication, which requires user authentication through an additional channel (e.g., telephone call backs, text messages).[4]

We also recommend that firms move beyond knowledge-based authentication to more technological authentication methods such as biometrics and soft tokens (i.e., apps that generate temporary PINs for authentication purposes). Additionally, FS firms can implement behavioral authentication, which uses algorithms to identify abnormal behaviors such as anomalous logins, credit card usage outside of typical locations or times, unusual IP addresses, and multiple failed login attempts. Because implementation costs and timeframes vary across technological authentication controls, FS firms should conduct proper due diligence on vendors to select the level of implementation, cost, and timeline that meets company needs.

It is important that FS firms consider how additional authentication techniques impact the customer experience. For example, text-based authentication (sending the user a text message to verify a transaction) is less disruptive than requiring a customer to call the firm. To provide the least disruptive customer experience necessary, FS firms should require different

[4] For additional information regarding multi-factor authentication and out-of-band authentication techniques, see the *Financial crimes observer* cited in note 1.

levels of authentication based on the fraud risk of the customer and transaction type.

3. *Develop a fraud taxonomy*

Due to the changing nature and complexity of fraud, FS firms often lack a clear understanding of which fraud schemes pose the biggest threat to their organization, and struggle with how to classify and report attacks when they happen. In order to achieve an organization-wide understanding of fraud, FS firms need a system to analyze fraud at enterprise, business line, and product line levels.

The first step to building consistency and awareness of the threat landscape is to develop a fraud taxonomy – i.e., a classification system designed to assist firms with the evaluation, organization, and grouping of fraud schemes when they occur. Fraud taxonomies classify fraud schemes by breaking them down into their elements, such as actors, method, channel (e.g., online, phone), exposure, and motives. When fraud schemes are evaluated by the elements of the fraud taxonomy, the results can help identify root causes and key risk areas, as well as support decisions around areas of investment. For example, a fraud taxonomy might reveal that several fraud schemes impact the same channel (such as a call center), alerting the firm to perform a deeper review of fraud controls for that particular channel.

4. *Conduct periodic fraud risk assessments*

While it is important that FS firms include fraud in their overall risk assessments, this alone is not enough. Without conducting periodic fraud-specific risk assessments, FS firms fail to provide leadership with the information necessary to understand the magnitude of fraud risk and to adjust controls and processes accordingly. Conducting fraud risk assessments allows FS firms to identify key fraud risks, establish processes for proactively monitoring fraud threats, and create fraud detection and prevention methodologies that organically mature with changes in the threat landscape.

However, we have observed that most firms fail to conduct fraud risk assessments with the frequency and depth necessary to effectively combat fraud. Only approximately 50% of firms conduct fraud risk assessments at least annually,[5] and those that do often treat such assessments as a check-the-box compliance exercise instead of a fundamental component of the organization.

FS firms should conduct fraud risk assessments at least annually. Key aspects of a robust fraud risk assessment include:

- Evaluation and prioritization of fraud threats based on historic, known, and emerging fraud trends.
- Estimated severity and likelihood of fraud attacks, and inventory of existing mitigating factors.
- Assessment of risks based on the existence of current controls, and recommendation of adjustments to controls and processes.

When conducting fraud risk assessments, FS firms should use data analytics to prioritize and maximize the returns on fraud program investment decisions. Additionally, given the rapid increase in mobile devices (including smartphones and tablets), FS firms should include fraud risks related to mobile apps in their fraud risk assessments.

5. *Assess fraud performance using metrics*

As regulatory bodies continue to place ultimate responsibility for the implementation and maintenance of effective fraud programs upon senior management and boards of directors, it has become more important than ever to be able to quantify the effectiveness of the fraud program.[6] As a result, metrics around fraud processes, controls, and technology investment have taken center stage.

FS firms should ensure that their fraud programs use fraud metrics to enable senior management and the board to assess the effectiveness of their fraud program. Sample metrics include overall fraud losses, expected losses, average fraud investigation time, false positive and false negative ratios, cost of fraud detection, customer interruptions, and riskiest fraud activity. When communicating these metrics to senior management and the board, FS firms should use dashboards (i.e., visual representations that provide leadership with a streamlined and real-time view of metrics) to identify fraud trends and inform decisions.

6. *Streamline fraud monitoring and invest in analytics*

FS firms should use data analytics to improve the detection and mitigation of fraud attacks. Data analytics range from reactive methods such as descriptive (i.e., what happened?) and diagnostic (i.e., why did it

[5] See PwC's *Global Economic Crime Survey 2016*.

[6] For example, existing Federal Financial Institution Examination Council (FFIEC) guidance provides that senior management and the board have final responsibility for establishing and monitoring policies for risk management, including fraud policies. The FFIEC is a regulatory council composed of the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Consumer Financial Protection Bureau, and the National Credit Union Administration.

happen?) to more sophisticated and complex models such as predictive (i.e., what else could happen?) and prescriptive (i.e., what actions should we take now?).

Data analytics can help FS firms:

- Increase the quality of fraud alerts.
- Reduce investigation costs related to excessive false positives, and avoid losses through reductions in false negatives.
- Generate automatic alerts based on known fraud schemes.
- Correlate independent events (e.g., suspicious inquiries, disbursement requests) that, when viewed together, could indicate fraud.
- Analyze existing and past fraud attacks to more effectively recognize trends and anomalies.
- Optimize the performance of monitoring tools.
- Identify emerging fraud threats, and use this information to develop controls.

Most FS firms lack the skills and resources required for the enhanced coordination, technical knowledge, and implementation capacity necessary to establish an effective standalone in-house data analytics program. Therefore, we recommend using an external technology vendor that can provide tools with more advanced capabilities than what may be developed in-house. Such tools must be coupled with sufficient in-house analytics capabilities to optimize performance.

7. *Increase fraud awareness and training*

Customer service resources and other front line employees should be knowledgeable on common fraud schemes and red flags. However, employees often do not consider understanding fraud risk to be one of their job responsibilities. We have seen that most firms believe that their employees have a high awareness of fraud risk, but in reality such awareness tends to be reactionary and is only prioritized after a major fraud attack occurs.

FS firms should build an overall fraud training and awareness program which:

- Considers role-specific fraud responsibilities.
- Uses various and impactful modes of delivery to build awareness of fraud threats and red flags.
- Promotes compliance with fraud policies and controls.
- Provides training at a frequency that can keep pace with the rapid rate of change of fraud threats.
- Supplements trainings with communications to reinforce key takeaways.

Additionally, FFIEC guidance provides that FS firms are expected to educate customers about fraud risks and mitigation techniques. FS firms should consider including such information in their existing communications with customers. For example, we have seen FS firms successfully communicate fraud risk during their customer authentication processes.

8. *Implement cohesive case management*

Many FS firms have several case management systems (i.e., central repositories for financial crimes data) for fraud, AML, cyber, corporate security, and investigations. With multiple systems used to capture financial crime data, fraud investigators fail to realize that cases they are working on have linkages to incidents in other areas of financial crime. FS firms that take a holistic approach to case management can respond more quickly to fraud, streamline and consolidate communication with stakeholders (e.g., customers whose accounts may be compromised, senior management and the board), maintain a clear audit trail, distribute investigation workload, and better prioritize investigations.

9. *Focus on operational efficiency*

As the prevalence of fraud continues to grow, the number and complexity of solutions and countermeasures will grow as well. Organizational spending on fraud programs has been consistently increasing in the past several years. While fraud programs have improved, many FS firms have found it challenging to balance enhancing processes and controls with promoting cost and resource efficiency.

To better mitigate fraud risks while reducing the cost of fraud operations, FS firms should perform a "health check," assessing existing processes, tools, and controls to identify potential efficiency gains, such as:

- Optimization of fraud models and alert vetting processes to reduce false positive volume and improve coverage detection.
- Prioritization of and review of automated alerts.
- Review of investigations process and tools.
- Improvements in data quality.

A key step to ensuring operational efficiency is to establish an organization-specific fraud program framework, focusing on updating policies and procedures, enhancing fraud controls, and regularly testing the effectiveness of such controls outside of standard regulatory testing.

10. Implement an insider threat program

Many FS firms have deprioritized internal fraud prevention, often dismissing it as a mere compliance exercise. However, while less frequent than external fraud, internal fraud has costly financial, reputational, and regulatory impacts.

FS firms should establish an insider threat program, focusing on the development of internal accountability, access controls, and awareness of the consequences of committing fraud. In developing an insider threat program, firms should implement a fraud hotline to provide employees with an effective means to report fraud without negative repercussions from coworkers or management. Reminders about the hotline and its purpose should be reinforced in trainings and in the firm's code of conduct.

Additionally, background investigations and ongoing due diligence are key measures in preventing internal fraud. FS firms should implement programs to conduct background checks on employees with high-risk roles (i.e., roles that can transfer significant sums of money or access sensitive customer data).

www.pwc.com/us/financialcrimes

Additional information

For additional information about this **Financial crimes observer** or PwC's Financial Crimes Unit, please contact:

Dan Ryan
Financial Services Advisory Leader
646 471 8488
daniel.ryan@pwc.com
@DanRyanWallSt

Sean Joyce
Financial Crimes Unit Leader
703 918 3528
sean.joyce@pwc.com

Joseph Nocera
Cybersecurity Leader
312 298 2745
joseph.nocera@pwc.com
@JoeNocera_PwC

Jeff Lavine
AML and Sanctions Leader
703 918 1379
jeff.lavine@us.pwc.com

Didier Lavion
Anti-bribery/corruption Leader
917 770 2196
didier.lavion@pwc.com

Armen Meyer
Director of Regulatory Strategy
646 531 4519
armen.meyer@pwc.com

Contributing authors: Genevieve Gimbert, Kristen Gaebel, and Kelsey Nencheck.

Follow us on Twitter @PwC_US_FinSrvcs

© 2016 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the US member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. PwC US helps organizations and individuals create the value they're looking for. We're a member of the PwC network of firms in 158 countries with more than 180,000 people. We're committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com/us