January 2018

Financial crimes observer

A publication of PwC's financial services advisory practice

Fraud's getting digital: 8 points to watch in 2018

Fraud was a consistent theme in 2017's headlines, causing significant financial and reputational losses to financial institutions. High impact data breaches plagued credit reporting bureaus, government agencies, and private companies, not only raising concerns around weaknesses in cybersecurity controls but also around fraudulent activity committed with stolen personal data.[1] Meanwhile, fraud schemes such as account takeover[2] and internal fraud[3] have continued to grow over the past year.

In response, financial institutions will need to enhance their authentication techniques – through biometrics or otherwise – to prevent criminals from using compromised data to open new accounts or access existing ones. Additionally, emerging threats such as artificial intelligence-powered attacks as well as new technologies including instant payment services will present a new series of risks. To keep up, financial institutions should reevaluate their operating models to become better aware of the threat landscape and more agile in responding to these new risks. Regulators are also stepping in, with new requirements around data privacy and anti-fraud controls coming into effect this year, and the Financial Industry Regulatory Authority (FINRA) listing fraud first in their 2018 examination priorities.

Below are our eight considerations for financial institutions in the fraud landscape this year, including emerging threats, industry developments, and next steps:

pwc

1. **Account opening fraud and account takeover risk will continue to rise, driven chiefly by digital data theft.**

   New attack methods (e.g., fileless malware) that enable threat actors to gain access to sensitive data without leaving a trace are becoming more common. As a result, high impact data breaches that expose sensitive personally identifiable information (PII) will continue to give rise to and feed downstream fraudulent activities. For example, attackers use PII to register fraudulent accounts by creating synthetic identities[4] (i.e., new account fraud) or to fraudulently access existing accounts using social engineering (i.e., account takeover).[5] One emerging threat is "cross-account takeover," where fraudsters take over a mobile account and access PII to gain unauthorized entry to additional accounts such as bank accounts and loans.

2. **Data privacy, security, and fraud risk management standards will be defined.**

   The upcoming compliance deadline for the EU General Data Protection Regulation (GDPR) in May is paving the way for renewed regulatory scrutiny, with higher expectations surrounding minimum standards for customer data protection against cyber fraud.[6] The GDPR and other data privacy regulations (e.g., China's cybersecurity law) will have a significant impact on US financial institutions with outsourced operations and offshore services, and firms and their third-party service providers will need to assess and adjust their data portability, consumer privacy, and data control policies to comply with the growing set of international standards.

   Meanwhile, regulators both in the US and abroad have been increasing their focus on financial institutions' efforts to prevent cyber-enabled fraud, and compliance deadlines are fast approaching. For example, the EU Payment Services Directive (PSD2) went into effect earlier this month, which introduced new requirements around authentication and transaction monitoring for payments processors. Additionally, the New York Department of Financial Services (NYDFS)'s rules around multi-factor authentication and data encryption go into effect later this year.[7]

   Finally, we expect regulators to increase their focus on firms' fraud risk management capabilities this year, as highlighted in FINRA's 2018 examination priorities. In particular, FINRA will focus on financial institutions' protections against elder exploitation (including the use of high-pressure sales tactics on elderly customers)[8] as well as controls and policies to prevent fraudulent microcap stock trading by brokers. Other regulators are likely to follow suit with increasing expectations around governance as well as anti-fraud policies and procedures.

3. **Faster payments will create new vulnerabilities.**

   As banks increasingly roll out faster payment systems – i.e., payments that can be transmitted instantly, often through mobile applications or text messages – fraudsters will increasingly exploit operational and control deficiencies to initiate unauthorized transfers and requests for funds. Because faster payments do not typically have a clearing period, financial institutions that offer these payments will need to have real-time transaction monitoring systems so they can require additional authentication should a red flag be triggered. Because fraudsters may attempt to circumvent this additional authentication by dialing into call centers and using social engineering, financial institutions will need to train call center staff on detecting and stopping these fraud attempts. Financial institutions will also need to adjust their operating models to ensure that fraud and cyber teams are working together to prevent and detect cyber-enabled fraud attempts on faster payments systems.

4. **The adoption of new authentication techniques, including biometrics, will continue to grow.**

   With major data breaches revealing millions of Social Security numbers and other personally identifiable information to malicious actors, the era of knowledge-based authentication which relies on static personally identifiable information is drawing to a fast close. In response, initiatives such as the White House-backed effort to replace the use of Social Security numbers as personal identifiers and pending legislation to permit the use of mobile-transmitted pictures to verify identification are emerging. Despite these developments, we believe the industry will lead the way forward, driving the adoption of new identity verification[9] techniques through biometrics such as Apple's Face ID and Samsung's iris scanner technology released to the mass market last year.

5. Financial institutions will use RPA to enhance fraud management effectiveness.

Financial institutions will increasingly use robotic process automation (RPA) to perform routine tasks, freeing up employees to focus on more complex activities. Many core fraud risk management capabilities can benefit from RPA, including the assignment of alerts to investigators, scoring and vetting of alert risk, and information gathering for investigations. An additional advantage to using RPA is that it reduces the potential for internal fraud by limiting opportunities for employees or third parties to access and wrongfully use sensitive client data to perform unauthorized transactions.

6. The industry will increasingly use artificial intelligence, but fraudsters will too.

While many financial institutions have turned to RPA to automate routine activities, some are now applying artificial intelligence to automate more complex procedures in fraud risk management and compliance. However, in an arms race against industry players, fraudsters are using scripting and machine learning technology to identify and manipulate financial institutions' processes and controls. As a result, financial institutions will need to increase their investments in redesigning or upgrading their fraud surveillance and analytics infrastructures.

7. Internal fraud will become a focus area.

High-profile instances of internal fraud have resulted in major financial losses and reputational harm[10] to financial institutions over the past year, and regulators have responded with increased scrutiny.[11] As a result, financial institutions will increasingly step up their efforts around insider threat management, conduct risk, employee sales practices, and data protection. We have noticed these efforts already underway, with firms increasingly setting "need to have" policies on access to sensitive data and expanding background checks on employees that do have access to such data. We expect these efforts to continue with advancements in surveillance technology and AI-driven behavioral analytics that will help financial institutions better identify and mitigate the risk of internal fraud before it occurs.

8. What should firms be doing now?

With the emerging threats, industry developments, and corresponding regulatory response highlighted above, financial institutions will need to adjust their governance and controls strategies to keep up. Notably, as fraud and cybersecurity become increasingly connected, financial institutions can no longer afford to approach these threats in silos. Accordingly, firms will need to ensure that anti-fraud and cyber teams are working together to gain a clearer view of the threat landscape, proactively detect threats, and better streamline investigations. Financial institutions will also need to develop leadership playbooks, perform prospective risk assessments, and adapt their operating models to become more agile in responding to the new threat landscape.

Finally, financial institutions should be upgrading their anti-fraud efforts to keep up with emerging threats and new technologies. This includes investing in mobile environment fraud detection as well as developing real-time monitoring capabilities and using data analytics to develop a complete view of customers and fraud risk profiles. Developing this view will in turn help financial institutions improve their authentication techniques by requiring more stringent authentication for higher-risk customers and transactions, while reducing friction for customers by requiring lighter authentication in low-risk situations.

Endnotes

1. For additional information, see PwC's *Financial crimes observer, Cyber and fraud: How to mitigate and prevent the next data breach* (September 2017).
2. For additional information on business email compromise, see PwC's *Financial crimes observer, Fraud: Email compromise on the rise* (February 2016).
3. For additional information, see PwC's *Financial crimes observer, Broker-dealers: New requirements for older customers* (December 2016).
4. A synthetic identity is the creation of a fake individual using bits of personally identifiable information from different, real individuals (e.g., one individual's postal address, another individual's social security number). Because most financial institutions only check these details in isolation from each other, attackers can potentially use synthetic identities to open fraudulent accounts.
5. For additional information on account takeover, see the publication cited in note 2.
6. For additional information on the GDPR, see PwC's *Operational impacts of the General Data Protection Regulation* (March 2017).
7. For additional information on the NYDFS requirements, see PwC's *Financial crimes observer, Cyber: New approach from New York regulator* (January 2017).
8. For additional information, see the publication cited in note 3.
9. For additional information, see the publication cited in note 2.
10. For example, the threat actors that committed the 2016 Bangladesh SWIFT attack had access to detailed information about the Bangladesh Central Bank, suggesting that insiders may have been involved. For additional information, see PwC's *Financial crimes observer, SWIFT action: Preventing the next $100 million bank robbery* (June 2016).
11. As examples, regulators have recently increased their scrutiny on elder fraud from broker-dealers and on protecting customers' sensitive data from unauthorized internal access. For additional information, see the publications cited in notes 3 and 7 respectively.

www.pwcregulatory.com

Additional information

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

Julien Courbe
Financial Services Advisory Leader
646 471 4771
julien.courbe@pwc.com
@JulienCourbe

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

Jeff Lavine
Financial Crimes Unit Chief Operating Officer
703 918 1379
jeff.lavine@us.pwc.com

Genevieve Gimbert
Fraud Management Leader
646 471 5145
genevieve.d.gimbert@pwc.com
@GenGimbert

Vikas Agarwal
Financial Crimes Technology Leader
646 471 7958
vikas.k.agarwal@pwc.com

Roberto Rodriguez
Financial Services Advisory Manager
646 471 2604
roberto.j.rodriguez@pwc.com

Contributing authors: Frank Badalamenti, David Fapohunda, Astrid Yee-Sobraques, Angela Watene, and Michael Horn.

Follow us on Twitter @PwC_US_FinSrvcs