Seminar on Fraud in the Payments Environment

On June 28th, 2016, the Payments Risk Committee (PRC) hosted a seminar, Fraud in the Payments Environment, to enhance industry awareness of the increasing incidence of fraud in the payments environment. The seminar provided education, awareness, and an opportunity for dialogue for over 150 participants from approximately 60 institutions that included law enforcement agencies, FinTech companies, vendors to the financial services industry, banks and a representation of their clients. The sessions highlighted common challenges related to payments fraud in today's rapidly evolving payments environment, and provided participants the opportunity to discuss current practices and initiatives that are being used by industry participants to detect fraudulent payments and to mitigate fraud in the payments environment.

On behalf of the PRC, we are pleased to provide the key takeaways of the seminar to the public.

Seminar on Fraud in the Payments Environment – Key Takeaways

Overall, industry participants indicated they are collectively challenged with implementing controls at a commensurate speed with increasingly sophisticated fraud techniques. Corporations and their banks are attempting to determine the appropriate level of investment in fraud controls, given the rapid evolution of the threat environment. One of the key takeaways from the seminar was that there is a need for the industry to better collaborate, liaise, and communicate on the common issues faced in addition to developing potential solutions together as a community. For more specifics on the individual sessions, please see the key takeaways below.

SESSION I: Bankers' and corporations' fraud experience with electronic payments: lessons learned, resolution, and best practices

Key Takeaways:

- The payments industry continues to work on the timely implementation of controls that offer adequate protection against fraudulent payment attempts.
    - Examples of fraud controls include comprehensive staff training, email filter tools, phone confirmation, management escalation processes, multifactor authentication, and biometric authentication. Banks and corporations should also ensure there is appropriate segregation of duties for sensitive tasks.
- Fraud mitigation is an on-going initiative, and requires proactive engagement by all participants.

SESSION II: Current and future technologies to combat fraud

Key Takeaways:

- The industry is working to find the optimal balance of technology investment for adequate fraud protection.
- Additionally, banks strive to implement enough fraud prevention tools to protect clients, while keeping online user experiences efficient and manageable. This is a critical line of defense and banks are focused on achieving the balance right.
- Corporations must implement a comprehensive suite of controls that are designed to protect against different aspects of fraud as one solution will not solve every problem.
- The industry can benefit tremendously from increased data sharing. Data sharing must be rules-based and non-discretionary, and all participants – corporations and banks – collectively need to move past the stigma of reporting cyber incidents.

SESSION III: Law enforcement initiatives

Key Takeaways:

- Reporting and data sharing through central sources is instrumental in identifying patterns of fraudulent payments.
- Suggestions and highlighted practices for fraud prevention include limiting postings to social media/public websites, escalating/reporting requests for secrecy over email, implementing 2-step verification processes and understanding hackers' behavior (e.g. fraudsters may try to initiate fraudulent payments on Fridays, especially before a holiday/long weekend, to ensure they have enough time to transfer funds before the compromised entity notices the attack).

- Customers should notify their banks of fraud attempts immediately, and report fraud attempts (both successful and unsuccessful fraud attempts) to both the FBI's Internet Crime Complaint Center (IC3) and the local FBI field office. Banks should contact their clients immediately when they believe a transaction appears fraudulent.
    - For more information on business email compromise, please see the following public service announcement from the IC3 (https://www.ic3.gov/media/2016/160614.aspx)

SESSION IV: Consultancy views: how can corporations protect themselves?

Key Takeaways:

- As countries move towards implementing faster/real-time payments, it is clear that the payments industry must implement controls which offer adequate protection against fraudulent payment attempts (faster payments are immediate and irrevocable and these new faster payments systems may need to be upgraded accordingly to combat fraud). Two primary fraud types that could impact firms are account takeover fraud and enrollment fraud.
- Fraud mitigation for faster payments requires two lines of defense: bank-level and network-level fraud framework. Information sharing could help mitigate fraudulent payment attempts when used at the network level.
- Technological innovations could improve efficiencies, create an audit trail, and enhance transparency between all parties while not necessarily exposing the parties' identities or the details of their transactions.

SESSION V: FRB Payment Systems Improvement Strategy and Secure Payments Task Force: Plans to keep the evolving U.S. payments infrastructure secure

Key Takeaways:

- In addition to speed, security is the priority for payment systems; users will not accept a reduction in security in return for faster payments.
- The industry should maintain a focus on the security of payments as they develop new technology to enable faster payments. An industry group – the Secure Payments Task Force – has been established to focus on reducing fraud risk and advancing the safety, security and resiliency of the payment system.
- Data shows that fraudulent activity has increased from 2013-2015, some of which can be attributed to an increase in wire fraud.