PRC PAYMENTS RISK COMMITTEE

Sponsored by: FEDERAL RESERVE BANK of NEW YORK

Conference on Securing the Payments Ecosystem

On June 7, 2019, the Payments Risk Committee (PRC) hosted a conference, Securing the Payments Ecosystem, to bring together leading banks and financial institutions, corporations, FinTech companies and public sector officials for a discussion focused on securing and protecting the payments system. The seminar provided education, awareness, and an opportunity for dialogue for over 150 participants from approximately 80 institutions. The panels highlighted approaches to secure payment system endpoints, address fraud in an evolving threat landscape, resolve suspicious or fraudulent payments, and respond to cybersecurity threats.

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

Sponsored by the Federal Reserve Bank of New York, the Payments Risk Committee is a private sector group of senior managers from several major banks in the United States. The primary goal of the Committee is to foster enhancements to the safety and efficiency of financial market infrastructures. The Committee identifies and analyzes issues of mutual interest related to risk in payment, clearing, and settlement systems. Current members of the Committee are Bank of America, The Bank of New York Mellon, Citibank, Deutsche Bank, Goldman Sachs, HSBC Bank, JPMorgan Chase, Morgan Stanley, MUFG Bank, State Street, UBS, and Wells Fargo.

Conference on Securing the Payments Ecosystem – Key Takeaways

As the payments landscape has evolved over the course of the last decade, so have the threats it faces. The techniques employed by bad actors have become increasingly sophisticated as attackers have sought to leverage every potential weakness of the payments ecosystem. Today's bad actors can exploit financial systems that are digital and global, making the threat remarkably larger than in the past. Under this constant pressure, industry participants are challenged with implementing controls at a commensurate speed and adopting increasingly sophisticated anti-fraud techniques. This is particularly important given that participants in the payment system are dependent upon each other to ensure the safety and security of each node within the payment chain.

One key takeaway from the conference is that the required response to these threats is not solely technological, but rather, should also address the vulnerabilities created by the human element. Commenting on the fact that the majority of security breaches continue to be the result of human error, many speakers emphasized the need to better educate both employees and clients on best practices to mitigate fraud risks. They reiterated the need to have effective governance structures in place to address fraud within financial institutions, including clearly defined incident response plans that are well-socialized by key stakeholders.

For more specifics on the individual sessions, please see the key takeaways below.

SESSION I: Securing Payment System Endpoints in a Real-Time Environment

Key Takeaways:

- With fraudulent payments on the rise, the industry is continuing its efforts to improve wholesale payments security, notably leveraging the comprehensive strategy to reduce the risk of payments fraud related to endpoint security published by the CPMI in May 2018.
- As the payment chain is only as strong as its weakest link, the education of end-users is key in strengthening the security of payment systems' endpoints. Firms should consider ways to effectively communicate with customers about fraud risks, implement controls to help customers manage fraud, and utilize real-time monitoring capabilities where possible.
- Beyond educating end-users, industry participants are also bolstering their fraud detection capabilities, in particular by expanding real-time monitoring, malware detection and anomaly detection through pattern recognition.
- The industry could benefit from greater cooperation on the identification of potential bad actors as the current level of information may not be sufficient at the individual level to take action. One approach to consider is learning from other fraud mitigation models, such as the practices used by the Card industry to share bad actor information.

SESSION II: Preventing and Detecting Fraud in an Evolving Threat Landscape

Key Takeaways:

- While preventive cybersecurity and ongoing hygiene are critically important, it is virtually impossible to prevent bad actors from penetrating systems. As such, the industry participants' main focus has shifted from attempting to avoid security breaches to detecting intrusions and reacting quickly and decisively once a breach has occurred.
- Well-defined escalation procedures, in combination with real-time reconciliation of transactions, anomaly checking and the ability to stop outgoing payments, are paramount to ensuring that financial institutions are able to effectively respond to fraud attempts.
- AI and machine learning, when utilized effectively to maintain a seamless customer experience while bolstering fraud protection, may be useful tools in efforts to strengthen the payment ecosystem while limiting additional friction in the payment process. The ability to collect and manage data is key to success.
- In using emerging technology for pattern detection, participants noted that including what may seem to be unrelated data points can be useful, particularly for wholesale payments which typically do not offer a deep, rich data set.

SESSION III: Sounding the Alarm: When Payments Go Awry

Key Takeaways:

- The first line of defense for financial institutions against fraud is a well-defined governance structure and internal code of conduct, complemented by a strong internal and external audit program and forward-looking training on a payments fraud response plan.
- Financial institutions should proactively conduct extensive fraud risk assessments in view of mapping out their potential vulnerabilities, risk appetite and countermeasures. Where known fraud has occurred, the ability to act quickly with the appropriate counterparties is critical. The investigative response also requires appropriate root cause analysis to implement the right fix to mitigate future incidents.
- Although financial institutions have limited time to recall fraudulent payments, the first step in incident response is to properly analyze the potential impact and take steps to contain it. Proper incident and impact analysis will enhance an institution's ability to effectively communicate with clients, counterparties and law enforcement as they attempt to recover lost funds. Pre-established relationships with counterparties' fraud departments may prove beneficial to expediting the recovery of misdirected funds.

SESSION IV: Cybersecurity: Responding to the Threat

Key Takeaways:

- Although the financial industry understood early the need to invest in cybersecurity and, as a result, is much more advanced in its thinking than other business sectors, it is important for all firms to continue prioritizing cybersecurity as the threat landscape is ever evolving.
- A holistic approach is required for effective cybersecurity, and reflections on the topic should encompass the following three components: threat intelligence and continuous monitoring of the evolving threat landscape; capacity to quickly detect and analyze potential security breaches; and clearly defined incident response plans, both from a business and customer-facing standpoint.
- There is value in getting everyone to understand that all individuals, inclusive of employees and customers, play a role in protecting and securing the environment, regardless of whether or not they are in an explicit cyber role.
- Continued coordination across industries and with official authorities, including an effort to widen table top exercises and communication avenues, is helping to respond to evolving threats from state-sponsored and private bad actors.