FedPayments Improvement COMMUNITY FORUM

Collaborate. Engage. Transform.

Remote Payments Authentication Fraud
Challenges and Opportunities

In late 2018, a diverse group of 300 industry stakeholders came together at the FedPayments Improvement Community Forum to engage in inclusive dialogue focused on improving the U.S. payment system. Through general sessions and topic-specific workshops, Forum attendees provided their candid feedback about the latest payment modernization efforts.

In this workshop, the panel discussion and audience Q&A focused on how the industry can engage to implement stronger payment account authentication to prevent and mitigate remote payments fraud.

Moderator

Marianne Crowe, Vice President
Federal Reserve Bank of Boston

Panelists

Christian Wilson, Vice President
Cyber, Fraud and Risk
First Data Corporation

Kolin Whitley, Senior Director
North America Risk Group
Visa

Reed Luhtanen
Senior Director, Payments Strategy
Walmart

Highlights From the Panel Discussion

Remote payments authentication fraud has increased in the United States, driven by growth in e-commerce. Remote payments fraud occurs when the cardholder and physical card are not physically present during the transaction. It's more difficult to authenticate the buyer without his or her physical presence.

The migration to EMV chip technology further secured in-person payments, but it has contributed to a shift in fraud to card-not-present payments in e-commerce and mobile channels. Weak authentication processes further enable fraudsters to use readily available and vulnerable stolen payment credentials and other personally identifiable information (PII) to create accounts and conduct remote payments fraud.

In her opening remarks, Marianne Crowe of the Federal Reserve said reducing remote payments fraud by implementing stronger authentication approaches and tools requires collective and coordinated action by the financial services industry, especially because fraud historically migrates to the weakest link in the payment chain.

Kolin Whitley of Visa noted that some merchants have sophisticated authentication controls to identify consumers, but adoption is not uniform across the industry. Sometimes small merchants can have an advantage in identifying and mitigating fraud if transaction volume is low. However, regardless of stakeholder volume or size, the industry shares concerns about adding friction to the purchase transaction or imposing too many barriers to the customer experience that can result in lost sales. Fraudsters have also extended their focus to personally identifiable information, another area of high vulnerability. This has enabled them to create synthetic identities and fraudulent accounts.

Whitley said the industry must continue to collaborate on authentication strategies that no longer rely solely on PII.

CONTINUED ON PAGE 2

Instead, they need to research stronger authentication approaches that incorporate analysis of customer behavior, purchase and transaction history and device fingerprints. Current examples include one-time passwords (OTP) and out-of-band authentication using SMS messages.

First Data's view of remote payments fraud is shaped by its role both as a major issuer (open and closed loop) and as a debit network.

Christian Wilson of First Data said no single solution will solve the authentication problem. The current approach is to think about security in concentric layers.

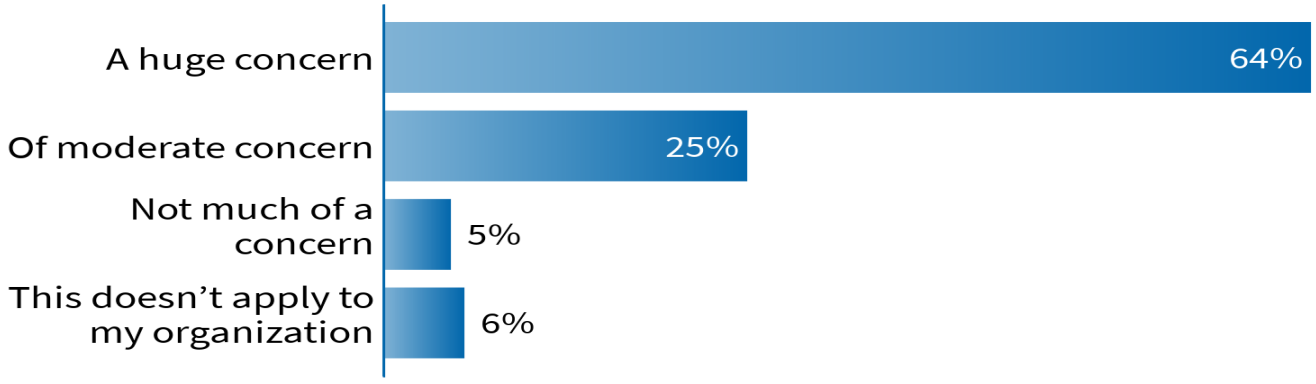
Combining knowledge-based answers with transaction monitoring is an example of a multi-layered solution. Next-generation solutions need to adapt to new payment methods. Wilson also said that good monitoring and alert systems are critical to address remote payments authentication.

Reed Luhtanen of Walmart said Walmart's card-not-present transactions are growing as it builds its e-commerce business. Walmart's priority is to maintain trust in its brand in all channels and this extends to the payment experience. The challenge for retailers is to balance transaction security that creates safety for the customer with a convenient payment experience. While strong payer authentication is also a primary concern, Luhtanen pointed out that merchants are limited to the authentication tools available on the payment products being put into the market by issuers.

The panelists agreed that fraud can be analyzed by concentration and merchant type, but more collaboration is needed to reveal reliable, real-time trends. Incentives need to align for merchants and payment networks, financial institutions of all sizes and aggregators. As a sign of this collaboration, a coalition of retailers and debit networks announced the Secure Payments Partnership (SPP) in June 2018 to promote security across the payment system.

FedPayments Improvement COMMUNITY FORUM
Collaborate. Engage. Transform.

How big of a concern is remote payments fraud at your organization?



Total Results: 107

Poll Everywhere

THE FEDERAL RESERVE
FedPayments Improvement
Collaborate. Engage. Transform.

To learn more about the Federal Reserve's work and engage in this collaborative effort to transform the U.S. payments system, join the FedPayments Improvement Community.