payments system research briefing

October 2015 | Federal Reserve Bank of Kansas City

The Puzzle of Payments Security: Fitting the Pieces Together to Protect the Retail Payments System

Highlights from the 2015 International Payments Policy Conference

By Terri Bradford, Payments Research Specialist

On June 25-26, 2015, the Federal Reserve Bank of Kansas City hosted its fifth international payments policy conference, "The Puzzle of Payments Security: Fitting the Pieces Together to Protect the Retail Payments System." More than 120 payments system participants and observers met to exchange their thoughts and views on payments security and fraud as matters of importance for preserving public confidence in worldwide retail payment systems. The conference began with opening remarks from Gov. Jerome H. Powell of the Federal Reserve Board of Governors. Gov. Powell emphasized that in this increasingly complex payments system, all parties need to work together to build a safer, more efficient payments system and asked for participants' support of efforts under way. This *Briefing* offers highlights from the conference.

Apply Game Theory to Payments Security

The opening session, "The Economics of Payments Security," discussed applying an economic perspective to payments security. The goal was to highlight how economics can help to better understand the dynamics of retail payments security and offer guidance as to why the payments system is not moving on to better, more secure technologies or practices as quickly as it might.

Game theory was a key aspect of the discussion. Game theory can be applied whenever the actions of two or more entities—individuals, organizations, governments—are interdependent; it also can reveal sources of conflicts. As it relates to payments security, game theory may be useful in evaluating whether strategies, technical solutions and policies employed by industry participants and policymakers can achieve security goals. If the results of the game suggest that achieving the desired goals is unlikely, game theory also enables participants to consider which part(s) of the game needs to be modified to achieve the desired level of security, providing insights into public policy and private entities' strategies.

A scenario discussed was the United States' migration to EMV, the proprietary chip technology based on a global standard called Europay, MasterCard and Visa. Instead of mandating EMV, effective Oct. 1, 2015, card networks shifted the fraud liability for a card present transaction from the issuer to the merchant, provided the merchant has not adopted EMV but the issuer has.[1] Using a game theory framework, this liability shift would be expected to incentivize merchants to adopt EMV and change equilibrium from neither issuers nor merchants adopting EMV to both adopting EMV. It was also noted that while the liability shift will likely generate the more secure outcome, it may not distribute the net benefit

equally to the involved parties. One party may benefit more than another or actually be worse off. However, it is difficult to infer the fairness of this liability shift because the payoffs are set relative to the status quo; the actual payoffs in absolute terms are unknown. Also, potential indirect benefits of EMV migration are disregarded: even if merchants incur a heavier burden than issuers for EMV migration, merchants may incur a lighter burden than issuers for other complementary security improvements, such as stronger authentication for card-not-present (CNP) transactions.

The discussant commented that game theory provides a foundation from which to better approach the understudied area of payments security economics, but a shortcoming is that it works best to analyze an idealized version of the world. For example, applying the EMV adoption game mentioned above to reality would require transparency about fraud losses. Such statistics require reliable data collected through a standardized method. Without knowing actual fraud losses, issuers and merchants cannot know their payoffs from adopting or not adopting EMV, which does not satisfy a key assumption of game theory.

Key takeaway: Data collection in standardized forms is a key to applying game theory to the real world. From a policy perspective, ideal security strategies would be broad in scope and meet longer-term needs rather than achieve a single security improvement. To encourage participation in such strategies, it is important that costs and benefits be fairly distributed among participants.

Data on Fraud and Payment Security Incidents Are Key Components

Improvements in payments security could not only reduce fraud rates and the incidence of data breaches, but also ultimately reduce the amount of money spent to protect payments transactions. Improved data collection of fraud and payment security incidents is needed to help focus and direct resources where they are most needed and can do the most good. In the session "Monitoring Payment Fraud: A Key Piece to the Puzzle," conference contributors from the Bank of France's Observatory for Payment Card Security and the Australian Payments Clearing Association (APCA) shared insights from their experiences collecting and analyzing payments data and data facilitating payment security improvements.[2]

The Observatory monitors security measures adopted by issuers and merchants, aggregates fraud statistics and maintains a technology watch for payment cards. It began data collection with an understanding of the information it wanted to capture; the Bank of France wanted to understand fraud rates, prevalence of fraud and where fraud originated. Information gathered since 2006 helped the Observatory identify fraud trends and make recommendations, one of which was the use of two-factor authentication and 3D Secure. The Observatory convinced involved parties of their incentives to adopt these stronger security methods and allowed for a risk-based approach for deploying stronger authentication. The Observatory recognized its efforts would be most effective if they were not "French-only"; the reach needed to be broader. As a result, the Observatory supported the emergence of a European forum for supervisors and central bankers through which there was a successful push to require strong two-factor authentication within the law. In December 2014, the European Banking Authority released guidelines on securing online payments across the European Union (EU) with an implementation deadline of Aug. 1, 2015, for EU companies to begin research and deployment.

Five years ago, after concluding that the lack of investment in payment security was partly due to the lack of appropriate data, APCA began collecting data to better understand fraud rates and prevalence, the consequence of fraud, and the threat matrix. Data are essential for risk management capability and for enhancing public debate when arguing for security improvements. With the data, an impact analysis can be undertaken to identify what happens when fraud occurs—who ultimately bares the losses, what are the real costs, and what is the cost of implementing new security technologies. Reporting requires cooperation, which has helped participating organizations manage their own fraud. As for capturing data and reporting, APCA found both are better done when the industry volunteers than when it is required by regulation. It is more cost effective and also enables a greater focus on industry needs. APCA also shares the information with the public to broaden the awareness of fraud and its prevention.

Key takeaway: Data collection is essential to understanding rates, prevalence and origination of fraud, and facilitates an understanding of the real costs of fraud and security breaches. What can be measured can be managed. Deciding between private action and public intervention is likely a false dichotomy; the private and public sectors need to work in tandem. Because fraud and payments security are everyone's concern, a collaborative approach to collecting data

on fraud and payments security incidents is most beneficial. Ultimately, facts make for better public debate about how best to allocate resources.

There's No One-Size-Fits-All Solution for Securing Data

Each deployment of enhanced security standards and applications chips away at the larger issue, but no one security standard or application is the "silver bullet." Consequently, payment security should be designed for defense-in-depth; if one defense is compromised, other defenses may mitigate losses. During sessions that addressed securing data against persistent and unforeseen vulnerabilities, contributors representing processors, networks, issuers, merchants, security services providers and standards committees discussed various security standards, protocols and procedures— including ways to devalue payments data.

Discussion began with the Payment Card Industry Data Security Standards (PCI DSS), which are developed and managed by the PCI Security Standards Council (SSC), a global forum established by the four U.S. credit card networks and the Japan Credit Bureau. Each of these card brands enforces compliance with the PCI DSS for merchants that accept their card brands and for entities that process those card payments. To ensure compliance, merchants and processors employ the services of PCI-qualified security assessors. However, PCI DSS compliance is assessed at a point in time and historically has been treated by the involved parties as a prescriptive checklist. Such a treatment may not address the various challenges faced by different types of merchants and processors. Because merchants and processors need to work with multiple enforcers, when breaches occur, compliance and resolution are at best confusing processes. Furthermore, security implications of a range of emerging payment technologies also present challenges for the PCI SSC, as does the slow pace of adapting to new technologies such as encryption and tokenization, which should reduce the scope of PCI DSS assessment.

One of the processors that contributed to the discussion invested to develop a point-of-sale (POS) encryption technology, which enables POS encryption that protects card data from point-of-capture throughout the transaction to the point at which the data are decrypted. Even if stolen, criminals cannot use the encrypted data to create counterfeit cards or make fraudulent CNP transactions, as long as the keys to decrypt the data are not stolen.

Tokenization, which replaces sensitive data with surrogate information, is one way to devalue payments data. Tokenization can take two forms: a pre-authorization (payment) token and a post-authorization token. EMVCo developed standards for pre-authorization tokens that are used for transactions made at a particular online merchant or mobile wallet provider, such as Apple Pay. This type of tokenization offers an opportunity for a paradigm shift from a payment environment in which a card number can be used for counterfeit purposes to one in which a token replaces a card, and a cardholder can only use that token in a particular situation. However, while purchases through mobile apps and at online merchants are growing, they are only a fraction of payments volume. More focus is needed on standards that address the POS, where the majority of card transactions are still made.

Key takeaway: No one solution addresses security in all of the different places and ways payments can be made. A multipronged security approach is needed. Encryption and tokenization technologies don't compete; they are complementary. Standards are a key component of payments security, but there is an underlying tension between proprietary and open standards. Coupled with technologies that enhance data security or devalue data, stronger payer authentication through EMV cards or multifactor authentication can be expected to improve payments security.

Collaboration is a Constant Throughout

While the importance of collaboration was addressed throughout the conference, sessions on the second day highlighted collaboration as integral to addressing payments security. Collaborative efforts have been made at many different levels—among industry participants, public authorities and across public and private sectors, both domestic and international. The greater good is a driving force for many of the efforts under way.

Challenges for collaborative efforts among industry participants include how best to measure success, overlapping initiatives and trust. Defining scope and deliverables are essential for successful collaboration. Success can be measured by metrics, but reliable statistics are rare. Adopting practices and standards is another objective measure. Subjectively, success

can be measured by sustained commitment to partnerships and networks that are built across private sectors, which historically in the payments ecosystem has not been the norm. Overlapping initiatives present another challenge. Many well-intentioned industry groups try to solve the same problem. Some are partnerships among private-sector participants, while others are private and public collaborations. To best allocate resources among the various initiatives, industry participants can categorize the problem that is being addressed, look at the mission and then choose carefully among the initiatives. Trust, however, is likely the biggest challenge. Participants have a shared customer, but they also have a shared enemy; the more trust among participants, the better. Private sectors have started collaborating where possible—for example, merchant and financial service sectors collaborate on cybersecurity.

Cooperation among public authorities is occurring at international and domestic levels. The Bank for International Settlements has established a Working Group on Cyber Resilience that consists of representatives from more than 20 central banks and financial service authorities to examine systemic risk and cyber resilience of financial market infrastructure (FMI). The Eurosystem has created SecuRePay as a forum among bank supervisory authorities to address issues pertaining to the security of online card payments. In the United States, the U.S. Department of the Treasury has created the Financial Sector Cyber Intelligence Group (CIG), a specialized team of analysts with expertise in financial services, cybersecurity, and intelligence analysis, to distribute timely and actionable information and analysis that financial institutions can use to protect themselves from cyberattacks. However, while public sector efforts in various countries are under way, international collaboration remains a challenge. From country to country, the optimal way to collaborate differs. In some countries, regulators need to push for collaboration; in others, regulation may hinder collaboration. The Financial Services Information Sharing and Analysis Center, which is expanding internationally, could stimulate international collaboration, as could crisis management exercises.[3] Promoting cross-border information sharing among FMIs also would be beneficial.

When self-regulation or market-based approaches prove insufficient to achieve socially desirable outcomes, public authorities may need to use moral suasion, cooperation, regulation, or operation to bring about desired change. Given the tendency to first employ a "lighter touch," moral suasion may first take the form of research on topics such as card security or assessment guides. Take, for example, the National Institute of Standards and Technology (NIST) guidance on baseline protections and best practices, information sharing and recovery planning, which can help bridge differences in how authorities deal with issues of payments security.[4] Cooperation may involve collaborating with many parties and/or encouraging collaboration and coordination in policy recommendations. Public authorities can become involved in private sector initiatives such as retail payments boards or task forces that allow for a neutral party to aid in the discussion of new private sector initiatives when competition provides a disincentive for agreement. The Observatory's work in fostering adoption of stronger online security methods is one example. Regulation may include policies and guidance for systemically important payment systems. For example, SecuRePay is developing new policies for cyber resilience of FMIs and retail payments services and, in cooperation with other banking authorities, will be analyzing and monitoring incidents and fraud reporting. Operation may entail central bank involvement in providing payments systems, much like the Federal Reserve is an operator of wholesale and retail payment systems.

Key takeaway: There are trade-offs between private and public collaboration. Private efforts may be best positioned to address security standards because of responsiveness and technical expertise. However, where problems of market power and the choice of security standards persist, some role for the public sector—moral suasion, cooperation, regulation, or operation—potentially may be required. Various initiatives in the global marketplace have demonstrated the power of collaboration. Though many efforts under way aren't intended to have an indefinite life, there is interest in continued collaboration as a means to address ongoing issues.

Conclusion

Securing the payments system is a matter of utmost importance to payments participants and policymakers. Ideally, payments participants can work together, as has been done at other pivotal moments in payments—the creation of the automated clearinghouse and modernization of the check system. Those efforts should serve as examples of moments when payments participants came together to do the work that was needed. Lessons may also be taken from instances where an opportunity to be more proactive was available, but the moment wasn't seized.

Efforts are under way in the private and public sectors—domestic and international—to address several payments policy issues. Furthermore, the recently formed Secure Payments Task Force, which is comprised of nearly 200 participants from a range of payments system stakeholders, is advising the Federal Reserve on payment security matters and identifying and promoting actions that can be taken by payments system participants collectively or by the Federal Reserve System.

This *Briefing* offers a few of the many conference highlights. Conference materials are available to view or download: *https://www.kansascityfed.org/research/bankingandpayments/pscp-2015*. A full proceeding from the conference will be available soon.

Endnotes

[1]For Visa, this shift only applies to counterfeit transactions. MasterCard, Discover and American Express introduced a security hierarchy in which fraud liability for lost or stolen cards will shift to the party with the highest risk environment. In this hierarchy, card networks consider an EMV card used with PIN to be more secure than an EMV card used with a signature.

[2]The Observatory, created in November 2001, is a forum for fostering dialogue and information sharing among all parties in France concerned with the smooth operation and security of card payment schemes. APCA is the self-regulatory body set up by the Australian payments industry to improve the safety, reliability, equity, convenience and efficiency of the Australian payments system. APCA's 100 members include leading financial institutions, major retailers and other principal payments service providers.

[3] The Financial Services Information Sharing and Analysis Center (FS-ISAC) is a global financial industry resource for cyber and physical threat intelligence analysis and sharing. While FS-ISAC works with members that have global operations, in early 2013, FS-ISAC's board extended its charter to share information between financial services firms worldwide.

[4]NIST is a non-regulatory federal agency within the U.S. Department of Commerce. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve quality of life.

payments system research

Website: http://www.kansascityfed.org/research/bankingandpayments/

The Payments System Research Department of the Federal Reserve Bank of Kansas City is responsible for monitoring and analyzing payments system developments. Staff includes:

Terri Bradford
Payments Research Specialist
Terri.R.Bradford@kc.frb.org
816-881-2001

Fumiko Hayashi
Senior Economist
Fumiko.Hayashi@kc.frb.org
816-881-6851

Richard J. Sullivan
Senior Economist
Rick.J.Sullivan@kc.frb.org
816-881-2372

Joshua Hanson
Research Associate
Joshua.Hanson@kc.frb.org
816-881-4762

Jesse Leigh Maniff
Payments Research Analyst
Jesse.Maniff@kc.frb.org
816-881-2091

William Todd Mackey
Vice President
William.T.Mackey@kc.frb.org
816-881-2459

The views expressed in this newsletter are those of the author and do not necessarily reflect those of the Federal Reserve Bank of Kansas City or the Federal Reserve System.