ESSAYS ON ISSUES

THE FEDERAL RESERVE BANK
OF CHICAGO

DECEMBER 2011
NUMBER 293a

Chicago Fed Letter

Improving security for remote payments

by Nour Abdul-Razzak, associate economist, Katy Jacob, business economist, and Richard D. Porter, vice president and senior policy advisor

Given the growing popularity of e-commerce and m-commerce over the past few years, remote payments have become commonplace. Unfortunately, remote payments fraud has grown in response. On September 26, 2011, the Federal Reserve Bank of Chicago and the Secure Remote Payment Council (SRPc) co-hosted a symposium to discuss strategies that help reduce such forms of fraud.

Some materials presented at the symposium are available at www.chicagofed.org/webpages/events/2011/fraud_symposium.cfm.

Remote payments, or transactions made in non-face-to-face environments, comprise many types of activities, including online shopping, peer-to-peer transactions, and music or ringtone purchases made on mobile devices. For the vast majority of remote payments, there are many parties involved: the consumer, merchant, issuer, acquirer, switch, possibly a telecommunications company, and multiple third parties.[1] Currently, no central body in either the public or private sector coordinates these parties in the U.S. payment system. The Federal Reserve serves as the statutory overseer of certain retail payment regulations, especially regarding checks, and the newly formed Consumer Financial Protection Bureau has some jurisdiction over consumer protection issues related to payments. However, no single entity has broad jurisdiction over U.S. retail payments. This decentralized structure is critical to understanding why it is so challenging to come up with workable solutions to payments fraud (whether committed online or offline) in the U.S.

The large number of parties involved in the U.S. payment system and the current lack of coordination by a central authority can make it difficult to pinpoint specific market failures that lead to payments fraud. Most fraud is inherently difficult to detect and probably even more difficult to measure, given the complexity of most payment systems. So, coming up with solid statistics on the magnitude of payments fraud is difficult. Nonetheless, most industry leaders agree that fraud costs are considerable. According to the *Norton Cybercrime Report 2011* produced by the Symantec Corporation, there were 431 million adult victims of cybercrime across the world over the past year, with losses (financial losses plus lost time) totaling $388 billion; the 2011 cybercrime ledger was $100 billion larger than the global black market for marijuana, cocaine, and heroin combined.[2] In addition, according to Verizon's *2011 Data Breach Investigations Report*, more than 1,200 cybercrime suspects were arrested by the U.S. Secret Service in 2010; their crimes had resulted in over $500 million in actual fraud losses, and their activities had the potential for $7 billion in further losses.[3] The Federal Bureau of Investigation is currently investigating more than 400 cases of corporate account takeovers[4] involving unauthorized wire and ACH (automated clearinghouse) transfers amounting to $85 million in losses.[5] Indeed, as organized crime around the world increasingly turns to remote payment channels to fund illicit, and even terrorist, activities, the ability to effectively combat payments fraud takes on greater importance.[6]

Complex contributing factors

Advanced technology has enabled new forms of commerce to flourish, but it has also opened up new channels for fraud. Remote payments fraud can occur in a variety of ways at a multitude of points in any given transaction. Vulnerabilities abound in many types of remote payments—and oftentimes such weaknesses are not isolated to specific transactions. Take, for instance, Internet transactions, which are typically secured by SSL (Secure Sockets Layer) encryption.[7] Cybercriminals can break the SSL encryption and decrypt data passing between a web server and an end-user's browser. SSL protocols can also be circumvented by tricking consumers into using fraudulent websites and revealing their personal information, i.e., by "phishing." In addition, mobile payments can be vulnerable to fraud if the hardware itself and the attending software are not properly secured—criminals can intercept wireless communications to access transaction information.

> Various means are currently being used to manage payments fraud, and each has its own benefits and risks.

Besides security vulnerabilities, we must consider other complicated and interrelated factors when examining remote payments fraud. For example, card issuers are generally less concerned about fraud risk for remote payments because they are often immune to losses in such cases.[8] Merchants are most often liable for losses due to remote payments fraud, especially since zero liability programs instituted by the card network companies often protect consumers. Partly in response to this liability issue, more and more online and mobile payments are now being made via alternative payment channels, including PayPal and other closed-loop, proprietary systems, which are not interoperable. These various new payment platforms may constitute a growing security risk because of the increased number of entry points for fraudsters. Even so, if remote payments fraud involving payment cards is not managed properly, consumers might increasingly move to alternative payment methods that work well in niche environments but are not ubiquitous. And if more consumers use these alternative platforms, overall market inefficiencies might arise because these platforms tend to be closed. Open platforms, wherein any payor and any payee can transact with each other, are critical to achieving overall efficiencies in a payment system as complex as that of the U.S.

Payments fraud management today

Various means are currently being used to manage payments fraud, and each has its own benefits and risks. For example, most merchants comply with the PCI DSS (Payment Card Industry Data Security Standard), which defines guidelines for merchants' handling and processing of payment card data.[9] However, compliance with PCI DSS does not guarantee total payments security; infamous data breaches have occurred when companies were nominally compliant with this industry standard.[10] Some industry players contend that because the major card network companies, such as Visa and MasterCard, determine how the standard is structured, it exists to protect the card network companies above and beyond other parties in the system. That said, it is arguable that while PCI DSS has its problems, there is currently no better alternative to take its place.

Encryption, which we touched on earlier, is also a vital means of mitigating payments fraud. Encryption converts cardholder data into an unintelligible form except to those with the relevant cryptographic key. Consumer- and transaction-level data can be encrypted at a variety of points; some in the industry are pushing for total encryption from the moment a transaction is initiated until it is finalized. While encryption is a valuable tool, there are no accepted standards for its use across the payment system. Another essential means of providing payments security is authentication, which is critical in non-face-to-face transactions. Firms use authentication to determine that the person making a transaction is who she says she is. For example, one can connect what an individual knows, such as a password or personal identification number (PIN), to something only an individual has, such as a payment card. Other forms of authentication include device identification and advanced analytics—which combines user identity, device identity, typical consumer behavior, and characteristic consumer–merchant interactions to identify fraudulent transactions. Of course, legitimate transactors can make illegitimate transactions, so authentication also has its limits.

Some industry leaders have argued that using dynamic authentication, i.e., security information that changes with each transaction, could provide even better protection than what is currently being used in the U.S. For instance, chip-based EMV (EuroPay, MasterCard, Visa) technology[11] provides dynamic authentication and has become the preferred payment technology outside the U.S.[12] Although adoption of this approach would improve security within the U.S. payment system, EMV is still susceptible to fraud. For example, PINs might be stolen or EMV terminals may be infected with malicious software, allowing transaction and PIN data to be used by criminals.

Finally, there are other security protocols that are not widely used in the U.S. today that might gain traction as the volume of remote payment transactions rises even further. Biometric security, which includes using fingerprint and retinal scans to authenticate consumers making transactions, can enhance protection against fraud. Voice and facial recognition and other similar technology are already commonly available on mobile devices; as they increase in popularity, we might see them being used for authentication purposes. One drawback of biometric security protocols is that consumers in the U.S. have been reluctant to use them because of privacy concerns.

Who pays for fraud?

Despite a plethora of strategies for attempting to prevent and manage payments fraud, two fundamental questions remain: Who is responsible for securing payment transactions? And how should the fraud costs be allocated and managed? From a public policy perspective, it is not necessarily useful to focus on a narrow cost–benefit analysis when examining the overall effects of payments fraud. In fact, if cost is the main driver of fraud solutions, efforts to improve fraud prevention and management could actually be seen as producing negative returns over the long term. Suppose, for instance, that sufficient investment is made so that fraudulent activity declines quickly. It might then be hard to justify continued large investments in such a system if fraud losses become and stay low.

As we mentioned before, it is currently difficult to gauge the overall costs of payments fraud—i.e., the infrastructure costs of fraud prevention and management; the actual losses to issuers, acquirers, and consumers; customer abandonment due to security concerns; and other intangible costs. One of the chief reasons that costs related to fraud are difficult to assess is that industry players have been hesitant to compete on the basis of fraud security, and therefore, few companies have publicly revealed information on their costs related to such matters. Many argue that exposing the relative risk within the industry has the potential to make the industry look insecure as a whole. Both merchants and banks may be particularly sensitive about the reputational risks associated with reporting fraud losses, and so they might see very little benefit to revealing to the public their tabulated costs due to data breaches and other fraud—especially given the intensely competitive landscapes for retailers and banks.

We can see that while payment platforms are rapidly evolving around the world, structural legacy issues are constraining the industry in managing fraud. Although significant investments have been made in shoring up security protocols of older systems, the industry has been slow to move to new, more comprehensive ways of addressing fraud. Data security improvements in payments have largely relied on using personal information to provide authentication. Unfortunately, personal information can be stolen and is also often used for marketing purposes, which can undermine relationships between consumers and financial institutions. To date, the industry has not made much progress in broadly implementing innovative fraud reduction strategies, such as dynamic authentication or biometric security, partly because many firms do not want to invest in new technology that they do not think will make a significant difference in fraud reduction relative to their investment.

Further, when it comes to preventing payments fraud, consumers have little “skin in the game.” Bundled account fees and zero liability policies mask the true costs of payments in general—and payments fraud in particular. If consumers fail to protect their PINs, for instance, such authentication measures lose their value. However, there was little consensus among symposium participants about how to incentivize consumers to behave more responsibly to minimize fraud. Some argue that it is unwise to focus on how much fraud is caused by consumer negligence or malfeasance. To quantify the costs due to such fraud, the industry would have to undertake the difficult task of gauging what portion of payments fraud was attributable to consumers rather than to security flaws in some other part of the complicated system. Unless specific incentives for good consumer behavior are developed or unless zero liability policies are eliminated, the industry might not be able to motivate consumers to change their behavior.

Governance and payments fraud

Clearly, there are no easy solutions to the complex problem of payments fraud. As stated before, there are a myriad of parties involved in any given retail payment transaction, and there is no central governing authority with broad jurisdiction over retail payments. Thus, business protocols developed by private companies can push payments in certain directions without much regard for how such moves affect the overall safety and efficiency of the payment system. For example, the business models of Visa and MasterCard have historically encouraged signature-based debit card transactions (over PIN-based ones) because they resulted in higher interchange fees for issuing banks.[13] Eventually, such transactions flourished, bringing with them increased fees for the card companies but also increased rates of fraud, since PIN-based transactions are generally more secure forms of payment.[14]

Because incentives related to cost and security are not perfectly aligned, public sector officials must carefully consider how new payments regulation will affect the payment system’s overall integrity and efficiency. Recent financial regulation reform prompted the Board of Governors of the Federal Reserve System to issue final rules about debit card interchange fees and routing.[15] This regulation attempted to lower the fee burden of electronic payments for merchants; credit card interchange fees were not addressed, however. Interchange fees for debit card transactions are now capped at $0.21 per swipe plus 0.05% of the face value amount of the transaction (compared with the previous average of $0.56 for signature-based debit and $0.23 for PIN-based debit transactions); banks may also now receive up to $0.01 extra per swipe if they comply with fraud prevention procedures. While the addition of incentives related to fraud prevention is positive, it is possible that the new pricing regime will alter incentives for merchants and banks to push certain types of debit

Charles L. Evans, *President*; Daniel G. Sullivan, *Executive Vice President and Director of Research*; Spencer Krane, *Senior Vice President and Economic Advisor*; David Marshall, *Senior Vice President, financial markets group*; Daniel Aaronson, *Vice President, microeconomic policy research*; Jonas D. M. Fisher, *Vice President, macroeconomic policy research*; Richard Heckinger, *Vice President, markets team*; Anna L. Paulson, *Vice President, finance team*; William A. Testa, *Vice President, regional programs, and Economics Editor*; Helen O’D. Koshy and Han Y. Choi, *Editors*; Rita Molloy and Julia Baker, *Production Editors*; Sheila A. Mangler, *Editorial Assistant.*

Chicago Fed Letter is published by the Economic Research Department of the Federal Reserve Bank of Chicago. The views expressed are the authors’ and do not necessarily reflect the views of the Federal Reserve Bank of Chicago or the Federal Reserve System.

ISSN 0895-0164

payments. If consumers are steered toward credit cards instead, other costs, such as those related to fraud losses, might rise, since credit card transactions are more vulnerable to fraud.

Without a central authority looking at all aspects of payments, new payments regulation is as likely to correctly address issues in some areas as it is to exacerbate problems in others. That said, some participants at the symposium argued that regulation may actually lead to innovation because some companies would be forced to come up with strategies to address the new rules that affect their business models.

A call for more standards

Participants at the symposium mostly agreed that more payments security standards would be helpful to combat remote payments fraud. It may well be constructive for industry players, with input from a public sector authority, to reach a consensus on a core set of standards to combat remote payments fraud. A centralized public sector organization might be able to effectively play an objective role in encouraging more robust antifraud measures without necessarily advantaging or disadvantaging certain participants. Moreover, such an organization could coordinate with other public sector players (such as bank regulators and law enforcement agencies) to collectively come up with effective solutions to cybersecurity problems. Some issues that might be addressed through payments security standards are:

- The level, nature, and number of authentication techniques employed;
- Best practices for encryption;
- Support from underlying device makers (e.g., hardware manufacturers) to improve the bases on which the secure networks can be built;
- Privacy issues, so that data used to combat fraud are not in turn used for marketing purposes;
- Appropriate time frames for addressing fraud when it occurs, and support of real-time fraud detection;
- Information-sharing on suspected fraud schemes;
- Exploration of the use of biometric security measures; and
- Best practices for increasing the interoperability of currently closed-loop, proprietary payment channels.

The diversity of those who make remote payments possible in the U.S. represents both a challenge and an opportunity. The challenge is to encourage highly diverse and competitive participants to cooperate on payments security. The opportunity is to utilize and integrate varying platforms and areas of expertise to achieve and maintain a more secure payment system that will operate efficiently over the long term. The Federal Reserve Bank of Chicago is committed to partnering with industry players to support such efforts.[16]

[1] An issuer is a bank that issues payment cards (credit, debit, and prepaid cards) to consumers; an acquirer is a bank that converts payment card receipts into bank deposits for merchants; and a switch is a gateway that routes payments communications between an issuer and acquirer.

[2] See www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/.

[3] See p. 6 of www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.

[4] Corporate account takeover is a form of corporate identity theft in which a business's online credentials are stolen by malicious software, enabling criminals to initiate fraudulent banking activity.

[5] Ira Apfel, 2011, "ACH and wire fraud cost corporates $85 million, FBI says," *AFPonline.org*, September 21, available at www.afponline.org/Article_Detail.aspx?id=24352. For more information on corporate payments fraud, see Association for Financial Professionals, 2011, "*2011 AFP Payments Fraud and Control Survey:* Report of survey results," Bethesda, MD, March, available at www.afponline.org/paymentsfraud/.

[6] See Stephen Castle, 2011, "Crime gangs in Europe are profiting from web," *New York Times*, May 4, available at www.nytimes.com/2011/05/05/world/europe/05iht-europol05.html; and Europol, 2011, "Major international network of payment card fraudsters dismantled," press release, July 12, The Hague, Netherlands, available at https://www.europol.europa.eu/content/press/major-international-network-payment-card-fraudsters-dismantled-1001. Note that these examples concern all cybercrime and are not only focused on payments fraud.

[7] SSL encryption relies on digital certificates, which are public keys issued by an authority entrusted with establishing organizations' credentials (e.g., Symantec Corporation's VeriSign).

[8] The merchant generally bears the direct cost of remote payments fraud. The exception is for card-not-present transactions made with authentication programs such as the Verified by Visa program and the MasterCard SecureCode program. See Duncan B. Douglass, 2009, "An examination of the fraud liability shift in consumer card-based payment systems," *Economic Perspectives*, Federal Reserve Bank of Chicago, Vol. 33, First Quarter, pp. 43–49, available at www.chicagofed.org/digital_assets/publications/economic_perspectives/2009/ep_1qtr2009_part7_douglass.pdf.

[9] According to Visa, approximately 97% of its level 1 merchants, 96% of its level 2 merchants, and 60% of its level 3 merchants are compliant with PCI standards. See Evan Schuman, 2011, "Level 3 merchants hit PCI compliance at 60 percent, Visa confirms numbers for the first time," *StorefrontBacktalk*, August 3, available at http://storefrontbacktalk.com/securityfraud/level-3-merchants-hit-pci-compliance-at-60-percent-visa-confirms-numbers-for-the-first-time/.

[10] See Thomas Claburn, 2009, "Heartland Payment Systems hit by data security breach," *InformationWeek*, January 20, available at www.informationweek.com/news/security/attacks/212901505.

[11] EMV is a global standard for credit and debit payment cards based on chip card technology. It is important to note that Visa has issued incentives for merchants accepting its brands to become compliant with EMV standards and NFC (near field communication) standards (which enable contactless point-of-sale transactions using mobile devices) by 2015; wider merchant compliance could lead to much faster adoption of EMV and NFC technologies.

[12] The U.S. still tends to rely on magnetic stripe payment card technology.

[13] Interchange fees are per debit or credit transaction fees paid by the acquiring bank to the issuing bank; these fees are typically passed on to the merchant by its bank (see note 1).

[14] One might contrast this system with the Canadian payment system, in which all debit card transactions are PIN based and operate on a network separate from credit card transactions.

[15] See www.gpo.gov/fdsys/pkg/FR-2011-07-20/pdf/2011-16860.pdf.

[16] The SRPc is conducting a pilot study to demonstrate the effectiveness of authentication techniques and to measure consumer behavior related to those techniques; see www.secureremotepaymentcouncil.org.