Cybersecuring PAYMENTS

Are we losing the fight against next-gen bank robbers?

BY TIM SABLIK

It isn't the kind of holiday news retailers want to deliver. On Dec. 19, 2013, Target announced that its payment terminals and computer systems had been hacked, allowing criminals to access credit and debit card data for as many as 40 million shoppers during the busy Black Friday weekend. The hackers also stole personal information for 70 million customers. In January, department store Neiman Marcus said that payment card information for its customers had been compromised, and arts and crafts chain Michaels said it was looking into a possible breach.

Breaches of payment systems at large retailers are not new. In 2007, hackers stole 45 million customer records from TJX Companies, the parent of T.J. Maxx. To date, such events have not changed the habits of most consumers: In the United States, plastic is king. Cards accounted for two-thirds

PHOTOGRAPHY: ANTHONY BRADSHAW/GETTY IMAGES

Worldwide EMV Payment Card and Terminal Adoption

Region	EMV Cards (millions)	Adoption Rates	EMV Terminals (millions)	Adoption Rates
Canada, Latin America, and the Carribbean	471	54.2%	7.1	84.7%
Asia Pacific	942	17.4%	15.6	71.7%
Africa and the Middle East	77	38.9%	0.7	86.3%
Western Europe	794	81.6%	12.2	99.9%
Eastern Europe	84	24.4%	1.4	91.2%

NOTES: Figures as of Q4 2013. EMVCo does not collect data on the United States, but estimates by other organizations suggest that adoption rates are very small (less than 2% of cards and 10% of terminals).
EMV is an open-standard specification for smart cards and acceptance devices. It is managed by EMVCo, which is owned by American Express, Discover, JCB, MasterCard, UnionPay, and Visa.
SOURCE: EMVCo

of noncash payments in 2012, increasingly displacing cash, checks, and other forms of payment, according to a 2013 Fed study of the payments system. But with convenience comes risk. The Fed's study found that payment cards were used in 92 percent of fraudulent transactions, with checks and electronic check transfers making up the remainder.

Cyberattacks have been growing in magnitude. While the number of reported data breaches (including both attacks on payment systems and other attacks) trended down to 2,164 in 2013 from 3,140 the previous year, hackers made off with over three times as many records: 823 million compared with 264 million.

According to a 2013 survey by Verizon, the most commonly targeted sectors were financial institutions and retailers, and payment card information was by far the most stolen type of data. That may not be surprising, given that one of the primary motivations for breaches identified by the Verizon report is financial gain. But an equal percentage of attacks were classified as "opportunistic," which raises the question: Is the payments system an easy target?

During a series of congressional hearings following the Target breach, legislators pointed to the prevalence of chip-and-PIN technology in other developed economies (known as "EMV" for developers Europay, MasterCard, and Visa). These so-called "smart" cards use an embedded microchip to process payments, allowing for more secure authentication that makes intercepted data from any one transaction largely useless to fraudsters. American cards still rely on magnetic stripes, the same technology that powers cassette tapes, to relay static payment data that can be intercepted and copied onto blank cards for fraudulent use. Many have argued that the old cards are well past their prime.

The major card brands — Visa, MasterCard, and Discover — announced their intent to hold merchants who have not upgraded to EMV by October 2015 responsible for fraud that could have been prevented by a smart card. Target plans to be an early adopter, beating the deadline by several months. But EMV is not entirely new — the technology debuted two decades ago. In fact, Target introduced smart cards at its stores in the early 2000s but abandoned the effort after a year, citing costs and consumer complaints that the new cards complicated checkout. The United States was a pioneer of payment cards but has been much slower to adopt smart cards. According to Javelin Strategy and Research, only 10 percent of payment terminals and less than 2 percent of cards in the United States are EMV compatible, compared with much higher numbers worldwide (see table). Has America fallen behind the times, and if so, why?

Costs and Benefits

Perhaps the highest hurdle to converting the payment network is the upfront cost. With roughly 15 million payment terminals, the U.S. retail market is the largest in the world, and estimates for converting all those terminals range from $7 billion to more than $15 billion.

"We were early adopters of credit cards, so we have a very large legacy infrastructure based on swipe card technology," says Catherine Mann, a professor of global finance at Brandeis University.

Depending on the losses they avert, the cost of upgrading all those terminals could pale in comparison to the benefits. In their 2005 book *Managing Cybersecurity Resources,* University of Maryland professors Lawrence Gordon and Martin Loeb concluded that it is generally uneconomical for firms to spend more than 37 percent of expected losses on security measures. Thus, determining the return on any security upgrade requires some knowledge of fraud costs.

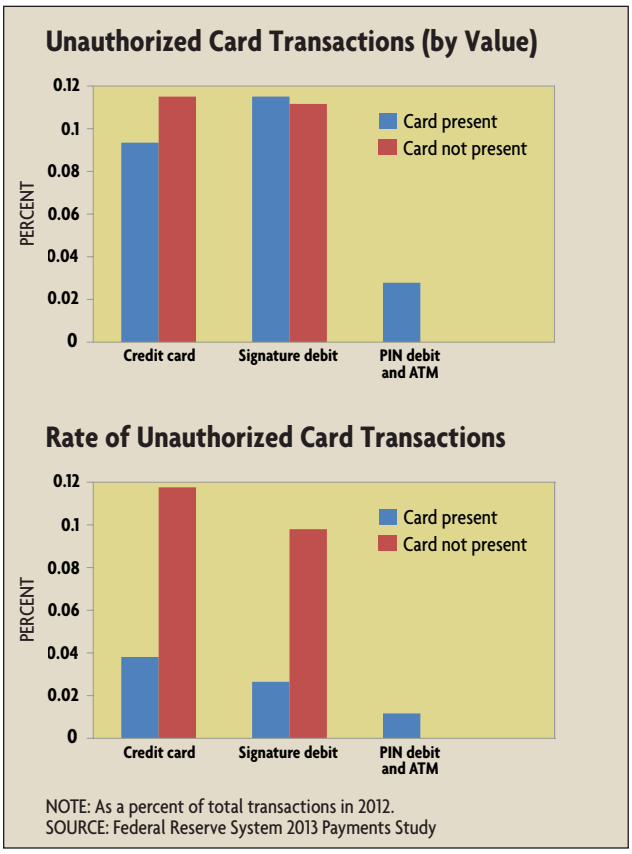
"That is a hard thing to figure out," says Richard Sullivan, a senior economist in the payments system group at the Kansas City Fed. "The thing that really holds us back is that we don't have good fraud statistics."

Unlike many other countries, the United States does not have a central source for fraud statistics. But data is improving. The Federal Reserve System reported payment fraud statistics for the first time in its 2013 payments study. According to that report, there were 28.7 million fraudulent payment card transactions in 2012, or about 0.04 percent of all card transactions. Losses from card fraud totaled

$4 billion, about 0.08 percent of total card transaction value. The August 2013 *Nilson Report*, a payments industry newsletter, documented somewhat higher card fraud costs for 2012, putting the total losses from credit and debit card fraud at $11.27 billion.

On a percentage basis, those numbers seem small, but in addition to the explicit costs of stolen funds, there are the implicit costs of damaged reputation and lost revenue for impacted firms. In a 2003 study, Gordon and Loeb found that stock prices declined an average of 5 percent for firms that announced data breaches. Target reported $61 million in expenses related to the breach, and its stock price remained 5 percent below the pre-breach level more than two months after the event.

Smart cards could reduce such costs, but it is unclear by how much. After the United Kingdom adopted EMV, payment fraud costs fell by 15 percent between 2004 and 2006. That decline was driven in large part by declines in fraud from lost, stolen, and counterfeit cards. But during the same period, fraud in card transactions that took place outside of physical points of sale, such as online transactions, grew by 41 percent. Smart cards increase security for point-of-sale transactions, but they don't provide additional protection for online sales, and fraudsters quickly migrated to the weakest link. The Fed study points to such card-not-present fraud already being a much bigger problem than point-of-sale (see charts). While point-of-sale still makes up the vast majority of transactions, online is growing, and consumers in the United States are more likely to shop online than their European counterparts.



NOTE: As a percent of total transactions in 2012.
SOURCE: Federal Reserve System 2013 Payments Study

EMV is not entirely safe at the point of sale, either. "It's not clear whether delivering EMV in its current form is a significant enough improvement to justify the huge expense of adopting it in the United States," says Tyler Moore, a professor of computer science and engineering at Southern Methodist University who has written about the economics of cybersecurity. He says that since its initial development 20 years ago, EMV has proven to be far less ironclad than many had hoped.

It's also possible that other countries had more to gain from smart cards. Sullivan notes that European countries have largely offline payment networks, while the U.S. card system was designed to be online, giving card networks the ability to remotely review and authenticate any transaction as it is being conducted. Smart cards allow for authentication to take place between the card and the terminal itself, granting greater security for countries without online payment networks, and it's not clear whether the marginal advantages for an online network would be as great.

"I think that part of the reason we are among the last countries to move to chip and PIN is that the online system already has features that help to control fraud that other countries haven't had," says Sullivan. But even if chip cards are not the ideal solution, most agree that the current system is due for some sort of upgrade.

According to the *Nilson Report*, the United States accounted for 47 percent of global card fraud losses in 2012, even though it made up only about 24 percent of global card volume.

"Because so much of the world has shifted to chip and PIN, hackers see the U.S. cards as weaker links because they are much easier to copy," says Moore. "It has made the U.S. a target."

Why, then, have we been slow to upgrade our defenses?

The Blame Game

In a 2001 paper, Ross Anderson, a security engineering professor at the University of Cambridge who launched the economic study of cybersecurity, wrote that lapses in security can be expected when "the party who is in a position to protect a system is not the party who would suffer the results of security failure."

Who bears the costs of payment card fraud in the United States? Certainly consumers bear some. They must protect their personal information, replace compromised cards, and monitor suspicious activity on their accounts. But on the whole, American consumers are relatively well protected. Regulations E and Z limit consumer liability for fraudulent credit and debit transactions to $50, but in practice this is reduced to zero, as financial institutions generally make consumers whole. This could potentially lead to consumer negligence by reducing the incentive consumers have to be vigilant. But not everyone agrees the onus for fraud prevention should lie with consumers.

"It's very difficult for consumers to observe the security levels of the businesses they interact with," says Moore. "Because they cannot make decisions based on the security of the company, there's not a lot they can do to really protect themselves." As a result, it makes more sense for financial institutions and merchants, which have greater control over security, to bear liability. Moore's research supports this theory. In a paper documenting how liability for payment card fraud in the United Kingdom shifted to consumers after the introduction of EMV, he found that banks there spent much more on security and also suffered greater fraud than their American counterparts.

> "There's always a tension between standardizing around something that's known versus allowing multiple different solutions to flourish."
>
> *– Catherine Mann*
> *Brandeis University*

But banks and merchants disagree over who should bear the larger burden for fraud. According to the August 2013 *Nilson Report*, fraud costs in the United States are split between card-issuing financial institutions and merchants 63 percent to 37 percent. To the extent that card issuers control the network, it might seem appropriate that they shoulder most of the risk. But banks argue that costs are misaligned because the banking sector suffers far fewer breaches than retailers. According to data collected by the Open Security Foundation, businesses and retailers were subject to more than a quarter of security breaches worldwide in 2013, while financial organizations accounted for about 5 percent.

"There are clearly misaligned incentives," says Doug Johnson, vice president of risk management policy at the American Bankers Association. "When you have an organization on the retail side that is responsible for a lot more of the breaches but less than half of the costs of those breaches, they are going to have different incentives for security than financial service companies."

But retailers respond that, like consumers, they have little control over payment card security. Mallory Duncan, general counsel and senior vice president at the National Retail Federation, says security measures are determined by the card networks, and retailers are forced to accept vulnerable cards from the major networks because they have no alternatives.

"Most of the decisions are made within the financial services sector," says Duncan.

The disagreement over how to allocate cybersecurity responsibilities mirrors challenges economists have identified with public goods. Because security expenditures by one party can benefit others who didn't pay for them, the allocation of responsibilities to protect payments is complicated. In a 2005 paper, George Mason University professor of law Bruce Kobayashi wrote that while resources aimed at identifying and punishing cybercriminals might be more effective at improving society's overall security, such efforts are likely to be under-produced. This is because firms that invest in such security cannot exclusively capture all of the benefits; that is, there are "positive externalities" to such investments. Because of this, some firms might attempt to free ride on the security expenditures of others, reaping the benefits without paying any of the costs. Foreseeing this problem, individual firms are more likely to invest in security measures that protect themselves (such as antivirus software or firewalls) and deflect attacks to firms that have not made such investments.

At the same time, the costs from inadequate security do not fall wholly on the firm making investment decisions; that is, a lack of investment in security imposes "negative externalities" on other firms. In this sense, cybersecurity can be likened to pollution. If you operate a factory that emits pollutants into the air, the people who live downwind from you might be the ones who bear the cost of that pollution rather than you. Similarly, individuals or firms who choose not to invest in strong security and connect infected computers to the Internet pass the costs of those decisions onto other users. As a result, overall payments security against cyberattacks may be determined not by collective effort but by the weakest links.

Indeed, security blogger Brian Krebs, who first broke the news of the Target breach, reported in February that the malware used to infect Target's system was introduced through a third-party HVAC company. Large firms like Target may have the budget to fund extensive security, but they are still at risk due to smaller firms that either cannot afford adequate security or choose to free ride on the investments of others. To the extent that overall cybersecurity is determined by the weakest link, coordinated action may be crucial to improvement.

"It's kind of like getting the entire herd to move in one direction, and that can be difficult," says Mann.

Moving the Herd

The Target breach could provide the push for coordinated improvement of payments. Mann says that unlike in previous breaches, the reputational and stock market damage to Target has been large and persistent, perhaps placing greater pressure on retailers to upgrade their own systems or risk being next. The effect on the bank side has been significant as well, costing them about $200 million to reissue compromised cards.

"I think the needle has been moved," says Johnson. "I'm more hopeful now than I would have been a month ago because of the recognition by leadership on both the retail and financial services sides that we need to work together to solve a common problem."

In March, Visa and MasterCard announced a new cross-industry group to explore security improvements across networks. Setting standards could also help encourage collective action. The Payment Card Industry (PCI) Security Standards Council develops security guidelines

for merchants, and in February, the National Institute of Standards and Technology released a framework for national cybersecurity standards in response to an executive order issued by President Obama last year.

But while financial regulators monitor and enforce risk standards on the bank side, no such enforcement exists for merchants. Standards developed by PCI are voluntary, and the organization has no authority to monitor or enforce compliance. Even when firms do comply, standards may fail to predict or adapt to ever-changing threats. In testimony, Target's chief financial officer said the company was compliant with PCI standards up until its breach.

Lack of enforced standards may not be entirely negative, though. "Sometimes creating a standard around which everyone can coalesce leads to greater efficiency," says Mann. "But there's always a tension between standardizing around something that's known versus allowing multiple different solutions to flourish."

Indeed, standards meant to improve payments can slow adoption of new technology. The Durbin Amendment to the Dodd-Frank Act requires that merchants be given a choice between at least two PIN networks for transactions in order to improve competition. But because EMV was designed to work with only one PIN network, such a requirement has created a speed bump for chip and PIN in the United States. This may prove to be a blessing in disguise. Countries with fewer payment participants were able to quickly adopt EMV, but it's not clear that this has led to the long-run improvements they hoped for.

"We know from its deployment elsewhere that chip and PIN has quite a few limitations and demonstrated weaknesses," says Moore. "If we're going to spend billions of dollars on upgrading, we want to be developing a standard that's better than what's out there. For now, the United States has been the easiest target, but if everyone increases their security to a common level, EMV's known vulnerabilities will suddenly become economically viable."

Duncan notes that given enough competition in the payments space, the market can often find new security solutions. Merchants have begun exploring mobile payments using smartphones, banding together to design their own mobile payment network. (See "A Wallet in Every Phone," *Region Focus,* Fourth Quarter 2012.) Many banks already employ behavioral analytics to monitor customer transactions and alert them to any purchases that don't fit their spending profile. Some have also started exploring biometrics, such as fingerprint or voice authentication, to replace passwords and PINs. Ultimately, economists and industry insiders agree on one thing: Keeping ahead of the criminals requires collaboration.

"All the interested parties, representing consumers, merchants, card issuers, and networks, need to be talking to one another when making decisions," says Sullivan. "And they need to do it early." **EF**

Readings

Gordon, Lawrence A., and Martin P. Loeb. *Managing Cybersecurity Resources: A Cost-Benefit Analysis.* New York: McGraw-Hill, 2005.

Kobayashi, Bruce H. "An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods." George Mason University Law and Economics Working Paper No. 05-11, 2005.

Mann, Catherine L. "Information Lost." National Bureau of Economic Research Working Paper No. 19526, October 2013.

Moore, Tyler, Richard Clayton, and Ross Anderson. "The Economics of Online Crime." *Journal of Economic Perspectives*, Summer 2009, vol. 23, no. 3, pp. 3-20.

Sullivan, Richard J. "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options." Federal Reserve Bank of Kansas City *Economic Review*, Second Quarter 2010, pp. 101-133.