





PROTECTING IDENTITIES

IMPROVING SECURITY WITHIN THE PAYMENT SYSTEM

High-profile payments data breaches are on the rise and have cost companies and consumers millions of dollars annually. Most recently, hackers stole 56 million payment cards from Home Depot's database after gaining access to the company's network. In 2013, Target Corp. disclosed that its data breach affected 40 million credit and debit card accounts.

Federal Reserve Bank of Kansas City Economist Richard J. Sullivan says the direct cost of fraud on automated clearinghouse (ACH), debit card, and credit card payments reached \$6.1 billion in 2012. And investments and ongoing expenses for preventing, detecting, monitoring, and responding to payment fraud added considerably to direct costs.

A 2014 Identity Fraud Study by Javelin Strategy and Research reported that although the amount of records criminals stole reached into the hundreds of millions, the number of victims who reported fraudulent activity on their accounts was 13.1 million.

Sullivan says the number of records exposed fluctuates from year to year and shows no trend.

"The year 2013 stands out as particularly

bad: breaches exposed 547 million records, nearly matching the cumulative 603 million records exposed from 2008 to 2012."

Megabreaches—those exposing 10 million or more records—occur infrequently, yet contribute to the large share of total records exposed. From 2008 to 2013, megabreaches accounted for only 17 of the 5,437 publicly disclosed data breaches, but together exposed 979 million records, 85 percent of all records exposed.

Data breaches

Hackers stole a third-party vendor's user name and password to enter Home Depot's network in 2014. According to a company statement, the stolen credentials allowed hackers direct access to Home Depot's point-of-sale devices. The criminals then acquired more rights to the system and installed custom-built malware on Home Depot's self-checkout systems in Canada and the United States. The company's security software was unable to detect the malware because hackers tailored it to the system.

In addition to the 56 million stolen payment cards, hackers downloaded separate

files containing approximately 53 million email addresses, though the files contained no payments data or customers' personal information.

The Home Depot incident was the largest disclosed retail data breach in U.S. history and built upon high-profile breaches in 2013.

Target's data breach during the Thanksgiving holiday in 2013 put 40 million credit and debit card accounts into the hands of hackers. That same year, Adobe was attacked, exposing thousands of user IDs, passwords and credit card information.

Other notable cyber-attacks included: Schnucks grocery store chain of St. Louis—2.4 million payment cards stolen;

JP Morgan Chase & Co. in New York: 500,000 corporate and government clients who held prepaid cards issued by JP Morgan were stolen.

In his recent research, "Controlling Security Risk and Fraud in Payment Systems," Sullivan says, "Fraudsters use exposed sensitive data in a decentralized, worldwide production process translating stolen data into fraudulent payments."

Instead of making direct or in-person purchases with the stolen information, criminals increasingly turn to eBay, PayPal and Amazon to make purchases.

Although direct losses in the United States from all methods of payment fraud do not show adverse trends, the number of data breaches has had an upward trend since 2009 and has put many consumers at risk.

The individual costs

Not all security breaches are large or concentrate on the payments system. Criminals' aspirations are the same, however. They hope to use personal data for monetary gain.

Criminals go after personal information through a variety of sources, such as a store clerk copying a customer's payment information or an office assistant selling files containing individuals' Social Security numbers. It could be as simple as someone phishing online or going through discarded mail.

But once a person's identity or payment information has been compromised, it's difficult to rectify the problems it causes.

A few years ago, Angela Stallings received



PHOTO BY GARY BARBER

ANGELA STALLINGS, who works at Kansas City CARE Clinic, a healthcare clinic serving the uninsured and underinsured of the Kansas City metro area has dealt with the ramifications of identity theft for almost a decade. Someone gained access to Stallings' personal information and has used it to commit fraud, including taking out college loans in Stallings' name and gaining employment under a false identity.

bills for college loan debt.

“It was for a college in St. Louis,” she said. “I’ve lived in Kansas City my entire life; I’ve never left Kansas City or gone to a college in St. Louis.”

She sent the statements back with an explanation that they had the wrong person, but the requests for payment kept coming. She contacted the administrator of the college loans and sent paperwork that included a brief explanation, her government identification and personal information.

The problem stopped for a couple years, but resurfaced when an agency tried to collect the debt. Stallings had hired a lawyer to help her clean up her credit and hoped to solve the issue.

Recently, however, an agency called Stallings’ employer to verify her work history. The woman who had used Stallings’ personal information for the college loans was now using it again for various activities, such as employment.

“I’ve never met the woman and have no idea how she got my information,” Stallings said. “She has the same first name, but a different last name, but she’s still able to use my information.”

Stallings, like many victims, is frustrated with the system. She has to prove she’s not responsible for the other woman’s debt and activities. She’s also responsible for the associated costs, such as lawyer fees.

There are several steps fraud victims can take to avoid further damage and address the problem (See sidebar: “What to do if you’re the victim of a data breach”). Sometimes the solution is simple, others times it’s a lengthy, complex process.

And when one considers the amount of information criminals glean in large data breaches, the opportunity to exploit more victims is staggering.

Securing the system

The payments system’s complexity, both within and across all payment types, makes the solutions to address the variety of vulnerabilities and inadequate approaches to security complex as well. Reducing fraud will take efforts on

WHAT TO DO IF YOU’RE THE VICTIM OF A DATA BREACH

Although private information may seem private, some information is public domain.

Names and street addresses are public information

Email addresses are sensitive because many emails are attached to account user identification

Account passwords are more sensitive

Social Security numbers and credit-card numbers have high priority

HERE’S WHAT TO DO IF YOU’RE THE VICTIM OF A DATA BREACH:

Find out what type of breach occurred.

Depending on the breach and the state in which you live, you may receive a breach notification letter that describes what happened, or you may find out about a breach through media reports.

Find out what kind of information was stolen.

Was it credit, debit, passwords or email addresses? This will help you know what steps to take to avoid further damage. Remember, hackers can crack even the most encrypted data and use bits and pieces of information to build profiles. All breaches of security, whether emails or credit cards, are important.

Beware of phishing scams: Even if criminals only stole email addresses, they often use the information they gain on a person to trick him or her into giving them more information.

Change the password on your account immediately.

Don’t use the same password for all of your accounts. If you do, change all your passwords.

Create strong passwords, more than eight letters with numbers and symbols. Do not use a word or words found in the dictionary.

Ask your bank and your credit-card issuers to alert you immediately if they detect suspicious activity on your accounts.

Ask consumer credit-reporting bureaus to place a fraud alert on your name. This way, if anyone tries to steal your financial identity, you’ll know.

Look into credit-protection services that will flag suspicious activity on your accounts.

Losing your personally identifiable information in a data breach doesn’t guarantee you’ll become a victim of identity theft. But if that does indeed happen, make sure to tell the credit-reporting bureaus right away.

If you detect credit- or debit-card fraud, contact the card issuer immediately. Doing so may limit your liability.

Contact the Federal Trade Commission to create an identity-theft affidavit, and then file a report with the local police force. Doing both will aid you in clearing your name, which, in the worst cases, can take years. Make sure you document each phone call made, and each email message and letter sent, during your efforts.

Information sources: Privacy Rights Clearinghouse and Tech and Gadgets (NBC)

both public and private fronts. Where to place security improvement efforts, many of which are under way, is a challenge.

“Given the poor recent record on data breaches, protecting sensitive data is a high priority in the short term, made even more urgent by evidence that consumers lose confidence in some payment types after a data breach,” Sullivan said.

Medium-term priorities focus on spurring progress on existing efforts in the industry to bolster network and payment security, Sullivan added. In the long term, more fundamental changes can help ensure the payment system is resilient and can adapt to the changing security environment.

In the near term, hackers will continue attacks aimed at acquiring data useful to payment fraud.

Public and private institutions have evolved

payment cards to minimize the risks should a data breach occur.

Europe began its migration to embedded microchip cards, or smart cards, for credit, debit and ATM in 2002, when EuroPay, MasterCard and Visa collaborated on EMV (EuroPay, MasterCard, Visa), the leading global standard for chip technology. The United Kingdom, Japan, Mexico, Canada and 80 other countries then spent the next decade transitioning to EMV-based cards.

The main barrier to implementation of smart cards in the United States is the cost associated with changing retail point-of-sale card readers and network systems. Today, less than 1 percent of the cards issued in the United States use embedded microchip technology, although supporters say it cuts down on fraud significantly because it uses dynamic authentication.

“... IMPLEMENTATION OF SMART CARDS COULD SIGNIFICANTLY REDUCE FRAUD AND EVEN REDUCE VULNERABILITIES WHEN DATA BREACHES OCCUR.”

a “control structure” to ensure payment security and deter fraud, Sullivan said. The control structure typically has four elements: network organization and governance, payment network rules, security techniques and protocols, and supervision and enforcement.

The elements control access to the network; coordinate payment security; set operational rules that embed security features; determine responsibility for security, including liability for fraud losses; determine and design appropriate security techniques and protocols; define and oversee adherence to security standards; and apply sanctions for noncompliance.

For example, Home Depot’s breach occurred when a third-party vendor employee’s credentials were stolen, compromising access security to the company’s payments network.

Because of recent breaches, several American retailers have concentrated on security techniques and protocols, and recently sped up the implementation of secure smart

In the dynamic authentication process, verification information on a microchip is encrypted and each transaction is assigned a unique code—no transaction code is ever the same. This code-generating process, industry supporters say, significantly reduces or even prevents thieves from copying and reusing payment verification information. And only the customer knows the PIN.

With the standard magnetic-stripe card, verification information is static, meaning it doesn’t change with each transaction. Also, most card readers are stationary and require a customer’s signature, enabling thieves to wirelessly skim transaction verification information, meaning even the most cautious cardholders, those using ATM cards with PINs, could have their information stolen.

Hackers breached Target’s network by scanning transactions at its point-of-sale card reader.

In response, Target announced it would

issue its branded credit and debit cards as MasterCard smart cards. Target's decision to replace thousands of store registers with ones that accept smart cards pressured other retailers to take action.

Wal-Mart Stores Inc.'s Sam's Club introduced its microchip-embedded card in June 2014. All Sam's Club locations now feature chip-enabled terminals, and the company plans to roll out the technology to all Wal-Mart locations by 2015.

Industry analysts say the implementation of smart cards could significantly reduce fraud and even reduce vulnerabilities when data breaches occur.

Most payment fraud breaches and theft, however, occur through out-of-sight transactions. For example: A customer at a restaurant gives the server a card, which is taken to a stationary reader out of the customer's sight. The employee can copy the card number or use a reading device to capture all the information on the magnetic stripe.

New payments technology has advanced to combat this type of fraud online. As European countries improved their payment systems, authorities encouraged merchants to use 3D secure payments, which require a cardholder to register a payment card with the issuer and create a PIN for Internet purchases.

The cards and systems aren't foolproof; however, it has cut fraud significantly in countries using the devices.

Taking risks

U.S. cardholders used more than 1 billion debit and credit cards in 2011, making 69 billion transactions valued at more than \$3.9 trillion. These payments accounted for about 50 percent of all noncash retail payments in the United States.

Although the incidents of payment card fraud in the United States is small relative to the number of daily noncash transactions, the immense volume of payment transactions adds up to big losses due to fraud.

In 2012, the estimated number of unauthorized transactions (third-party fraud) was 31.1 million, with a value of \$6.1 billion, according to "The 2013 Federal Reserve System Payments Study."

Companies not only face the loss of money and reputation with data breaches, they are vulnerable to legal actions if they do not make improvements. Consumers also lose confidence in certain payment methods as a result of data breaches.

Sullivan says that because of the modern payment system's complexity, policymakers and industry leaders need a broad perspective to judge weaknesses in the control structure over payment security and the control structure's ability to adapt as new fraud methods arrive.

"A long-term perspective is especially important because fraudsters' incentives to exploit security weaknesses will not disappear," he said. "Critical contributions to the control of payment fraud will continue to come from private security services. Improvement could also come from contributions that take a payment system-wide approach, such as a group coordinating diverse payment participants, promoting cooperation, and finding effective solutions to weak payment security."



KEVIN WRIGHT, EDITOR

FURTHER RESOURCES

"Controlling Security Risk and Fraud in the Payment Systems," By Richard J. Sullivan

www.KansasCityFed.org/publicat/econrev/pdf/14q3Sullivan.pdf

COMMENTS/QUESTIONS are welcome and should be sent to teneditors@kc.frb.org.