Opportunity Knocks: How Card Issuers Can Address Consumer Concerns Around Payment Security

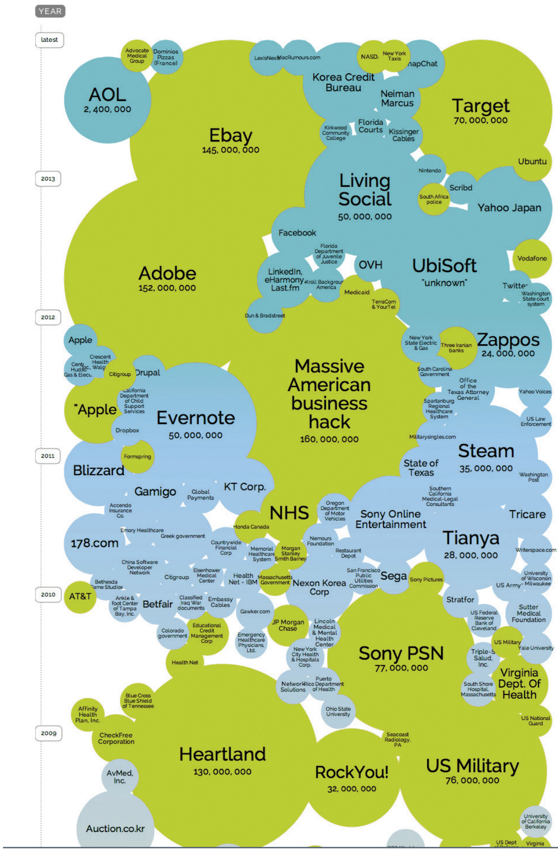
By Jonathan D. Hancock

> *"It's not a question of if — but when — your organization will experience a serious security breach. Cybercriminals are using more sophisticated and targeted attacks to steal everything from valuable intellectual property to the sensitive personal and financial information of your customers, partners, and employees. With enough time and money, they can breach the security defenses of even the largest enterprises."*[1]
>
> *– Forrester Research*

EXECUTIVE SUMMARY:

Data breaches have become an unfortunate reality in today's business world, and the number appears to be rising at a rapid pace. Verizon's 2014 Data Breach Investigations Report identified 64,337 security incidents and 1,367 data breaches in 2013 — up 37 percent and 120 percent respectively from 2012.[2] Data thieves frequently target payment card data because it gives them access to money, whilst at the same time providing key personal identification information, such as cardholders' addresses and Social Security numbers, that can be used to commit other crimes. The Verizon study notes that "payment card data remains one of the easiest types of data to convert to cash, and therefore is the preferred choice of criminals."[2]

World's Biggest Data Breaches



Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Several recent headlines have raised awareness of the great risks — and significant potential financial and reputational costs — of data breaches for businesses. In May 2014, online commerce giant eBay notified its 145 million members that cyber-attackers had infiltrated its database containing customer passwords, email addresses and other personal data. The breach has raised questions among some government regulators about whether the company moved fast enough to uncover the breach and alert its users. It is certainly too early to know the actual repercussions.

eBay's situation is among several recent high-profile cybersecurity incidents, including a payment card data breach experienced by Target in late 2013. However, history shows that many types and sizes of organizations, including small businesses and financial institutions, are at high risk. Heartland Payment Systems, a payment processor, had 130 million credit card accounts exposed to thieves in 2009, which cost banks and insurers more than $200 million. Ingenicard U.S. racked up losses of $9 million in fraudulent automatic teller machine (ATM) withdrawals in a 24-hour period in 2012.[3] For a more comprehensive list of breaches, see the "Worlds Biggest Data Breaches" found at http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

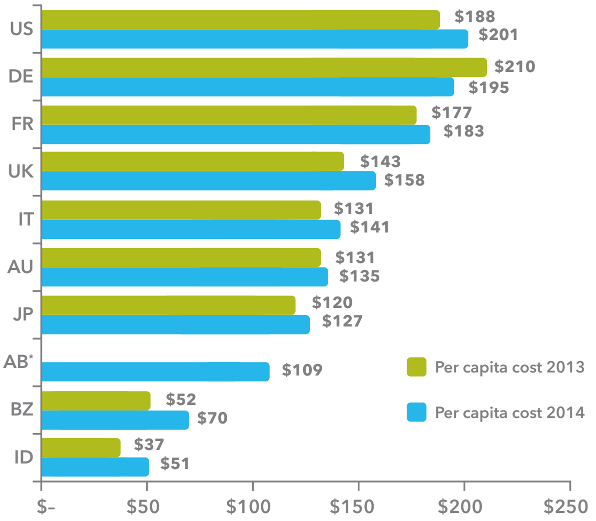
The many types and increasing number of data breaches faced by businesses illustrate why companies large and small must not take data security lightly. This report looks at consumers' changing sentiments and their growing wariness about the security of their data by highlighting the results of the 2014 *TSYS Consumer Awareness Data Security Study.*[4] This report explores key ways financial institutions can more effectively manage potential risks, including getting customers more involved in protecting their data and financial accounts and building a stronger, more secure payments ecosystem. Lastly, it provides recommendations for how issuers can better manage the increases in merchant breaches by preparing a disaster-recovery plan as they would for other crises. Building a robust strategy for both educating cardholders and merchants on how they can reduce the risk of account breaches — but also preparing for breaches when they do happen — can give an issuer a competitive edge.

What is a data breach?

Data breaches come in many forms, but essentially they occur when an unauthorized person or party accesses and obtains information. It may be someone intercepting the transmission of a file containing encrypted data, hacking a database, or compromising a lost laptop containing customer information. Thieves seek different types of data, depending on their objectives and technical proficiency. eBay's breach, for example, affected a database containing up to 145 million customer names, encrypted passwords, email addresses, physical addresses, phone numbers and dates of birth.[5]

Figure 2

The average per capita cost of data breach over two years – Measured in US$



*Data not available for FY 2013

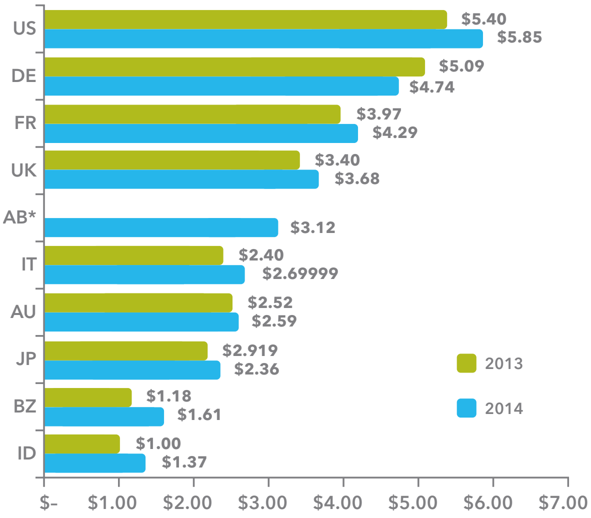
Source: Ponemon Institute, LLC. "Cost of Data Breach Study: Global Analysis."

The nature and breadth of a data breach affects the degree of financial and reputational risk, and one breach may affect anywhere from one individual to millions of people. Issuers must consider some key factors when designing their breach remediation efforts: the number of people or data records affected by the breach, how the data was exposed (accidentally or maliciously), and the type of information obtained — whether account-level information such as account numbers and online passwords, or personal information, such as Social Security numbers and dates of birth.[6]

Figure 3

The average total organizational cost of data breach over two years

Measured in US$ ($000,000 omitted)



*Data not available for FY 2013

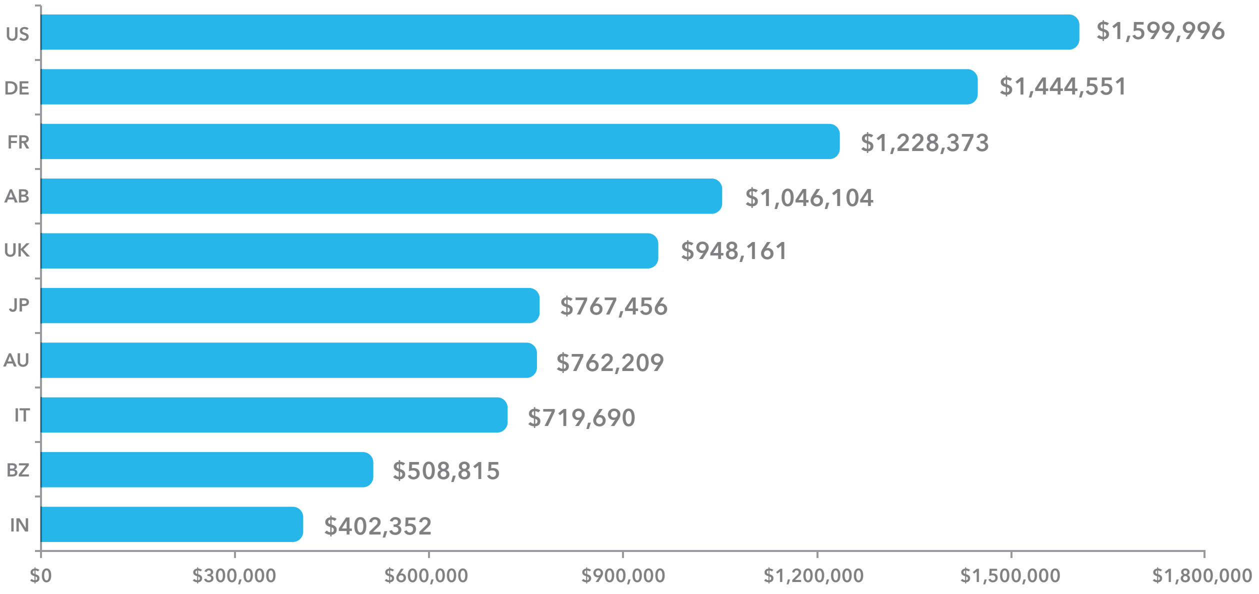
Source: Ponemon Institute, LLC. "Cost of Data Breach Study: Global Analysis."

What's the True Cost of a Breach?

Certain direct losses from a data breach, such as how much a financial institution or card issuer reimburses affected individuals or companies for fraudulent transactions are easily quantifiable. A survey by the Consumer Bankers Association (CBA) found that its 58 member banks have already suffered more than $170 million in losses due to a recent major breach.[7] CBA members reported that the breach cost them an average $10 per breach-affected card, which is the amount the banks spent reissuing one plastic credit or debit card and sending it to the cardholder. But the total losses for the retailer will exceed $170 million — they include the additional expenses of staffing customer-service departments and call centers in order to address customers' questions or concerns about the incident. The breach led to a 46-percent decline in year-over-year Q4 2013 profits and the resignation of the CEO.

Figure 4

Average post data breach costs



Source: Ponemon Institute, LLC. "Cost of Data Breach Study: Global Analysis."

According to this year's benchmark findings from The Ponemon Institute, Cost of Data Breach: Global Analysis,[8] "data breaches cost companies an average of $145 per compromised record in 2013 – this is more than 9 percent increase from the previous year ($136) in 2012. However, [in 2014] German and US organizations on average experienced much higher costs at $195 and $201, respectively." [8] (See Figure 2) According to their research study, the average total cost of a data breach increased 15 percent to $3.5 million where as Germany ($4.74 million) and the U.S. ($5.85 million) experienced the highest total cost.[8] (See Figure 3). The study also points to several post-breach costs (See Figure 4) faced by organizations, including "help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions."[8] It's important to note that all the participating organizations included in the study experienced breaches with fewer than 100,000 exposed records, which is significantly fewer than some of the recent high-profile incidents involving hundreds of millions of records.

Having the right security and protection in place could be a point of strategic differentiation for issuers.

Beyond the direct financial losses associated with a breach, organizations suffer many types of indirect costs — such as negative publicity or a surge in consumer mistrust. A report by AllClear ID, titled *Customer Security is the New Marketing Challenge*, emphasizes that when a brand's reputation is at risk, security is no longer an issue limited to the chief information officer or chief technology officer.[9] In fact, Target's chief marketing officer, Jeffrey Jones, continues to deal with the repercussions of the company's breach.

Identity Theft and Identity Fraud Defined[10]

Identity theft: A crime that occurs when a thief gains unauthorized access to a person's private information with the *intention* of using that information to impersonate the victim or to create a new identity and thereby fraudulently use the victim's credit, assets or benefits.

Identity fraud: A crime that occurs when a thief *actually utilizes* a person's private information to purposefully and fraudulently take control of the victim's credit, assets or benefits.

Using these definitions, we can clarify that a significant number of data breaches result in multiple cases of identity theft, but not every identity theft will result in fraud. *In other words, identity theft is a privacy issue and identity fraud is a security issue.*

For consumers, the cost of a breach extends beyond the potential for identity theft or card fraud. It can take a personal toll on their lives and leave many feeling frustrated, scared and confused as they try to figure out what actions must be taken to protect themselves. Additionally, they must contend with the hassles of canceling cards, receiving new ones and

"Zero-Liability" for Cardholders?

Credit card issuers typically provide "zero-liability protection" to their cardholders, which means they are not held responsible for fraudulent charges to their accounts. But that protection is not as strong as it once was. Some financial institutions in Canada, for example, now routinely refuse to fulfill the zero-liability policy when a consumer's card is compromised after he or she provides card information online.[11] Other issuers are requiring cardholders to cover the first $50 of unauthorized transactions. Under the Electronic Fund Transfer Act, if a customer notifies their bank or card issuer within a pre-determined timeframe that their card is missing, they are not held responsible for any transactions on the missing or stolen card. However, and a customer can, in fact, be liable if they do not report their card lost or stolen in a timely manner.

For a cardholder, a compromised debit card can be financially catastrophic since an account can be emptied of funds in a matter of hours, and recovery can take days or weeks to resolve. In these situations, consumers could anticipate encountering late payments, overdraft fees and limited cash flows. In response to recent high-profile breaches, MasterCard announced that it is "extending its zero-liability policy for cardholders in the United States to include all PIN-based and ATM transactions."[12] The new policy will take effect in October 2014.

The more serious impacts of a breach on consumers are often identity theft and fraud. They can leave a consumer on the hook for legal and financial obligations tied to their driver's license, Social Security number, credit score, bank account, or credit card — and it can take years to untangle from an identity theft incident.

setting up new accounts in order to avoid missed or late payments. It's not uncommon for a consumer to spend more than 20 hours addressing the fallout from an exposed debit card, considering the time it takes to contact banks, stop and redirect automatic payments, and file police reports.

Consumer Trust: Hard to Earn, Easily Broken

For many consumers, any risk of fraud stemming from a data breach is unacceptable and constitutes a fundamental breach of trust with the organization. Even if a breach does not result in fraudulent transactions, customers should be encouraged to take protective steps, such as contacting credit reporting agencies, creditors, banks, health care providers and other relevant institutions to clean up their records and prevent potential fraud. So, while the consumer may not suffer direct financial losses from a breach, the time and stress involved can be large. That time commitment of cleaning up a breach may leave victims feeling aggravated and angry. Whilst most households are generally reliant on payment cards for their day-to-day purchases, they may seek accountability from an issuer or retailer when a breach occurs. In other words, data protection is a key aspect of the customer relationship, and when a breach occurs a customer may decide to shop elsewhere or use alternative financial instruments.

Regardless of the type of data breach, the financial services industry must make a concerted effort to prevent breaches and engage consumers in protecting their accounts.
This is best articulated by Forrester Research: "Your key stakeholders, clients, and other observers do expect you to take reasonable measures to prevent breaches in the first place, and when that fails, to respond quickly and appropriately. A poorly contained breach and botched response have the potential to cost you millions in lost business and opportunity, ruin your reputation, and perhaps even drive you out of business."[1]

TSYS Study: Consumer Awareness & Expectations

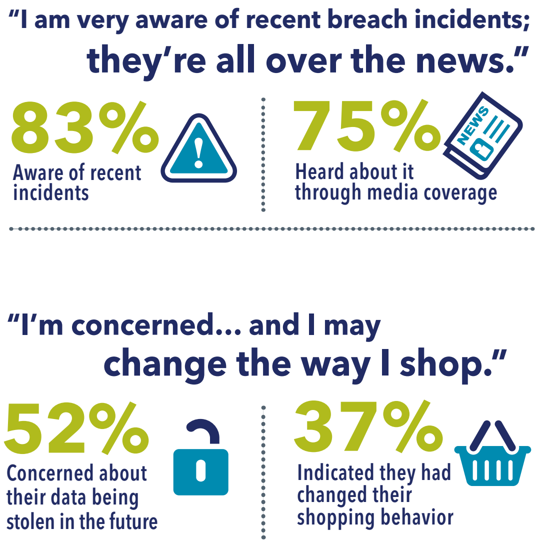
Protecting cardholder data is critical when breaches are seemingly increasing in complexity, scale and frequency, leading to increased consumer concern about identity theft and fraud. With data breaches threatening the payments landscape, it is essential that customers feel comfortable conducting business with banks and merchants. The 2014 *TSYS Consumer Awareness Data Security Study*[4] was conducted to gauge consumer awareness of breach incidents, and to capture their expectations. The study found that consumers often think merchants are at fault when a breach occurs, yet they expect card issuers to notify and guide them through the recovery process.

Consumers' shopping habits are impacted by high awareness of breaches

Today, the high frequency of data breaches and the widespread media coverage means that consumers often learn about breaches through media or via word of mouth. Eighty-three percent of participants in the TSYS study were aware of recent incidents where credit or debit card information had been stolen, and 75 percent of those indicated they had heard about the incident through media. This high awareness of breaches, in turn, is affecting consumer perception and trust of the organizations with which they have a financial relationship. Fifty-two percent of participants indicated they were concerned their personal information would be stolen in the future, and 37 percent indicated that, as a result, they had changed their shopping habits in some form. (See Figure 5).

Figure 5

Consumer Awareness and Behavior



"I am very aware of recent breach incidents; they're all over the news."

83% Aware of recent incidents

75% Heard about it through media coverage

"I'm concerned... and I may change the way I shop."

52% Concerned about their data being stolen in the future

37% Indicated they had changed their shopping behavior

Source: TSYS Consumer Awareness Data Security Study

Consumers believe merchants, banks and card networks hold responsibility

The TSYS study also looked at which entities consumers feel should be held accountable for data breach incidents — and for repairing the damage afterwards. Sixty-four percent of participants believe that merchants are responsible for incidents, while 28 percent say the card networks and banks hold responsibility.

When participants were asked which party they expect to notify them of a breach, their reaction was the opposite: Sixty-seven percent expect card networks and banks to notify them, while only 28 percent expect to hear from the merchant. When asked who should rectify the situation, 61 percent said the responsibility falls upon banks and card networks, while 33 percent indicated it falls upon merchants.

Consumers indicate willingness to taking charge of protecting their information

The TSYS study revealed a strong willingness among consumers to be more involved with protecting their own information. Eighty-eight percent feel they should play a role in protecting themselves.

Engaging consumers to proactively protect their accounts may include providing tools or other controls that allow for ongoing monitoring and protection of their accounts (See Figure 8). Four specific features that study participants felt would support their ability to better protect their accounts:

- Transaction controls on one's phone to stop unauthorized purchases (60 percent)
- SMS text messaging alerts each time a purchase is made (59 percent)
- Instantly viewable credit and debit transaction details by phone (51 percent)
- The ability to turn one's card on or off using one's phone (47 percent)

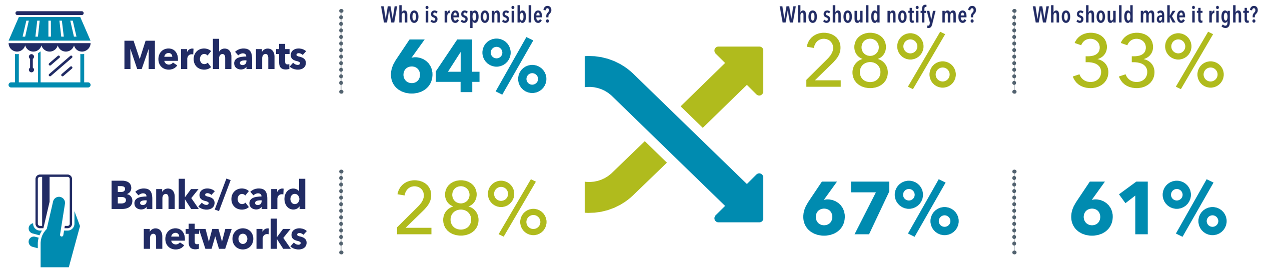
Consumers will switch banks for better security features

Study participants said they want their personal information protected and will switch from one bank to another in order to feel safer. Sixty-three percent of consumers indicated they would likely switch accounts in order to obtain more robust security features, and 31 percent would willingly pay for controls or monitoring tools to prevent fraud (See Figures 7 and 9). An overwhelming 71 percent responded that they would likely switch accounts in order to guarantee that any losses related to a breach would be reimbursed (See Figure 9). An infographic that highlights the study results can be found at www.tsys.com/consumerdatasecurity.

The findings of the study offer three key implications for issuers: 1) Cardholders want to be involved in protecting against fraud; 2) A stronger payments industry ecosystem is needed; and 3) issuers should create and implement a plan for data breach recovery.

Figure 6

Consumer Sentiment Regarding Responsibility for Data Breaches



	Who is responsible?	Who should notify me?	Who should make it right?
Merchants	64%	28%	33%
Banks/card networks	28%	67%	61%

"I hold merchants responsible, but I expect my issuer to notify me and make it right."

Source: TSYS Consumer Awareness Data Security Study

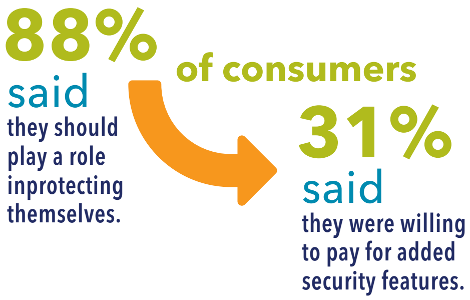
IMPLICATION 1: Cardholders Want Involvement

Monitoring and account access via smartphone

Findings from the TSYS study identified four specific features that participants would value for ongoing protection and monitoring (See Figure 9). Two desired features — monitoring alerts and account information access via smartphone — suggest that real-time mobile access to card-usage and account information is important to cardholders. Most banks and card issuers offer their customers mobile apps for viewing and accessing transactions, whether from a tablet computer or a smartphone. Some banks, like Bank of America, provide customers with a menu of spending and other types of alerts that one can turn on or off and customize to their needs.

Figure 7

Consumer Willingness to be Involved



88% of consumers said they should play a role inprotecting themselves.

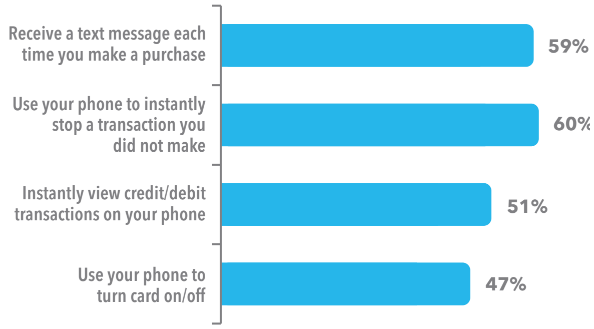
31% said they were willing to pay for added security features.

Source: TSYS Consumer Awareness Data Security Study

Common alerts include those for card transactions made in foreign countries, debit card transactions or ATM withdrawals over a dollar amount — as well as electronically drafted deductions. Unfortunately, many of these alerts are buried in online banking interfaces, and are not well-promoted by banks, so most consumers do not take advantage of them.

Figure 8

Interest in Features that Help Protect Card Accounts



Source: TSYS Consumer Awareness Data Security Study

Card issuers may also offer alerts and other tools that can be set to monitor card activity and minimize the potential damage from card fraud. Capital One allows customers to set up text and email alerts notifying them when their card balance goes above or below a certain amount, when a charge occurs above or below a certain dollar amount, when any charge occurs, and if a payment doesn't go through due to insufficient funds in the account. Citibank cardholders can elect to receive an alert when they are within a certain dollar amount of their credit limit. Chase's alerts text a cardholder if its systems detect an unusual charge, which the cardholder can then reject.[13] American Express's alerts can notify cardholders whenever a cash advance is made using the registered card.

One thing is certain: Issuers need to choose their alert options carefully and not flood cardholders with too many options — as cardholders often get lost in a sea of alerts and end up not using any of them. Two particularly useful alerts given today's card-fraud risks are those that alert cardholders of transactions over a certain dollar limit and when a suspicious transaction occurs. Such alerts ideally allow cardholders to reply "yes," it was them who made the transaction, or "no," it wasn't. Technically, cardholders cannot reject a fraudulent transaction before it is authorized, but if a cardholder replies "no," they can immediately receive a call from the issuer's fraud department to resolve the situation.

Why Is EMV More Secure Than Magnetic Stripe?

As magnetic stripe (magstripe) technology has aged, it has become the weakest link in payment-card security. When swiped at the point of sale by an authorized merchant — or by a "skimmer" with intention of fraud — the magstripe releases all cardholder data, essentially making the card vulnerable to counterfeiting and other fraudulent activities.

EMV payment technology, on the other hand, offers advanced controls, data encryption and other security measures that the magstripe cannot provide. EMV is a chip-based technology embedded into what is often referred to as a "smart card." Unlike static data found on the magnetic stripe of a payment card, a smart card contains an embedded microprocessor that stores dynamic data needed for payment transactions.

Storing payment information on a secure chip offers a safer alternative to magstripe payment cards that dominate U.S. card-based payment transactions. Compelling reasons to convert to EMV include: a liability shift for payment providers due to stronger card security; a reduction in losses due to counterfeit and lost or stolen cards; global acceptance of EMV-based payments; and a greater level of security and comfort for cardholders, especially when used with PIN verification for face-to-face transactions.

Greater control of account transactions before fraud occurs

Another feature that study participants said they would value is the ability to control account transactions by locking and unlocking their debit or credit card before each purchase. According to a recent *Boston Globe* article, "There's something that all cards should have but most don't: an on/off switch accessible from a mobile app that could keep most fraud from happening."[13] Some issuers are currently exploring the on/off switch concept and even using biometrics to lock and unlock card access. One example is Hidden® — a battery powered credit card device that includes five buttons on the face of the card and a paper-thin flexible display. The display hides a portion of a cardholder's payment card number. To turn the device on, a user must enter a personal unlocking code on the card. If the user enters the correct unlocking code, it then displays the user's payment card number so that he or she can read the number and the magnetic stripe can be read by magnetic stripe readers.[14] Another solution, CardControl, is a mobile application that allows people to use their smartphone as a remote control for their credit and debit cards by enabling them to lock and unlock their cards. According to the company's website, "When you're ready to make a purchase or withdraw cash from an ATM, just slide your finger across the screen and instantly activate the card."[15]

Pradeep Moudgal, an analyst with the Mercator Advisory Group, said about the CardControl app: "People have to get comfortable with this technology and use it, but eventually systems like this will provide greater flexibility for consumers and help them manage the cards in their wallet in a better way."[15] Until the right solution is designed, some skepticism exists. According to Ellen Richey, Visa's chief legal officer, "One thing we have found is that consumers are remarkably impatient with anything that gets between them and making a payment."[13]

IMPLICATION 2: Building a Stronger Payments Industry Ecosystem

The payments industry could do more to protect data by making it more difficult for compromised data to be used by fraudsters. In response to recent cyber attacks, U.S. members of Congress recently demanded that financial and retail industry leaders work together to strengthen customer card data security. However, the government also has an opportunity to take on a deeper and more collaborative role that extends beyond regulation.

EMV, 3D Secure and Tokenization offer the payments industry greater protection

It's difficult to know how fraudsters will evolve, but the payments industry could more quickly adopt new technologies that protect both card-present and card-not-present (CNP) transactions. Three technologies exist — EMV, 3D Secure and tokenization — that, if adopted by issuers, would significantly reduce fraudulent activity involving exposed cardholder data. As detailed in the TSYS report, *EMV is Not Enough: Considerations for Implementing 3D Secure*, one of the primary reasons EMV technology decreases card fraud is that it uses dynamic data authentication along with a PIN that is securely encrypted on the chip and known only to the cardholder, and entered at point of sale to verify a transaction. Because of the high use of EMV cards in Europe and other parts of the world, much of today's card fraud has migrated to the United States. According to Neira Jones, of the Information Security Media Group, "You see a migration of fraud going to countries that have not deployed chip and PIN" technologies."[4] While fraud won't be completely eradicated by EMV, deploying such smartcard-based technology will significantly reduce it across the card-present channel. It is expected that Visa and MasterCard's impending fraud liability shift from card issuers to merchants — expected to take effect in October 2015 — will financially motivate U.S. merchants to upgrade existing point-of-sale terminals to accept EMV technology, thereby accelerating EMV's U.S. adoption rate. In recent press releases, Target announced its accelerated plans to both upgrade their point-of-sale terminals and transition their payment card, REDCards, to chip-and-PIN-enabled ones, "Target has long been an advocate for the widespread adoption of chip-and-PIN card technology," said John Mulligan, executive vice president, chief financial officer for Target.[22]

Deploying EMV and 3D Secure together achieves an effective and multi-layered optimal security fraud protection for customers without impacting their shopping experience.

EMV + 3D Secure

EMV adoption, while proven to combat fraud in card-present transactions, ultimately pushes fraudsters to other, less secure channels, such as online and mobile commerce. Issuers and merchants in the U.K. have focused their efforts on using EMV technology to reduce card-present fraud, while Spain has focused its energies on reducing card-not-present fraud. Both countries have greatly reduced the incidence of fraud across those channels.

Issuers must be aware of the increasing shift to CNP fraud and should deploy tools and solutions to prevent and detect it. The most widely adopted solution in this space is 3D Secure, a system designed to make online shopping transactions safer by authenticating a cardholder's legitimacy at the time of purchase.[16] The 3D Secure service is more commonly recognized by its various commercial nomenclatures: MasterCard SecureCode, Verified-by-Visa, American Express SafeKey, JCB International J/Secure and Diners Club ProtectBuy.

> **"3D Secure's most advanced security features minimize disruption to transactions by authenticating in a manner that is invisible to cardholders for the vast majority of transactions."**

3D Secure is not a silver bullet for eliminating card fraud, but it creates a powerful value proposition when used in conjunction with EMV chip-and-PIN technology: It provide issuers and merchants more control by allowing them to better assess transaction risks and authenticate cardholder identities online. Furthermore, 3D Secure's most advanced security features minimize disruption to transactions by authenticating in a manner that is invisible to cardholders for the vast majority of transactions. Deploying EMV and 3D Secure together achieves an effective and multi-layered fraud protection for customers without impacting their shopping experience.

Tokenization Protects Sensitive Card Data

With the proliferation of mobile devices and subsequent rise in malware targeting these devices, consumers need a more secure way to shop and transact using their smartphones, tablets, personal computers and other Internet-enabled devices. Tokenization entails using a single token to replace and represent a customer's primary account number, and is "restricted in how it can be used with a specific device, merchant, transaction type or channel."[17] The procedure benefits all industry stakeholders, including cardholders, banks, issuers and merchants, since tokenization removes the need for merchants to store card account information, as this is stored by the tokens. It is also a process that is invisible and does not disrupt a cardholder's shopping experience. Tokenization is considered so useful that MasterCard, Visa and American Express announced a joint proposal in 2013 for a new global standard to make online and mobile shopping simpler and safer through tokenization.[18] Ed McLaughlin, chief emerging payments officer at MasterCard, said this about the trend: "This continued transition from plastic cards to digital is all about providing consumers with the ability to easily and safely make a purchase. They would no longer need to store their actual card account number when shopping online or with a smart device; the token would serve as that stand-in."[18]

In simplest terms, the value of tokenization for issuers is that it provides an additional layer of fraud protection and security. It can reduce a fraudster's ability to steal card information since the stolen token information is useless on its own. Tokens may also reduce risk and help merchants meet their PCI compliance requirements since they will not be storing or using account information that can be monetized if stolen. The benefits of tokenization include improved transaction efficiency and security and a more obvious service offering to cardholders.

Governments: Collaborate, don't just regulate.

Strong government and industry cooperation and collaboration would greatly benefit end-to-end data security and fraud prevention. Local, state and federal government bodies have the ability to pass and enforce legislation and implement important change — and studies show that consumers want such government action. Since the financial crisis of 2008, consumers have become mistrustful of financial institutions, according to Edelman's *Financial Trust Barometer* study. "Consumers' confidence in banks' ability to 'do the right thing' has plummeted — a stunning 46 [percent] in the US, and an equally-shocking 30 [percent] in the UK," the authors note.[19] The study found that consumers want protection provided by government: "31% of consumers think more regulations are needed to curb irresponsible business practices. 25% want the government involved to ensure companies are behaving responsibly."[19] The study also found that U.S. consumers are more trusting of financial services brands than consumers in other developed countries.[19] Cooperation between industry and government could strengthen the payment ecosystem, ultimately benefit all stakeholders, and move decision-making away from the sole consideration of positive and potential ROI. Collaboration would help bring to fruition technologies based on benefits for all stakeholders involved in the transaction. And such collaboration could help with focus on forward progress with a foundation in both technological advancement and an orientation of consumer protection.

Cooperation between government and the payments industry could entail using data collection and security methods used at federal agencies such as the FBI to help issuers and card networks identify better ways to protect customer data — without stepping on consumers' privacy rights, of course. Moreover, government data could be leveraged for fraud-identification initiatives, enabling better cross-industry data pooling that supports anti-money laundering initiatives and aids law enforcement in the apprehension of the perpetrators of fraud.

IMPLICATION 3: Instituting a Plan for Data Breach Recovery

Duncan McDonald, former general counsel to Citigroup's Europe and North America card businesses, says recent high-profile data breaches offer some valuable takeaways.

"The key lesson of the [major retailer] security breach may be that it is impossible to prevent data crimes against the card system," McDonald says. "The ease of access to valuable consumer information, the considerable rewards for stealing it, the failure of law enforcement to prevent it, and the increasingly prohibitive cost of protecting it all militate against any easy solution."[20]

The TSYS study found that consumers expect issuers to compensate them for any fraud-related losses, and having a data breach recovery plan can improve issuers' internal recovery processes with the least amount of financial and reputational impact. On a positive note, consumers' confidence in banks' and card networks' recovery assistance is high: Sixty-three percent of participants indicated confidence in the ability of banks and card networks to assist with recovery, but that only adds to their expectation of swift notification and assistance. Though complying with various states' breach laws can be complicated, notification should ideally happen sooner rather than later. One notable criticism of how eBay handled its breach was its slow response. The company didn't post a notice about the breach on its website until days after it happened, which angered and shocked many. According to Paul Stephens of the Privacy Rights Clearinghouse, which maintains data breach statistics, "Nor should it have taken weeks for the company to start emailing users about the possibility their data was stolen. This may be one of the largest, if not the largest, data breach in history. Why didn't they immediately email their customers?"[21]

Given the importance of responding to a breach quickly and efficiently, here are two strategic imperatives for issuers in creating their recovery plans:

Strategic imperative #1: Treat the internal breach-recovery process as a full crisis recovery exercise.

A data compromise event is a time-consuming and resource-intensive process. It impacts an issuer in several ways, and some of the toughest challenges include: knowing when to block and reissue cards, how to handle cardholder communication, not having automated tools, card fulfillment issues and insufficient personnel.

Having a robust breach-recovery plan — including securing the best technological solutions in advance, rehearsing the internal breach-recovery process and ensuring all key stakeholders are well-versed on the plan and their role in it — will ultimately protect issuers from the fallout other organizations have experienced after a major data breach. As Heartland, TJ Maxx, Target, eBay and many other companies have learned, how an organization responds to a data breach determines the true cost — including both direct financial costs and long-term reputational costs — of such an incident. In fact, Ponemon Institute's *2014 Cost of Data Breach Study: Global Analysis* found that having a business continuity plan for breach remediation can reduce financial losses by an average of $8.98 per compromised record.[8]

Visa's Five Principles for Effective Data Breach Communications:[20]

1. Consider a Breach Likely, and Prepare Accordingly

- Designate and empower an internal breach-response team
- Have an ongoing PCI-DSS compliance program
- Identify and establish relationships and/or agreements with key vendors
- Have breach-response communications

2. Be Accurate and Fast

- Give yourself permission to notify before you know everything
- Offer timetables on what you know and when you will know more
- Acknowledge that the situation may change

3. Be Open, Honest, and Transparent

- Be transparent in your activity and demonstrate that you are getting the word out
- Follow normal media routine
- Avoid absolutes, misleading statements and withholding information

4. Be Accountable — Always

- Take ownership
- Don't play the victim
- Express regret

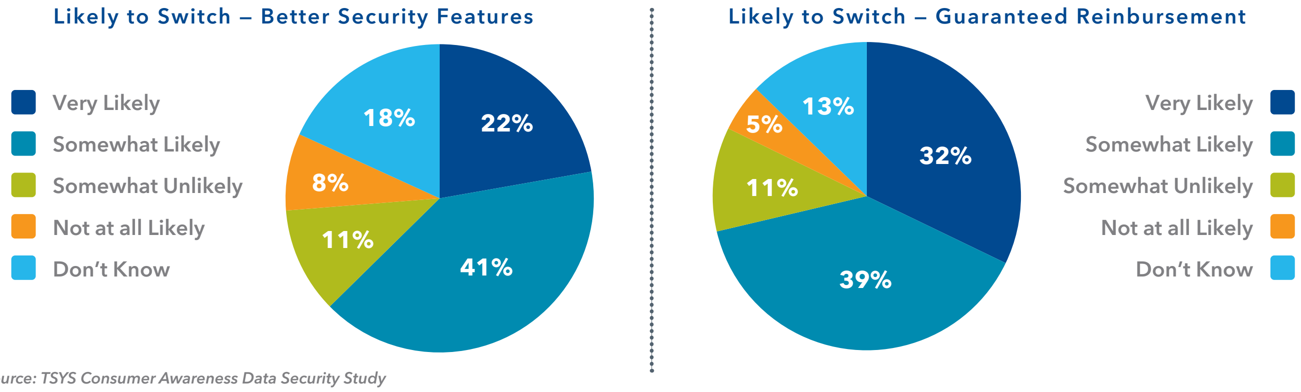
5. Get the Word Out

- Consider all audiences (cardholders, employees, customer service representatives , shareholders, analysts, media, partners, regulators and legislators)
- Leverage the power of zero-liability
- Provide real, customer-focused support
- Use the Internet to inform

Issuers must also recognize the importance of customer communications and service in the breach-recovery process and in helping to minimize long-term reputational damage. If a data breach incident occurs, customers expect financial institutions to provide them with immediate access

Figure 9

Consumers Vulnerable to Security Messaging?


Likely to Switch – Better Security Features

Likely to Switch – Guaranteed Reinbursement

Source: TSYS Consumer Awareness Data Security Study

to customer service representatives, who can answer questions or resolve any fraudulent charges resulting from the breach. This often entails establishing a special hotline devoted to helping customers affected or worried about the breach, and providing clear and useful information that helps them better protect their accounts. Part of the plan or solution should add security fraud options such as flagging cards and sending cardholders immediate correspondence and triggers that initiate replacement of compromised cards. A strong communication plan, when executed properly, restores customer confidence, reduces potential costs and streamlines the management process.

Strategic imperative #2: Educate cardholders on proven data security best practices and tools available to them.

It's become more important than ever that companies make their customers aware of security risks while also putting them at ease. In other words, companies can build customer confidence by explaining what they are doing to protect their customers' personal data. As Richard Edelman, president and CEO at Edelman Worldwide, puts it: "It is not good enough anymore to say smart words. You have to have smart deeds."[19] Customers want to know, for example, what measures issuers and merchants are taking to protect them from fraud. These security measures ideally require minimal effort from cardholders, but just the awareness of such initiatives or data-security tools could bolster consumer confidence and, in turn, build cardholder loyalty. An issuer that uses strong data security as a way to differentiate itself in the market could earn "top-of-wallet" status for its cards.

Conclusion:

Data breaches have increasingly become a fact of life. The payment industry now has a wealth of tools available to protect against fraud, including EMV "chip-and-PIN" technology for card-present transactions, and 3D Secure for card-not-present transactions. However, even greater action by the payments industry is needed to protect against today's growing risk of data breaches, and to reduce consumers' wariness over their payment security. Offering cardholders protective tools and technologies, including card tokenization and account alerts, can help greatly bolster cardholder confidence, enhance cardholder loyalty and ultimately increase payment card usage.

It can't be stressed enough: Issuers that are most proactive about preventing breaches and helping their cardholders recover from such incidents will ultimately be best-positioned in the years and decades ahead.

SOURCES

1 Kindervag, John and Rick Holland. "Planning for Failure." *Forrester*.com. 9 November 2010. Web. June 2014.
<http://www.forrester.com/Planning+For+Failure/fulltext/-/E-RES60564>.

2 "2014 Data Breach Investigations Report." *Verizonenterprise.com*. Web. June 2014.
<http://www.verizonenterprise.com/DBIR/2014/>.

3 Daly, Jim, "Wide-Ranging Hacker Indictment Casts New Light on Some Notorious Breaches." *Digital Transactions.net.* 25 July 2013. Web. June 30, 2014.
<http://digitaltransactions.net/news/story/4205>.

4 TSYS Consumer Awareness Data Security Study. May 2014.

5 "Ebay Inc. to ask Ebay Users to Change Passwords." Blog.ebay.com. 21 May 2014. Web. June 2014.
<https://blog.ebay.com/ebay-inc-ask-ebay-users-change-passwords/>.

6 "Trends & Perspectives." *Idanalytics.com*. Web. June 2014.
<http://www.idanalytics.com/ida-labs/trends-and-perspectives/>.

7 Kitten, Tracy. "Target Breach: The Cost to Banks." *BankInfoSecurity.com*. 12 February 2012. Web. June 2014.
<http://www.bankinfosecurity.com/interviews/cba-i-2182>.

8 "2014 Cost of Data Breach Study: Global Analysis." Benchmark research sponsored by IBM. Independently conducted by Ponemon Institute, LLC.
IBM.com. May 2014. Web. June 2014.
<http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/>.

9 Holland, Bo. "Customer Security is the New Marketing Challenge." *Allclearid.com*. 2014. Web. June 2014.
<https://www.allclearid.com/files/5813/9396/2404/CMOs_and_Customer_Security_-_AllClear_ID_Whitepaper.pdf>.

10 "2005:The Year of the Breach?" Intersections, Inc. Feb. 7, 2006.

11 Thibeault, Glenn. "E-commerce fraud victims may be out of luck." Letters to the Editor. *Northernlife.ca*. 17 March 2014. Web. June 30, 2014.
<http://www.northernlife.ca/news/letterstotheeditor/2014/03/17-Thibeault-credit-cards-sudbury.aspx>.

12 "MasterCard Strengthens U.S. Cardholder Security." Press Release. *MasterCard.com*. 28 May 2014. Web. June 30, 2014.
<http://newsroom.mastercard.com/press-releases/mastercard-strengthens-u-s-cardholder-security/>.

13 Lieber, Ron. "Consumers Need to Arm Themselves Against Fraud." *NewYorkTimes.com*. 18, March 2014. Web. June 2014.
<http://www.bostonglobe.com/business/2014/03/17/consumers-not-powerless-face-card-fraud/VQZmi3xPTL5o7JcgyPmtLK/story.html>

14 "Dynamics, Inc. Fights Credit Card Fraud with Hidden® Electronic Credit." *Arlingtoncardinal.com*. 5 April 2014. Web. June 2014.
<http://www.arlingtoncardinal.com/2014/04/dynamics-inc-fights-credit-card-fraud-with-hidden-electronic-credit/#sthash.eLepLwiA.dpuf>.

15 Cathey, Carrie. "Fight Fraud with Remote Control for Cards." *Unlockyourwealthradio.com*. 5 May 2014. Web. June 2014.
<http://unlockyourwealthradio.com/2014/05/05/fight-fraud-with-remote-control-for-credit-cards/>.

16 "About 3D Secure." *Securepay.com*. Web. June 2014.
<http://www.securepay.com.au/products-services/3d-secure/>.

17 "EMVCo Expands Scope to Develop Tokenisation Specifications" *Smartcard.co.uk*.17 January 2014. Web. May 2014.
<http://www.smartcard.co.uk/NOLARCH/2014/January/170114.html>

18 "MasterCard, Visa and American Express Propose New Global Standard to Make Online and Mobile Shopping Simpler and Safer." Press Release.
Mastercard.com. 1 October 2013. Web. June 2014.
<https://newsroom.mastercard.com/press-releases/mastercard-visa-and-american-express-propose-new-global-standard-to-make-online-and-mobile-shopping-simpler-and-safer/>.

19 Zilka, Jeff. "Trust in U.S. Financial Services Still Low Despite Economic, Market Gains." *Edelman.com*. 13 March 2012. Web. June 2014.
<http://www.edelman.com/post/trust-in-u-s-financial-services-still-low-despite-economic-market-gains/>.

20 "Responding to a Data Breach." Visa. 2008. *Usa.Visa.com*. Web. June 2014.
<http://usa.visa.com/download/merchants/cisp_responding_to_a_data_breach.pdf>.

21 Greenberg, Andy. "EBay Demonstrates How Not to Respond to a Huge Data Breach." *Wired.com*. 23 May 2014. Web. June 2014.
<http://www.wired.com/2014/05/ebay-demonstrates-how-not-to-respond-to-a-huge-data-breach/>.

22 "Target Appoints New Chief Information Officer, Outlines Updates on Security Enhancements." Press Release. *Target.com*. 29 April 2014. Web. June 2014.
<http://pressroom.target.com/news/target-appoints-new-chief-information-officer-outlines-updates-on-security-enhancements>.

About the Author

Jonathan D. Hancock *Director, Global Fraud Management Solutions*
In his current role as Global Director of Fraud Management Solutions, Jonathan is responsible for setting and driving the strategic development of TSYS' existing fraud management solutions to TSYS processing clients, along with solution innovation and new product development. Prior to joining TSYS in 2009, Jonathan's career in payment card fraud prevention included leadership positions at Barclaycard, Travelex and Visa Europe.

About TSYS

At TSYS® (NYSE: TSS), we believe payments should revolve around people, not the other way around℠. We call this belief "People-Centered Payments®." By putting people at the center of every decision we make, TSYS supports financial institutions, businesses and governments in more than 80 countries. Through NetSpend®, a TSYS company, we empower consumers with the convenience, security, and freedom to be self-banked. TSYS offers issuer services and merchant payment acceptance for credit, debit, prepaid, healthcare and business solutions.

TSYS' headquarters are located in Columbus, Ga., U.S.A., with local offices spread across the Americas, EMEA and Asia-Pacific. TSYS is a member of The Civic 50 and was named one of the 2013 World's Most Ethical Companies by Ethisphere magazine. TSYS routinely posts all important information on its website. For more, please visit us at www.tsys.com.

Contributors

This report was prepared by TSYS. Contributors to this paper under the guidance of Jonathan Hancock include: Product Marketing Director, Jeff Hampton; Marketing Consultant, Cheryl Benton; and Independent Writer, Carolyn Kopf.

TO LEARN MORE

contact 1.706.649.2307
or email sales@tsys.com.

twitter.com/tsys_tss

facebook.com/tsys1

linkedin.com/company/tsys

GET TO KNOW TSYS

AFRICA	ASIA-PACIFIC	COMMONWEALTH OF INDEPENDENT STATES	EUROPE	INDIA & SOUTHEAST ASIA	MIDDLE EAST	NORTH & CENTRAL AMERICA, MEXICO & THE CARIBBEAN	SOUTH AMERICA
+27 21 5566392	+603 2173 6800	+7 495 287 3800	+44 (0) 1904 562000	+911204191000	+971 (4) 391 2823	+1.706.644.3819	+1.706.644.3819