iSMG
INFORMATION SECURITY
MEDIA GROUP

FACES OF FRAUD: THE 2016 AGENDA

Impact of Retail Breaches & the Future of Payments Security

INSIDE

- *Complete Survey Results*
- *Expert Analysis*
- *Insights from Daniel Ingevaldson of Easy Solutions*

EASYSOLUTIONS®
TOTAL FRAUD PROTECTION

Tom Field

As 2016 begins, financial institutions find themselves at a fateful crossroads. They continue to see the impact of retail payments breaches, such as those that struck Target, Home Depot and other merchants.

Yet, they also are at the cusp of a significant payments evolution, as the U.S. slowly embraces EMV, and enterprises worldwide open up to evolving forms of mobile payments.

This convergence begs the question: What are the new opportunities for fraud? And what investments are organizations making to protect themselves from new forms of fraud, as well as the tried and true?

These are among the questions to be answered by this latest study, *Faces of Fraud: The 2016 Agenda*. The newest of ISMG's annual Faces of Fraud surveys, this fresh research looks at:

- Retail breach impact and emerging payments;
- The latest fraud trends and key security gaps;
- Top anti-fraud investments for 2016.

This survey was conducted online during the fall of 2015, and we had more than 200 respondents from financial institutions of all sizes.

Join me in a review of the full survey responses, and then let's discuss how you can put this data to use to help improve your organization's capabilities to detect and prevent fraud in all its forms.

Tom Field
Vice President, Editorial
Information Security Media Group
tfield@ismgcorp.com

About this survey:
This study was conducted online during the fall of 2015. More than 200 respondents participated from financial institutions of all sizes, primarily based in the U.S.

Table of Contents

Fraud Perspectives

PCI's King: European Banks, Retailers Should Brace for Card Fraud Uptick

Javelin's Pascual Predicts Many More Sophisticated Attacks Are Likely

Gartner's Avivah Litan on Fraud Trends

A Look Into the 2016 Faces of Fraud

Survey Analysis by Daniel Ingevaldson, CTO of Easy Solutions

Note: In preparation of this report, ISMG VP Tom Field sat down with Easy Solutions CTO Daniel Ingevaldson to analyze the results and discuss how security leaders can put these findings to work in their organizations. Following is an excerpt of that conversation.

Ingevaldson is Chief Technology Officer of Easy Solutions, responsible for technical strategy and overseeing the research team. He was previously Director of Technology Strategy and oversaw the industry-renowned X-Force R&D team at Internet Security Systems (ISS), which was acquired by IBM for $1.3 billion. Most recently, he was co-founder and SVP of Product Management at Endgame Systems.

Gut Reactions to Results

TOM FIELD: Gut reaction: What jumps out at you from these survey results?

DANIEL INGEVALDSON: Overall the results are in line with the activity that we're seeing in the industry and in line with our projections; however, a few things in particular do jump out to us.

First is the fact that retail breaches were an accelerator for the adoption of EMV, even though 57 percent admitted that they will not be fully EMV compliant by the October 2015 deadline. The second is that although 55 percent of respondents reported that their financial losses linked to fraud increased, one of the main concerns (39 percent) from management is that fraud losses are within an "acceptable" level. This may be true to some extent because the financial institutions have invested millions of dollars in fraud prevention technologies in the last five years or so. We think the potential mistake here is to think that the problem has been fixed forever because we may win one battle, but the war is far from over. Threats are in a constant evolution, and fraud prevention solutions should also be constantly assessed to make sure they remain capable of protecting organizations from today's fraud environment.

Emerging Trends

FIELD: From the years you have sponsored this survey, what trends do you observe?

Threats are in a constant evolution, and fraud prevention solutions should also be constantly assessed to make sure they remain capable of protecting organizations from today's fraud environment.

Daniel Ingevaldson

INGEVALDSON: With more than 50 percent of the population under the age of 30, financial institutions need to understand that demand for digital transactions will continue to grow, which means that the fraud problem is going to get really hot on digital channels, including digital wallets and other emerging payment solutions. These channels open the door to fraudsters to develop and implement new techniques and lead to more fraud. This is a clear indication that fraud prevention is core to the future of banking. It becomes a strategy initiative that enables the growth of the business.

Impact of Retail Breaches

FIELD: What impact have retail breaches had on financial institutions, and what is within their power to change?

INGEVALDSON: The retail breaches over the last couple of years have forced financial institutions, and nearly every other company, to have all-time high security awareness, which have resulted in a lot of security improvements and investments being made. We still have a long way to go, though. These investments take a long time to deploy; however, steady progress is being made.

Financial institutions do have the power to focus on preventing fraud throughout the lifecycle of the incident, starting in the early and planning stages (when the criminal is building attacks or the launch stage, when the criminal is compromising a device) of an attack. Here, they can significantly reduce the criminals' possibilities to complete to the fraud cycle, and therefore, maximize their return.

Therefore, financial institutions no longer can remediate fraudulent transactions as they happen. They need to consider the entire lifecycle of the fraud, which are: planning, launching and cashing. Exclusively focusing on only one of these stages, without seeing the entire picture, will result in a segmented view of their risk and fraud environment.

The Impact of EMV?

FIELD: Are we putting too much faith in the EMV rollout in the US?

INGEVALDSON: EMV for in-store card transactions will definitely help in promoting less fraud at the register; however, expect fraud to shift with a dramatic uptick in e-commerce and other kinds of "card-not-present" fraud to happen in the US, as it has happened in other countries when they adopted EMV (chip-and-PIN) credit card technology. However, fraudsters will not stop attempting to conduct credit card fraud. Instead, they will simply shift their attempts to more vulnerable channels, where chip protection is rendered useless.

Also, as major retailers have implemented chip-and-PIN capable machines, stores are seeing their checkout times increase, as consumers must learn and then use the new EMV credit cards. Cards must now be "dipped" into the machine and left there for several seconds, as opposed to a momentary swipe. As such, we expect that this will be a boon for digital wallets, including Apple Pay, which in comparison, are easier and faster to use than the new EMV readers. With the increase in Apple Pay use, it's important to make sure that Apple Pay is secure.

Fraud Migration

FIELD: Following the EMV rollout, what type of fraud migration are you seeing already in the US, and how must institutions respond?

INGEVALDSON: As we said, we will see an important spike in card not-present fraud. The organizations who are successful at fighting fraud have come to the realization that fraud is rarely a one-channel, one-incident kind

With more than 50 percent of the population under the age of 30, financial institutions need to understand that demand for digital transactions will continue to grow.

of problem. In order to mitigate the risk, there's an imperative need to develop a strategy that looks at the entire lifecycle of the fraud, including the planning stage, the attack launch stage and the cashing stage, across all the different transactional channels.

Detection Dilemma

FIELD: Detection remains a challenge – too often banks learn of fraud when their customers alert them. How can we improve this area?

INGEVALDSON: It has to be a multi-layered approach. Combining the benefits of fraud intelligence with attack takedown are a must. Email and multifactor authentication, safe browsing solutions and transaction monitoring systems also are definitely ways to improve detection and protection against fraud.

Building the Business Case for Fraud Resources

FIELD: Institutions are struggling a bit to get appropriate funding for anti-fraud measures. What are the business cases that get senior management's attention?

INGEVALDSON: Traditionally, we have seen business cases relying on the reduction of fraud losses to justify investments in fraud prevention technologies. Proactivity is key. It's impossible to think strategically about fraud prevention when getting 1,000 attacks per day. Instead, think about it when the waters are calm. In terms of getting funding, there is an important difference between fraud losses and fraud attempts. Attempts are many and happen regularly. This is an important tool that should be leveraged.

> The organizations who are successful at fighting fraud have come to the realization that fraud is rarely a one-channel, one-incident kind of problem.

In today's world, fraud prevention technologies are core to the business of banking, and you can think of a lot more than just the reduction of losses:

- Simplifying the end-user experience
- Business enabler

The Fraud Disconnect

FIELD: We continue to see the disconnect between the top forms of fraud afflicting institutions vs. the forms they are best prepared to face. How can we change this dynamic?

INGEVALDSON: If we start to protect the entire fraud cycle from beginning to end, we can start to move one step ahead of cyber criminals.

Account Takeover

FIELD: Nearly five years after the FFIEC authentication update, incidents of account takeover haven't decreased appreciably. What's wrong? How can we reduce that number?

INGEVALDSON: Ransomware is not the only method that cybercriminals use to extort money from financial institutions. Other tactics, such as a denial of service (DoS) attack, the theft of sensitive business and customer information to extort payment or other concessions from victims, may also be employed. To reduce that number, it's imperative for institutions to have a robust cyberattack protection platform in place – something that proactively detects and eliminates a complete range of malware attacks – including ransomware attacks – before harm can be done to the business or customer base. This includes spotting all the malicious activity that cybercriminals are carrying out in the moments leading up to a fraud incident, so that attacks are stopped before they are even launched.

Mobile Trends

FIELD: Institutions don't quite seem to see the pain yet from fraud via the mobile channel. How do you see this changing in 2016?

INGEVALDSON: With the growth in smartphone usage, organizations have to take a cross-channel approach to prevent fraud effectively. As a transactional channel, mobile is part of the equation.

Today's attacker will leverage one or more than one channel to commit fraud. Mobile devices today might not be necessary during the cashing-out stage of the cycle because high-risk transactions like wire, ACH, etc. are not performed from a mobile application. However, mobile devices are used in the different stages, such as when downloading malware disguised as an app, through fictitious SMS text

“As more and more payments move to digital channels, we foresee all kinds of sophisticated and cross-channel attacks to continue to grow.”

messages to perform phishing or install rogue app or SMS redirection to steal OTP (One-Time Password), to name a few.

These actions often lead to various forms of fraud, including account takeover, stolen credit cards used for mobile payments and email spoofing.

As more and more payments move to digital channels, we foresee all kinds of sophisticated and cross-channel attacks to continue to grow.

Top Concerns for 2016

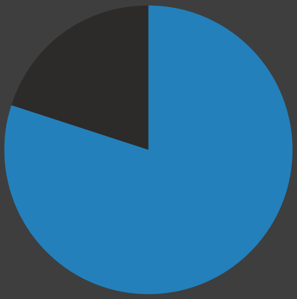
FIELD: What are the forms of fraud that concern you most in 2016?

INGEVALDSON: **Synthetic Identity Fraud**: In addition to card-not-present fraud, we anticipate an increase in synthetic identity fraud, which happens when a fraudster uses personal information from various individuals (such as Social Security numbers, addresses, DOB) and combines them with additional fake information to create a new identity. They will then use this information to open new bank accounts or credit cards. With all of the personal identifiable information (PII) that has been stolen from breaches of healthcare companies like Anthem, Premera and Blue Cross, and government agencies like the Office of Personnel Management (OPM), we project this kind of fraud to grow significantly in 2016.

Corporate Email Takeover: With a record number of credentials having been stolen, and password reuse rampant, corporate email takeover is likely to increase in 2016. The scams use email (seemingly from someone within the company or within a partner of the company) to trick small businesses into transferring large sums of money into fraudulent bank accounts. ■

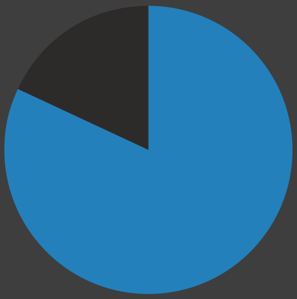
Big Numbers

Some standout figures from this survey.



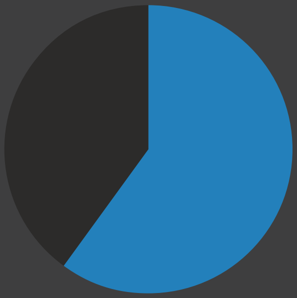
80+%

Of respondents impacted by Target, Home Depot breaches



82%

Say payment card is top form of fraud



60%

Say they first detect fraud when notified by a customer

Impact of Retail Breaches

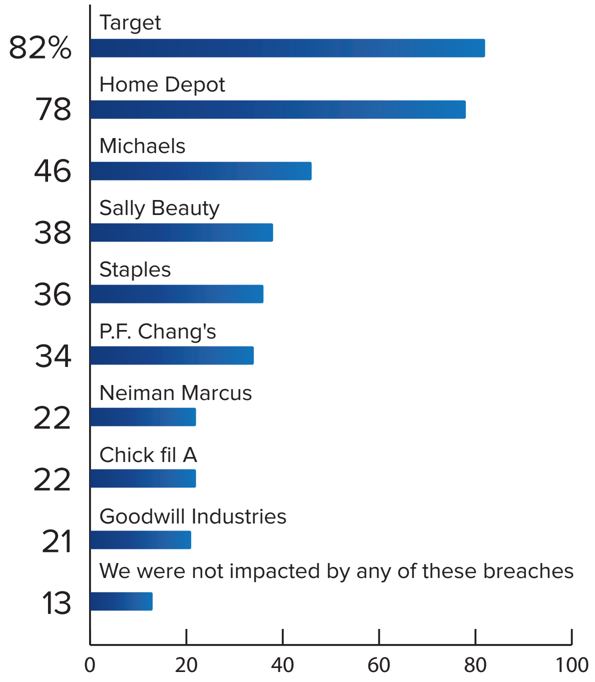
This opening section explores the impact of recent high-profile retail breaches on banking institutions. Results show that banks and credit unions continue to pay the price – in terms of card reissuance and loss of productivity – for attacks suffered by merchants, such as Target and Home Depot.

Among the key results in this section:

- 87 percent of respondents were struck by at least one of the retail breaches;
- 73 percent say merchants and vendors must be held more accountable for these breaches of their systems and data.

Following is a detailed look at each question in this section.

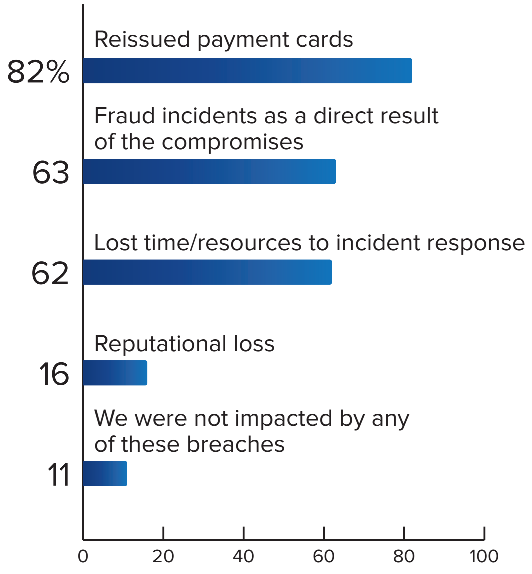
Which of the following high-profile retail breaches impacted your organization and customers within the last 12 to 16 months?



Perhaps the easier question would be: How many banking institutions were not impacted by these high-profile retail breaches? The answer would be: 13 percent. The other 87 percent reveal that they felt the effects of at least one of the newsmaking breaches, predominantly Target (82 percent) and Home Depot (78 percent).

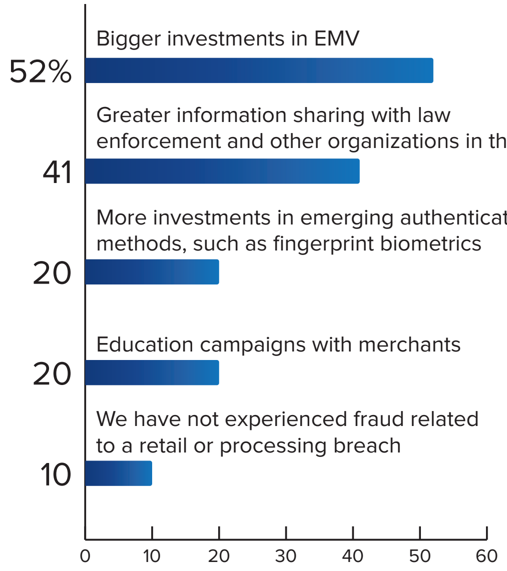
What were the impacts?

In what ways did these breaches impact your organization or customers?



Most often (82 percent of the time), institutions were forced to reissue payment cards that were compromised in these merchant attacks. The other major impacts: lost time and resources to incident response in the wake of the breaches (62 percent) and actual incidents of fraud that can be tied directly to the compromises (63 percent).

How have retail and payments processing breaches changed the way your organization addresses fraud-prevention?



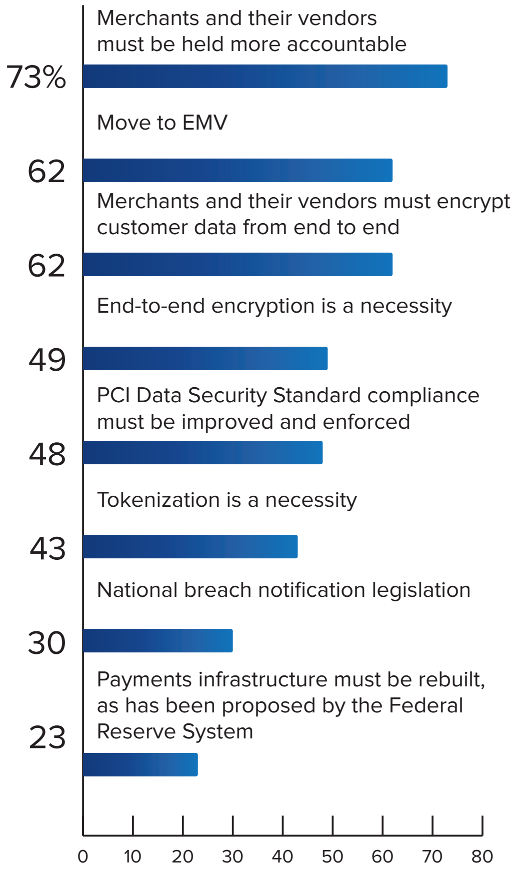
2015 was the second straight year of ongoing retail breaches. And although none has been an attack directly against a bank, institutions still (clearly) are left to help clean up the mess. What have institutions started to do differently?

For one, in conjunction with the Oct. 2015 fraud liability shift in the U.S., they have made bigger investments in EMV card security technology (52 percent).

And also, responding to cybersecurity instructions from the president himself, 41 percent of respondents say they are participating in greater information sharing with law enforcement and other bodies.

Only one-fifth of respondents say they are making more investments in emerging authentication methods such as biometrics, which remains an unproven commodity to many banking security leaders.

What do you propose as a solution to the growing number of retail breaches?



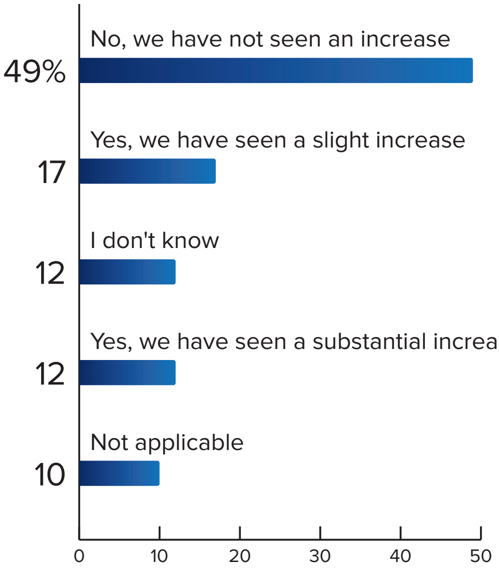
So, what will banking institutions do to help prevent a third straight year of devastating retail breaches?

Alas, there is little in their direct control. The move to EMV in the U.S. will at least curb the spread of counterfeit payment cards. But it will not stop card-not-present fraud, nor will it be a barrier for impersonators if merchants don't take time to validate signatures.

To truly curb these breaches, survey respondents feel strongly that merchants and their vendors (such as payments processors) must be held more accountable for attacks that occur against their own systems (73 percent of respondents), and that merchants and vendors must encrypt customer data throughout the transaction (62 percent).

Nearly half of respondents say a move to true end-to-end encryption is a necessity.

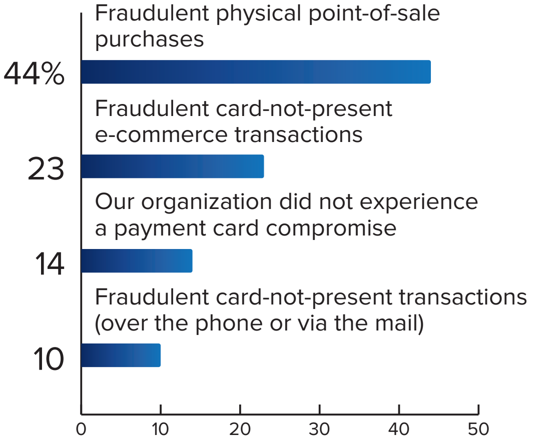
As part of one of these retail breaches, have you seen upticks in ATM cash-outs linked to cards compromised?



One fraud vector that has not increased substantially as a result of retail breaches: ATM cash-outs linked to cards compromised.

Only 29 percent of respondents see any kind of increase here. Forty-nine percent report no increase whatsoever.

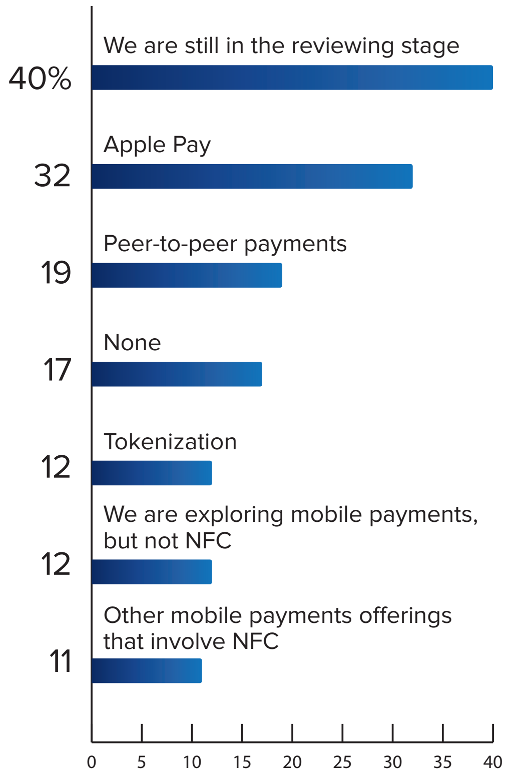
After a payment card compromise, how were compromised cards most often used to perpetrate fraud?



If cash-outs were not the ultimate fraud payoff, then where did the fraudsters turn once they compromised card data?

Most often (44 percent of the time) they conducted fraudulent point-of-sale purchases, which frankly, were easier to conduct before EMV chip cards were issued in the US. Only 33 percent of respondents reported fraudulent card-not-present transactions, but this number is expected to grow exponentially in the US as part of the post-EMV fraud migration.

Which of the following emerging payments options has your organization launched in the past 12 months?



Concurrent with payments breaches, the industry over the past two years has been rife with emerging digital payments methods – chief among them, ApplePay and peer-to-peer payments via near field communication.

How quick are banking institutions to embrace these emerging technologies? Not very. Only 32 percent of respondents say their organizations have dabbled with ApplePay in the past year, while 40 percent say they are just in the reviewing stage with all of these options.

Banks traditionally are conservative with their investments, and many seem to want to see these consumer technologies proven in the marketplace before they move to adopt.

Only 32 percent of respondents say their organizations have dabbled with ApplePay in the past year, while 40 percent say they are just in the reviewing stage.

Fraud Perspectives

Why U.S. EMV Migration Will Spur Global Fraud Shift

PCI's King: European Banks, Retailers Should Brace for Card Fraud Uptick

NOTE: This is an excerpt from an interview between ISMG's Tracy Kitten and Jeremy King, international director of the PCI Security Standards Counci

TRACY KITTEN: U.S. merchants now face the EMV fraud liability shift which took effect October 1. What impact might we see on fraud losses in other markets, such as Canada, which have already made the migration to EMV?

JEREMY KING: I was talking to Interac, the card Canadians get, and they were saying that what they find is when the card details are stolen in Canada the fraud would always occur in the U.S., because they could go across the border, create a mag-stripe clone card, and then use it to undertake fraudulent transactions. So it's not just in Canada that that happens -- it is around the world.

In the U.K. and in Europe, the U.S. tops all of our fraud charts, so when we see cards stolen, they turn up because it's easy to use them still in the mag-stripe environment that is the U.S. So the migration to EMV is a fantastic move forward in the fight against crime, against card theft and card fraud in the face-to-face environment, and it's been celebrated and welcomed globally. The challenge is that it is just one step. It isn't solving the whole card fraud problem, it's just tackling the biggest issue that we're facing at the moment.

KITTEN: How do you see the U.S. migration impacting other markets?

Jeremy King

KING: Interestingly enough, this year, as the migration has been gaining momentum and support, I've started talking to organizations and merchants in Europe saying: Please be aware that what we're seeing is the U.S. is getting the latest chip cards ... Their levels of security are going to be the best there are. Now the criminals will move. The criminals will now start looking for other options, and the next big option is going to be in the card-not-present space. The criminals don't have to be in the U.S., they don't have to be in Europe, they can be anywhere in the world. Are they going to target the organization in the U.S., or are they going to target an organization in Europe, where if your levels of security aren't as high as those in the U.S. you will be a target? So actually, the U.S. is going to leapfrog us slightly, and for reasons in Europe, their security is going to be at a higher level; therefore, we will be the target, and we've got to be aware -- everyone's got to be aware -- that fraud will go to the card-not-present space. They will try and steal the card data that's still in the clear text, they will use it in card-not-present for e-commerce fraud, for m-commerce fraud -- we're seeing that as the biggest fraud category in Europe, and everyone is now at risk globally. You know, this changes the whole playing field in the fraud space.

To hear the entire interview, go to: http://www.bankinfosecurity.com/interviews/us-emv-migration-will-spur-global-fraud-shift-i-2937

> "The criminals will now start looking for other options, and the next big option is going to be in the card-not-present space."

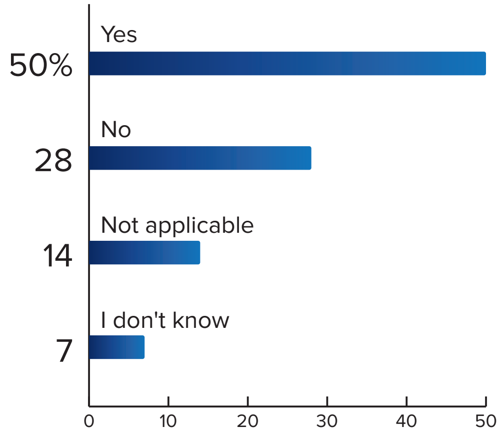
Anti-Fraud Resources

Do high-profile breaches and fraud schemes help organizations secure additional resources to fight fraud? This question arises frequently in conversations with banking security and fraud leaders.

And their response? Sometimes these incidents help. But not always.

This survey posed the question to respondents: Have recent card compromises and breaches helped your ability to secure funding for fraud prevention?

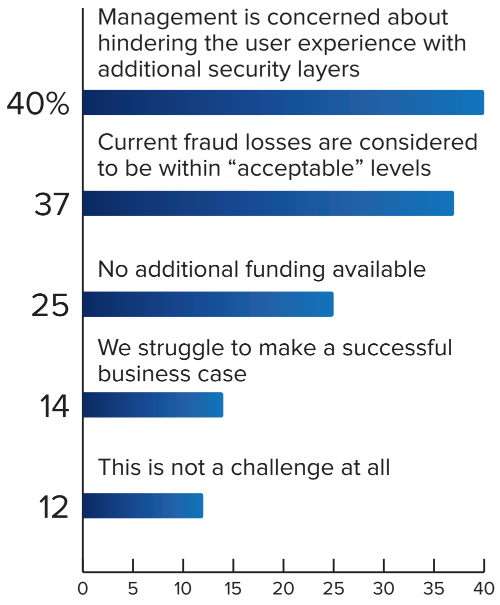
Have recent card compromises and HIGH-PROFILE breaches helped your ability to secure funding for fraud prevention?



Fifty-one percent of respondents say yes; 28 percent say no; and another 21 percent say either they do not know, or the question does not apply to them.

If resources are so hard to come by, what are the barriers?

What are the biggest challenges your organization faces when it comes to securing additional funding for fraud prevention?



Forty percent of respondents say their senior management is sensitive to hampering the user experience by adding additional security layers. After all, if users find a system or process too daunting, they will move elsewhere.

Meanwhile, 37 percent say the issue is that current fraud losses simply fail to generate significant concern. They fall within the range of “acceptable losses.”

Only 12 percent (about one-eighth) of respondents, meanwhile, claim that securing resources is not at all a challenge.

Faces of Fraud

Check fraud, account takeover and money laundering – these remain among the classic forms of fraud that banking institutions always face. But what forms are they best prepared to face?

Therein lies the disconnect.

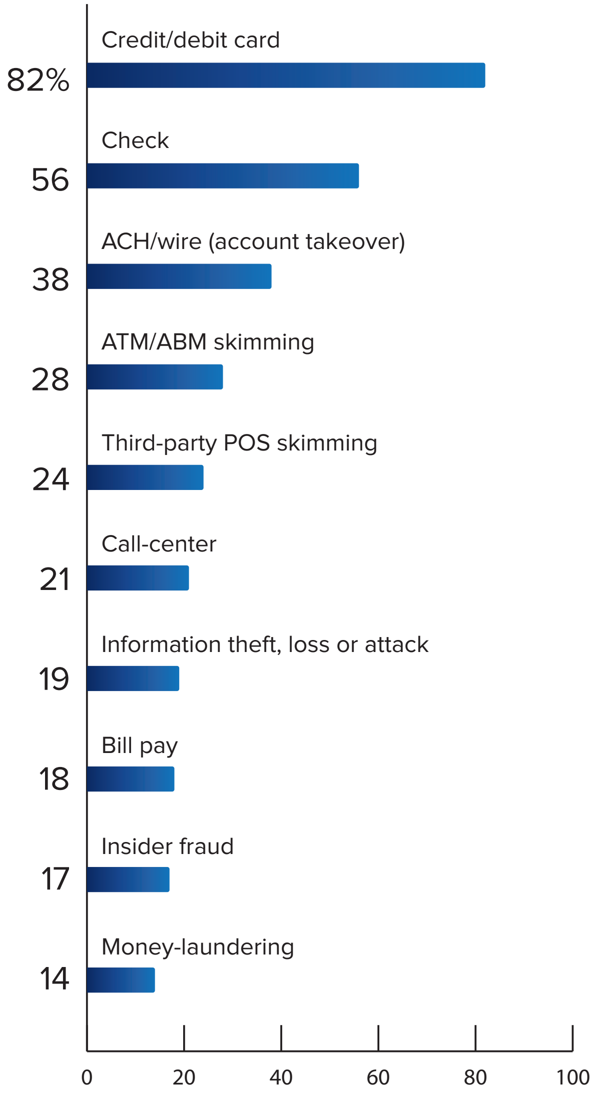
Highlights from this report section:

- 82 percent say payment card fraud is the most common form of fraud they see;
- 51 percent say money laundering is the one they are best prepared to defend against.

Next, review the full responses from this section:

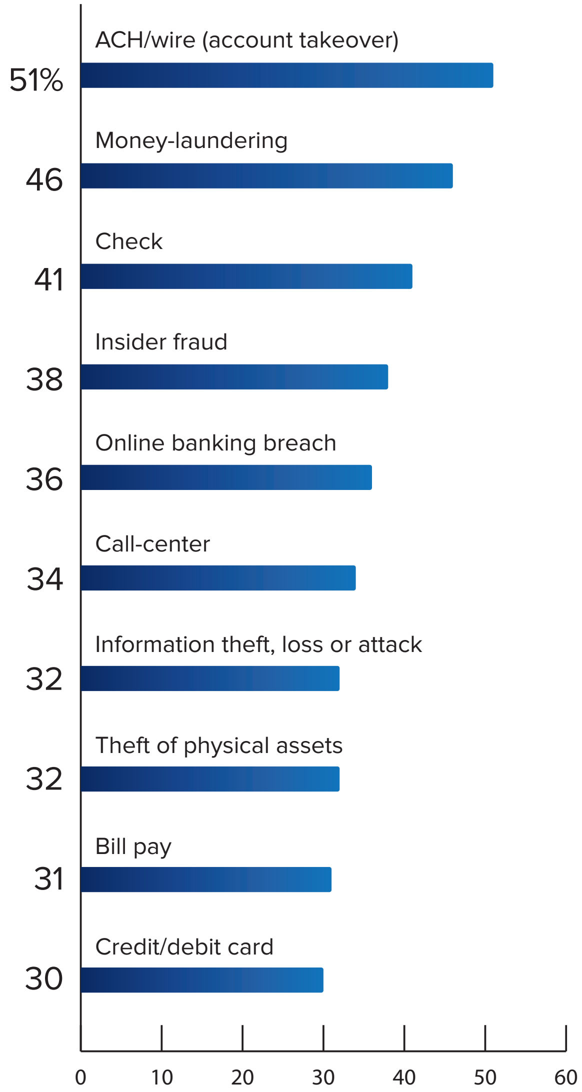
82 percent of respondents say payment card fraud is the most common form of fraud they see.

Overall, which types of fraud has your organization experienced in the past year?



No surprises here. Given the news headlines, it's expected that payment card fraud would be first on the list. Check fraud is the classic that never quite goes away – even if we do write fewer paper checks. And account takeover remains a popular crime, particularly against commercial accounts.

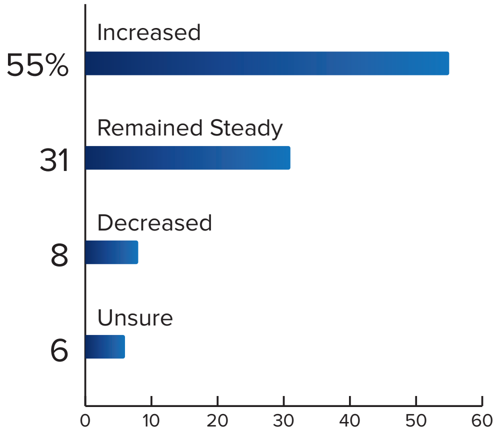
Which types of fraud do you feel your organization is currently best prepared to prevent and detect?



No surprises here, either. Yes, there is a disconnect. The top three defenses do not match directly to the top three pain points. But they do map to three areas where banking institutions feel regulatory pressure to prevent: account takeover, money laundering and check fraud.

Industry analysts expect to see a fraud shift in the coming years, as the U.S. adopts EMV technology. Will fraud defenses also shift in the months ahead?

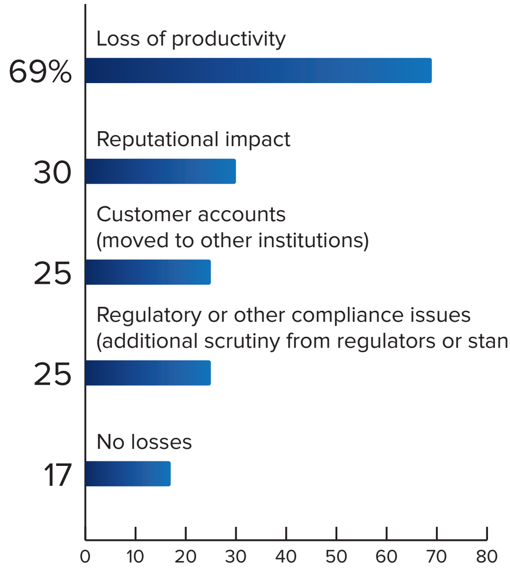
Have financial losses linked to fraud increased, decreased or stayed steady in the past year?



No matter what resources and defenses institutions have thrown into the fight against fraud, financial losses continue to mount. Eighty-six percent of respondents say financial losses have either remained steady or increased in the past year.

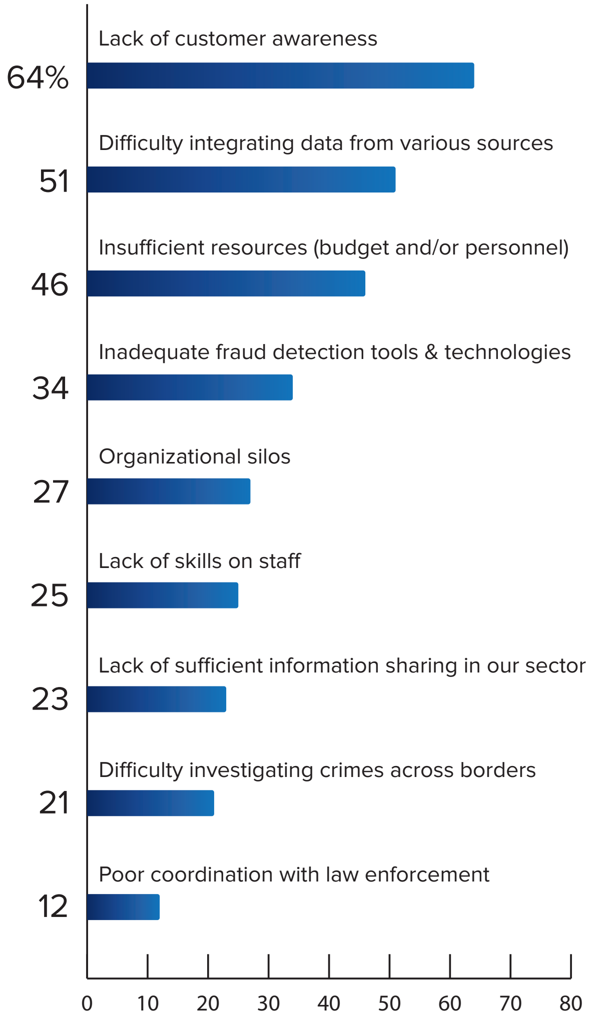
And non-financial impacts?

Beyond the financial toll from the fraud incidents, what non-financial losses did your organization suffer from fraud incidents?



Productivity takes the biggest hit. Sixty-nine percent of respondents cite loss of productivity when they have to shift resources to respond to fraud incidents. Other key non-financial impacts are reputational damage (30 percent) and customers moving their accounts to other institutions (25 percent).

Which are your organization's biggest challenges to fraud prevention?

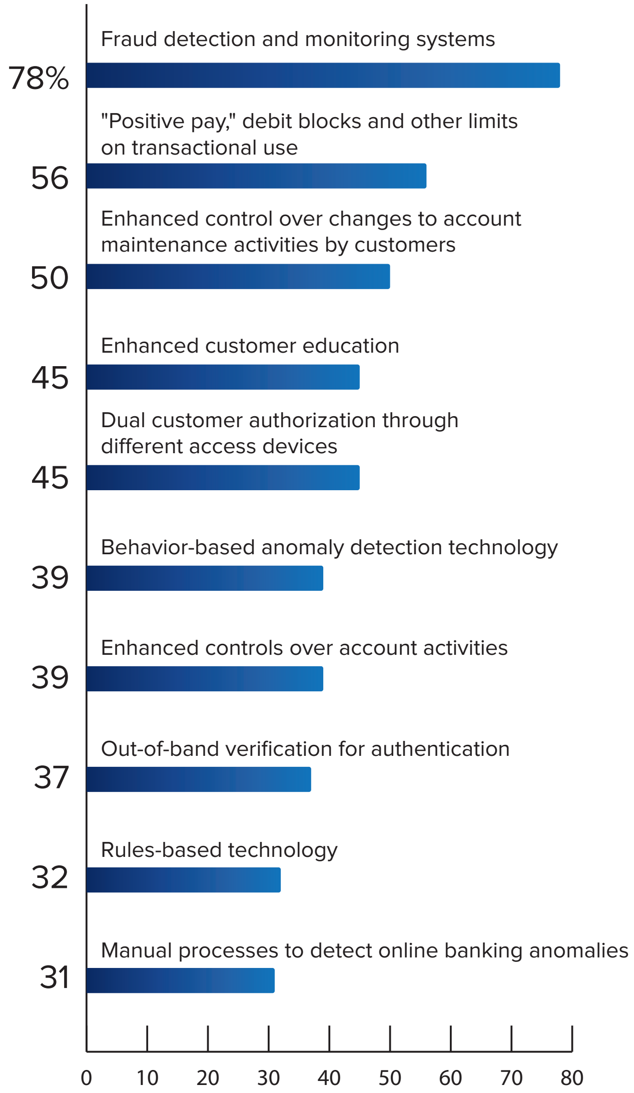


When it comes to fighting fraud, 64 percent of respondents say their biggest challenge is the lack of customer awareness. And at a time when Internet and mobile banking are emerging as the customer channels of choice, lack of security awareness plays a significant role.

Sixty-nine percent of respondents cite loss of productivity when they have to shift resources to respond to fraud incidents.

But there are other major obstacles as well, such as difficulty integrating data from disparate sources (51 percent) and insufficient budget and/or personnel to fight fraud (46 percent).

Which of these anti-fraud controls has your organization already deployed?

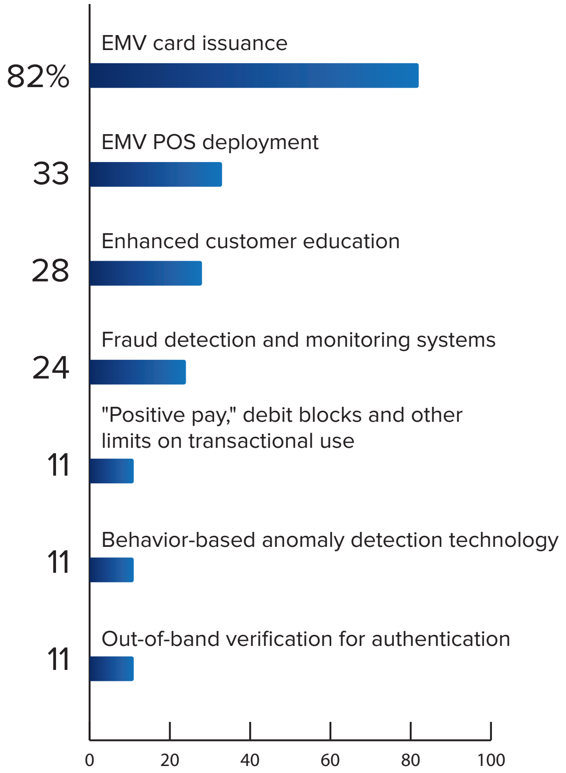


When reviewing the technology tools that organizations deploy to fight fraud, it is clear that federal regulators have had an impact. Institutions commonly deploy the controls recommended in the 2011 FFIEC authentication guidance update – fraud detection, transaction limits, dual authorization, etc.

But given the growth in fraud losses, it is clear that the prescribed controls are not sufficient.

What, then, will institutions invest in during the year ahead?

Which anti-fraud investments do you plan to make within the next 12 months?



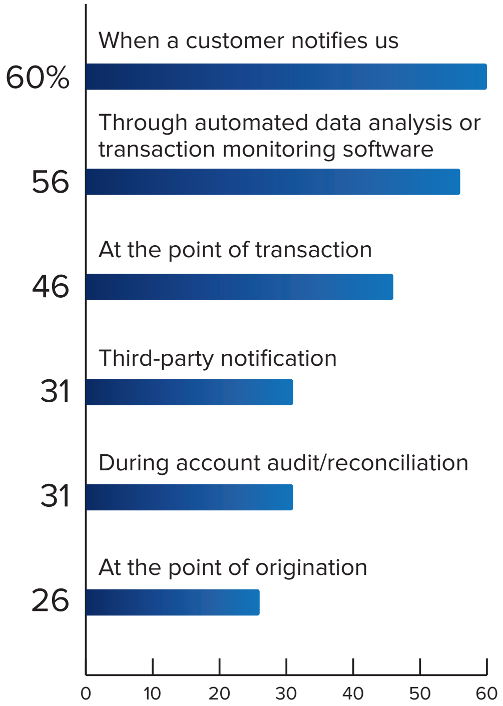
EMV card issuance is the big ticket for 82 percent of respondents. And then the priorities fall under the category of "more of the same" – fraud detection and monitoring, enhanced customer education and out-of-band authentication.

If traditional controls are unsuccessful now at preventing fraud, then it is reasonable to demand new controls. Later in this report, our analysis will offer insights into new tools being brought into the fraud fight.

Detection Debate

Detection has been a recurring theme in ISMG's Faces of Fraud surveys, and in recent years it has become increasingly common for automated tools to play second fiddle when it comes to detecting fraud incidents. This year is no exception.

How is a fraud incident involving your organization typically detected?



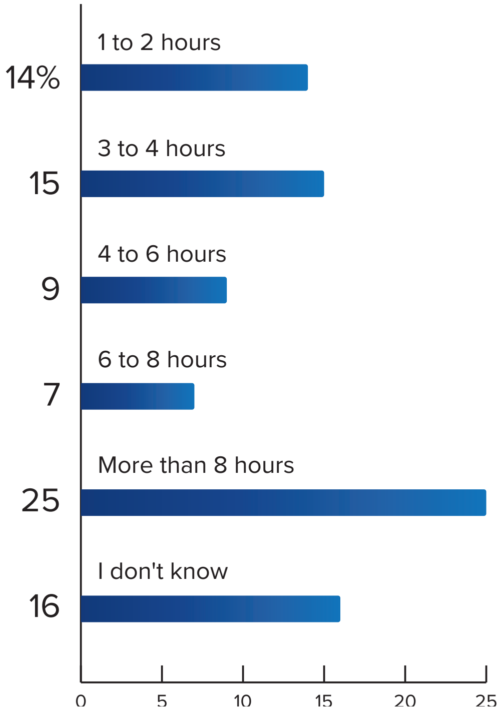
When asked how fraud incidents typically are detected, 60 percent of respondents say: "When a customer notifies us."

Fifty-six percent say they detect fraud primarily through automated data analysis or transaction monitoring software.

Other common methods: at the point of transaction (46 percent), during account audit (31 percent) and through third-party notification (31 percent).

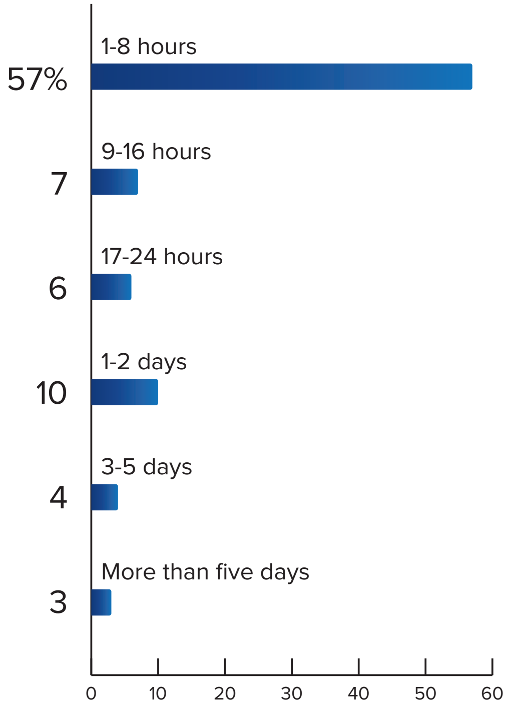
And while it is preferable for the institutions to discover fraud incidents before their customers are aware, what matters just as much or more is the speed of detection.

When fraud occurs, how long do you estimate it takes your organization to uncover a fraud incident?



And unfortunately, for one-quarter of survey respondents, it often takes more than eight hours – an entire business day – to even uncover an incident of fraud.

Upon discovering fraud, how long does it take for your organization to react, respond and resolve the incident?



When it comes to reacting, responding to and resolving fraud incidents, 43 percent of respondents say it takes more than an eight-hour business day.

And when it comes to reacting, responding to and resolving fraud incidents, 43 percent of respondents say it takes more than an eight-hour business day. In fact, 17 percent say it can take anywhere from one day to more than five.

To truly reduce fraud incidents and losses, institutions in 2016 must put a premium on improving their abilities to detect and resolve these incidents before they result in significant damage.

A Deeper Dive

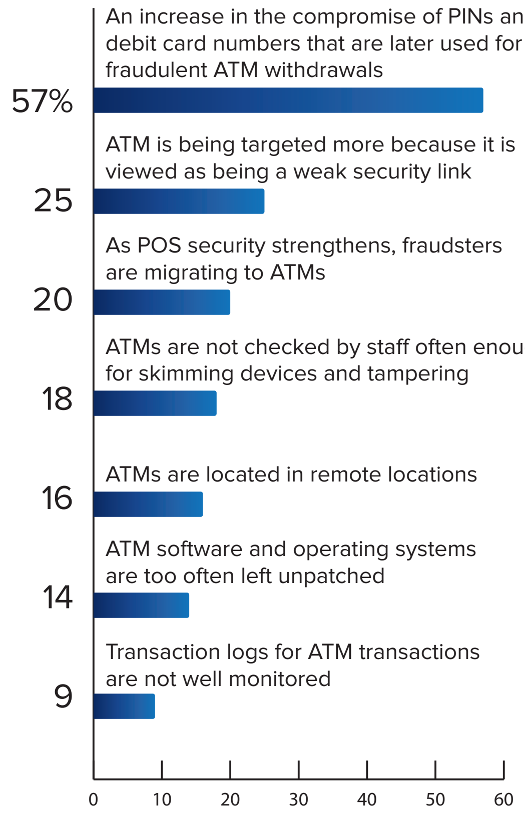
In this section, the report takes a deeper look at some specific forms of fraud and how institutions are fighting back against them. Some standout stats:

- 88 percent of respondents say incidents of account takeover have remained steady or grown;
- 56 percent say the number of targeted phishing attacks against employees has grown.

Full results follow.

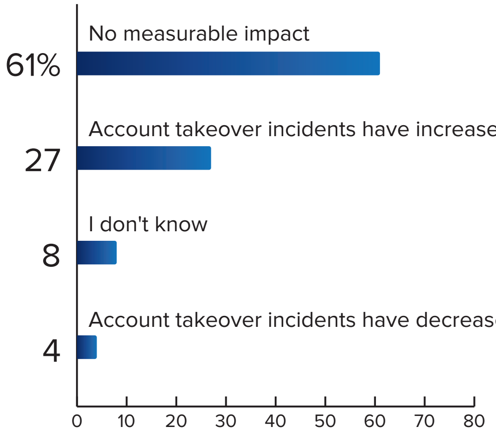
88 percent of respondents say incidents of account takeover have remained steady or grown.

If you have seen ATM-related fraud increase over the past 12 to 16 months, to what do you attribute that increase?



The ATM remains a vulnerable channel, and so the survey asked respondents where they are seeing increased in ATM-related fraud. The top responses: fraudulent withdrawals attached to compromises cards and PINs (57 percent); the ATM targeted simply because it is perceives as a soft target (25 percent); and, as POS security strengthens, fraudsters are migrating to the ATM (20 percent).

What change have you seen in account takeover activity in the past year?

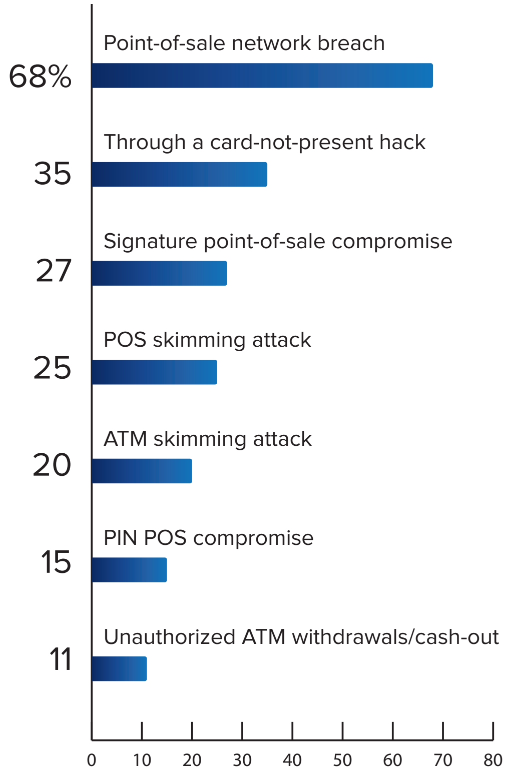


Account takeover statistics bear watching, as this was the crime the FFIEC sought to reduce almost five years ago, when it updated the regulatory guidance on authentication. Regulators spelled out specific security controls to reduce account takeover, and they established guidelines by which banking institutions would be examined for conformance.

Yet, nearly five years later, after deploying many of these controls and after being examined by regulators, 88 percent of institutions now tell us that account takeover incidents have either remained steady, or they've increased.

That is a bold statement about the ineffectiveness of traditional security controls in the face of evolving fraud threats.

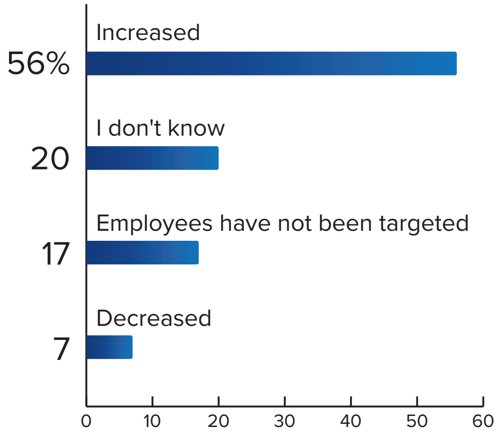
Over the past year, how were cards most often compromised?



This report established earlier that payment card fraud is the dominant crime afflicting institutions. But in which specific ways are cards being compromised?

Through POS network breaches primarily, say 68 percent of respondents. Other top vectors: card-not-present hacks (35 percent), signature POS compromises (27 percent) and POS skimming attacks (25 percent).

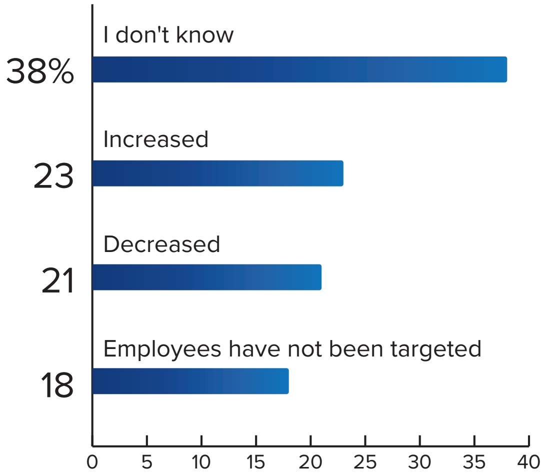
How has the number of targeted phishing attacks aimed at your employees changed in the past year?



From the help desk to the CEO, social engineering is at the heart of so many fraud schemes. And no form of social engineering is any more effective than phishing – particularly targeted phishing attacks.

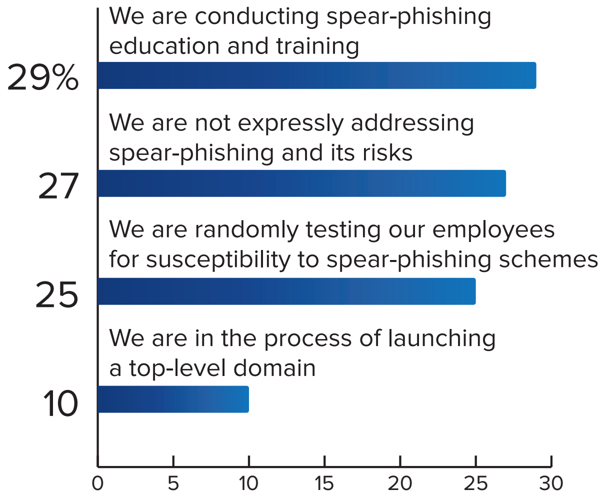
Asked how these incidents have changed in the past year, 56 percent of respondents see an increase, while only seven percent cite a decrease.

How has the number of fraud incidents resulting from these targeted phishing attacks changed in the past year?



How effective are these attempts? It's a mixed bag. Nearly one-quarter of respondents see an increase in fraud incidents resulting from phishing attacks, while roughly one-fifth see an actual decrease.

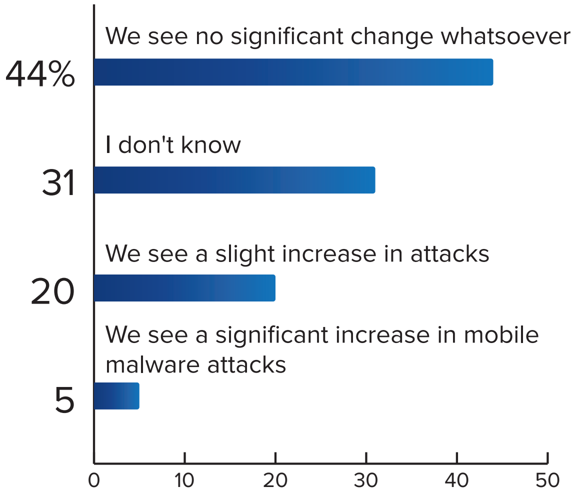
How is your organization addressing spear-phishing and its risks?



But if there is a decrease in fraud resulting from phishing, then it's owed to the efforts organizations are making to educate and test their employees. In fact, 25 percent of respondents say they randomly test their employees to see how susceptible they are to targeted phishing schemes.

Interesting to see that 27 percent of respondents are not particularly concerned about these phishing attacks.

What mobile malware trends have you seen over the past year?



Despite industry alerts that mobile malware is evolving and becoming a growing fraud vector, the average banking institution is not seeing such an uptick.

In fact, 44 percent of respondents see no significant change whatsoever in mobile malware trends, and only 25 percent see any kind of increase.

This does not say mobile malware will not be a threat in the coming months – just that it has yet to make a significant impact.

Fraud Perspectives

Why Banks Need to Prepare for More Chase-Like Breaches

Javelin's Pascual Predicts Many More Sophisticated Attacks Are Likely

NOTE: This is an excerpt from an interview between ISMG's Tracy Kitten and Al Pascual, director of fraud and security at Javelin Strategy & Research.

TRACY KITTEN: With all of the focus that banks have placed on cybersecurity, namely because of regulatory mandates in recent years, how could breaches [such as JPMorgan Chase's] still be possible?

AL PASCUAL: The fact of the matter is we know that certain types of attacks work. We know that the endpoints tend to be more vulnerable, and so I think we've seen some indication here that that could have been involved. And there was some manipulation of accounts from inside as well. So I think they kind of worked every angle, right? And ultimately that's what it comes down to: the fact that you can't depend that every door and window into your organization from a cyber perspective can be completely sealed, and so they're going to test for that weekly, and they've found them in certain places.

And so despite the best efforts of regulators, the new cyber assessment tool, updated guidance even now, it doesn't mean that we're going to be able to remediate or plan for all of these threats. So, not a surprise, but the fact of the matter is this was a complex crime. And they made money any way that they could. They had no qualms about trying different things. They were simply doing whatever worked.

KITTEN: Al, what do you think that the implications could be for banking institutions?

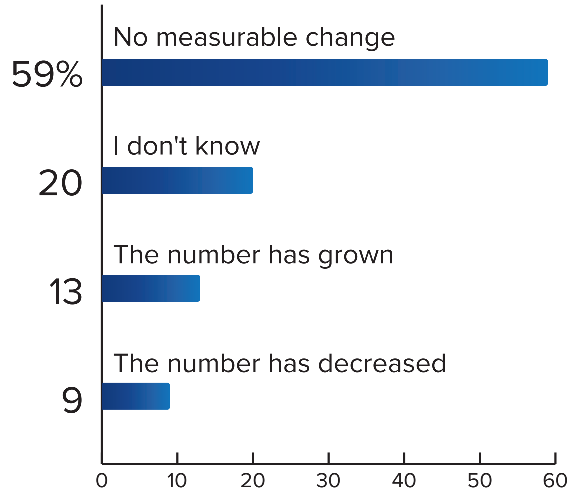
Al Pascual

PASCUAL: Well, first and foremost, I think it acts as a bit of a wake-up call. Cybercrime isn't unique to this organization or to the folks who were indicted. This level of complexity, while it is among the most complex that I've seen or heard of, it doesn't mean that there aren't others out there trying to replicate this or who have been trying to replicate this type of scale and diversity of crime. I mean, we're hearing that the Mafia in the United States is actually spread out quite a bit into cybercrime. So this is going to become much more than norm, than the outlier and so the financial industry ... should be taking this as that wake-up call, the clarion call, for action and to prepare themselves for more of this. Every bit of data that you have has value. They're going to find a way to take advantage of it. They're going to want to gain access to your systems not only to commit fraud from the accounts that you're servicing and it'll affect the trust that you have among your accountholders, but also, again, to use your good name in order to manipulate customers. And there's probably going to be schemes in the next few years that we haven't even conceived of yet. And so at the end of the day, this is going to become a tougher environment because while our city streets may be experiencing lower crime than we've seen in a decade, in most places in cyberspace, we're only just getting started.

To hear the entire interview, go to: http://www.bankinfosecurity.com/interviews/banks-need-to-prepare-for-more-chase-like-breaches-i-2980

> "While our city streets may be experiencing lower crime than we've seen in a decade, in most places in cyberspace, we're only just getting started."

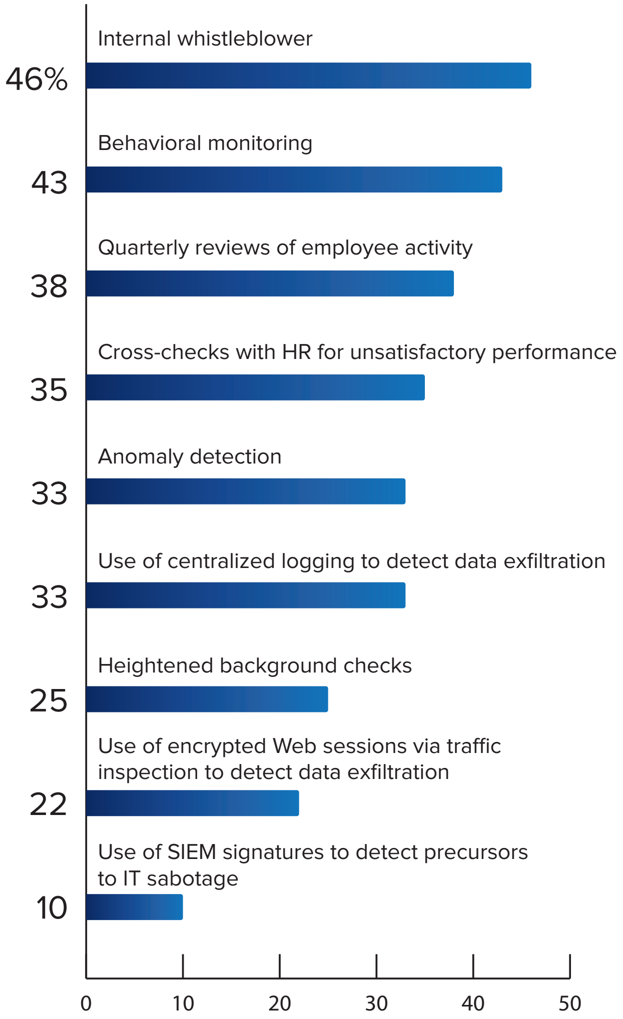
How has the number of insider fraud incidents changed in the past year?



With ubiquitous access to privileged networks from remote locations, insiders have never had more opportunity to commit fraud. And 78 percent of respondents say incidents of insider fraud have either remained steady or grown. Only seven percent report a decrease in incidents.

Worth noting that researchers today site an increase not just in malicious insider crimes, but also "unintentional insider incidents" that can be caused by malicious outsiders manipulating insiders via social engineering or other means.

How does your organization currently address insider fraud risks (select all that apply)?



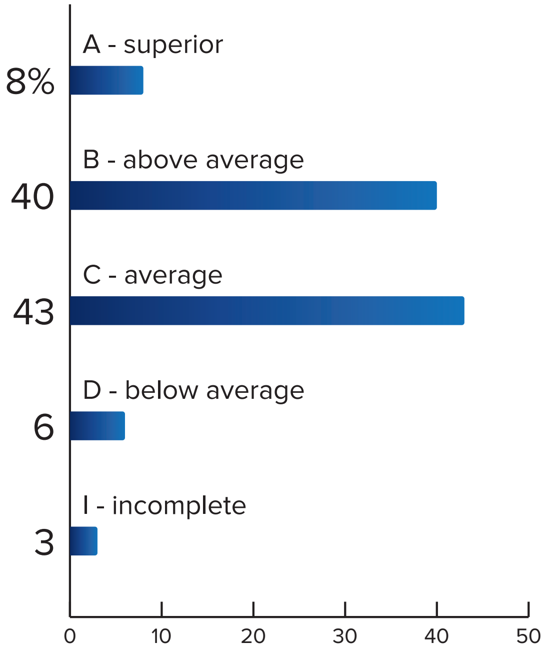
How are organizations attempting to prevent insider fraud? Through a mix of non-technology and tech-enabled solutions. Forty-six percent of organizations report use of internal whistleblowers, while 43 percent use behavioral monitoring tools, and 38 percent conduct at least quarterly reviews of employee activity.

2016 Agenda

Inevitably, when asked how they can and will improve their security posture, organizations point to security awareness. It often is cited among their biggest weaknesses as well as their biggest objective for the coming year.

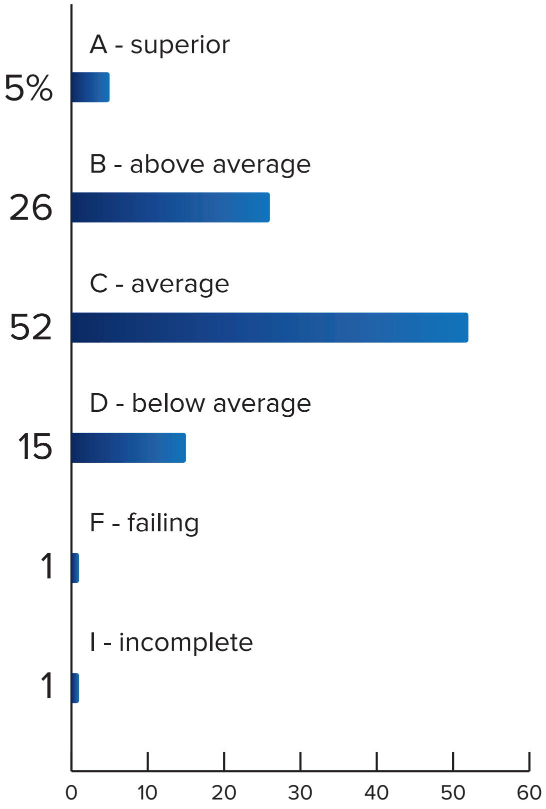
It's useful before transitioning into survey conclusions and analysis to see how organizations assess their current training programs.

How do you assess your organization's current anti-fraud awareness & training programs for employees?



For employees, survey respondents assess their anti-fraud awareness programs at average or above. In fact, 48 percent say their programs are above average or superior.

How do you assess your organization's current anti-fraud awareness & training programs for customers?



For customers, though, the numbers dip a bit. Only 31 percent of respondents grade their programs at above average or superior; 69 percent grade them at average or below.

The important point to remember: When talking about cybersecurity, "average" is not the benchmark any organization is looking to attain.

Conclusions

After years of discussing many of the same fraud topics – account takeover, fraud detection, the lack of employee and customer awareness – in 2016 we may be on the verge of a very different fraud conversation.

And not just because of the EMV rollout and likely fraud migration in the U.S. That is part of the new landscape, certainly. But so is the rise of enterprise mobility and the challenges it brings (how do you influence the security of your customer's devices?). So is the growing discussion among fraud, security and business leaders about achieving the right balance between transaction security and customer ease-of-use.

In light of the survey results and the 2016 fraud outlook, the authors of this report put forth these conclusions:

Be Wary of the EMV Fallout

For years up until now, the payments security discussion has been dominated by preparing for the EMV rollout in the U.S. Would banks be ready to issue chip-enabled cards? Would merchants have new POS terminals in place? That conversation is over, the rollout has begun, and now institutions and merchants must track what happens to fraud when card-present security has been tightened. We already are seeing an uptick in card-not-present transactions – online and via the phone. Will those numbers just grow? And will other fraud channels see similar growth? U.S. institutions need not go through this transition in a vacuum. Banks in Europe and Canada have gone through their own EMV transitions, and they have lessons-learned to share. If ever there were a time for U.S. banking institutions to practice the information-sharing gospel that has been preached, now is it. To paraphrase, all that's necessary for fraudsters to succeed is for the defrauded institutions to say nothing.

Time to Talk the 'Business Impact of Fraud'

The historic business-side pushback against granting additional anti-fraud resources is that the level of fraud incidents doesn't exceed parameters of what the institution deems "acceptable fraud losses." One can argue that "reputational damage" is missing from that debate. But there is a new point of discussion that fraud and security leaders must be prepared to dissect with business leaders: the critical balance between providing the right level of security and maintaining customer ease-of-use. Call it frictionless security. As banking customers increasingly go mobile, they are looking for the easiest way to conduct secure transactions. And if your authentication methods or transaction limits get in their way, customers will go elsewhere. For fraud and security leaders to get the resources they need in 2016 and beyond, then they need to be prepared to discuss unacceptable losses and how to ensure both security and ease-of-use.

Time to Get Serious about Detecting Account Takeover

Midway through 2016 will mark the fifth anniversary of the FFIEC issuing its updated authentication guidance. And where are we today? Eighty-eight percent of institutions say they see no change or an increase in account takeover incidents, despite anti-fraud investments they've made. And while the courts have waffled a bit on who ultimately is responsible for account takeover losses – the customer whose credentials were compromised or the bank that failed to spot the fraudulent transactions - it's time for banking institutions to realize there is much more they can do to improve authentication and anomaly detection, so they can improve fraud detection before the money leaves the bank. When customers are the top form of fraud detection, that's a problem. Institutions must resolve to tackle that problem in 2016.

Prepare for the New Faces of Fraud

It is easy, perhaps, to be consumed by the U.S. EMV rollout and the fraud migration the analysts all discuss. But there are other faces of fraud on the horizon in 2016, and institutions need to give those due attention, starting with the mobile channel. Mobile devices quickly are becoming the top channels of choice for banking customers – and the top target of choice for fraudsters and their newest exploits. How do banking institutions influence security on their customers' mobile devices? How do they migrate their static authentication methods for mobile users? How do they protect their customers and accounts from evolving strains of malware that seek both financial and user data? Fraud incidents and losses will not decrease in 2016, but the fraud conversation is likely to change dramatically.

In the next and final section, survey sponsor Easy Solutions weighs in with analysis and insight on how to put this survey to work in the coming months.

Mobile devices quickly are becoming the top channels of choice for banking customers – and the top target of choice for fraudsters and their newest exploits. How do banking institutions influence security on their customers' mobile devices?

Fraud Perspectives

Gartner’s Litan on Fraud Trends

Analyst Outlines Top Banking/Security Concerns for 2016

NOTE: This is an excerpt from an interview between ISMG’s Tracy Kitten and Avivah Litan, vice president at Gartner Research.

TRACY KITTEN: Now that the rollout in the U.S. is in full swing, do you think that we could see updates to EMV or the way that we implement EMV changing somehow?

AVIVAH LITAN: I think there are a few big issues with EMV that most parties are talking about. One is how it slows down the checkout, and the second is the PIN versus signature debate. So let’s talk about each of those separately.

On the slowdown of the checkout, it’s true that checking out with an EMV contact card takes at least eight seconds. It can take up to 10 or 12 seconds from what I’ve been told. And that’s the problem for everyone. The retailers don’t like it, the consumers don’t like it, the banks don’t want people to be turned off from their credit cards and debit cards. So luckily -- or not luckily -- but fortuitously, Visa is well aware of this issue, and they are working on a new protocol that will speed up the EMV checkout considerably. Because right now, as part of the EMV handshake, the system has to wait for the total amount to be tallied in the system, and that total amount goes into the cryptogram that’s used for the one-time code that’s part of the EMV protocol. So it expects to see this final amount, and that’s why everyone has to sit there and wait for the handshake. So what they’re working on is filling that amount up with an estimated amount for the authentication process and then wait for the total amount that’s used only for the authorization. That means you could do the authentication almost right away and then just send another message at the end. And I think Visa is trying to get MasterCard on board, and they may have a similar initiative for all I know. But these card brands are well aware that the American public is not used to sitting and waiting for the handshake, and it’s frustrating.

Secondly, you know, the security debate has been a big issue - the PIN versus signature, with the retailers wanting PINS, the banks saying no PIN. And what I’ve found out recently is that, first of all, 70 percent of transactions don’t require a signature or a PIN. They don’t require any cardholder verification because they’re under the threshold of $50.00. And according to one of the card brands, 50 percent of merchants in the United States don’t even have PIN pads associated with their point-of-sale terminal, so they can’t even accept PINS. So the argument from the card brands and the banks is we don’t take any verification on 70 percent of our transactions, and why do we want to start taking it now, with chips, and why do we want to force 50 percent of merchants to upgrade their terminals to take PINS?

Aviviah Litan

In any event, I think the PIN versus signature versus nothing debate needs more enlightenment because these new statistics I just learned about, the 50 percent merchants and the 70 percent transactions not requiring cardholder verification, shed a lot of light on why we should not introduce PINS in the United States because it would force expenses and inconvenience that may not be necessary. And we are seeing a lot of advances in biometrics that may start becoming very easy for customers to use also and as an alternative to a PIN or a signature. But

“This is one of the biggest fraud issues that banks face is: How do you know who you’re dealing with on the other end of the line?”

in general, I think what we can expect is more progress, more innovation with regards to EMV rollout making it faster, keeping it convenient, and making it much more secure than mag-stripe has been. Of course, that will push the fraud to card not present. In other countries that are EMV enabled and adopted, 70 percent of the card fraud is card not present fraud.

KITTEN: Let’s shift just a little bit to talk about some of the massive data breaches that we’ve seen over the course of the last two years with a lot of the breaches that we’ve seen in 2015 exposing personally identifiable information. With the theft of all of this PII, how is it impacting banks from a user authentication and identification management perspective?

LITAN: Theft of PII data has enabled up to 60 percent of criminals to beat the knowledge-based authentication questions that most banks use to verify identity. And I get that number from banks and from government agencies, like tax collection agencies, that tell me 60 percent of the criminals that attempt to answer those questions based on life history succeed because they’ve stolen all that data. And so this is one of the biggest fraud issues that banks face is: How do you know who you’re dealing with on the other end of the line? Whether you’re setting up a new account or executing a high-value money transfer, you can’t rely on this PII data anymore because so much of it’s been stolen.

One state collection agency for taxes told me that more of their citizens have had their identity compromised than haven’t. And when I heard that from the tax collection agency, I just kind of gasped, but I don’t know why I was surprised when you hear and you read about all these data breaches -- you know, 80 million records here, 20 million records there -- of course this is getting put to use by the criminals.

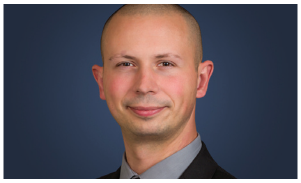
The banks have to look for alternative methods to verify customer identities, and I do know of some that are using non-PII data very successfully. They still have to use PII data with most patrons because the regulators require it, especially for money laundering and compliance. But they find that they get better results, even though they are hesitant to say that, by using non-PII data like e-mail, and phone number, and address, and device, and how all those elements link to each other, and the speed of a transaction, and how someone’s moving through the screen. So, it’s more or less the same techniques that all the big e-commerce companies are using, like Facebook, and Apple and PayPal, and lots of different methods to verify an identity without relying on PII data that’s been compromised in the majority of cases anyway. So, this is definitely the single largest issue I’m seeing them try, and thankfully there’s lots of solutions out there, but you have to be able to piece them together which isn’t always easy.

To hear the entire interview, go to:
http://www.bankinfosecurity.com/interviews/gartners-litan-ffiec-assessment-tool-falls-short-i-3044

Resources

Want to learn more about fraud prevention and the latest trends in payment security?

Check out these content resources.



Why Banks Need to Prepare for More Chase-Like Breaches
Banks need to prepare for many more massive cyberattacks along the lines of the sophisticated campaign that hit JPMorgan Chase and other financial services organizations, says Javelin Strategy & Research's Al Pascual, who offers risk management insights.
http://www.bankinfosecurity.com/interviews/banks-need-to-prepare-for-more-chase-like-breaches-i-2980

Payment Security: What Factors Are Essential?
The future of payments security hinges on a combination of factors, including widespread use of the EMV chip, tokenization and encryption, as well as near real-time payments, says Liz Garner, vice president of the Merchant Advisory Group, a featured speaker at ISMG's Fraud Summit New York on Oct. 20.
http://www.bankinfosecurity.com/interviews/payment-security-what-factors-are-essential-i-2951

Why U.S. EMV Migration Will Spur Global Fraud Shift
In the wake of the Oct. 1 EMV fraud liability shift date, U.S. merchants can expect to pay for counterfeit fraud losses previously absorbed by European issuers, says Jeremy King of the PCI Council. Longer-term, he expects European banks will experience more fraud as U.S. POS and card security leapfrogs other markets.
http://www.bankinfosecurity.com/interviews/us-emv-migration-will-spur-global-fraud-shift-i-2937

How the FBI Helped Recover Millions from Wire Fraud
FBI Special Agent Charles Gunther says collaboration with FinCEN, international law enforcement and U.S. banks has helped the FBI recover millions of funds stolen from customers via emerging wire fraud schemes.
http://www.bankinfosecurity.com/interviews/how-fbi-helped-recover-millions-from-wire-fraud-i-2906

Gartner's Litan: Top New Threats to Banks
Extortionists and "free agent" rogue insiders have emerged as the top two most malicious cybercrime threats to banking institutions, says Gartner's Avivah Litan. How should institutions bolster their defenses?
http://www.bankinfosecurity.com/interviews/gartners-litan-top-new-threats-to-banks-i-2853

Faces of Fraud: Panel Discussion
As recent incidents prove: Retail point-of-sale breaches are on the rise, creating greater payment card fraud headaches for banking institutions. How does the impact of these crimes compare to that of account takeover, check fraud, insider crimes and the emerging realms of virtual and mobile payments? Receive insights from BankInfoSecurity's latest "Faces of Fraud" survey, with analysis from Easy Solutions' founder and CEO, Ricardo Villadiego.
http://www.bankinfosecurity.com/webinars/2015-faces-fraud-london-w-825

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

(800) 944-0401

sales@ismgcorp.com

BANK INFO SECURITY®   CU INFO SECURITY® *Just for Credit Unions*   GOV INFO SECURITY®   HEALTHCARE INFO SECURITY®

infoRisk® TODAY   CAREERS INFO SECURITY®   Data Breach® TODAY Prevention. Response. Notification.

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com