

SURVEY RESULTS REPORT



2014

# ***FACES of FRAUD***

## **THE IMPACT OF RETAIL BREACHES**

ISMG's Latest Research into Top Financial Fraud Trends, Solutions

### **INSIDE:**

Complete Survey Results

In-Depth Analysis

Expert Commentary

Sponsored by



# From the Editor

## 2014: The Year Fraud Hit Home



Tom Field  
VP - Editorial  
Information Security  
Media Group

Not that fraud needs better promotion, but could the crime be any more high-profile than it's been in the months since the Target breach?

Think of the string of names we've seen: Neiman Marcus, Sally Beauty, Michaels (again), P.F. Chang's. After several years of a relatively low-and-slow assault on retail point-of-sale systems, fraudsters have succeeded at breaching several big-name merchants. And as a result, their crimes are now considered mainstream news. People who never considered payments security before are now talking about POS, PCI and EMV.

And so, frankly, are the 2014 Faces of Fraud survey respondents.

I knew going into this study that retail fraud was going to be a big topic. But I had no idea how big, nor how emotional.

Yet it's clear to me in analyzing and interpreting these results that there is no overestimating the impact of these breaches on financial institutions. And one better not underestimate the groundswell of support to overhauling our antiquated electronic payments system.

Several key topics emerge in the pages ahead. Retail fraud is foremost – see how banking institutions have been impacted by these crimes and how they believe responsibility for these breaches should be apportioned. But look, too, at some other key topics such as:

- » Account takeover – where institutions are not reporting significant changes since conforming to the 2011 FFIEC authentication guidance update.
- » New technology investments – where the power of big data analytics is increasing its influence.
- » Customer awareness – where institutions acknowledge they are failing at a mandated initiative that could help banking customers help themselves from being fraud victims.

There's much to review in this report, and I'm eager for your feedback. Write to me, please, with your own take on the 2014 Faces of Fraud. Tell me, please, what you're going to do to help write a different storyline for 2015.

Best,

**Tom Field**

Vice President, Editorial  
Information Security Media Group  
[tfield@ismgcorp.com](mailto:tfield@ismgcorp.com)

# Table of Contents

## 2014 **FACES of FRAUD**

### The Impact of Retail Breaches



Introduction .....	8
Hard Numbers .....	10

## Survey Results

Daniel Ingevaldson of Easy Solutions on How to Put Survey Results to Work .....	4
Impact of Retail Breaches .....	11
Faces of Fraud .....	16
Deeper Dive .....	24
2015 Anti-Fraud Agenda .....	34

## The Expert's View

David Pommerehn of the Consumer Bankers Association on Responding to Retail Breaches .....	14
Avivah Litan of Gartner on Context-Aware Security .....	22
David Pollino of Bank of the West on Improving Customer Awareness .....	32
Ellen Richey of Visa on the Future of Secure Payments .....	36
Resources .....	38



### Avivah Litan Interview

Gartner analyst on context-aware security.



### Ellen Richey Interview

Visa executive on the future of secure payments.

## Sponsored by



Easy Solutions is a security vendor focused on the comprehensive detection and prevention of electronic fraud across all devices, channels and clouds. Our products range from fraud intelligence and secure browsing to multi-factor authentication and transaction anomaly detection, offering a one-stop shop for end-to-end fraud protection. The online activities of over 60 million customers at 220 leading financial services companies, security firms, retailers, airlines and other entities in the US and abroad are protected by Easy Solutions Total Fraud Protection® platform.

[www.easysol.net](http://www.easysol.net)

# Fighting Back Against Retail Fraud

Daniel Ingevaldson of Easy Solutions on How to Put Survey Results to Work

So, financial institutions feel the deep impact of recent retail breaches, and they are looking toward new ways of securing electronic payments and fighting fraud. This message is resonant from the Faces of Fraud survey results.

But how can security leaders put these results to work and influence changes within their own organizations?

To help answer these questions, Information Security Media Group's Tom Field sat down with Daniel Ingevaldson, CTO of survey sponsor Easy Solutions. In this excerpt of that discussion, Ingevaldson talks about:

- » The impact of retail breaches;
- » The future of secure electronic payments;
- » The customer's role in fraud detection.

**TOM FIELD:** Where do you see the real pain that banking institutions are feeling from the Target and Neiman Marcus breaches? Do you think it's inconvenience, the financial loss, or is it this accountability that they have for breaches they really can't control?

**DANIEL INGEVALDSON:** I think really the answer depends on what size bank you're talking about. The larger banks are obviously much better equipped to be able to handle these kind of events. Just any sort of crisis management, obviously, is something that a larger bank will have more capability to deal with, and that really goes down to the cost and the resources and the amount of time they have to focus on these things, as well as certainly the bank setting aside larger amounts of



*“There’s been a lot said publicly around how we have an antiquated payment system ... The part that is underreported is the payment system works really well from a convenience standpoint.”*

---

money for a rainy day, if you will.

The smaller banks are really a different story. We talked to numerous smaller institutions, which were really hit very, very hard. They got hit with the brunt of the cost, they got hit with the brunt of the time wasted in really dealing with the event internally or the events internally. And that goes from identifying accounts at risk, identifying accounts which had been compromised, as well as the massive reissue cost, which is certainly higher for smaller banks that don't have the same volume as the large card issuers.

**FIELD:** Realistically, what can banks do about this retail breach trend?

**INGEVALDSON:** That's really the \$50,000 question. The payment system, if you look at it holistically, it's designed to very carefully balance security and convenience. There's been a lot said publicly around how we have an antiquated payment system, which goes back to using mag stripe cards and mag stripe readers for the vast majority of payments here in the US. The part that is underreported is the payment system works really well from a convenience standpoint. A lot of the reasons why contactless payments, near field communication and digital wallets haven't taken off is that credit cards are just really, really convenient. Everyone has one or many. They're very easy to use. The system works pretty well -- except for when it doesn't, when there's a large breach.

So there are a lot of things we can do, but a lot of them are incremental steps. Obviously, we should update the entire US payment system over time, but do so from a managed point of view. There's no silver bullet; there's no one solution which can solve this problem. And EMV is only really one arrow in the quiver, if you will. It's only one of the techniques we can use to cover some of the risks associated with large retail breaches, but certainly not all of them.

*“The problem is: Once you start to layer in additional security controls or additional factors for authentication, in some cases the convenience factor goes down dramatically.”*

## The Future of Secure Payments

**FIELD:** What is your vision for the future of secure payments?

**INGEVALDSON:** Again, it comes back to convenience. We could design a very secure payment system in the US, which would scale, it would provide a lot of different functionality to deal with lots of different payment scenarios, whether it's card present or card not present ... The problem is: Once you start to layer in additional security controls or additional factors for authentication, in some cases the convenience factor goes down dramatically.

EMV is something which is very powerful in securing the physical card-present transaction, actually walking into a store with a card and authenticating that card to the point-of-sale device. The problem is: EMV does not protect against the exact scenario that happened at Target and reportedly several other retailers, and it doesn't touch the online side of things either, unless an additional second factor authentication is deployed. So things get very ugly and messy and complicated very quickly.

One of the primary things that can be done, but at significant cost with a significant investment, is to enforce end-to-end encryption from

---

## *“How much fraud do you want to detect yourself internally before your customer serves as an early warning?”*

a keypad all the way to the issuing and acquiring networks, to make sure that there's no clear text credit card information ever available to malware. Tokenization comes into that; encryption comes into that; using chip and PIN, or EMV technology comes into that. But there are lots of layered incremental technologies that can make the cost of perpetrating these large credit card heists much higher and make it much more difficult or much more low probability that a large number of cards exist in one centralized place, where they can be extracted and bought and sold like you saw with the major breaches.

### Fraud Detection

**FIELD:** Institutions say that their best means of detecting fraud is through their customers. How can organizations improve their ability to spot and stop these incidents before they get the attention of the customer?

**INGEVALDSON:** The way to answer the question is to first answer a previous question: Where do you want that number to be? How much fraud do you want to detect yourself internally before your customer serves as an early warning? Because there's lots of associated costs around that issue. You know, we operate globally, so we deal with lots of different regulatory climates, lots of different political climates, lots of different banking sectors which have different rules of liability and accountability on behalf of the financial institution and the actual retail banking user. And a lot of those things determine exactly how reliant the organizations are on their end users.

We certainly believe that the best technology out there to perform pattern recognition on an account is the person holding that account. They know their activities; they know what's good or bad. They can look at a whole statement, glance past it, and they'll see something which is abnormal because they know all that activity. So, some level of customer-driven reporting is important, and I don't necessarily see that as a failure just in and of itself. I think when that becomes the most important component of an antifraud program or for actual monitoring of transactions, that's when you have problems.

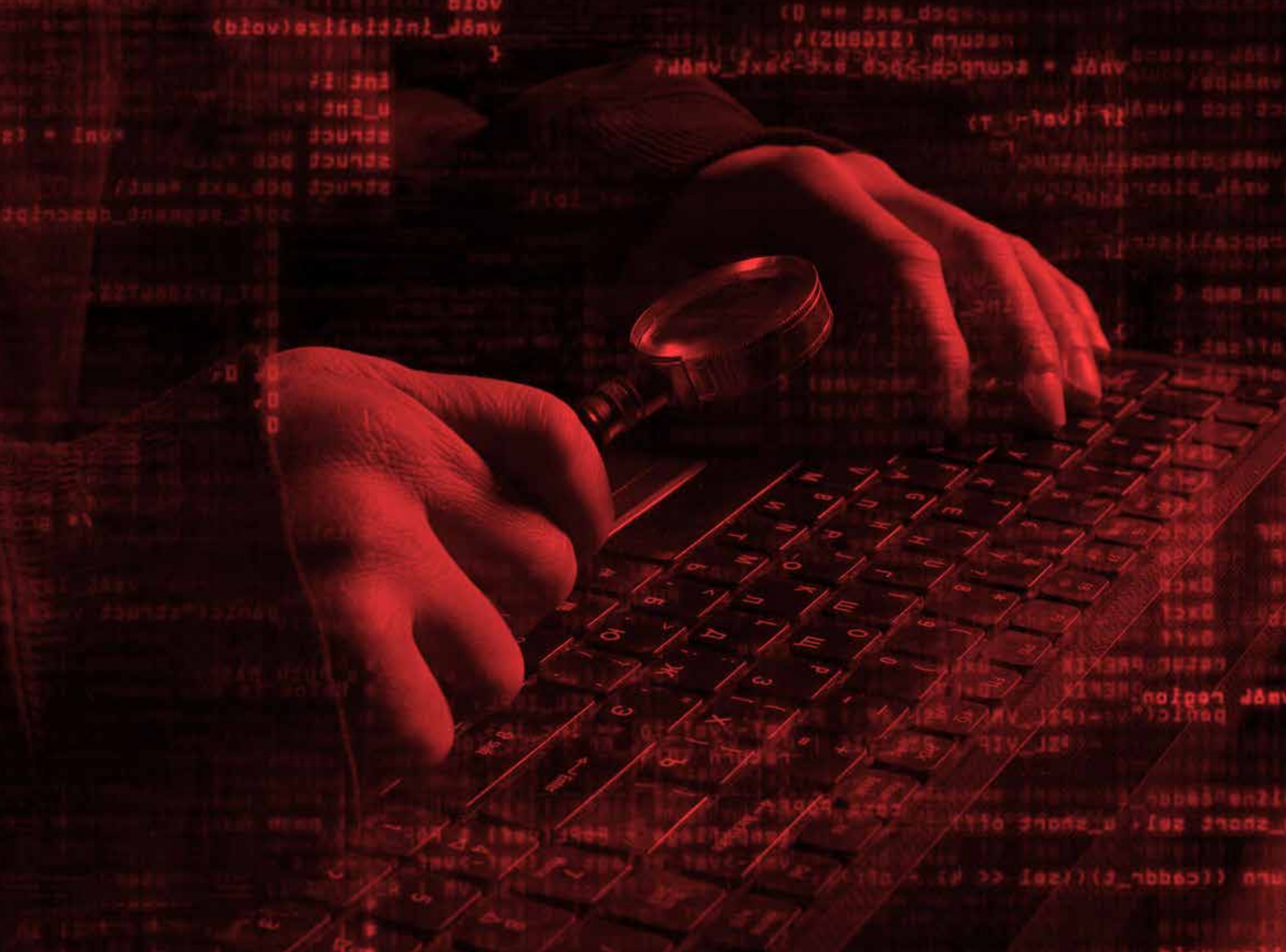
### Anti-Fraud Investments

**FIELD:** It's pretty clear that organizations have been investing in solutions that aren't effective against evolving attacks. Where must future investments be directed?

**INGEVALDSON:** We believe, of course, in multi-layer protection. It's an overused term. It's something which everyone in information security and antifraud deals with every day. To us, it's about building a truly flexible antifraud program. And I say program specifically because I'm not talking about technology, I'm not talking about products, I'm not talking about services. I'm talking about the appropriate application of all of those things rolled up into one program which is sophisticated enough to be able to manage fraud losses down, but provide flexibility when fraud losses are down to deal with the next thing.

We always look at the world through the lens of the fraud lifecycle. To move money out of an account, lots of things have to happen. There has to be some sort of campaign in a lot of cases to acquire information about an accountholder or to acquire credentials for them to log into the online banking or mobile banking environment. Attacks are then launched to gain control of those accounts and bypass two-factor authentication in some cases. And the money has to be moved around or muled around within the bank to be able to prepare for a transfer. And then of course at the last stage to be able to bypass any





risks or context-based controls to actually transfer money out.

Within a well-designed antifraud program, there are controls in place for each one of those phases. So what we try to do is to figure out the best way and the most inexpensive way to break that chain, to break that cycle, so you reduce the number of events which make it all the way around to actually moving money out of the bank.

## Final Thoughts on Survey

**FIELD:** If you were to sum up everything we've discussed and boil it down to a single piece of advice, what would it be?

**INGEVALDSON:** Resist the temptation to reduce the funding line for antifraud programs when fraud decreases. It's certainly something which should be evaluated, but carefully and realistically to make sure that the reduction of fraud is not a one-time event, but something that can be maintained and can be made persistent with our organization. That's really the mark of a very successful program that's realistic, functional and highly effective. ■

To hear the entire interview, please visit:

<http://www.bankinfosecurity.com/interviews.php?interviewID=2395>

# Introduction

---

## About the 2014 Faces of Fraud Survey

If ever we could say banking institutions are mad as hell and not going to take it anymore ...

In the wake of the Target, Neiman Marcus and other retail breaches, banking/security leaders clearly feel abused and frustrated – and they want to see changes in how merchants conduct and process secure payments. This is the key theme of the 2014 Faces of Fraud Survey, subtitled The Impact of Retail Breaches.

Some key findings about retail breaches and their deep impact:

70% of respondents say they or their customers were impacted by the Target breach, while 25% felt effects from Sally Beauty, and 24% from Neiman Marcus.

The direct impacts reported by respondents include:

**60%** reissued payment cards

**50%** lost time/resources to response

**43%** saw fraud incidents result from these breaches

48% believe the breached merchants ultimately should be held responsible for the compromises, while 28% say it's a shared blame because of the flawed payments system.

**When asked how to address breach vulnerabilities going forward, respondents prescribe:**

**57%** merchants and their vendors must be held more accountable

**56%** merchants and their vendors must encrypt customer data in their systems

**56%** U.S. must expedite move to EMV

**52%** PCI DSS must be improved and enforced.

Of course, retail breaches are not the only topic covered by the Faces of Fraud Survey. Additionally, this study continues ISMG's annual look at the top fraud trends and how banking institutions are prepared to defend themselves and their customers.

*"In the wake of the Target, Neiman Marcus and other retail breaches, banking/security leaders clearly feel abused and frustrated."*





#### **Among the hot topics to be explored in this report:**

##### **Impact of Retail Breaches**

How have institutions been struck by Target and other major retail breaches? How will they respond?

##### **2014 Faces of Fraud**

What are the primary types of fraud against banking institutions, and where are the biggest security gaps?

##### **Deeper Dive**

How have specific forms, such as account takeover and insider fraud, advanced in the past year?

##### **2015 Fraud Agenda**

Where will institutions make their biggest anti-fraud investments in the year ahead?

The survey was developed by the editorial staff of Information Security Media Group, with the assistance of members of ISMG's boards of advisers, which include leading information security, IT and risk experts.

This survey was conducted online during the spring of 2014. More than 300 respondents participated in this international study. Key characteristics of the respondent base:

**80%** are from the U.S.;

**48%** of banking institution respondents are from institutions of \$2 billion in assets or less;

**18%** of respondents are from institutions of \$2 billion or more.

# Hard Numbers

Among the statistics that jump out from the survey results:



**70%**

Were impacted by the Target breach;



**62%**

First learned of fraud incidents from  
their own customers;



**73%**

Grade their own customer awareness  
programs as average or worse.

# The Impact of Retail Breaches

It's a topic that has been simmering since the TJX breach, came to a head with Heartland Payment Systems, and now has fully exploded with the slew of recent breaches headlined by Target.

Who should be held responsible when a merchant is breached?

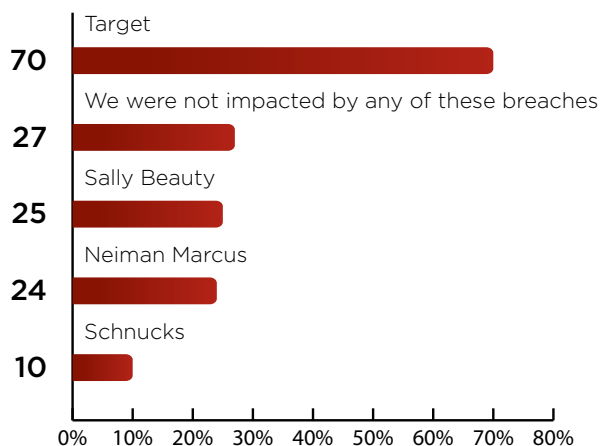
It is the bank or credit union that is continually contacting customers to replace compromised cards. And so, however unfairly, it also is the banking institution that bears the brunt of the customers' frustration. It matters not which entity is legally responsible for a breach. The average customer blames the bank.

In this "Year of the Retail Breach," we dive deeply into the topic and emerge with insights on how banking institutions have been affected by the incidents – and what they believe should happen next to improve electronic payments security.

In this section of the report, we review survey participants' responses regarding Target, Sally Beauty and the slew of recent retail breaches. These responses very much set the tone for the overall survey results. Among the key points to consider:

- » 70% of respondents impacted by Target breach;
- » 48% believe merchants should be held responsible for such compromises.

## Which Retail Breaches Impacted Your Organization or Customers?

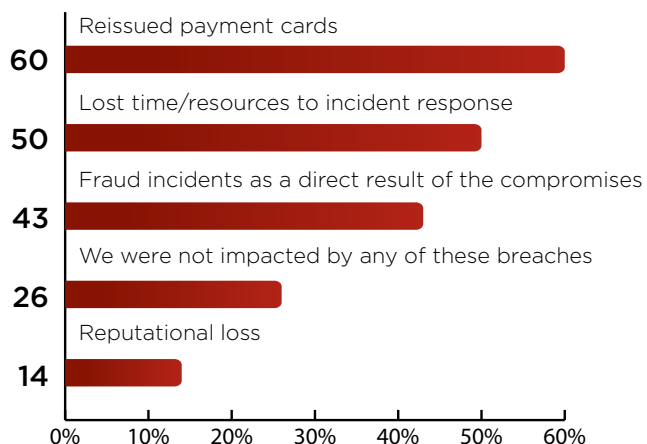


We knew the Target breach was broad in its impact. But it's still bracing to see that an even 70 percent of respondents were impacted specifically by that incident. At the same time, roughly one-quarter were affected by the Sally Beauty and Neiman Marcus breaches, which bore marked similarities.

In what ways were organizations struck? Let's review the impacts of these attacks.



### How Did These Breaches Impact Your Organization or Customers?



Like so many past breaches – TJX and Hannaford come to mind – these latest incidents have a costly impact on the institutions. And let's start with the effect that's not measureable: the amount of blame institutions absorb from customers who are frustrated to have another card replaced because of a breach. The banks are not responsible – they weren't breached – but they are playing the unfortunate role of messenger here.

As for tangible costs, you see them in the chart: the cost of card reissue, lost time/resources, the reputation hit and, of course, direct fraud losses.

### What Steps Has Your Organization Taken to Address These Risks?



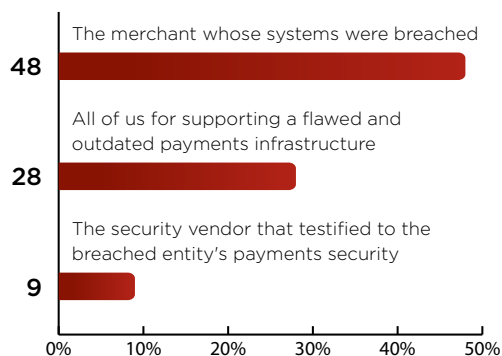
So, what are banking institutions doing in response to the outrage they feel over these breaches?

Not a lot, really.

The survey results show that banks are attempting to share more information, work with industry associations and conduct education campaigns with merchants and their customers.

And not one of these steps is being overwhelmingly adopted. When it comes to “action,” institutions, in fact, say they are doing very little.

### Who Ultimately Should be Held Responsible for These Breaches?



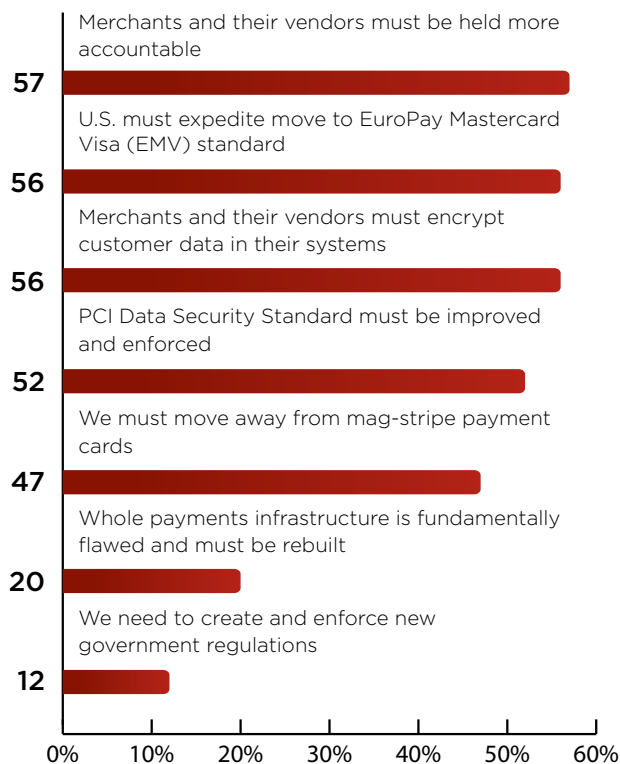
But when it comes to intent, these same respondents have some definite ideas about where blame for these breaches should be assigned.

Nearly half want to see more accountability from the merchants whose systems suffered the breach.

A small percentage want to lay some blame on whatever security vendor or assessor testified to the breached entity's security posture.

And a reflective percentage – nearly one-third – accept a share of responsibility, saying we all are accountable for continuing to support a fundamentally flawed payments system.

### What do You Propose as a Solution to These Breaches?



So, as we leave this section, what exactly do respondents prescribe as a proper solution to the retail breach rash?

Accountability is a big part of it – on the part of their merchants and their own third-party service providers.

Technology is another element, with a renewed call for encrypting customer data, so that it cannot be read when compromised.

But then there also is the acceptance that it's time for the U.S. to evolve from the outdated mag stripe payment card system and move into EMV and other modern security solutions.

With the retail breach results as our backdrop, let's review the other forms of fraud afflicting our respondents.



# Retail Breaches: Sharing the Impact

## David Pommerehn of the Consumer Bankers Association on Picking Up the Pieces after Target

In the immediate aftermath of the Target breach, the Consumer Bankers Association surveyed its 58 member banks and determined the cost to those banks had already surpassed \$170 million in losses.

In this excerpt of an interview with ISMG Executive Editor Tracy Kitten, Pommerehn discusses the impact of retail breaches and the responsibilities of banking institutions and merchants.

Pommerehn's expertise covers a wide range of legal, legislative and regulatory issues associated with consumer financial services. At the CBA, he focuses on deposits and payment issues, as well as small business banking issues. Before joining the CBA in 2008, he served as a defense attorney for the State of Maryland and as counsel to several not-for-profit financial services companies.



### Cost of Target Breach

**TRACY KITTEN:** The CBA notes that so far approximately 17.2 million cards have been re-issued by its member banks because of breaches. How did the CBA come up with those figures?

**DAVID POMMEREHN:** We surveyed member banks from some of our largest down to our small asset-size and asked them what the number looked like for them, and then we approximated that number and came up with an average of cards that were affected by this based on our membership side. One of the questions we asked them was, "How much did this cost per card to replace and all the things that go along with it?" The average amount came out to about \$10 per card, which of course includes actually replacing the plastic and sending

*"We diligently have put in systems within financial institutions to help protect our customers' information, and we'd like to work with merchants to do the same."*

that plastic to the customer, but also includes other things such as a higher increase in call center activity, customer outreach to explain the parameters around the breach, and what the bank is doing.

With smaller institutions it could be quite large; they don't have the economy of scale to bring down those costs. So, the more cards that were breached, the higher the cost are going right now.

Advice to Banks

**KITTEN:** What advice do you offer to banking institutions?

**POMMEREHN:** Banks are already pretty well-versed in the issues surrounding fraud and fraud prevention. We've been doing this for a long time. We have some of the most sophisticated fraud detection systems available in the industries. We are constantly working to innovate and improve our systems. They're checked, double-checked, and it's important to note that our customers' information and safety in using our products is one of our top priorities, and that there is actually very little breach from financial institutions and a lot of the breach comes from retailers. We diligently have put in systems within financial institutions to help protect our customers' information, and we'd like to work with merchants to do the same.

**KITTEN:** What more would the CBA like to see happen, from a legislative perspective?

**POMMEREHN:** First and foremost, to establish a national standard for security breach notification. Right now we have a fairly piecemeal system, which is state by state. It would be nice to have a standard notification system that can be utilized by both merchants and financial institutions to make sure that customers are notified in a timely manner about breaches.

We would also like to see federally-mandated standards for merchants to comply with when it comes to protecting their customer's information. Banks have standards in place currently that are dictated to us mainly through the Gramm Leach Bliley Act. But we ... think that merchants should have a similar set of standards applied to them.

*“What we would like to see is when there are costs that our incurred through breaches, that the responsible parties cover those costs.”*

There should be better sharing of threat information. There shouldn't be unnecessary legal or other barriers to effect threat information being shared between law enforcement and those responsible for breaches.

Lastly, I would say that we would like to see is when there are costs that our incurred through breaches, that the responsible parties cover those costs, such as cost of reissuing cards and making customers [aware].

We want to work with all the parties here, with the merchants, Capitol Hill, and Congress to make sure that we come to a place where we can ensure that customers can go out and use their cards without the fear that their data is going to be compromised. Let's face it; the card is king these days. Very few people use cash. ... Hackers are out there coming up with innovative ways to hack systems and break firewalls. We have to be one step ahead of them. ■

To hear the entire interview, please visit:

<http://www.bankinfosecurity.com/interviews/target-breach-cost-to-banks-i-2182>

# The Faces of Fraud

With the impact of retail breaches as our backdrop, we now move into the review of the true faces of fraud – the trends institutions are seeing and responding to now. This is our annual barometer of how financial institutions are adapting to ever-sophisticated fraudsters and their ever-evolving schemes.

In this section, we review the common forms of fraud afflicting institutions, as well as the scope and strength of their defenses. And we assess where the greatest prevention/detection gaps exist.

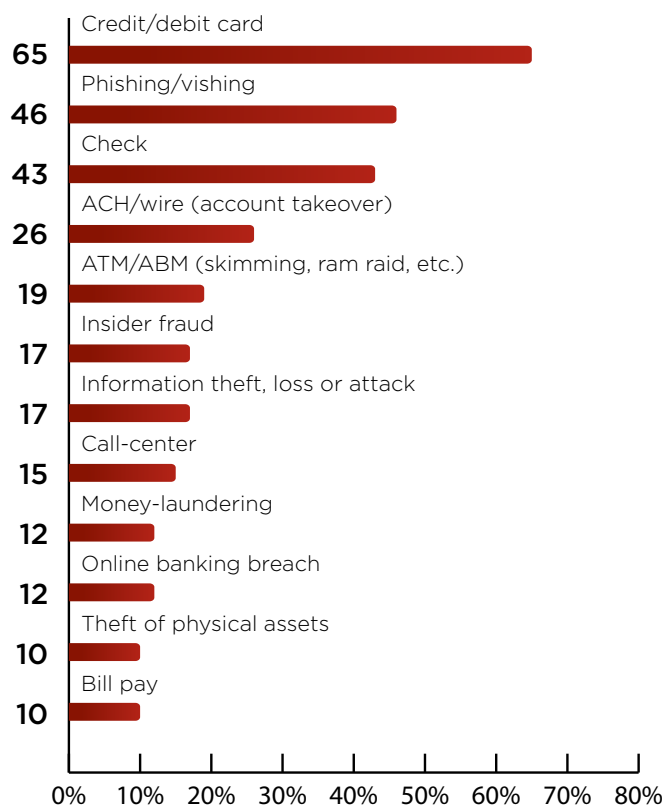
**A couple of key takeaways to start this section, and they're recurring themes in our annual fraud surveys:**

**65%** of respondents say payment card fraud is most common;

**62%** first learn of fraud from their customers.

## Key Findings:

### Top Types of Fraud Experienced in Past Year:

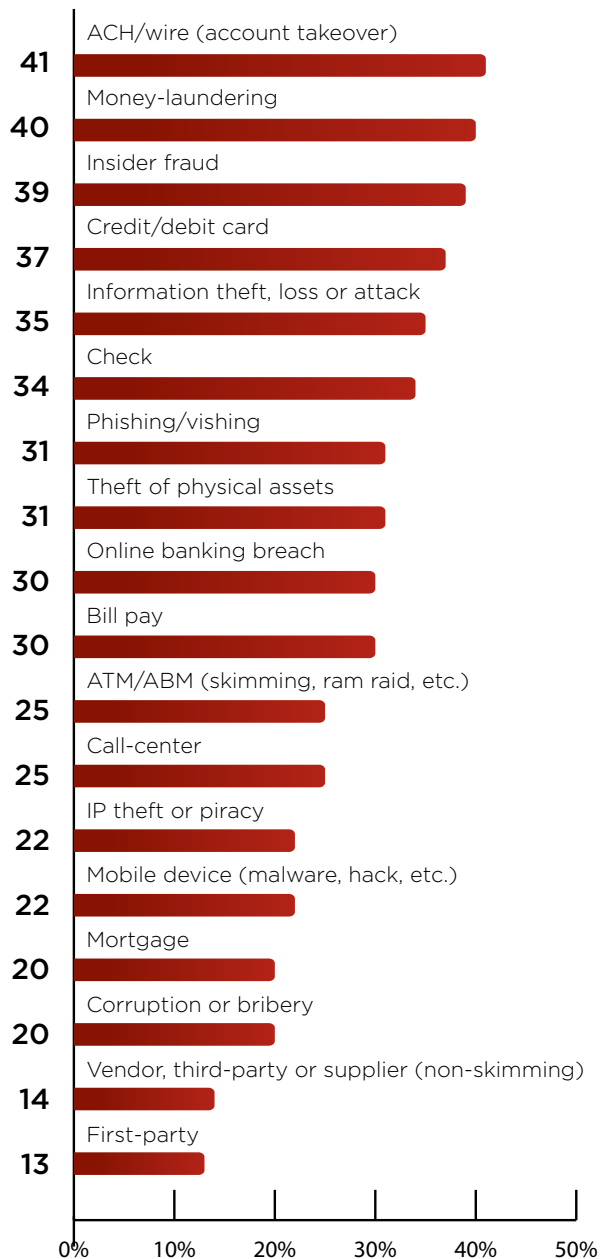


Let's begin with a look at the most common forms of fraud afflicting institutions. No surprise; they reflect what we see in the news: Payment card breaches and incidents that result from phishing in all its forms.

The perennial check fraud, too, rates highly, as it does every year. The average banking customer may be writing fewer checks, but that doesn't deter fraudsters from exploring new means of counterfeiting them.

Now, bear in mind the top three forms of fraud. Next we look at the types of fraud that institutions feel best prepared to defend against.

## Types of Fraud We're Best Prepared to Detect and Prevent

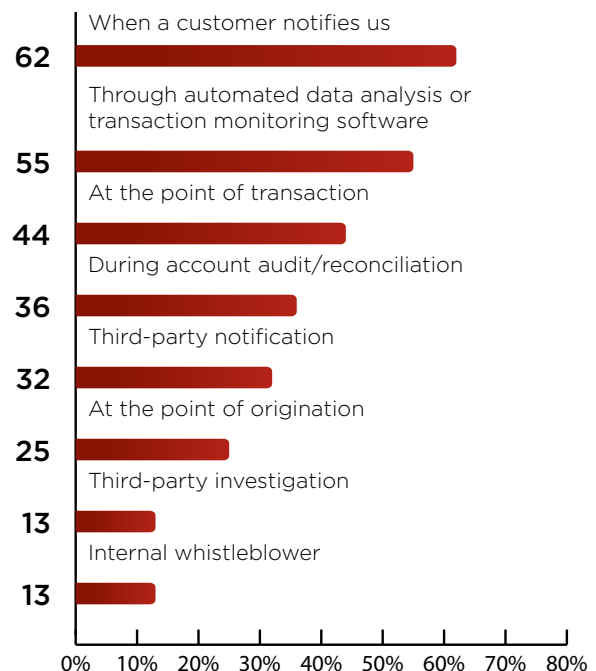


And here is where you see a stark disconnect. ACH/wire fraud, money laundering and the insider threat top the list here.

Now, there is some rationale here, and it relates to regulatory compliance. As a result of the 2011 FFIEC authentication guidance update, institutions are under enormous pressure to control account takeover attempts (which typically come via ACH/wire transactions). And money laundering has long been a huge regulatory focus. Plus, you don't have to read deeply into the past year's news to understand that all sectors have heightened awareness to insider threat and compromises that can result from malicious or unintentional behavior.

Still, the disconnect is disconcerting ... and consistent from year to year, revealing perhaps an institutional delay in responding to fraudsters' new tactics.

## How is Fraud Detected?



Another annual consistency: the prominent role that customers play in first detecting fraud incidents.

In past years, the customer element has been a secondary factor, behind technology solutions. This year it is number one, having swapped places with automated data analysis/transaction monitoring, which headed the list in the 2013 fraud study.

Given the mood from customers when they learn of fraud – and, frankly, given the resources that institutions have invested in fraud detection – it’s an unfortunate trend to see that customers increasingly are banking institutions’ best method of fraud detection.

### How Long to Detect Fraud?

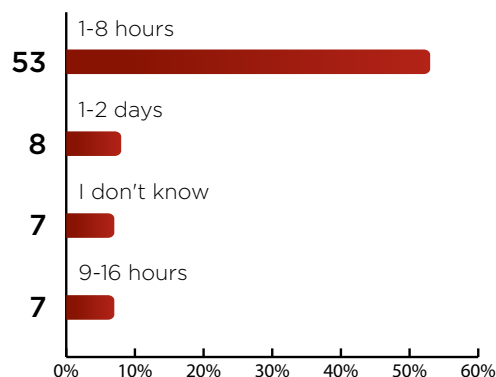


How long does it take institutions on their own to detect incidents of fraud?

Dangerously long – dangerous in that great damage can be done before anomalous transactions are spotted. For 17 percent of respondents, detection can take longer than a business day.

Worse, a fifth of responding organizations are not even certain how long it takes to detect fraud.

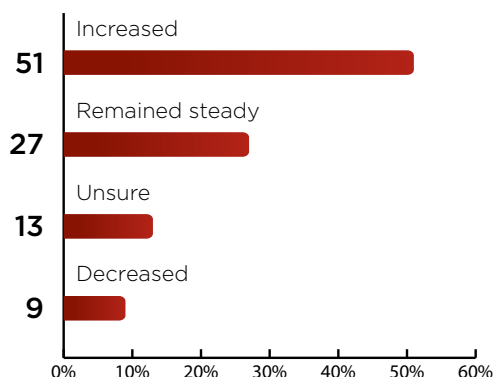
### How Long to React, Respond and Resolve?



And upon detection, how long does it take organizations to respond to and resolve incidents? Up to a business day for a majority of organizations. Again, more than enough time for significant damage to be done. And, of course, we’re discussing only the incidents that institutions are aware have occurred. This is a key differentiator. Institutions cannot measure response to incidents they do not see.



## How Have Financial Losses Changed in Past Year?

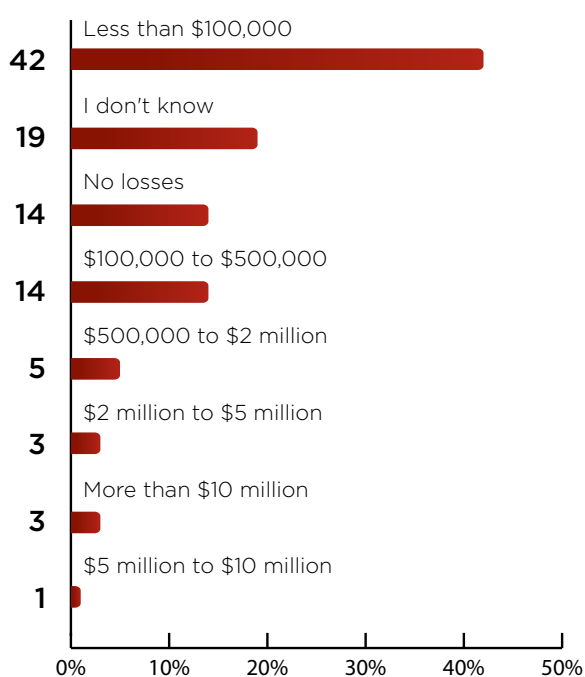


Reviewing financial losses from fraud, we uncover a disturbing trend: More than half our respondents note an increase in losses over the past year. In the 2013 study, that figure was 39 percent.

In all, 78 percent of this year's respondents say financial losses have either increased or held steady – hardly the ROI security leaders sought from their anti-fraud investments.

*“78 percent of this year's respondents say financial losses have either increased or held steady.”*

## Total Fraud Losses in Past Year

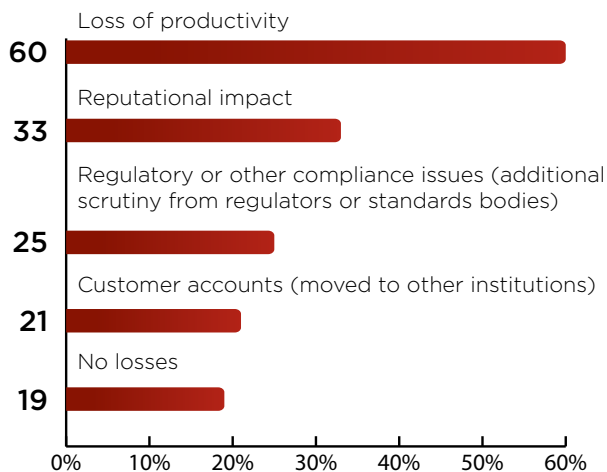


When reviewing total fraud losses, this is consistently a challenging area for our respondents to self-assess, and the numbers consistently are low. Startlingly low. A theory: respondents don't necessarily have visibility into fraud impacts across all channels, so their answers are estimates. And no one in the position of estimating fraud losses is going to guess high.

A more accurate gauge of fraud losses on an institution, perhaps, is to look at the non-financial impact.

## Non-Financial Losses

### What Non-Financial Losses Has Your Company Seen?



And here we see the consistent message from past surveys: that organizations are being paralyzed by fraud response. These incidents result in a growing loss of productivity, as resources are diverted into response roles. And the brand impact grows, as does the likelihood of a regulatory hit in the event of a breach.

These non-dollar losses exact a heavy toll that cannot be overstated.

*“Fraud incidents result in a growing loss of productivity, as resources are diverted into response roles.”*

## Biggest Challenges to Fraud Prevention

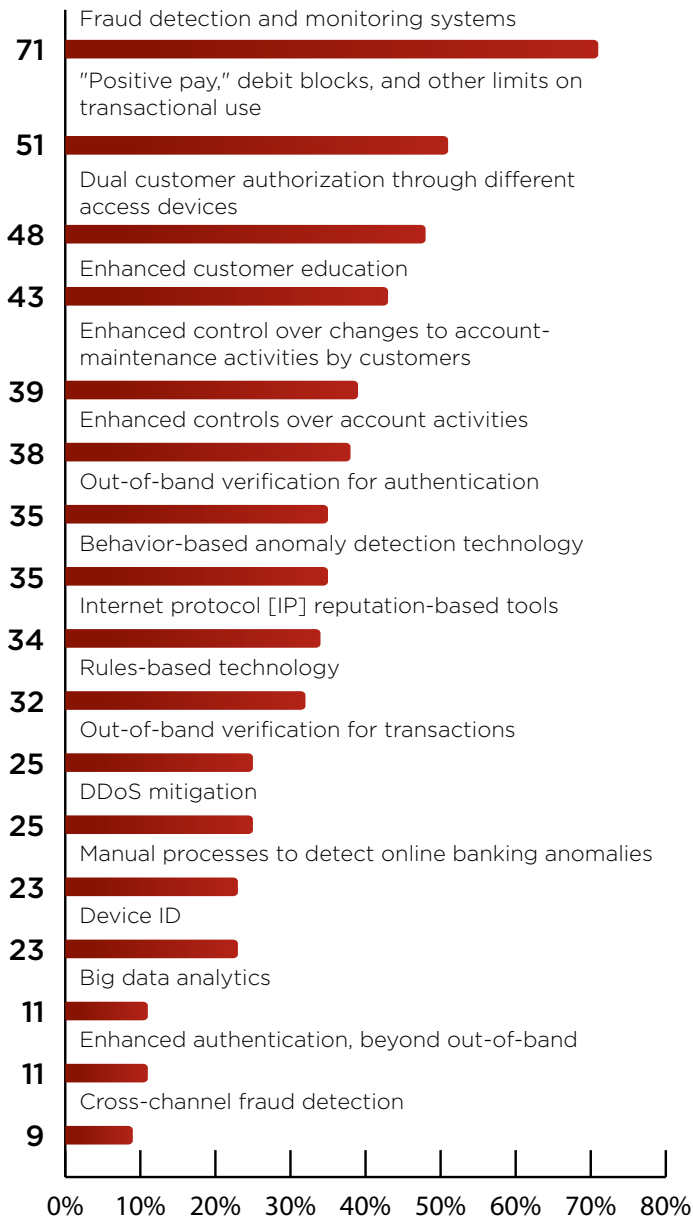


Given the backdrop we’ve just reviewed about incidents, response times and losses, what do organizations see as their biggest fraud prevention challenges?

Lack of budget and personnel creeps up the list from the number four spot to number two over the course of the past year. This is a topic to which we’ll return when we review planned investments for 2015.

But the number one challenge remains the ubiquitous topic of customer awareness. Institutions always place this as a top challenge, as well as a top priority. Yet, as we’ll see later in this overview, despite all this attention ... customer awareness still isn’t conducted effectively.

## Which Recommended Controls Already Invested?



One last stop in this section, and that's to review technology investments that organizations have already made.

The term "recommended controls" comes from the 2011 FFIEC authentication guidance update, in which several specific security controls were recommended as methods of curtailing account takeover incidents. Those controls are listed here, and you can see that institutions consistently report investments in these tools ... yet fraud incidents and losses continue to mount. Clearly, traditional tools are ineffective against evolving threats – at least as they are currently deployed.

In the next section, we take a deeper dive into specific fraud topics such as account takeover and insider fraud.

# Avivah Litan on 'Context-Aware' Security

## Gartner Analyst Describes How to Build an Effective Strategy

A multi-layered approach known as “context-aware security” is the most effective strategy for fighting both insider and external cyberthreats, says Gartner analyst Avivah Litan, who explains how this strategy works.

In the interview, Litan describes:

- » The role of data analytics in this new approach to security;
- » How multiple layers of intelligent security can help pinpoint the most relevant alerts that systems generate;
- » How context-aware security might have helped to detect the Target breach.

Litan, a vice president at Gartner Research, is a recognized authority on financial fraud. She has more than 30 years of experience in the IT industry. Her areas of expertise include financial fraud; authentication; access management; identity proofing; identity theft; fraud detection and prevention applications; and other areas of information security and risk. She also covers security issues related to payment systems and PCI compliance.

**HOWARD ANDERSON:** Could you very briefly describe what you mean by context-aware security and why we need it?

**AVIVAH LITAN:** Context-aware security is basically about making your system smarter. Right now there is not a lot of context awareness or situational awareness in our security systems. So they are pretty linear, and we can't tell a good action from a bad action in many



*“Context-aware security is basically about making your system smarter.”*

cases, because we lack that situational awareness. So for example, if someone is accessing credit card data, and that's part of their job we may ignore it. But if we've seen that the person is accessing the credit card data from 2,000 miles from their desk and they are doing this at three in the morning, then that would look unusual and it would raise a red flag.

## Circles of Security

**ANDERSON:** You've talked about using circles of security. What do you mean by that?

**LITAN:** The easiest way to think of that is the airport security. The best airports in the world, for example in Israel, have layers of security. Meaning, when you sign up for a flight they've already done a background check on you, and then you go into the airport and there is this security gate that you have to drive through. Then you go into the airport, and there is all kinds of video cameras. Then you go through questioning. Then you go through a security line. Then there is security on the boarding process. There is multiple rings of security, so by the time you get on that airplane you've been checked out. Your background is checked out. They know where you're flying. They know the context. That is the same thing with our security systems. You have to know where the person is coming from, do background checks, have different layers when they access your system -- when they get into your accounts, when they start moving money or conducting transactions. There are layers at every stage.

What's Missing

**ANDERSON:** So what's the missing element in the current security approach, then?

**LITAN:** Well one of the missing elements is there is not context awareness, as we talked about. We're not looking at these transactions in relation to past history and relation to what's happening today and relation to peers. So there is not good situational awareness, and secondly people are just doing the bare minimum they can in many cases because of budgetary constraints. They are just doing what the regulators will check off as enough. And third, if they're doing even more than that, there are a lot of siloed systems, so the alerts are going off, and people can't distinguish a false alarm from a real alarm.

***"We're not looking at these transactions in relation to past history and relation to what's happening today and relation to peers."***

## Breach Prevention

**ANDERSON:** You mentioned that this could have theoretically helped with detecting the Target breach. How is that?

**LITAN:** By putting these layers of security in and making what they had more intelligent -- for example in the Target case. We all know from the press that there were alerts that were generated by a threat detection system, but they weren't in context of anything else. You have to imagine that Target is probably getting thousands of alerts a day, so why should these two alerts be that important? Even if they're high priority, there are other high priority alerts.

So what context-aware security does is it correlates the alerts coming out of that threat detection system with other access alerts. For example from different layers of the stack, so it's making each layer smarter and correlating them and now you can see the alerts you really need to pay attention to. So if Target had these kind of layered systems that were intelligent, the thinking is that these alerts that they did get and didn't pay attention to would have been highlighted as: You've got to pay attention to this because this is correlated with other things that we've seen in your organization in the enterprise and you really have to pay attention to this. It's not an isolated event. ■

To hear the entire interview, please visit:

<http://www.bankinfosecurity.com/interviews/avivah-litan-on-context-aware-security-i-2317>



# A Deeper Dive

## Account takeover, mobile banking and the insider threat are all key fraud topics worthy of further analysis.

And they are among several specific fraud topics we touch upon in this section of the overview. We then conclude with a look at how organizations self-assess their security awareness efforts.

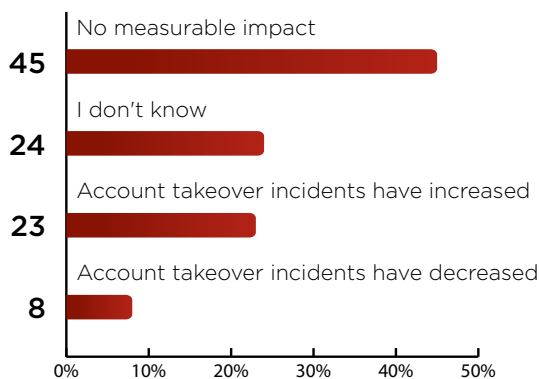
A couple of key data points to consider upfront:

- » 45% see no measureable impact on account takeover incidents post-FFIEC update;
- » 73% grade customer awareness programs at average or below.

### Key Findings:

#### Account Takeover: Impact of FFIEC Guidance

##### Following Investments, What Impact on Account Takeover?

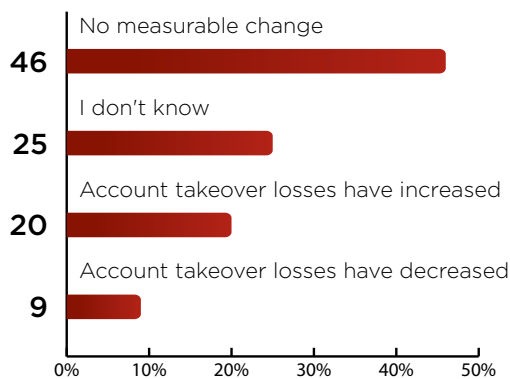


We start with account takeover because that is the topic that has inspired so much regulatory action in recent years.

Yet, despite the attention, the FFIEC update and the investments in recommended controls, 68 percent of respondents say that incidents either have increased, or there has been no measureable impact. Only eight percent note a decrease.

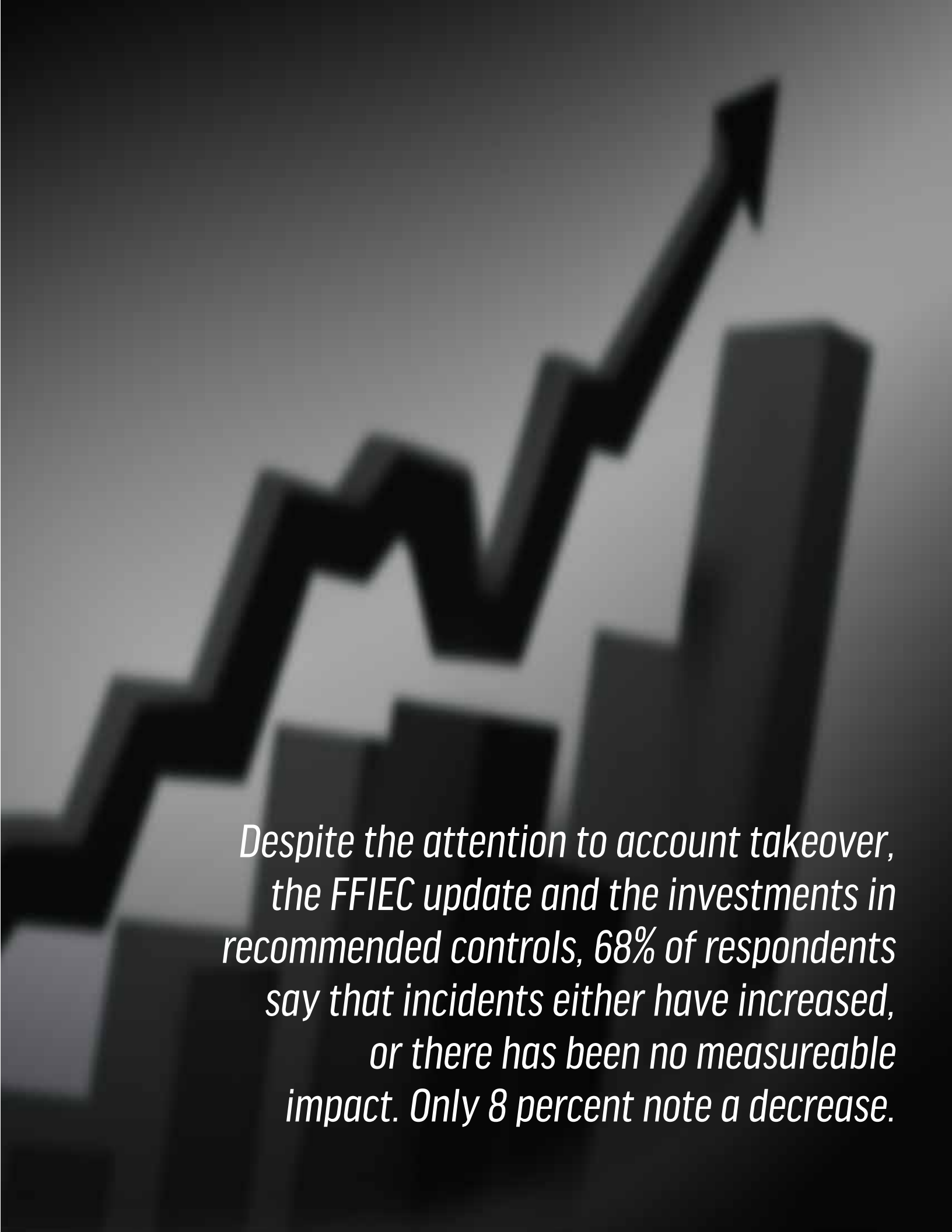
This number is up significantly from 2013, when 56 percent noted an increase or no measureable impact.

##### Impact on Account Takeover Losses?



And in terms of losses attributed to account takeover, the numbers are the same this year as last: 66 percent of respondents see either no measureable impact or an increase.

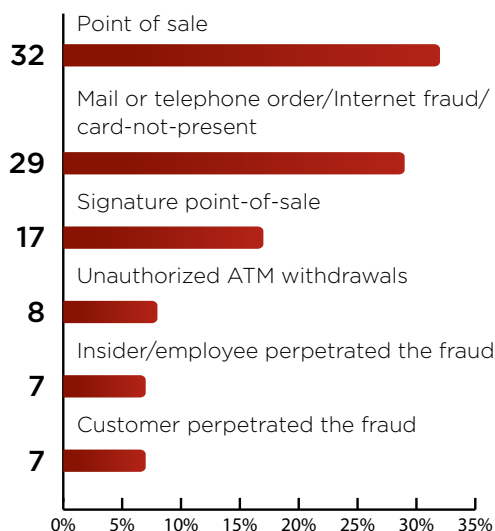
The message: either the schemes are evolving beyond the solutions; the solutions are inadequate ... or both.



*Despite the attention to account takeover, the FFIEC update and the investments in recommended controls, 68% of respondents say that incidents either have increased, or there has been no measureable impact. Only 8 percent note a decrease.*

## Payment Card Fraud: The Rise of Card-Not-Present

### How did they occur?



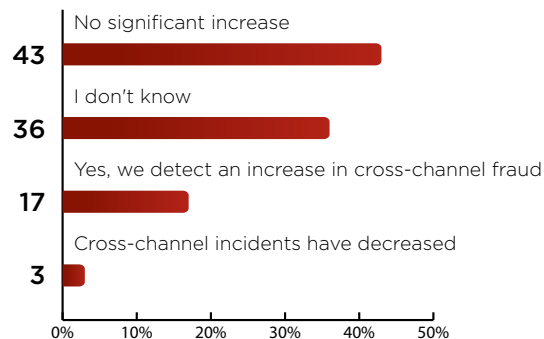
We've spent a fair amount of time discussing payment card fraud already, so we won't dwell on the topic again here.

Worth noting, though, is the growth in point-of-sale incidents from 18 percent in 2013 to 32 percent this year, with card-not-present fraud very close behind.

With all the industry discussion of EMV solutions – which do not impact card-not-present incidents – these figures are worth consideration.

## Cross-Channel Fraud: Under the Radar?

### Detected a Rise in Past Year?



Cross-channel fraud is a complex topic in this survey. A significant number of respondents note no significant increase in incidents – but they also have told us they lack the abilities to easily detect fraud in their systems.

In fact, if a majority of respondents are waiting for their customers to inform them of fraud incidents, then it's no surprise there may be an inability to detect cross-channel schemes.

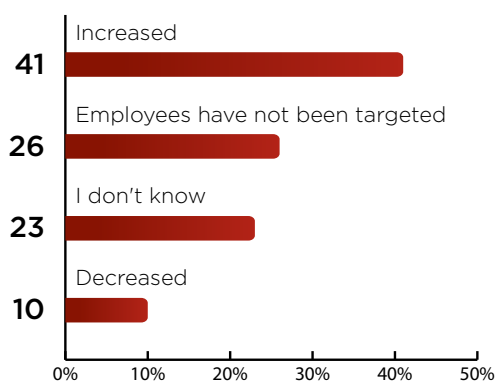
The number of such incidents is likely much higher than respondents report, and we do discuss this topic at length in our survey analysis.

*“Worth noting is the growth in point-of-sale incidents from 18 percent in 2013 to 32 percent this year.”*



## Phishing: Where Targeted Attacks are Born

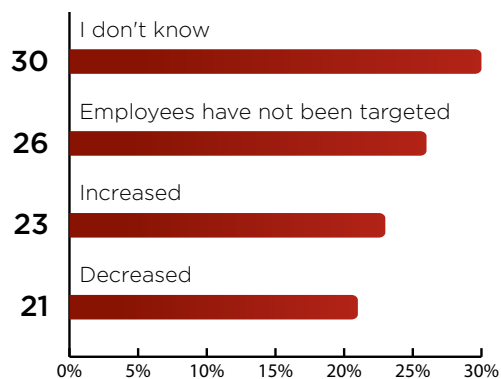
### Attacks on employees over past 12 months:



One of the hottest topics of the past year has been the targeted attack, which often is carried out via sophisticated phishing schemes that lure unsuspecting users to visit sites or click on links that imbed malware.

As you can see, phishing remains a growth scheme, with 41 percent of respondents noting an increase in attacks on employees.

### How Has the Number of Fraud Incidents Tied to These Attacks Changed?



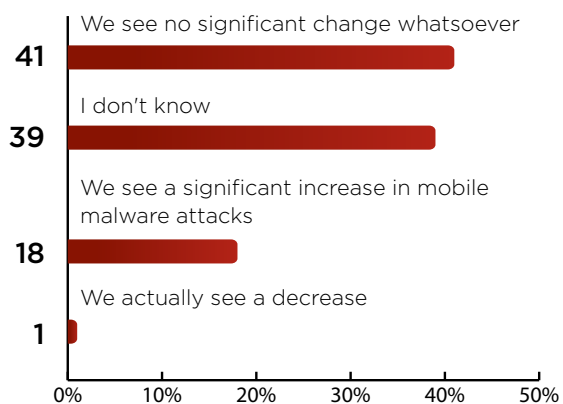
In terms of losses attributed to phishing schemes, respondents offer a mixed message: nearly as many see an increase as they do a decrease.

Of greater significance, though, is the 30 percent "I don't know" figure, which is a testament to inadequate detection.



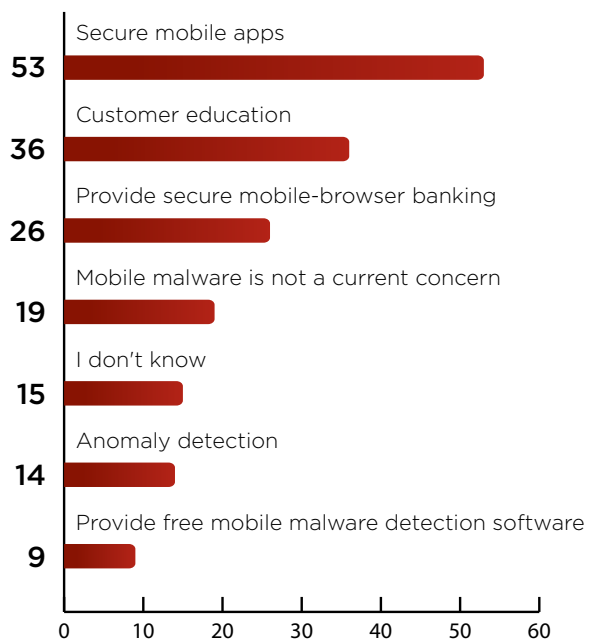
## Mobile Malware: Steady Growth

### What Mobile Malware Trends Have You Seen in Past Year?



Mobile remains both an emerging channel and an emerging fraud vector. Nearly one-fifth of respondents see an increase in mobile malware – a data point that matches what industry researchers tell us of the rise of such incidents.

### How do you defend against mobile malware?

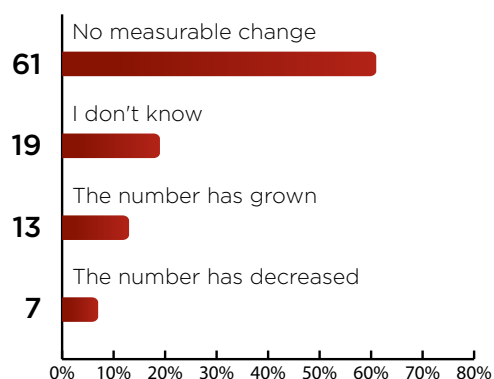


And when we review how institutions currently are defending the mobile channel, the responses are consistent year-to-year. Secure apps and customer education are the top responses by far. We'll return to that latter topic very soon.



## Insider Fraud: 'Low and Slow' Rings True

### How Has Number of Incidents Changed?

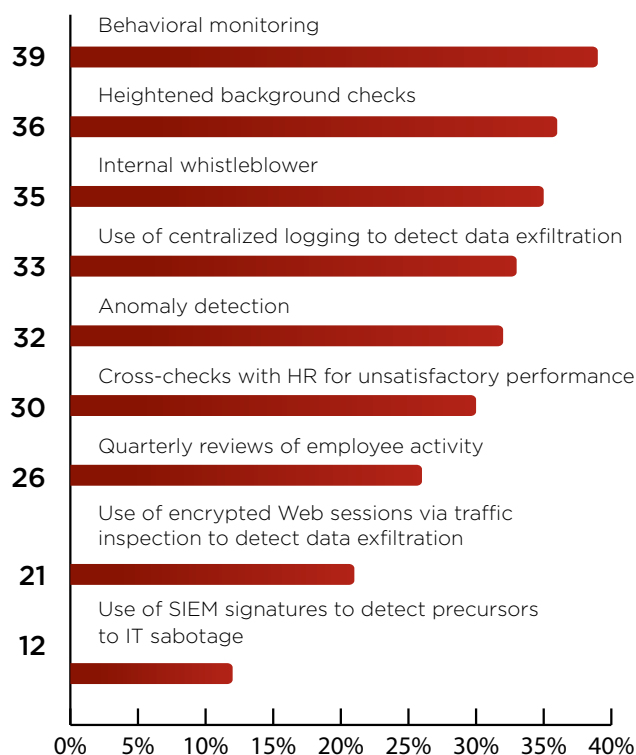


For our last specific fraud topic, let's review insider incidents. Despite the attention given to the topic by the NSA/Snowden affair, the stats have not changed substantially since last year. Seventy-four percent of respondents say the number of incidents has either stayed the same or increased.

*"If the topic of insider fraud is getting so much attention, why aren't the numbers going down?"*

Which begs the question: If the topic is getting so much attention, why aren't the numbers going down?

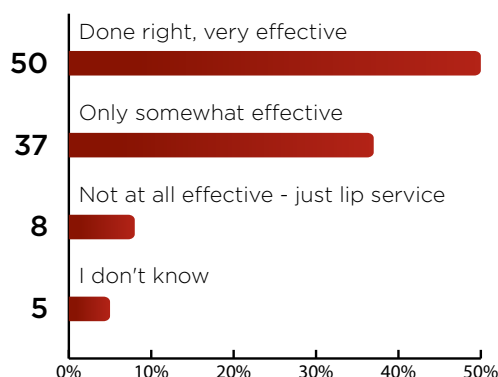
### How Do You Address Insider Fraud:



Security controls for insider fraud also are consistent. Organizations say they are investing in anomaly detection, background checks and even internal whistleblower programs. But clearly malicious insiders are succeeding at their 'low and slow' schemes, and unintentional insiders are being manipulated under the radar.

## Awareness and Training: Average = Failure

### How Effective Are Awareness & Training Programs in Reducing Fraud?



Now we get to the topic everyone wants to discuss, but no one seems to do well: awareness.

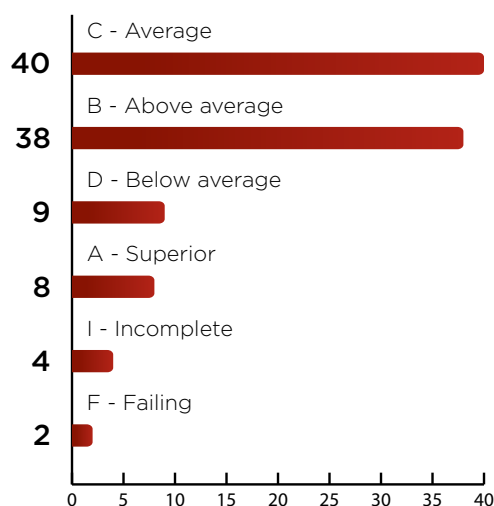
Regulators demand it, institutions say they prioritize it. But how effective are awareness programs?

Done right (however one defines “right”), 50 percent of our respondents say these programs are very effective. Of course, 50 percent is hardly a ringing endorsement for a program done right.

Thirty-seven percent say these programs are only somewhat effective.

Now, let's look at employee awareness vs. customer.

### How Do You Assess Your Current Programs for Employees?



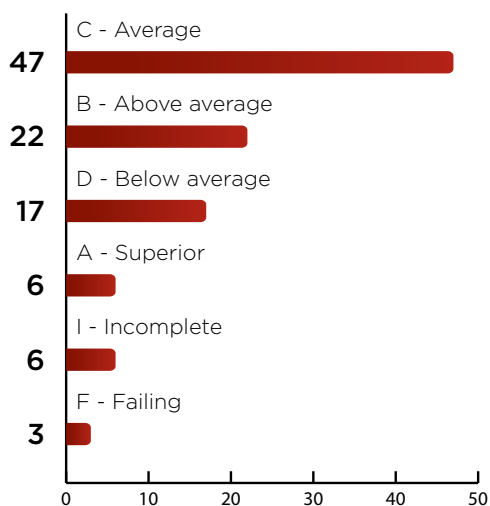
On the plus side, 46 percent of respondents give their employee awareness programs an A or a B.

But more significantly, that leaves 54 percent assessing themselves at average or below.

At a time when targeted attacks against employees are giving fraudsters access to the financial crown jewels, “average” is not a good benchmark for employee awareness.



#### How Do You Assess Your Programs for Customers?



The news for customer awareness is only worse.

Here, a full 73 percent of respondents rate themselves at average or below. That is a stunningly low figure, given the amount of attention regulators and institutions alike have paid to the topic of awareness.

And it's one that security leaders must ponder as they consider how to respond to evolving fraud threats in the year ahead. The fraudsters clearly are getting smarter and more effective. What can we do to arm employees and customers with greater awareness to the signs of these schemes?

# Social Media's Role in Fraud Prevention

## How Bank of the West Is Beefing Up Customer Awareness

Because most online banking customers are active social media users, banking institutions should leverage social media in their fraud awareness campaigns, says David Pollino of Bank of the West.

As fraudsters' social-engineering tactics have evolved, it's become crucial for banking institutions to use social media to help customers understand emerging cyberthreats, says Pollino, Bank of the West's enterprise fraud prevention officer.

During this interview, Pollino discusses:

- » How Bank of the West measures the success of its social media educational campaigns;
- » Why getting buy-in from upper management, and ensuring executive teams are up to speed about customer awareness campaigns, is a critical to success;
- » How Bank of the West shared information with its customers about the Target Corp. attack, and news about online risks, such as the Heartbleed bug

Pollino is a senior vice president at Bank of the West, where he has worked since 2011. Previously, he served as manager of online fraud-prevention strategy and analytics for Wells Fargo and was the online risk officer for Washington Mutual. He has a background in information security and combating online fraud. Pollino also is an information security author and conducts ongoing research on cybercrime techniques.



*“We’ve tried to make sure that we’ve modified our education, so it’s more relevant in this day and age.”*

**TRACY KITTEN:** David, what steps has your institution taken to address customer education?

**DAVID POLLINO:** Well, we’ve seen a lot of the classic social engineering scams that started in the real world with phone calls, letters and those

types of things migrate to the online world. We've seen scams such as the 419 scams, the foreign lottery scams, collection scams targeted against business, and even romance scams which would take place in the physical world migrate into the online world. It's important for our customers to understand these issues and be able to protect themselves, because in many cases if they are scammed they may be financially liable for the losses.

But what we've done at our financial institution is we've tried to make sure that we've modified our education, so it's more relevant in this day and age. We've tried to put together short digestible chunks of information that are convenient to our customers. And that has involved not only updating our content on our security and fraud centers on our website, but also being actively engaged with our social media team and making sure that our content is finding regular eyes through our social media channels.

We found that in many cases our customers are getting information through social media, and sometimes just the headline or just getting the impression is important enough for the thoughts to come across. For example, I might not necessarily like or comment on a Facebook post about my aunt traveling to Hawaii, but just by going through my Facebook page I know and I'm aware that my aunt might be traveling to Hawaii. It's the same way with some of our fraud and security content that we put on Bank of the West. Because of our presence in social media, we are getting the ideas and the thoughts out, and hopefully creating a more informed customer, which means a better customer for us. And whether it's a consumer or business, healthier customers make for healthier banks. So we think it's important for all of us.

## Compliance

**KITTEN:** How do you see customer education as a compliance issue?

**POLLINO:** Well, there are government regulations through the FFIEC guidance that talk about ... us being actively engaged in the community and educating our customers. So we try to make sure that we're inventorying those activities, that we have that information available. That way when we're being viewed from a regulatory perspective either by our internal auditors or by our regulators, we can show that we are trying to be thought leaders in this space, not only in getting out there online in social media, but also through our community involvement and our participation in industry conferences as well as with our customer industry groups.

## Gauging Effectiveness

**KITTEN:** What questions have banking regulators asked you about your customer awareness programs?

**POLLINO:** One big question that we're asked is: Are you being effective? And how do you know, and how is management being informed as to the effectiveness of the program? So, what we've been doing is making sure that we're tracking quantifiably the activities that we're doing, so we have a full inventory of all the efforts that we're doing both online and offline. And then as there are quantitative metrics that we can use around visitors, impressions, favorites, tweets, shares, comments ... we can also report on the success of those to make sure that we're showing that our content is not only being created, it's also being consumed in the environment. And what we have seen is that as information security issues and fraud issues become mainstream, we get a lot of question, and our content gets a lot more eyeballs. For example, two recent examples are the Target breach as well as the Heartbleed bug. We were able to get content on our site quickly after those events. ■

*To hear the entire interview, please visit:*

<http://www.bankinfosecurity.com/interviews/social-medias-role-in-fraud-prevention-i-2313>

# 2015 Anti-Fraud Agenda

It's time to look ahead to 2015 and where institutions are planning their investments, as well as to offer some advice for how to reconsider the fight against fraud.

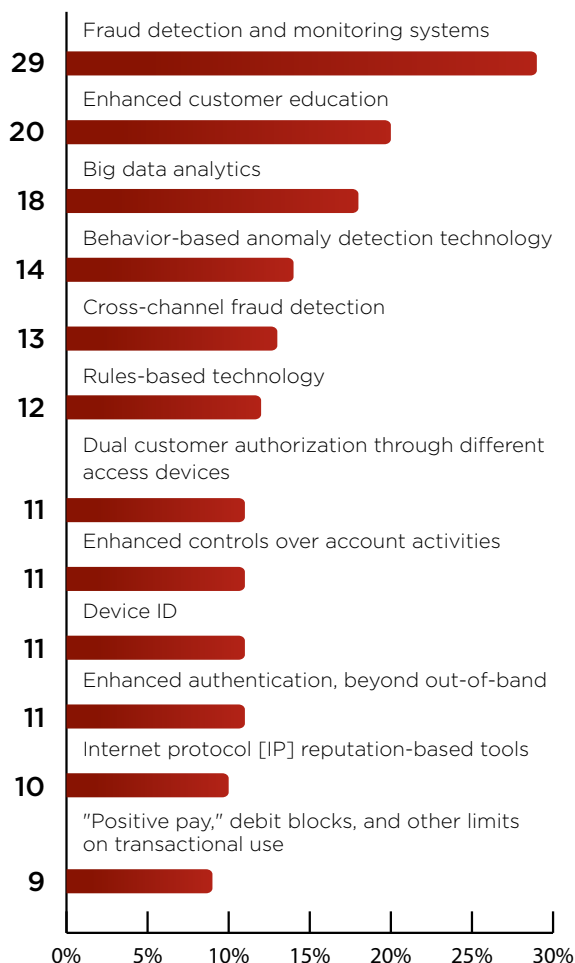
**To start, here are the top three investments that institutions say they will make:**

- » Fraud detection and monitoring
- » Enhanced customer education
- » Big data analytics

*If the awareness self-assessment grades do not go up, fraud rates will not go down. It really is that simple.*

## Key Findings:

### Anti-Fraud Investments Planned for Next 12 Months?





---

Let's revisit the topic of technology investments. We've seen where institutions have already invested. What do they plan for the year ahead?

Many of the traditional technology solutions remain popular targets, but pay attention to the emergence of big data analytics, which many analysts see as the key to effectively detecting and preventing sophisticated schemes.

Automation needs to be a significant focus of those new fraud detection and monitoring tools, as there are far too many alerts for any team of fraud analysts to manage effectively today.

The emphasis on customer education is noted ... but it also is consistent from year to year, with far too little to show for the efforts.

So, weighing these factors we've discussed, what emerges as the top anti-fraud priorities for the year ahead?

## 1 The Future of Payments Security

The retail breaches have hammered home the point that researchers have argued for years: Our 50-year-old electronic payments infrastructure is fatally flawed. It's time to evolve. The EMV migration is one answer, but it's insufficient. We need additional responses to the rise in card-not-present fraud, and we need to include merchants and even customers in the discussion about new security strategies and tactics. Each of the constituents must be actively engaged in the future of secure payments.

## 2 Traditional Tools Insufficient

A consistent message not just from this survey, but from conversations with banking/security leaders, is that there is too much fraud data for organizations today. They're overwhelmed by alerts and threat intelligence, to the point where they simply cannot react fast enough to distinguish false positives from real incidents. We need to migrate into more advanced security solutions that put a premium on automation, big data analytics and real-time alerts that can be acted upon before the customer detects fraud. Traditional security solutions can be part of the mix, but they cannot be considered the entire equation.

## 3 Time to Put an 'A' in Awareness

In an increasingly mobile world, the security-savvy customer is key. Far more power is now in the customer's hands, and we need to respect the ability of fraudsters to take advantage of customers to carry out fraud schemes. It's no longer sufficient to say "we value customer awareness." It's time now to develop valuable customer awareness programs. To find effective new media and messages to convey the criticality of concerns and simplicity of security steps customers can take.

If the awareness self-assessment grades do not go up, fraud rates will not go down. It really is that simple.

# Visa on the Future of Secure Payments

## Risk Officer Ellen Richey Stresses Adoption of Chip Cards, Tokenization

Card issuers, retailers, payments processors and others handling card data must go far beyond compliance with the PCI Data Security Standard to effectively fight fraud, says Ellen Richey, chief legal officer and enterprise risk officer at Visa.

In this excerpt of an interview with ISMG Executive Editor Tracy Kitten, Richey discusses steps to ensure card data is protected and emphasizes why it is critical that all industry players take steps to enhance retail security. She also speaks about the security limitations of emerging chip cards and why Visa is pushing for more standardized use of tokenization.

Richey oversees Visa's compliance, audit and risk teams, including payment system risk, settlement risk and enterprise risk. She also serves as the company's primary legal adviser. Before joining Visa in 2007, she worked at Washington Mutual Inc. as senior vice president of enterprise risk management and executive vice president of card services. Earlier in her career, she served as vice chairman of Provident Financial Corp., where she led the enterprise risk management, legal, corporate governance, corporate relations, compliance and audit functions. Richey also was a partner in the San Francisco law firm Farella, Braun & Martel, where she specialized in corporate, real estate and financial institution matters.

### Limiting Access to Data

**TRACY KITTEN:** Explain how limiting the amount of data merchants access is expected to reduce fraud?



*"Today in data security, you need to be getting away from strictly building a fortress to protect data and pay more attention to what you do in case hackers should be in your environment."*

**ELLEN RICHEY:** First, we need to ensure that no one is storing anything they don't need. The good news on that front is that we've made tremendous progress since the early days of data compromises in the payments industry. Now, upwards of 90 percent of our retailers have certified that they no longer store unnecessary data. So that's one big step forward we've already accomplished. The next step, and something that is already in progress, is to devalue the data that passes through their systems. So even if they're not storing it, they are vulnerable to attack as the data moves through their system. We have multiple ways of devaluing the data, one of which is our primary focus right now, in 2014, which is rolling out with EMV chip.

## Beyond PCI Compliance

**KITTEN:** Could Visa mandate that the industry go beyond PCI compliance?

**RICHEY:** There are already best practices out there, particularly on the processing side, that we've published and are available on our website to go beyond the technical side of PCI; also, to do more along the resilience side of data security, such as improved or more frequent vulnerability monitoring and intrusion detection. Today in data security, you need to be getting away from strictly building a fortress to protect data and pay more attention to what you do in case hackers should be in your environment. Then, the second big item is to restrict the utility of the data in the hands of the retail industry. By that I mean, if we can make the data less valuable to criminals by using dynamic data that can't be reused to commit fraud, we can actually take the retailers out of harm's way. And, of course, one of the examples there is the EMV chip; another example would be our initiative around tokenization, which would devalue data in large portions of the industry.

## Additional Security Layers

**KITTEN:** What additional security layers is Visa pushing?

**RICHEY:** The big three in our mind right now are the chip, tokenization and point-to-point encryption, which is a valuable tool available right now for retailers to protect themselves from the moment data is entered at the point-of-sale. In addition to that, we're always looking at the next generation of predictive analytics for fraud control; we're also improving our response technologies, the way we identify when breaches have occurred and get that intelligence out into the industry.

**KITTEN:** Can you talk about some of the steps that are being taken to help retailers enhance their adoption of EMV?

**RICHEY:** We've certainly been working for some years to make sure that the standards are really implementable here in the United States, and tailored to our market. One of the more recent initiatives there is to make sure we've licensed the technology to ensure all the merchants can route their transactions as is required by the Dodd-Frank Act. That has been resolved, really, with some of the major processors, like First Data, for example, in recent months. That is one big effort that is coming to a conclusion. In addition, Visa and MasterCard recently formed a cross-industry working group that will meet to accelerate EMV adoption, by working together collaboratively. We also, across all the brands, provide services on behalf of smaller institutions that might not want to make the investment themselves. We can actually do that for them.

**KITTEN:** What are some of EMV's security limitations?

**RICHEY:** The great thing about EMV is it will eliminate, if it's fully deployed, counterfeit fraud. But counterfeit fraud is only one type of fraud, and probably the biggest gap, if one did not pursue tokenization, would be card-not-present fraud. In today's world, that means e-commerce fraud. That is why we are so interested in pushing forward with our tokenization initiative. ■

*To hear the entire interview, please visit:*

<http://www.bankinfosecurity.com/interviews/visas-richey-on-card-fraud-i-2263>

# Faces of Fraud Resources

---

## From ISMG Archives



### **Card Fraud: Why Consumers Don't Get It**

New research shows consumers believe online purchases are more secure than those made at bricks-and-mortar retailers. Researcher Shirley Inscoe of Aite explains why misconceptions about card fraud should be worrisome to banks.

<http://www.bankinfosecurity.com/interviews/card-fraud-consumers-dont-get-it-i-2385>



### **Fraud: Defining 'Reasonable Security'**

FFIEC guidance and case law are helping banks define what constitutes "reasonable security." In a panel discussion, three experts debate the long-term impact of two recent account takeover fraud cases.

<http://www.bankinfosecurity.com/interviews/fraud-defining-reasonable-security-i-2380>



### **New Insights on Fighting Check Fraud**

Check fraud remains the No. 3 source of losses for financial institutions, but fraud expert Wesley Wilhelm says behavioral analytics can help mitigate the risks.

<http://www.bankinfosecurity.com/interviews/new-insights-on-fighting-check-fraud-i-2379>



### **Data Breaches: What the Victims Say**

What is the consumer impact of big data breaches such as Target's and P.F. Chang's? Victims blame the breached entities, and they want government action, says Al Pascual of Javelin Strategy & Research.

<http://www.bankinfosecurity.com/interviews/data-breaches-what-victims-say-i-2374>



### **The Limitations of EMV**

In response to the crisis in trust and the anger of consumers and merchants, the card brands and issuers seem to have finally committed to EMV in the U.S. A colleague suggested that we might experience yet another crisis in trust when consumers and merchants realize that EMV does not solve all their problems.

<http://www.bankinfosecurity.com/blogs/limitations-emv-p-1674>



### **First Data: How to Tackle Cyberthreats**

Paul Kleinschnitz, general manager of payment processor First Data's cybersecurity solutions team, says there are plenty of technologies to address payment card security, but cyberthreat awareness is still lacking.

<http://www.bankinfosecurity.com/interviews/first-data-how-to-tackle-cyberthreats-i-2272>



### **Tips for Fighting Fraud with Big Data**

Most organizations, including banks, have more data than they know what to do with, says Allison Miller, a cyberthreat and data analytics expert. So why aren't they more effectively using big data analytics for fraud prevention and detection?

<http://www.bankinfosecurity.com/interviews/tips-for-fighting-fraud-big-data-i-2269>

# **2014 Faces of Fraud Survey: The Impact of Retail Breaches**

Receive insights from BankInfoSecurity's latest "Faces of Fraud" survey, as well as expert analysis of:

- Today's most predominant and damaging fraud incidents impacting banking institutions and their customers;
- New anti-fraud investments institutions are making to thwart the fraudsters and satisfy the demands of regulatory agencies.



**WEBINAR**

Sponsored by



**REGISTER NOW**

<http://www.inforisktoday.com/webinars/2014-faces-fraud-survey-impact-retail-breaches-w-438>



## 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](mailto:sales@ismgcorp.com)

