2010 Survey Results

The Faces of Fraud: Fighting Back

EXECUTIVE SUMMARY

December 2010

iSMG
INFORMATION SECURITY
MEDIA GROUP

Introduction


Tom Field

In February, the U.S. Secret Service broke up an alleged ring of **ATM skimmers** in Massachusetts – one of a series of similar skimming sprees around the U.S. in 2010.

In March, the **Hancock Fabrics** national retail chain publicly confirmed that it had been breached by fraudsters who brazenly swapped out point of sale PIN pad units at some stores, thus skimming payment card data during transactions.

In May, the Federal Deposit Insurance Corporation hosted a day-long symposium on **corporate account takeover**, bringing together diverse industry groups and thought-leaders to create a new plan to stop the rampant growth of ACH and wire fraud against business banking customers.

And in early November, authorities reported a rash of **targeted phishing schemes** – which included hits to military account holders and their families at USAA and Navy Federal Credit Union, as well as a separate attack on officials at the World Bank.

These have been just a few of the noteworthy examples of financial fraud this year. From **skimming** and **POS attacks** to **ACH fraud** and **payment card hacks**, 2010 has been "The Year of Fraud," and the year's incidents have left banking institutions and their customers anxious for new solutions to prevent fraud in all its forms.

In response to the growing fraud threats – and to the demand for new solutions – Information Security Media Group just concluded its latest survey, "The Faces of Fraud: Fighting Back."

This is the Executive Summary of the survey results and what they suggest for fighting fraud in 2010.

Tom Field,
Editorial Director,
Information Security Media Group

Survey Sponsors

41st Parameter prevents person-not-present fraud for the world's most valued and recognized brands. 41st customers report some of the lowest fraud loss rates in the industry while enjoying review rates as low as 1%.

FICO™ Falcon® Fraud Manager is the industry leader in financial fraud detection, protecting over 2.1 billion accounts globally, saving institutions over $10 Billion worldwide. Go to http://www.FICO.com/fraud to find out how.

FIS provides the expert guidance and leading solutions our clients need to detect and prevent new types of fraudulent activity, track and maintain regulatory updates and manage risk levels.

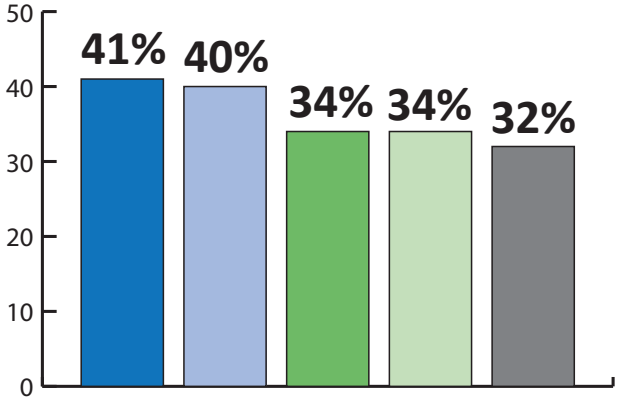
Why Study Fraud?

The seeds for this survey were planted earlier this year, when we concluded the 2010 Banking Information Security Today survey. Two of the questions focused specifically on fraud:

Which types of fraud have you experienced over the past year?

- Credit/Debit Card 72%
- ATM 41%
- ACH 30%

Which area of fraud do you feel best prepared to prevent in 2010?



41% - Credit/debit card
40% - Money laundering
34% - ACH/wire (account takeover)
34% - Check
32% - Online banking breach

The answers told us very clearly that the types of fraud banking institutions were facing – ACH, ATM and payment card – were not necessarily the ones they felt best prepared and resourced to fight.

Which frankly begged the question: Exactly which types of fraud are most prevalent at institutions today, and how are they responding in terms of detection and prevention?

This question was the genesis of the Faces of Fraud survey.

Survey Goals

This study was crafted with assistance from some of the industry's top thought-leaders on fraud, and it was conducted electronically throughout the month of October 2010. In all, more than 230 respondents participated – 83% from banks and credit unions of all sizes. The remaining 17% represented non-banking financial institutions.

It's important to note that while responding institutions vary in size from small (under $500 million in assets under management) to large ($2 billion and more in assets), the responses generally do not. With few exceptions (which will be noted) the responses are consistent across institutions of all sizes.

The survey's four main objectives were to:

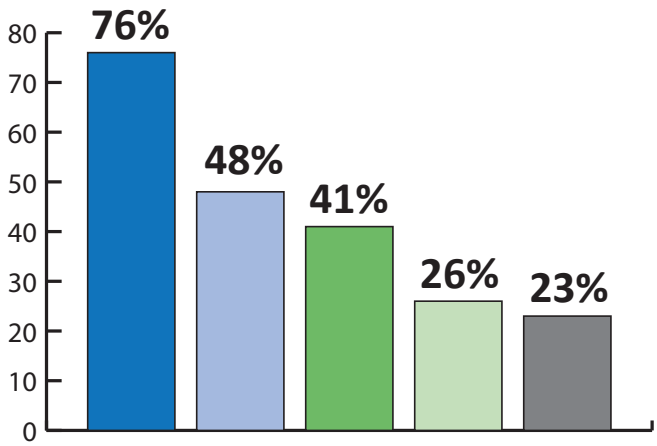
- **Gauge the scope of the multi-faceted fraud threat to U.S. banking institutions;**
- **Measure the industry's preparedness for evolving threats;**
- **Identify specific strategies and solutions employed by banking/security leaders to fight fraud;**
- **Predict the emerging technologies and strategies where institutions are investing their resources.**

Survey Results: The New Faces of Fraud

Survey Results: New Faces of Fraud

One of the most telling responses of the survey is to this question:

When is a fraud incident involving your organization usually detected?



76% - When a customer notifies us
48% - At the point of transaction
41% - Third-party notification
26% - At the point of origination
23% - During account audit/reconciliation

In other words, despite the availability today of world-class fraud detection technology, despite broad awareness of the current fraud threats and incidents – nothing spreads faster than word of a breach – and despite what we've all learned about customer confidence and loyalty in the wake of fraud incidents such as the **Heartland Payment Systems breach** ...

76% of respondents learn of fraud incidents from their customers.

More than three-quarters of financial institutions learn of fraud incidents when notified by their own customers.

This response underscores the need for better fraud detection – before the incidents strike the customer – and it sets the tone for the survey results, which break down into four main themes.

Survey Results: New Faces of Fraud

1. The Faces of Fraud: Today's Top Threats

What are today's top threats? Which threats do institutions feel most prepared to face? What impact have we seen from highly-publicized ACH/wire fraud incidents?

2. Cross-Channel Fraud: The Great Mystery

Industry analysts tell us that cross-channel fraud is the growing trend. That no longer are fraudsters targeting just ATMs or payment cards or checks – they're seeking to compromise your customers in every way you interact with them. But how prepared are institutions to measure and respond to these cross-channel threats?

3. Resources: The Ongoing Challenge

It's been a tough two years for banking. As a result of the global recession and U.S. financial crisis, human and fiscal resources have been hard to come by for banking institutions. Yet, the survey results show encouraging trends on both fronts.

4. Need for Awareness, New Tools

If there is one overriding theme of this survey, it's this: Respondents recognize that awareness programs – for employees and customers alike – as well as fraud detection and prevention tools, are their best weapons to fight fraud. Their challenge is to find the right tools and take the right approaches to awareness.

We'll explore each of these key themes in the sections to follow.

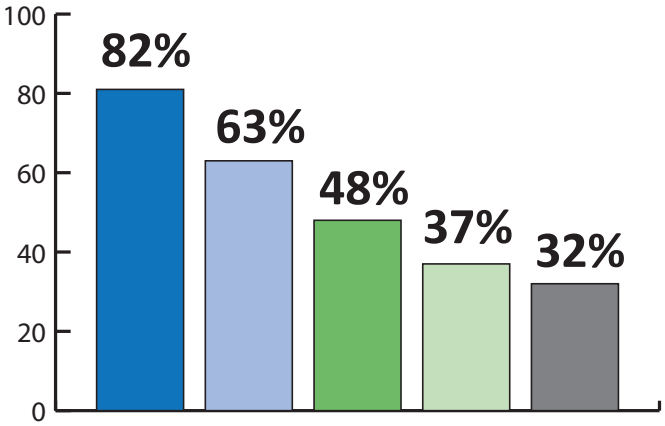
The Faces of Fraud: Today's Top Threats

The Faces of Fraud: Today's Top Threats

It's clear that the faces of fraud are ever-changing. While classic forms of fraud are still prevalent – i.e. payment cards and checks – new electronic schemes such as phishing and vishing also are taking a greater toll, based on the latest incidents reported by institutions.

82% experienced credit/ debit card fraud in 2010.

Which types of fraud has your organization experienced in 2010?



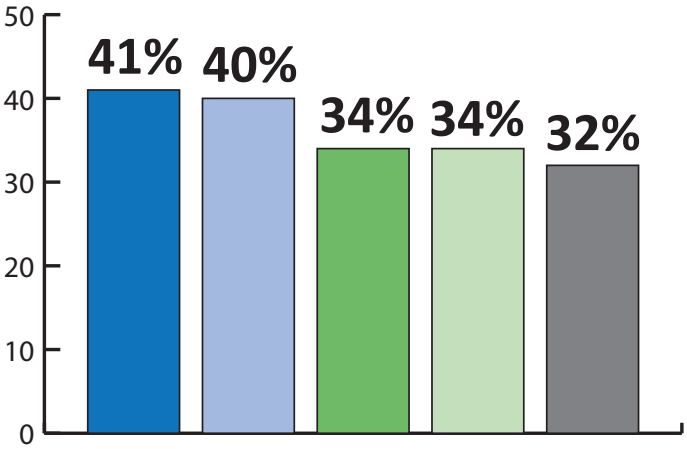
82% - Credit/debit card
63% - Check
48% - Phishing/vishing
37% - ACH/wire (account takeover)
32% - Third-party POS skimming

It's no surprise that payment card and check fraud top the current list of schemes that institutions face – these are traditional banking scams, and they reflect areas where institutions invest great resources. What is noteworthy is the rise of phishing/vishing – a relatively new form of fraud – to the #3 spot. And ACH/wire fraud as a #4 threat validates the recent attention that regulatory agencies, law enforcement and banking institutions have paid to the spread and costly risk of corporate account takeover. These crimes are risks to institutions of all sizes, and their impact is growing.

Looking at the types of fraud institutions are prepared to face, it's equally clear that their resources are focused most on the traditional forms of fraud, as well as those such as anti-money laundering that are reviewed most closely by banking regulators. Phishing/vishing, for instance, doesn't even make the top five of this list:

Only 41% feel best prepared to prevent credit/debit card fraud.

Which area of fraud do you feel your organization is best prepared to prevent?



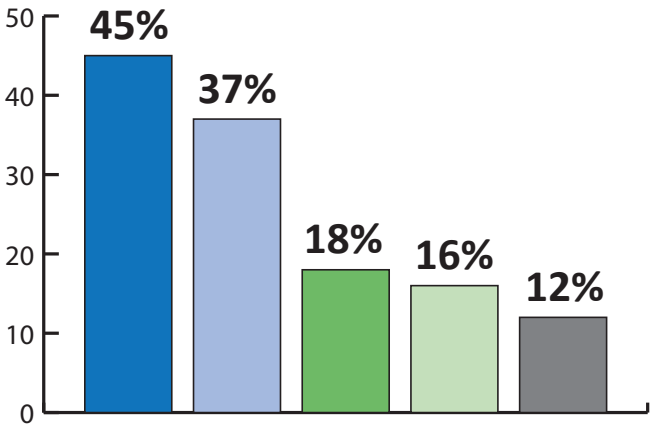
41% - Credit/debit card
40% - Money laundering
34% - ACH/wire (account takeover)
34% - Check
32% - Online banking breach

The message here isn't that banking institutions have their resources in the wrong places. Clearly, payment card and check fraud remain serious risks to major lines of business, and money laundering continues to be an evolving (and scrutinized) crime. But institutions do need to diversify their detection and prevention approaches to include newer forms of fraud such as phishing/vishing, as well as the surge in ACH/wire fraud – corporate account takeover. These crimes clearly are increasing – as is public exposure when these schemes are uncovered. But it is not clear how – or if – institutions are prepared to respond to these new faces of fraud.

How does your organization currently measure fraud losses?

- By Account 44%
- By Fraud scheme 40%
- By Channel 35%

What non-financial losses has your organization suffered because of fraud incidents?



45% - Loss of productivity

37% - Customer confidence and reputational loss

18% - Customer accounts (moved to other institutions)

16% - No losses

12% - Regulatory or other compliance issues

45% cite loss of productivity as top non-financial fraud loss.

Traditionally, institutions have measured fraud losses solely by dollars and cents. When fraud hits a certain financial threshold, it is taken seriously. But in the wake of the financial crisis and resulting loss of confidence in banking, institutions now are paying more attention to "soft" metrics such as customer confidence and the potential loss of accounts. Trust is the most important element of the banking relationship, and if that trust is damaged by a fraud incident and subsequent publicity, customers are likely to take their business elsewhere. This potential customer churn now is a significant and growing part of the equation when considering fraud losses.

In terms of ACH/wire fraud, or corporate account takeover, we know from an earlier response that 37% of institutions have faced these incidents in 2010. And we know from a separate question that 60% of respondents stick to the "safe" stance that ACH fraud prevention is a shared responsibility between banks and their business customers.

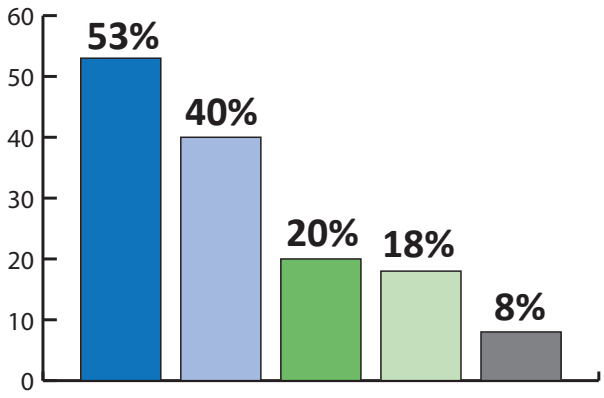
The interesting discussion begins with questions about what recent high-profile incidents – and subsequent publicity over lawsuits – have done to the industry's reputation, as well as how individual institutions have responded to these crimes.

How have recent, well-publicized incidents of skimming and ACH/wire fraud impacted the reputation of the financial services industry?

- Negligible damage 32%
- No way of knowing 29%
- Moderate damage 26%
- We've taken a serious hit 7%

40% have invested in new technology solutions to combat ACH fraud.

What has your organization done in response to recent ACH/wire fraud (corporate account takeover) incidents?



53% - Increased internal monitoring of ACH transactions

40% - Improved customer awareness efforts

20% - No response - we have not been impacted

18% - Implemented out-of-band authentication

8% - Don't know

The mantra of the banking industry in response to ACH fraud has been "We must raise customer awareness." And it's clear by their answers that institutions have taken seriously the desire to put more energy both into monitoring ACH transactions, as well as into customer outreach – educating corporate customers to security measures they can take to protect their assets. The concern, though, is that despite this avowed dedication to improving customer awareness, respondents say later, in response to a separate question, that their current education efforts are in serious need of improvement. If awareness is indeed key, then greater efforts need to go into improving the programs – not just increasing them.

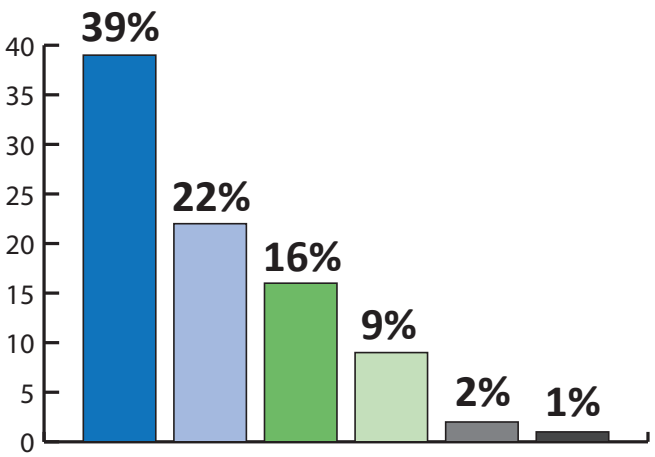
Cross-Channel Fraud: The Great Mystery

Cross-Channel Fraud: The Great Mystery

In crafting this survey, industry experts were particularly keen to dive into the topic of cross-channel fraud. In their view, cross-channel schemes are becoming the rule, not the exception, as fraudsters seek to compromise customer accounts in every venue. And survey respondents validate this view, at least based on what they know now about cross-channel schemes.

61% say up to 25% of their fraud incidents are cross-channel.

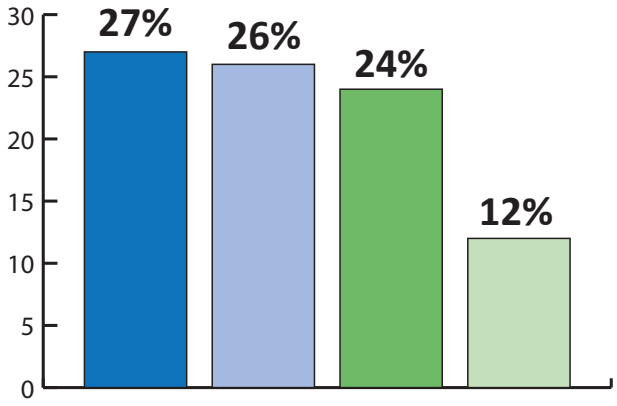
In your opinion, what percentage of your organization's incidents is considered cross-channel fraud?



39% - Under 10%
22% - 10-25%
16% - Don't know
9% - 25-50%
2% - 50-75%
1%- 75-100%

The operative phrase is "based on what they know," as subsequent responses show that institutions do not have the teams or the tools to adequately detect cross-channel patterns.

Does your organization have a defined plan, a team assigned to execute this plan and controls to detect cross-channel fraud?

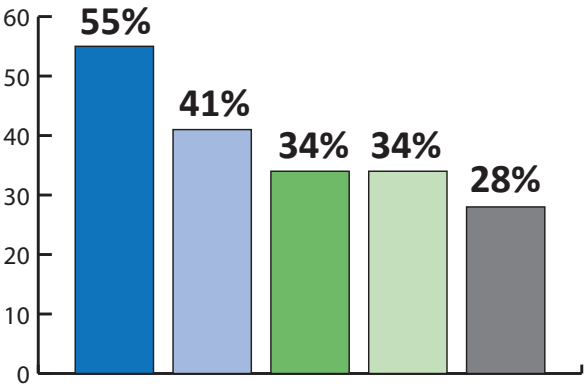


27% - No
26% - Yes
24% - Working on it
12% - Don't know

The disconnect emerges from how banking institutions are organized. Many still break down into organizational silos, and those gaps are challenging to bridge. But part also is that too many banks and credit unions have prepared themselves only to face traditional forms and venues of fraud, and they view these incidents as isolated. They're not resourced or structured to consider – never mind detect or prevent – cross-channel schemes that impact customers in multiple accounts. This is a mindset that must change in 2011.

Organizational silos aren't the only challenge. Institutions also lack the tools to adequately detect cross-channel patterns.

Which type of fraud detection tools does your organization currently employ?



55% - Manual reports
41% - In-house fraud detection system
34% - Third-party neural net
34% - Third-party rules-only system
28% - Independent fraud detection tools & technologies for each channel

55% rely on manual reports to detect fraud.

In analyzing survey results, this is one of the answers that most stood out – 55% of respondents still rely on manual reports to detect fraud. It isn't necessarily that institutions don't have information systems in place to derive relevant data – often they do. The challenge is that they have no systems or processes to share and analyze this data across the organizational silos or impacted channels.

Are your organization's fraud detection tools aligned to detect cross-channel patterns?

- No 36%
- Somewhat 23%
- Yes 13%
- Working on it 6%

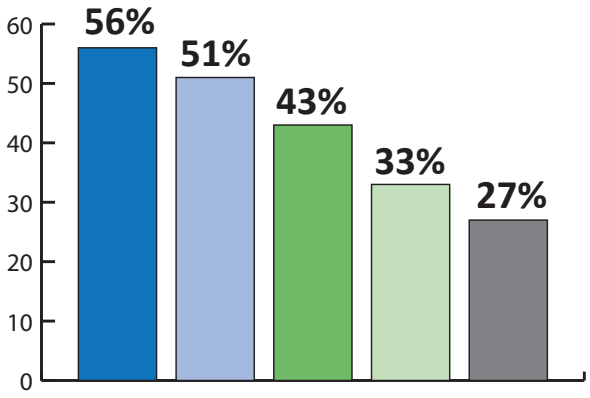
Resources: The Ongoing Challenge

Resources: The Ongoing Challenge

Despite the prevalence of fraud threats, institutions have kept to bare-bones their resources dedicated to fighting fraud. This frugality is evident when respondents discuss their current challenges and the size of their fraud prevention teams.

56% cite insufficient resources as challenge to fraud prevention.

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



NOTE: Larger institutions do tend to have larger staffs dedicated to fraud prevention, but generally the numbers above are consistent among respondents of all size institutions.

56% - Insufficient resources (budget and/or personnel for this task)
51% - Inadequate fraud detection tools & technologies
43% - Lack of customer awareness
33% - Organizational silos - fragmented approach to fraud prevention
27% - Difficulty investigating crimes across borders

How many people in your organization are assigned to fraud prevention?

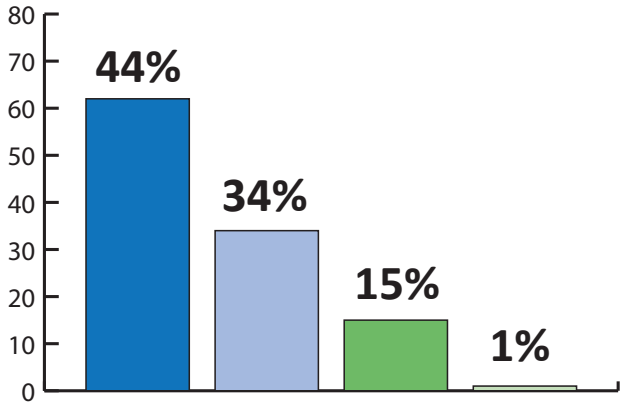
- Between 1 and 5 66%
- 6-25 15%
- No dedicated staff 6%
- 25-100 5%
- 100-plus 1%

2010 has not been a strong year for investment in fighting fraud – only 17% of respondents have increased budget or staff. But the outlook for 2011 is much more encouraging.

What has your organization done this year to reduce your vulnerability to fraud?

- Improve awareness 63%
- Invest in new technology 40%
- Increase budget/staff 17%
- No new measures 12%

Do you plan to increase or decrease resources (budget and/or personnel) dedicated to fraud prevention at your organization?



44% - No change
34% - Increase
15% - Don't know
1% - Decrease

34% plan to increase fraud prevention resources in 2011.

In any year, it's a positive statement when more than one-third of organizations plan to increase resources. But in the wake of the worst financial crisis in modern times, it's a significant move when 34% of banking institutions intend to add resources in the fight against fraud.

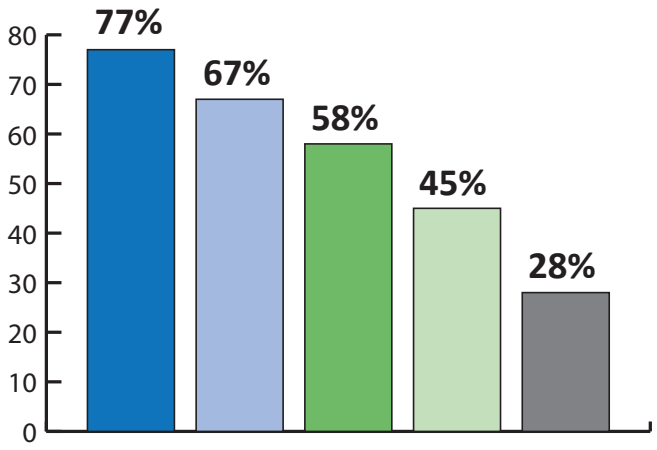
Need for Awareness, New Tools

Need for Awareness, New Tools

In quantitative responses, as well as in verbatim answers to open-ended questions, respondents are consistent in their support of customer/employee awareness and technology tools to effectively detect and prevent fraud. The disconnect comes when you look at the effectiveness of the awareness programs that respondents deem so crucial.

67% say customer education is the best way to prevent fraud.

What have you found to be the most effective ways to prevent fraud?



77% - Employee education emphasizing identification and response to fraudulent activities

67% - Customer awareness emphasizing the techniques used by fraudsters, such as phishing, vishing, etc.

58% - Fraud detection tools & technologies

45% - Real-time decision tools

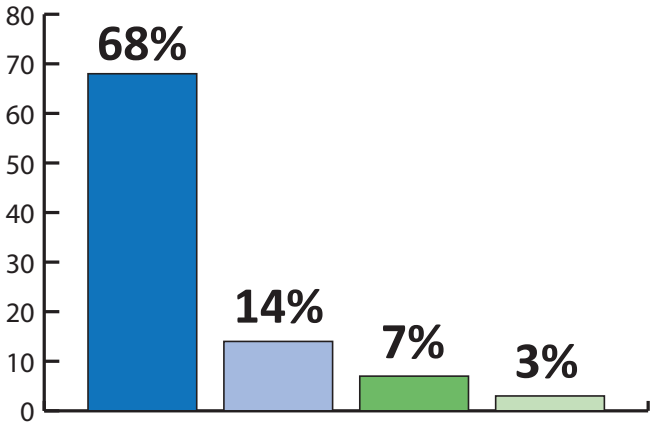
28% - Manual account monitoring

How do you grade the effectiveness of your organization's fraud awareness program for employees?

- Needs improvement 70%
- Extremely effective 15%
- Does not exist 5%
- In next year's plan 3%

These responses hammer home a point that's been evident for years: Banking institutions have never put sufficient resources into developing effective awareness programs. But in the wake of fraud incidents (particularly account takeover) and pressure from regulators to improve identity theft awareness programs, it's time for institutions to step up their efforts, or risk losing valued customers. In the panel discussion that closes the survey results webinar, Matthew Speare of M&T Bank details his bank's unique efforts to get into the community and educate corporate customers.

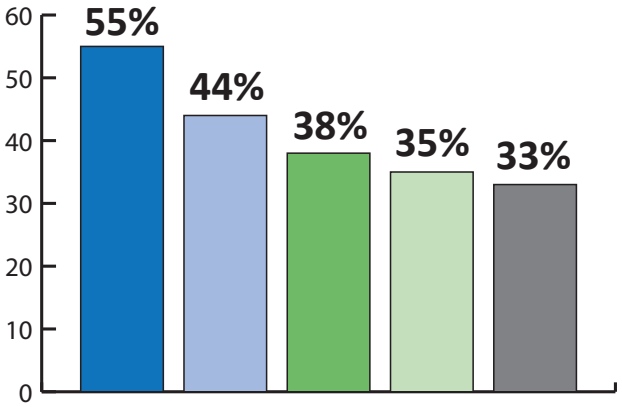
How do you grade the effectiveness of your organization's fraud awareness program for customers (consumers and commercial)?



68% - Like many other initiatives, needs improvement
14% - This program doesn't exist
7% - Extremely effective
3% - It's in plan for next year

And while we established earlier that manual reports are the most common fraud detection tools, they are not the only ones. And, in fact, institutions do plan to make upcoming investments in new technologies and tools to improve fraud prevention.

As part of the organization's on-going fraud prevention and detection program, are you planning to use any of the following technologies?



55% - Authentication: strong authentication, out-of-band authentication (e.g., telephone-based authentication, etc.), knowledge-based authentication

44% - Intrusion prevention technologies

38% - Fraud case management system

35% - End-to-end encryption (protecting the data that can be used for perpetrating fraud)

33% - Neural net fraud detection technologies

55% intend to invest in authentication technologies in 2011.

Organizations are setting their bars higher in 2011. They do want to bridge their silos, leverage information they already have and maximize the latest technologies. The metrics to watch in 2011 are: 1) Do institutions indeed make these key investments? 2) Do they maximize the tools to improve their ability to detect and prevent schemes starting at the customer level? This evolution represents not just an investment in technology, but an evolution of the institutions' current siloed mindset. In the survey webinar, Mike Urban of FICO discusses fraud detection tools and new strategies that could be most effective for institutions that want to take an enlightened approach to fighting fraud.

2011 Agenda

The bad news: Banking fraud isn't going away. The good news: The resources to fight fraud will increase for financial institutions in 2011. As they add budget and resources, institutions must consider these points:

1. Evolving Threats Need Greater Attention

It's easy to understand why banking institutions are best prepared for check fraud and money laundering. These are the schemes that either have been most common or most examined by regulators. But with the advent of phishing/vishing, as well as looming threats to mobile banking, it's time for fraud prevention and detection efforts to realign with the times.

2. Cross-Channel Risks Must be Monitored

If institutions admittedly have inadequate detection teams and tools yet already are aware that up to 25% of their fraud incidents are cross-channel, then one has to wonder about the actual scope of cross-channel schemes. Especially as more institutions expand online and mobile banking efforts, cross-channel monitoring becomes critical. This is a gap institutions must bridge in 2011.

3. Fraud Costs Money … and Customers

Traditionally, fraud has been measured in terms of financial losses. If losses met a pre-determined threshold, then the institution had a "fraud problem." But increasingly institutions are concerned about customer loyalty – the customer experience. To retain valuable customers and accounts, institutions must reduce the risk of fraud by investing more in detection and prevention – and then make customers aware of those extra investments. Security no longer should be considered a corporate secret; it's a competitive advantage to be marketed.

4. Awareness Efforts Must be Improved

It's good that institutions recognize the importance of employee/customer awareness in terms of fraud prevention. But it's discouraging to see that such a high priority fails to earn better than "needs improvement" in a self-assessment. To truly curtail risks posed by ACH/wire fraud, phishing, vishing and other electronic schemes, institutions must increase and improve their education – for consumers and corporate accounts alike.

5. New Tools Must Emphasize Detection

As institutions plan their 2011 technology investments, fraud detection must be high upon those lists. In some cases this means investing in new intrusion detection systems; in others it means bridging organizational silos to leverage information that has already been mined. In all cases, it means improving the institution's odds of detecting a fraud threat before it reaches the customer. Nobody wants to revisit this survey in 2011 and find that 76% of fraud incidents are still being discovered by customers.

For more analysis of the Faces of Fraud survey, please see the **Faces of Fraud webinar** and check BankInfoSecurity.com and CUInfoSecurity.com for related articles, interviews and blogs.

Fraud Trends to Track in 2011

Banking, Fraud Experts Weigh in on the Top Concerns for Financial Institutions

NOTE: *Following is an excerpt from the panel discussion between Matthew Speare of M&T Bank and Mike Urban of FICO, as presented in the* Faces of Fraud: Survey Results Webinar.

Matthew Speare
SVP of IT, M&T Bank

TOM FIELD: Matt, what are the fraud trends that banks really ought to be concerned with as we go into 2011?

MATTHEW SPEARE: Over time what we've seen is none of the old techniques ever go away. I think that the newest trend – while it has not affected anyone yet – is what is going to happen with some of the advanced functionalities that we're putting out into mobile devices or remote channels such as remote check deposit. Where we're giving both corporate and retail customers the ability to really not have to spend any time at the branch or ATM at all, but conduct their business via mobile-type devices or image-capture devices that get placed at their place of business for convenience purposes.

> ***"Over time what we've seen is none of the old techniques ever go away."***
>
> **- Matthew Speare**

While we have not seen those exploited today because that trend is happening so quickly, I would caution financial institutions not to get enamored with the functionality or the vendor, but really figure out what are the security controls to prevent IDs from being stored locally on the device – any type of non-public personal information such as accounts. Otherwise, anytime that you have that data even existing for a very short period of time on the device, well then there is potential that it is going to be exploited.

Because what we've seen is just a rapid increase in the number of both businesses and consumers that are taking advantage of these new technologies for the convenience sake, and that is going to continue to grow rather rapidly over time. I think it is going to become just as important as the Internet channel in the long term, but what steps are we taking right now to make sure that we don't have to go and rework 18 months down the line because of new laws [governing] the control systems that we put in place?

FIELD: Mike, what do you see as the trends that the banks ought to be most concerned about as we head into the New Year?

Mike Urban
Senior Director of Fraud Solutions
FICO

MIKE URBAN: To piggyback on Matt's comment about remote deposit capture, one of the areas that I'm fairly concerned about is after the consumer takes a picture of that check or scans the check for deposit – what do they do with the check? I know people say, "Well, I put it in a shoebox at least until it clears." That shoebox may collect a lot of dust and someone may come across that, so I think that is a great point around the entire chain on remote deposit capture.

I'd say that as long as we've got magnetic stripe cards, we will have card compromises, and that includes the new way of POS data compromises where it appears that criminals are able to get down into the POS systems within merchants; targeting smaller merchants, and then distributing those cards over the Internet. As well as the ATM skimming compromises that have been popping up all over the place. So, I think those are going to continue.

Criminals are going to keep reinvesting in those attacks. With the amount of malware that is out there, you really have to expect that computer your customer is using to interact with you while online is compromised. So, there are going to be new methods and techniques that criminals are going to use to target the money in the account, including online banking transactions and card not present.

I expect the criminals are going to adjust behavior and do a lot of other things, so it is going to continue to be a cat and mouse game. I expect that criminals are also going to find their way around authentication and out-of-band communication techniques. One of the more recent MOs that we've seen is a criminal who has taken over all online banking accounts, initiating a transfer and then blocking the real customer's phone number by continually calling it during the out-of-band authorization window, and then calling the financial institution to complain that the transfer didn't take place – acting very irate as if they were the customer.

> ***"I'd say that as long as we've got magnetic stripe cards, we will have card compromises."***
>
> **- Mike Urban**

Matthew Speare oversees security for M & T Bank Corporation, the nation's 17th largest bank holding company, based in Buffalo, New York. He is responsible for developing and sustaining an information risk program that effectively protects the personal information of millions of M & T Bank customers. His responsibilities include information security management, IT compliance and risk management, corporate emergency and incident response, and business continuity management.

Matt is also a Major in the Army National Guard, serving as the 42nd Infantry Division Aviation Operations Officer, and is an AH-64 Apache Attack Helicopter pilot.

Mike Urban has 15 years experience in financial fraud management. Mike currently serves as Senior Director & Fraud Chief, Fraud Product Management, for FICO. He analyzes fraud issues and trends to provide continuous improvements in fraud detection technology and fraud management. He regularly works with law enforcement to help prosecute criminals and has been responsible for uncovering several crime rings in the US. Mike's industry recognition includes GASA Crime Fighter of the Year 2005 and ATMIA Most Influential Member of the Year 2004.

For More on the "Faces of Fraud"

See These Additional Resources from Information Security Media Group

The Faces of Fraud: How to Counter 2011's Biggest Threats

Join a distinguished panel of fraud experts for an exclusive first look at the eye-opening survey results and how institutions can act upon them, including:

- How to ensure you're prepared to defend against the most common fraud threats;
- Bridging the institutional silos that stand in the way of fighting fraud;
- How to improve employee and customer awareness, ensuring that fraud prevention is a shared responsibility.

http://www.bankinfosecurity.com/webinarsDetails.php?webinarID=196

PANEL DISCUSSION

Faces of Fraud: Survey Analysis

Banking, Fraud Experts Weigh in on Detection, Prevention

Matthew Speare of M&T Bank and Mike Urban of FICO on fraud trends and technologies that financial institutions should track in 2011. http://www.bankinfosecurity.com/surveys.php?surveyID=9

INTERVIEWS:

Faces of Fraud: Banking Still Siloed

TowerGroup's Tubin: Institutions Don't Have a True Picture of Fraud

Fraud detection and lack of cross-channel integration pose big security challenges for financial institutions, and a lack of resources is to blame.

http://www.bankinfosecurity.com/podcasts.php?podcastID=868

2011 Fraud Focus: Integration and ACH

Doug Johnson Says Banks Will Spend More on Automated Detection Tools

Enhanced integration of AML and fraud-prevention tools will be top priorities for 2011, says ABA's Johnson.

http://www.bankinfosecurity.com/podcasts.php?podcastID=887

2011 Card Skimming Fraud Threats

ATM and POS Skimming Is Getting More Sophisticated

"What's interesting is that the criminals are now using cryptographic technology to protect the card information they steal, and that's posing challenges for detection and law enforcement," says Jeremy King of the PCI Security Standards Council.

http://www.bankinfosecurity.com/podcasts.php?podcastID=892

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.

BANK INFO SECURITY®

CU Just for Credit Unions INFO SECURITY®

GOV INFO SECURITY®

HEALTHCARE INFO SECURITY®

Contact

Information Security Media Group, Corp.
(800) **944-0401**
info@ismgcorp.com

ISMG INFORMATION SECURITY MEDIA GROUP

4 Independence Way | Princeton, NJ 08540
ISMGCorp.com