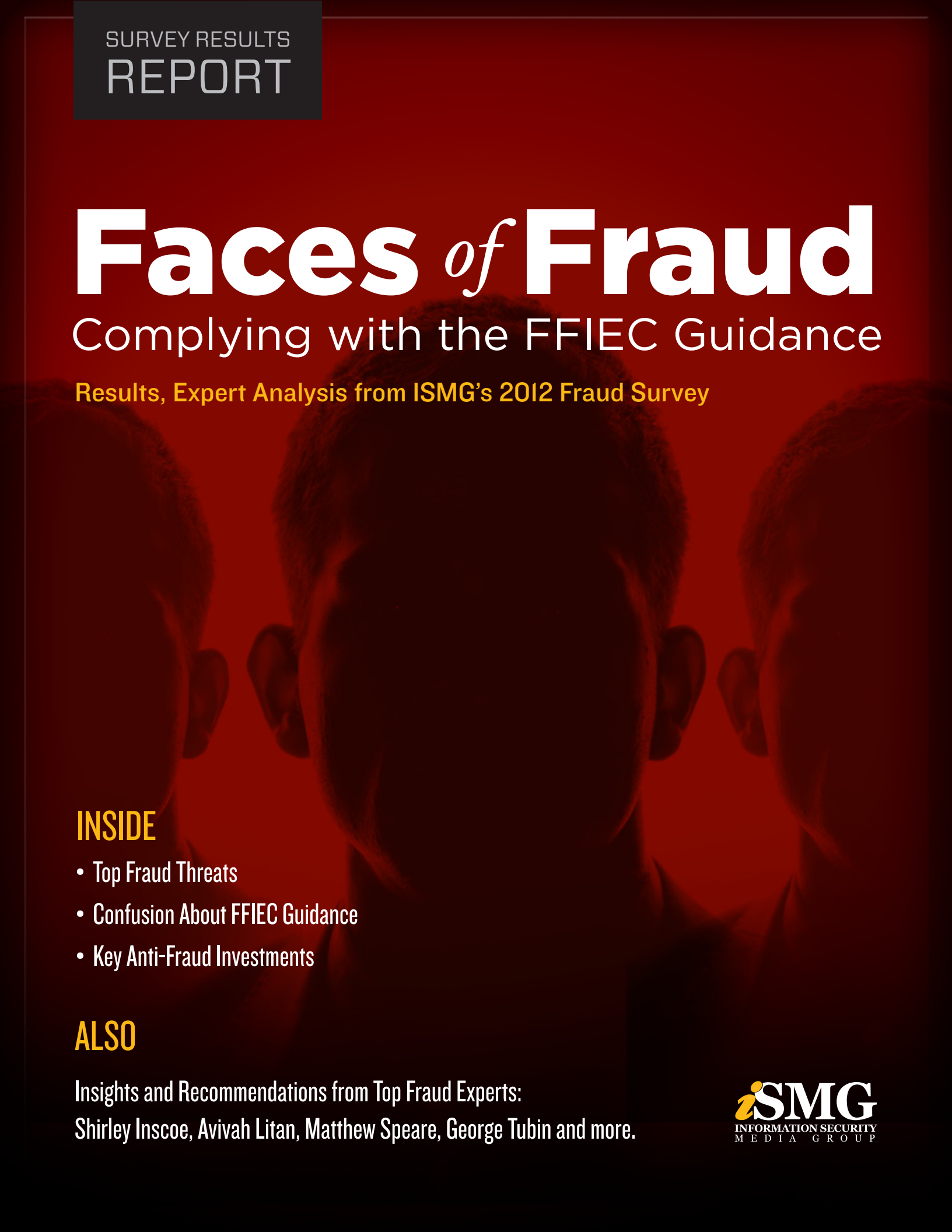
SURVEY RESULTS
REPORT

Faces *of* Fraud

Complying with the FFIEC Guidance

Results, Expert Analysis from ISMG's 2012 Fraud Survey



INSIDE

- Top Fraud Threats
- Confusion About FFIEC Guidance
- Key Anti-Fraud Investments

ALSO

Insights and Recommendations from Top Fraud Experts:
Shirley Inscoe, Avivah Litan, Matthew Speare, George Tubin and more.

ISMG
INFORMATION SECURITY
MEDIA GROUP

From the Editor

The Future of Fraud

Tom Field
Vice President, Editorial

Typically, one doesn't introduce fraud research with the phrase "there's good news," but this year is an exception.

The good news is: For the first time since the economic upheaval of 2008, U.S. financial institutions say they expect an increase in funds and personnel dedicated to fighting fraud – in some cases, a substantial increase. This optimistic message is the main headline of the 2012 Faces of Fraud survey, the results of which are encapsulated and analyzed in this report.

Of course, the good news comes with a caveat: Institutions also can expect an increase in fraud attempts as fraudsters hone their techniques and broaden the scope of their attack vectors. Payment card fraud, phishing attempts and point-of-sale hacks will continue to be common in the months ahead. And as consumers increasingly conduct financial transactions on mobile devices, well, we can expect the fraudsters to migrate there, too.

As you review the 2012 survey results, do so with an eye on 2013, and please consider these questions:

- What will be the dominant fraud threats? Institutions may be getting better at detecting and preventing ACH/wire fraud, but how prepared are they for attacks in the mobile channel?
- What will be the impact of the FFIEC Authentication Guidance? Federal regulators are examining institutions now for conformance with the updated guidance. Will periodic risk assessments, layered security controls and improved customer awareness truly reduce incidents of fraud?
- Where will the resources go? Which will be the most popular anti-fraud technology solutions, and how will institutions augment their current fraud teams?

As you consider these questions and review the survey results, please don't hesitate to share your thoughts with me. I'm eager to hear how these results compare with your own experience. And I welcome your thoughts on how banking institutions can improve their anti-fraud techniques across all channels.

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

Contents

Faces *of* Fraud

Complying with the FFIEC Guidance

Results, Expert Analysis from ISMG's Latest Fraud Survey

Survey Results

12 Faces of Fraud
18 Conforming to the FFIEC Guidance
24 2012 Fraud Investments
28 Fraud Agenda

84 percent of survey respondents faced credit/debit card fraud in the past year.

See **p.10** for sponsor analysis from:

IBM

Introduction

Following the Money Trail

After four years of slashed budgets and deferred expenses, 2012 brings good news to many financial institutions: They are getting an increase.

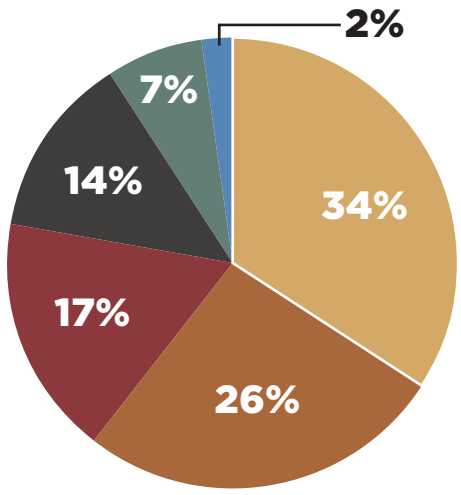
This is one of the bright spots of the 2012 Faces of Fraud survey. When asked how their 2012 anti-fraud resources will change, a whopping 58 percent of respondents say they expect an increase. This number is up considerably from 34 percent in 2010.

The troubling news is how ill-prepared institutions are to conform to the FFIEC Authentication Guidance – the highly publicized online banking security update that U.S. banking regulators issued in 2011. It was the year's single largest piece of security guidance for financial institutions, laying out expectations for regular risk assessments, layered security controls for online transactions and improved customer awareness programs. Regulators were clear that institutions needed to demonstrate conformance with this guidance beginning with their 2012 examinations.

Yet, in a series of questions about the guidance, survey respondents say:

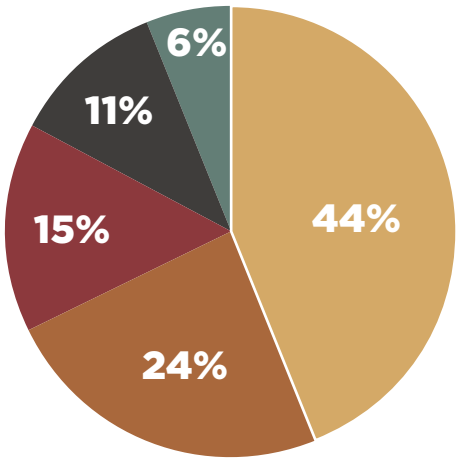
- Only 11 percent have come into conformance since the guidance was issued;
- 29 percent don't fully understand regulators' expectations;
- 88 percent expect no significant reduction of online fraud as a result of this guidance.

How will your fraud resources (budget and/or personnel) change in the coming year?



And while nearly 90 percent of respondents say they have conducted a risk assessment since the guidance was issued, only 41 percent say they have remediated any vulnerabilities uncovered during these assessments.

How do you assess your current level of conformance with the FFIEC Authentication Guidance?



- 44% - We are in partial conformance, but will be fully conformant later in 2012
- 24% - I don't know
- 15% - We were in full conformance before the guidance was issued
- 11% - We are in full conformance now
- 6% - We are in partial conformance, and we will not be fully conformant in 2012

Answers such as these beg the question: If institutions expect such significant resource increases, yet many do not even understand the FFIEC Authentication Guidance, then where will they make their anti-fraud investments?

This report aims to answer that question, presenting survey results and expert analysis to offer:

- A look at 2012's top fraud threats;
- How banking institutions plan to counter these threats;
- Top security investments to fight fraud and conform to the FFIEC Authentication Guidance.

About This Survey

Why We Study Fraud

This study marks the second time Information Security Media Group has studied fraud trends.

In 2010, ISMG released its inaugural Faces of Fraud survey, which was conducted in the wake of the 2009 surge of high-profile ACH/wire fraud incidents that ultimately led to the FFIEC Authentication Guidance. Among the first survey's findings:

- Fraud threats were growing ahead of available resources to deter and detect them;
- Cross-channel fraud growth was acknowledged, but not dealt with appropriately by technology solutions;
- 76 percent of institutions first learned about fraud incidents after the fact from their customers.

Since that initial survey, fraud has only continued to evolve and spread. Recent times have seen a steady stream of corporate account takeover incidents – a result of ACH/wire fraud targeting commercial accounts.

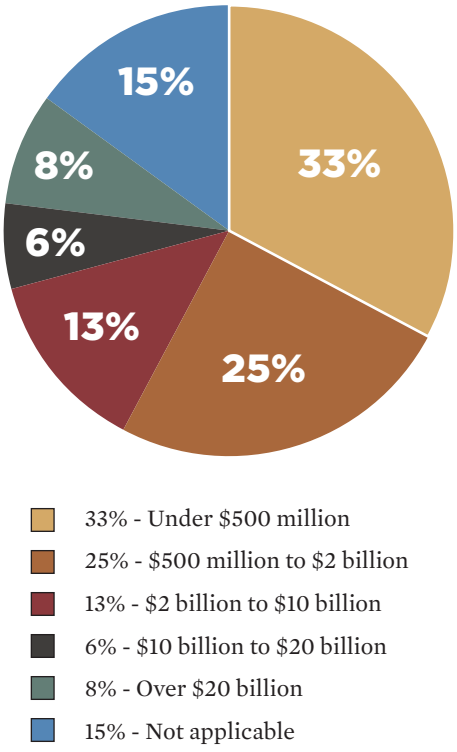
Skimming continues to be a thorn in the side of institutions – and not just conventional ATM skimming, but third-party point-of-sale hacks, such as 2011's breach at the Michaels craft store chain, which affected store customers and their financial accounts across the U.S.

Most recently, we saw the Global Payments Inc. payments processor breach, where potentially millions of payment cards were exposed to fraudsters.

Beyond the incidents of fraud, we also have the FFIEC Authentication Guidance. Even as U.S. banking regulators begin their first round of examinations to determine how well banks and credit unions conform to this guidance, our Faces of Fraud survey asks institutions for a self-assessment.

With this 2012 Faces of Fraud survey, we again set out to measure fraud trends, track anti-fraud investments and, of course, gauge institutions' responses to regulatory guidance. But we also want to identify the lessons learned since the first study. Where have institutions gained ground in the fraud fight? Where have they lost?

If a bank or credit union, what is your size by assets?



For the banking/security practitioner, these survey results and analysis provide a rare benchmarking opportunity.

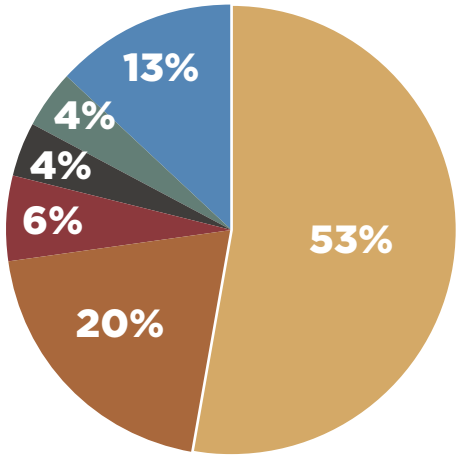
"The No. 1 thing, as you're going through those numbers, is realize that none of us is perfect and that not all of us can be in compliance with every rule and regulation that might be out there in the world," says Matthew Speare, senior vice president of IT at M&T Bank, Buffalo, N.Y. "But I would certainly hone in on 'How do I compare?' Because, as an example, where we're seeing this 58 percent increase in anti-fraud spending within banks, if you're cutting your budget back, you would be very out of sync with what your peer group is doing."

Financial institutions should review fraud trends and compare their experiences with the survey results, Speare says. "If I see that [incidents] are low, can I truly say that I'm doing better than those numbers? And if I'm not, then why not? And what do I do to fix it?"

This survey was crafted with expert insight from banking/security executives at top financial institutions, as well as leading fraud experts from major analyst firms and technology providers. Special acknowledgement goes to the five sponsors of this survey: Authentify, Guardian Analytics, i2, RSA Security and Wolters Kluwer.

The 2012 Faces of Fraud survey was conducted online in February, targeting subscribers to *BankInfoSecurity* and *CUInfoSecurity*. In all, the study attracted more than 200 respondents – more than 90 percent of them from banks and credit unions ranging from less than $500 million in assets to more than $20 billion.

How large is your organization's department assigned to fraud prevention and detection?



- 53% - 1 to 5
- 20% - 5 to 10
- 6% - 10 to 25
- 4% - 25 to 100
- 4% - More than 100
- 13% - We do not have a designated dept. Duties are managed by audit, compliance, IT, risk, etc.

Hot Topics

Key Themes Emerging from the Survey Results

The survey results unveil four key topics that will be explored in depth in this report:

The Faces of Fraud

What are the most common fraud threats institutions face, and which threats are they best prepared to face? We also explore the factors that increase institutions' exposure to fraud, as well as the toll fraud incidents take – hard costs and non-financial losses, too.

Conforming to the FFIEC Guidance

Why are financial institutions so unprepared to meet the expectations of the guidance, and when do they expect to achieve conformance? We show which recommended steps institutions have taken, and we share their overwhelming response to the question, "What's missing from the guidance?"

Anti-Fraud Investments

Some 58 percent of respondents expect increased anti-fraud resources in 2012, so where are they investing the money and personnel? We show a prioritized list of institutions' planned technology investments, then look at their stance on some emerging solutions.

The Agenda

2013 will be all about more - more fraud threats, more threat vectors, more anti-fraud solutions, perhaps even more regulation. How should banking institutions shape their fraud-fighting strategies? We share the tips gleaned from our survey results and expert analysis.

58 percent of respondents expect increased anti-fraud resources in 2012, so where are they investing the money and personnel?

2012 Faces of Fraud Survey

Complying with the FFIEC Guidance

This webinar looks not only at the latest fraud trends and how institutions are fighting back, but also at their progress in putting together layered security controls in conformance with the FFIEC Authentication Guidance.

The FFIEC Authentication Guidance update has been in circulation since mid-2011. But as banking examiners begin testing for conformance, we find:

- Only 11% of surveyed institutions have come into conformance since the guidance was issued;
- Nearly 30% don't fully understand the guidance;
- 88% do not believe the guidance will result in a significant reduction of online fraud.

Presented by

George Tubin
Information Security Officer
Wells Fargo Bank

Matthew Speare
Information Security Officer
M&T Bank

Tom Field
Vice President, Editorial
Information Security Media Group

Sponsored by

IBM · RSA · Guardian Analytics · Wolters Kluwer Financial Services · AUTHENTIFY

View This Webinar Now

Visit http://goo.gl/GvcFX

Or scan the QR code with your mobile device.

SPONSOR ANALYSIS

Faces of Fraud Survey: A Smarter Big Data Approach

By Robert Griffin, Head of i2 at IBM

Fifty-nine percent of banks say that investigation, forensics and recovery represent their biggest expense in combating fraud, according to the survey.

Robert Griffin

This is a strong indicator that the banking industry takes fraud seriously. At the same time, 82 percent of respondents say that customers are the first to make them aware of fraudulent activity. Clearly, there's a big desire for a smarter solution with enhanced alerting functionality, more flexibility and the ability to make use of existing data. The power of Big Data analytics solutions can better help address the problem.

IBM's Watson team estimates that 90 percent of the world's information was generated in the last two years. According to IBM's analytics solution center, 80 percent of it is unstructured information. As you make information access easier, it unfortunately – without the right infrastructure in place – opens up the doors for potential fraud.

A fellow IBMer, Anjul Bhambhri, vice president of development for Big Data projects, was recently quoted in a *Forbes* magazine article where she said, "The key to the Big Data approach is to be able to analyze all of this data, without moving it around, to gain better insights and to be able to do it in near-real-time when necessary."

As an example, an insurance company relies on a Big Data analytics solution to proactively review new policies to determine if they represent a potential for fraud – primarily through links/associations with known scammers or suspicious prior claims activity by policy holders.

Previously, an analyst would spend approximately 40 hours to manually evaluate more than 50,000 new policies each month. Because of the manual nature of the analysis, the analyst was not identifying all the potentially problematic policies and also had no real way to discern if there was a case of user error.

By creating a single repository and using sophisticated visual analysis capabilities, the analyst now can identify and understand the links between new policy holders and known scammers as well as identifying prior suspicious or problematic

At the end of the day, it's about a smarter approach to fraud prevention...

claims which have been filed by the new policy holder. The analyst now completes the work in about 12 hours and finds three times as many problematic policies.

At the end of the day, it's about a smarter approach to fraud prevention: detecting the problem before it happens, maximizing investments in existing systems and data sources, and employing solutions that can help banks easily distinguish potential fraudulent transactions from the legitimate ones.

For more insights on fraud, check out this video on YouTube: http://www.youtube.com/watch?v=0gXiK7Pcq1M

Griffin has spent more than 35 years in the software and services industry as a key player and successful entrepreneur. In Oct. 2011 he facilitated the sale of his current company, i2, to IBM into its Industry Solutions, Software Product Group, where he remains a business leader for Public Safety and Intelligence. Griffin joined i2 as the CEO in July of 2009, as a result of the merger between i2 and his former company, Knowledge Computing Corporation (KCC). The merger resulted in a global organization with over 350 employees servicing over 4,500 organizations in 150 countries.

Survey Results: Part I

Faces of Fraud

Threats. Detection. Loss.

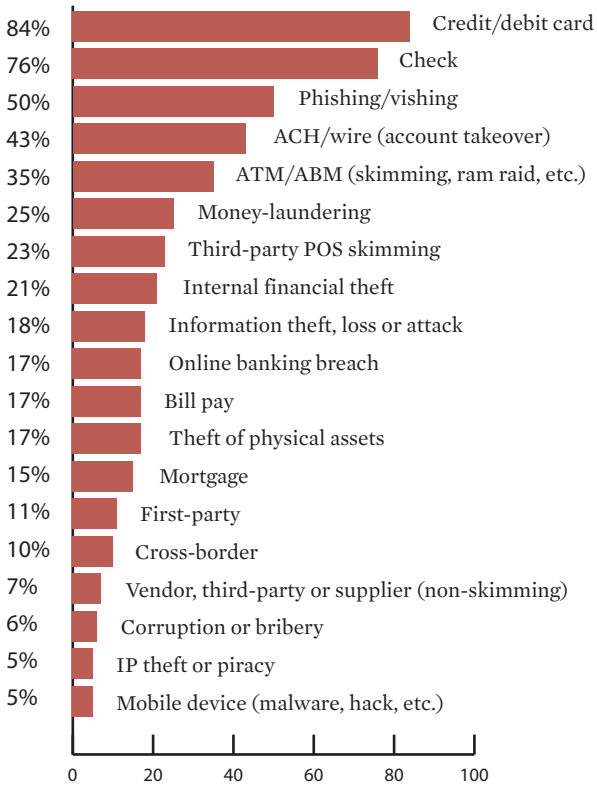
Fraud schemes have evolved. For example, conventional ATM skimming has morphed into growing incidents of vestibule skimming (devices placed on entrances of ATM lobbies) and pay-at-the-pump retail breaches.

But fraud threats to financial institutions are consistent. The top three threats in 2010 were payment card fraud, check fraud and phishing/vishing. These continue to be the top three threats of 2012.

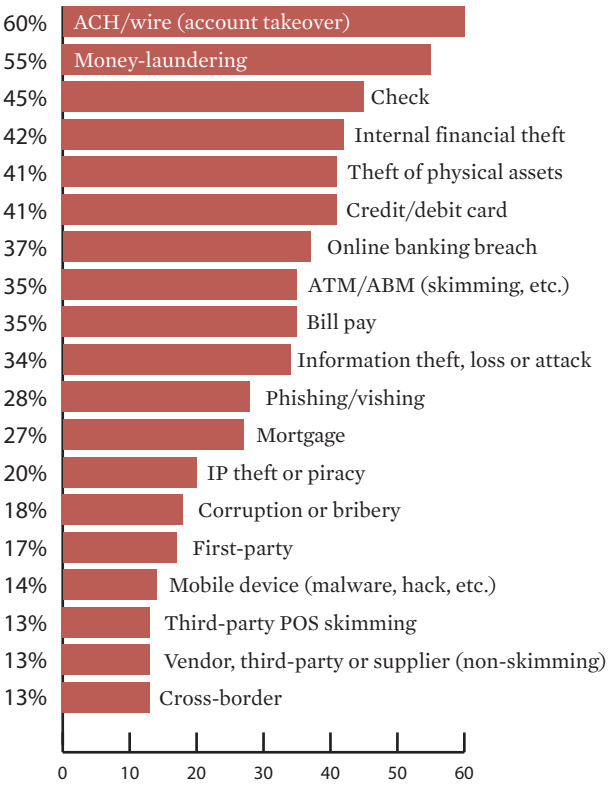
Also notable is the prevalence of ACH/wire fraud attacks. We hear less about these in the wake of 2011's high-profile lawsuits involving banks and commercial customers (i.e. Comerica v. Experi-Metal). But law enforcement officials and banking/security leaders maintain that ACH/wire is still a popular attack vector. And 2011's FFIEC Authentication Guidance calls these out as incidents institutions can and should prevent.

The other consistency between the 2010 and 2012 fraud surveys: The disconnect between the threats institutions face and those they feel best prepared to prevent and detect. Payment card fraud and phishing are among the top threats, but money-laundering and theft of physical assets are among the top threats banks feel best-prepared to thwart.

Which types of fraud has your organization experienced in the past year?



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



That ACH/wire fraud heads the "best prepared to prevent" list is a direct result, no doubt, of the FFIEC Authentication Guidance, which spells out specific security controls and process changes to prevent such incidents.

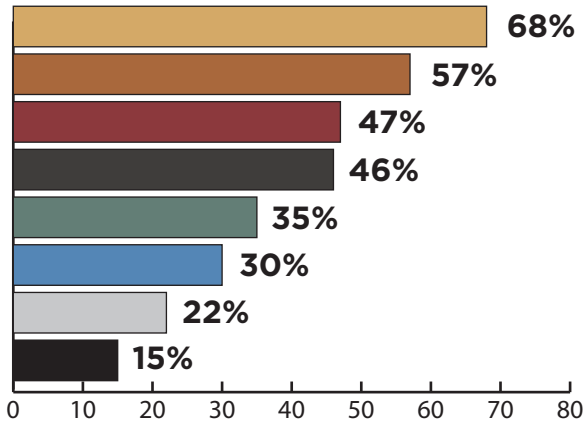
It's also no surprise to see check fraud near the top of the list of threats for which organizations are best prepared. This long has been a popular threat vector, and institutions have been well-fortified to defend against these attacks.

The lack of preparedness for thwarting phishing/vishing attacks is a concern because these incidents typically are an entry point for criminals. Once a fraudster implants malware through a phishing e-mail or talks a banking customer (or employee) into surrendering an account number, this is the start of account takeover, which can lead to huge fraud losses – particularly for commercial customers.

And while institutions are not getting better at being able to prevent these incidents, which typically occur outside the institutions' own communications channels, the fraudsters are getting better at mimicking corporate communications. They are also doing so cross-channel – through e-mails, telephone calls and text messages. So institutions must focus on educating staff and customers alike about the risks of socially-engineered schemes.

Indeed, survey respondents say their organizations' biggest challenge to fraud prevention is a lack of customer awareness.

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



- 68% - Lack of customer awareness
- 57% - Insufficient resources (budget and/or personnel)
- 47% - Inadequate fraud detection tools & technologies
- 46% - Difficulty integrating data from various sources
- 35% - Lack of staff awareness
- 30% - Difficulty investigating crimes across borders
- 22% - Organizational silos
- 15% - Poor coordination with law enforcement

Speare of M&T Bank believes awareness is always going to be an issue – because of human nature.

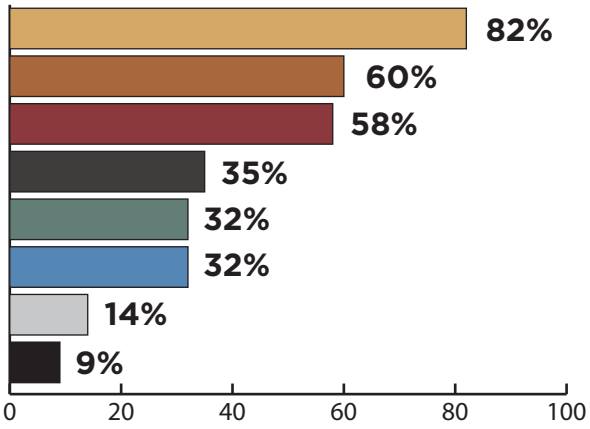
"I could take the investment that we make in awareness up 100-fold, but at the same time, I'm not sure that I would have any greater measurable results," Speare says. "We as humans just have this default setting that 'If I don't understand it, well, then that's okay,' and at the same time if it becomes difficult for me to take that extra step, well, I'm not going to do it."

Customers are not bankers or security professionals – all they want to do is access their funds – so many of the awareness efforts fall on deaf ears, Speare says. "But I think that we're all going to continue to make those investments because even if we get a 1 percent result, then it's 1 percent less that we have to respond to."

Detection

When it comes to detecting fraud incidents, banking institutions have lost ground. Asked in 2010 how a fraud incident involving your organization was typically detected, 76 percent said "when a customer notifies us." That number in 2012 has risen to 82 percent.

How is a fraud incident involving your organization typically detected?



- 82% - When a customer notifies us
- 60% - Through automated data analysis or transaction monitoring software
- 58% - At the point of transaction
- 35% - Third-party notification
- 32% - At the point of origination
- 32% - During account audit/reconciliation
- 14% - Internal whistleblower
- 9% - Third-party investigation

The issue is not so much that institutions lack fraud monitoring and detection tools that can pick up these fraud incidents. The problem is that the tools do not always work cross-channel, nor do they necessarily detect anomalous activity. Hence, the customers are the first to detect the incidents.

As we will see when we explore fraud investments in a later section, this is a hole institutions are looking to plug. Another fraud detection avenue to note: whistleblower or internal notification programs. When asked what type of program they currently employ, only 27 percent of respondents say they have none. The remaining breakdown (note: some organizations employ multiple techniques):

- Telephone hotline - 48 percent;
- Verbal - 38 percent;
- Computer-based - 37 percent;
- Written notification - 22 percent.

Other noteworthy points about fraud trends:

- 82 percent of respondents say fraud threats have increased in the past year;
- The top three factors to influence this increase: Evolving online threats, poor economic conditions and the complexity of the IT infrastructure (more points of attack);
- $5,000 is the most common financial threshold at which an incident transitions from a write-off to one that an organization will take action against.

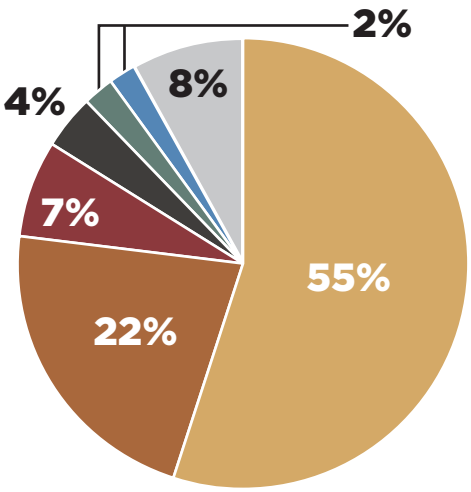
> "I could take the investment that we made in awareness up 100-fold, but I'm not sure that I would have any greater measurable results."
>
> – Matthew Speare, M&T Bank

Losses

Fraud losses are measured three ways in this study: Total dollar losses to fraud incidents; post-incident expenses (account monitoring, legal fees, etc.); and non-financial losses, such as productivity and reputation.

In terms of dollar losses, fraud incidents have exacted a relatively low toll. More than half of survey respondents lost less than $100,000 to fraud in 2011.

What do you estimate to be your organization's total dollar losses to fraud in the past year?



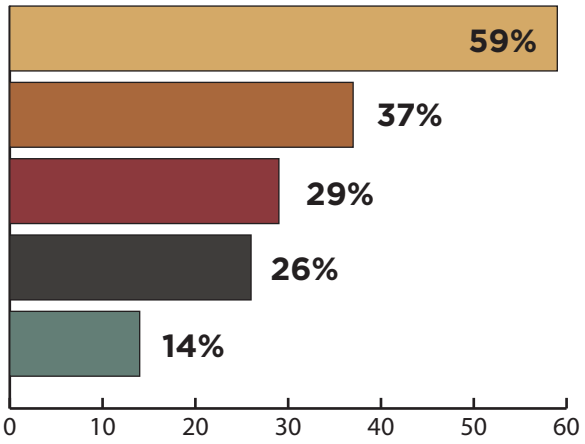
- 55% - Less than $100,000
- 22% - $100,000 to $500,000
- 7% - $500,000 to $2 million
- 4% - $2 million to $5 million
- 2% - $5 million to $10 million
- 2% - More than $10 million
- 8% - I don't know

But that's only a part of the picture. The true expense emerges when you look at the post-incident expenses institutions face (percentages refer to number of respondents who said they incurred these expenses):

- Investigations, forensics and recovery-related costs - 60%;
- Account monitoring - 43%;
- Legal costs - 32%.

And then there are the non-financial losses, which can exact an immeasurable toll (see chart).

Which non-financial losses did your organization suffer from fraud incidents?



- 59% - Loss of productivity
- 37% - Reputational impact
- 29% - No losses
- 26% - Customer accounts (moved to other institutions)
- 14% - Regulatory or other compliance issues (additional scrutiny from regulators or standards bodies)

It's troubling enough to lose customer accounts after incidents of fraud. But how does an institution measure the reputational loss post-breach? And what about the nearly 60 percent productivity loss?

At a time when breaches are not only more common, but more commonly reported in news media, the impact of "soft" fraud costs must be weighed more heavily.

Top non-financial losses suffered by organizations:

59% productivity

37% reputation

Expert Insights

Matthew Speare of M&T Bank on the Faces of Fraud

We see on a regular basis that the fraudsters themselves are not going to use the same techniques consistently. There's a lot of variability into how they are going to attempt to break in, and in some of these attempts we've seen what appeared to be some kind of a scripted playbook: "When the bank reacts like X, then we will do Y." It's quite the mix of old techniques and new techniques and multiple techniques at the same time.

And I think that makes it very difficult to be able to predict what is going to occur because certainly for the fraud attempt types that we've seen over the last couple of years, everyone's built up defensive mechanisms around those. What do you do, for example, when you provide cash management or wire transfer services to commercial customers and their machines are infected with Zeus malware? And at the same time, or immediately following attempts to do fraudulent wire transfers, you're hit with a denial-of-service attack? Your focus gets diverted to look at the denial of service because you have to keep those services up for your customers, and that opens that short window for fraudulent transactions to go out the back end.

So it's a constant variety of techniques coming at banks. We get good at looking at the historic impact of the schemes, but none of us is great at being able to predict what the fraudsters are going to try next.

Matthew Speare is senior vice president of IT at M&T Bank, based in Buffalo, N.Y.

Survey Results: Part II

Conforming to the FFIEC Guidance

Risk Assessments. Layered Security. Customer Awareness.

One of the top objectives of the 2012 Faces of Fraud survey is to gauge institutions' preparedness to conform to the FFIEC Authentication Guidance, including how they are prioritizing their efforts.

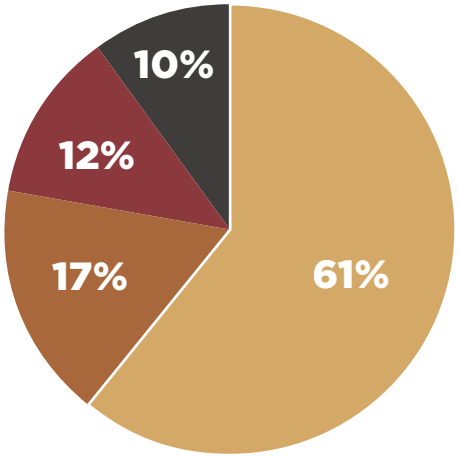
A draft of the guidance was inadvertently released at the end of 2010, and then the final guidance was issued in June 2011, so institutions have had more than a year to weigh their conformance options. In short, the guidance calls for:

- Periodic risk assessments;
- Layered security programs;
- Enhanced customer awareness.

U.S. institutions were told to demonstrate conformance to the guidance by the time of their next regulatory exam, starting in January 2012. Indeed, examinations are under way, but our survey finds institutions ill-prepared to show conformance – or even full comprehension.

In fact, only 61 percent of respondents say they clearly understand regulators' expectations.

Do you fully understand the expectations outlined in the FFIEC Authentication Guidance?



- 61% - Yes, the expectations are clear to me
- 17% - No, I have outstanding questions to be addressed by my examiner
- 12% - I don't know
- 10% - The guidance does not apply directly to my organization

This confusion may influence respondents' attitudes about the effectiveness of this guidance. When asked how the guidance will help reduce fraud at U.S. banking institutions, respondents say:

- Slight reduction - 51 percent;
- I don't know - 22 percent;
- No reduction -16 percent;
- Significant reduction - 12 percent.

Respondents also express widespread belief that the guidance fails to address the emerging mobile channel.

Gartner analyst Avivah Litan, a fraud expert, agrees that the absence of mobile in the guidance has confused banking/security leaders.

"The guidance does not address mobile with respect to authentication," Litan says. "So, the guidance spends some paragraphs talking about out-of-band authentication and how it is safer, how it should be used – that you can't use simple challenge questions; you should use more complex challenge questions ... and it doesn't address how that would work in mobile banking."

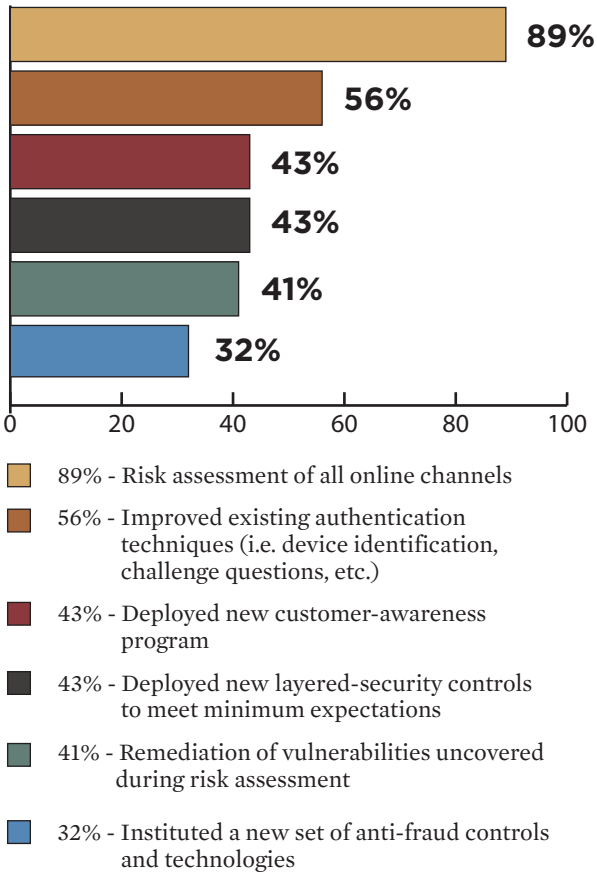
We'll review now how institutions say they have addressed the key elements of the guidance.

Risk Assessments

Most institutions have conducted their initial risk assessments, but far fewer have remediated any vulnerabilities uncovered by those assessments.

> The guidance does not address mobile with respect to authentication."
>
> – Avivah Litan, Gartner

Which elements of the FFIEC Authentication Guidance has your organization completed?



When asked how they conduct risk assessments, respondents say:

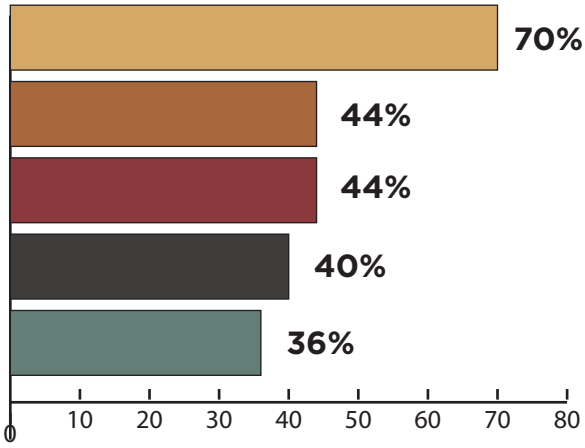
- 50% - We have an internal team/department that conducts assessments;
- 43% - We rely on a mix of internal and external resources;
- 4% - We use a third-party service provider.

Layered Security

When it comes to layered security programs, the FFIEC guidance lays out two minimum requirements: The ability to detect and respond to suspicious activity; enhanced controls of administrative functions for business accounts.

To this point, survey respondents say they have focused their efforts mainly on enhancing user authentication.

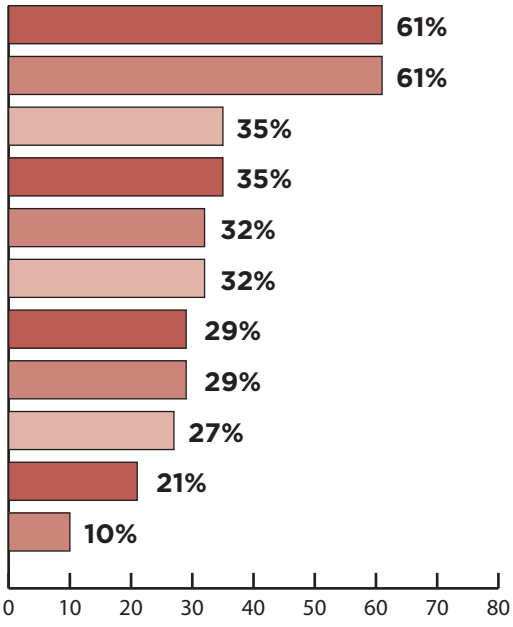
Which controls has your organization implemented to conform to the FFIEC's minimum requirements (process changes or technology) for layered security?



- 70% - Enhanced authentication
- 44% - Behavior-based anomaly detection technology
- 44% - Device ID
- 40% - Manual processes to detect online banking anomalies
- 36% - Rules-based technology

In describing a layered security program, the FFIEC also details nine effective controls that could be part of a program. Of these nine controls, survey respondents overwhelmingly favor enhanced customer education and fraud detection and monitoring systems – a consistent theme for investments institutions plan to make in the coming year.

Which of these recommended technology-based controls is your organization planning to invest in to conform to the guidance?

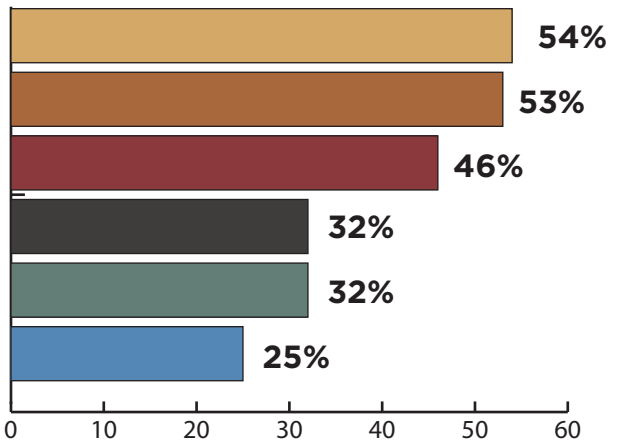


- 61% - Enhanced customer education
- 61% - Fraud detection and monitoring systems
- 35% - Out-of-band verification for authentication
- 35% - Enhanced controls over account activities
- 32% - Policies and practices for addressing customer devices identified as potentially compromised
- 32% - Enhanced control over changes to account-maintenance activities by customers
- 29% - "Positive pay," debit blocks, and other limits on transactional use
- 29% - Dual customer authorization through different access devices
- 27% - Out-of-band verification for transactions
- 21% - Internet protocol [IP] reputation-based tools
- 10% - None of the above

Customer Awareness

Customer awareness is a common thread throughout the survey results. It's recognized as a security vulnerability, and institutions rate it high among their planned investments. To get a glimpse of exactly what form awareness might take, we look at the FFIEC's specific expectations. Of the five recommendations spelled out in the guidance, two have been implemented by more than half of survey respondents.

Which elements of the guidance's customer awareness recommendations have you employed?



- 54% - An explanation of under what, if any, circumstances and through what means the institution may contact a customer
- 53% - An explanation of protections provided, and not provided, to account holders
- 46% - A listing of alternative risk-control mechanisms that customers may consider implementing
- 32% - A listing of institutional contacts for customers' discretionary use
- 32% - A suggestion that commercial online-banking customers perform a risk assessment
- 25% - None of the above

Why such a tentative approach to FFIEC conformance?

Fraud expert George Tubin, CEO of GT Advisors, believes some institutions are taking a "wait and see" attitude with regulators – treating their first post-guidance examination as a "dress rehearsal" for conformance at a later, drop-dead date.

"Institutions could be playing a very dangerous game here if they're waiting for a drop-dead date," Tubin says, because the regulators were clear that conformance was expected by 2012. "Institutions really do need to press on an accelerator pedal and finish this up and get stuff implemented."

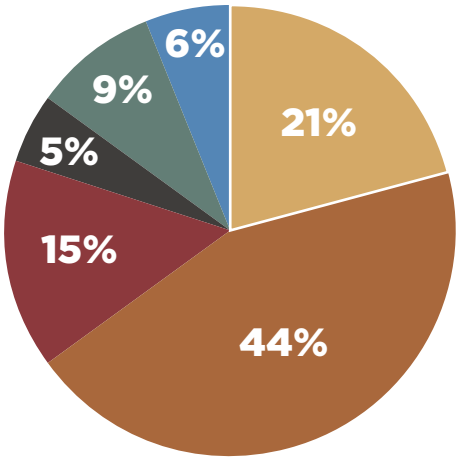
Also Notable

Few banking institutions enter into FFIEC conformance alone. They depend on third-party service providers to be conformant themselves or to help institutions achieve conformance.

Institutions need to ask their vendors many questions about conformance. For example, how often are security audits conducted for the vendor's products? And do these products conform to the FFIEC Guidance?

Judging by the following response, institutions are pleased with the answers they have received: 65 percent are somewhat or completely confident that their vendors are in conformance.

How confident are you that your key third-party service providers also conform to the FFIEC Authentication Guidance?



- 21% - Completely confident
- 44% - Somewhat confident
- 15% - Somewhat unconfident (some do, some don't)
- 5% - Not at all confident
- 9% - I don't know
- 6% - Not applicable

Yet, while institutions are confident in their vendors' conformance, they do not necessarily find their anti-fraud security controls to be effective. This is a topic to be explored in our next section.

65 percent of respondents are completely or somewhat confident that their third-party service providers conform to the FFIEC Authentication Guidance.

Expert Insights

Shirley Inscoe of Aite Group on FFIEC Conformance

I suspect that institutions are investing in the right things to achieve the letter of the law, but not necessarily the spirit of the law, as interpreted in the FFIEC guidance. They will probably achieve compliance, but they may not see much in terms of actual fraud-loss reduction, particularly in an environment where fraud attempts – and the sophistication level of many attempts – are increasing.

Compliance in the spring of 2012 does not automatically equate to compliance next fall. Every time institutions release a new product, a product enhancement or make changes to a delivery system, such as online banking, for example, they have to evaluate that change, in terms of compliance, and make sure they take the appropriate action.

Most banks and credit unions are rating the FFIEC requirements with goals of passing an examination. Only the smartest ones are really using this as a tool to better fight cross-channel fraud and to reduce losses effectively.

Even though it is 2012, don't be in a rush to buy anything. Take the time to do a thorough risk assessment right now, if you haven't already, and factor in the changes your institution is planning, as well as the environment. Develop a strategic plan for the next three to five years to fight fraud and protect your customers.

Aite Group analyst Shirley Inscoe, formerly of Wachovia Bank, has 30 years of banking experience in enterprise fraud and payments issues.

Panel Discussion: Top Fraud Threats

Which Trends Should Concern Banking Institutions Most?

Editor's Note: Following is an excerpt from the panel discussion that accompanies the 2012 Faces of Fraud Survey webinar. Participants are Tom Field, vice president, editorial, Information Security Media Group; Matthew Speare, senior vice president of IT at M&T Bank; and George Tubin, CEO at GT Advisors. To hear the full discussion, please register for the session. For more details, see pages 9 and 38.

George Tubin

Matthew Speare

TOM FIELD: What are the trends that concern you the most, and what do financial institutions need to do in terms of solutions to better detect and prevent fraud?

MATTHEW SPEARE: From just overall trends, the number one thing has been the volume, and that has caused the most problems for the larger banks. As we went into the economic downturn, what we saw was just a steady increase in the types and the sheer numbers of fraudulent attempts. So, how does an institution respond? One would hope that you could do it systematically, but at the same time it's up to the individual banks and their ability to be able to scale those processes and keep up the level of due diligence.

It becomes fatiguing after a while. [The fraudsters] are getting customers to click on links that they shouldn't, which infects PCs. Or they're doing drive-bys, meaning that just by someone going to a perfectly legitimate website they get infected because security controls on a lot of the websites aren't what they should be. So, I don't think that it's any particular [kind of] fraud that's gone up; it's just the sheer volume.

GEORGE TUBIN: The things that are being done right now to prevent some of the more advanced cyberfraud -- the browser types of attacks -- are the right things to be focusing on, as well as putting in layered security controls and really understanding that you don't know what you don't know. You need to have multiple ways of detecting potential fraud.

Having a platform that's flexible and extensible and able to be modified as you see the need to do so -- that's where layered security really helps. And I think once institutions get their arms around that and really understand how to put those components together and how they work with each other, you will start to see better ability in detecting and reducing fraud.

We're seeing man-in-the-browser now, and in a short amount of time we'll see something else, and eventually we'll see mobile. We'll be fighting fraud forever. It keeps changing, and we keep trying to stay ahead of it. The industry just shouldn't be surprised anymore when new threats come out, but [banks] really should have the types of systems and architecture in place that can be flexible enough that they can sort of reform themselves to be able to deal with whatever new is hitting them.

Survey Results: Part III

2012 Fraud Investments

Anti-Fraud Controls. Effective Solutions. Emerging Technologies.

We have established that 58 percent of survey respondents expect to increase their anti-fraud resources in 2012.

But why such a sudden surge – up 24 percentage points since 2010?

One of the drivers is that institutions no longer can put off the anti-fraud investments they avoided beginning with the 2008 economic crisis, says Speare of M&T Bank. "You can only defer certain types of solutions for so long, and then you have to deal with them."

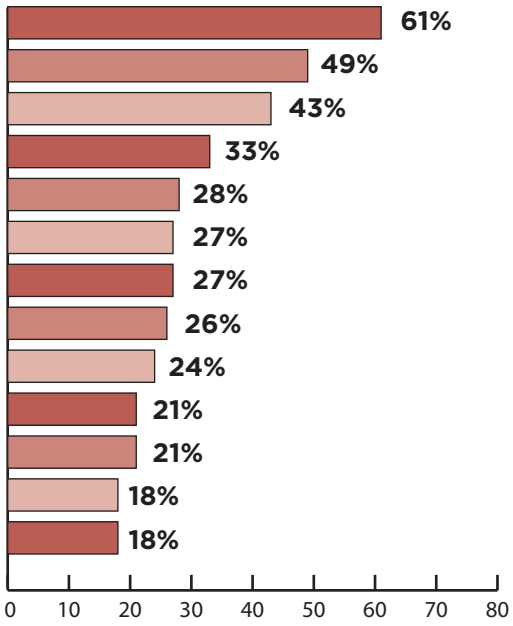
And then there is the immediacy of the FFIEC guidance, says Tubin of GT Advisors. "Regulation drives spending," he says. "Banks are in a situation where the regulators are telling them they have to do something – they have to make improvements – and therefore the bank has to spend some money on technology."

Now, where will they invest these increased resources? Here are their top priorities:

- Technology - 41 percent;
- Personnel - 12 percent;
- External services - 9 percent;
- All of the above - 20 percent.

Asked about specific investments planned over the next year, respondents heavily favor fraud monitoring and detection, as well as customer/staff awareness – in line with the expectations of the FFIEC Authentication Guidance.

Which of the following anti-fraud controls and measures does your organization plan to invest in over the next 12 months? (Top 12 answers)



61% - Fraud detection and monitoring systems

49% - Staff training

43% - Enhanced customer education

33% - Out-of-band verification for a) authentication and b) transactions

28% - Enhanced controls over account activities

27% - Vendor management

27% - Internal or external audit

26% - Anti-money laundering tools

24% - Dual customer authorization through different access devices

21% - Case management or investigation management systems

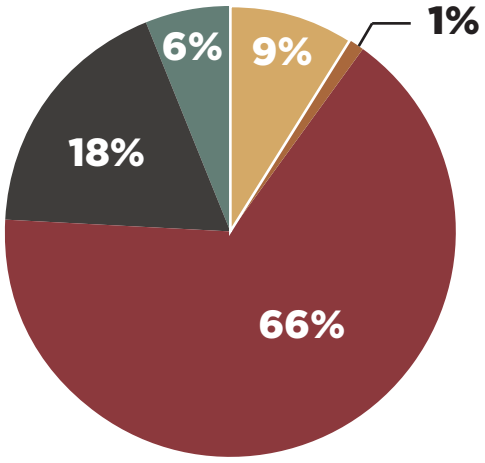
21% - Enhanced tracking of high-risk customers

18% - "Positive pay," debit blocks, and other limits on transactional use

18% - Anti-phishing related technologies and services

It's important to balance these priorities, though, with a look at institutions' opinions about the effectiveness of current security controls. Only 9 percent consider these controls "very effective," which suggests that technology vendors have some work to do to change this perception.

In your opinion, how effective are current anti-fraud security controls?



- 9% - Very effective: Consistently detect cross-channel patterns; keep pace with fraud trends
- 1% - Effective
- 66% - Somewhat effective: Struggle to work cross-channel; difficult to integrate with other applications and tools
- 18% - Ineffective: Fail to keep up with evolving threat landscape
- 6% - Not applicable: Current levels of fraudulent activities don't warrant the investment in controls

Inscoe, the analyst with Aite Group, says institutions also must improve their understanding of what technology can and cannot do.

"Sometimes it is a mistake to consider a case management system a fraud detection tool. When a case arises, a potential loss has already occurred," Inscoe says. "At this point in time, bankers and credit union executives should be looking for systems that handle a wide variety of types of fraud, not just one silo, like check fraud or debit card fraud. They need to be looking for a vendor that can help them with multiple types of fraud, and, hopefully, tie information together in an attempt to identify cross-channel fraud when it occurs."

The survey also asks questions about specific technologies. The responses show that institutions are conservative about investing in some emerging or evolving solutions. Among them:

Device Identification

Device ID is an important topic in the discussion of security controls. The FFIEC discourages the sole use of simple device ID – a cookie on a user's PC – urging institutions toward complex methods such as one-time cookies and device fingerprinting. Respondents are closely split on the methods they employ, with only 17 percent saying they do not use device ID at all.

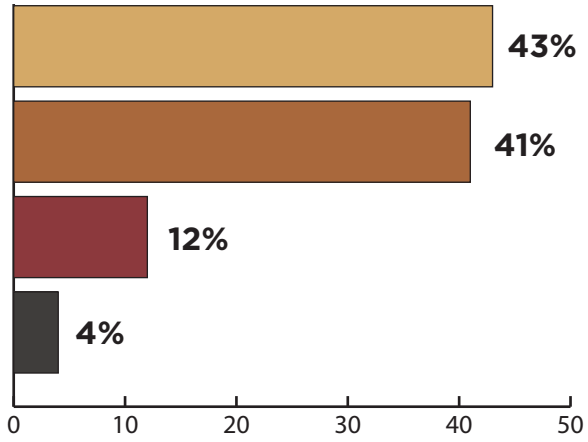
What type of device-identification techniques do you currently employ?

- We do not employ device identification - 17%
- We employ complex device identification (i.e. one-time cookies, device reputation checks, device finger-printing) - 36%
- We employ simple device identification (i.e. a cookie loaded on the user's PC) - 47%

Challenge Questions

In the FFIEC Authentication Guidance, banking regulators are critical of institutions that rely on static challenge questions that depend on answers that might be readily available on a social networking site. The security trend is more toward out-of-wallet questions that rely on less accessible information. Again, survey respondents are split on their use of the different methods.

What type of challenge questions do you currently employ?



- 43% - Out-of-wallet questions that rely on information that is not publicly available
- 41% - Static challenge questions that rely on information that may be publicly available (i.e. mother's maiden name, favorite sports team)
- 12% - We do not employ challenge questions
- 4% - Red-herring questions meant to trick a fraudster

Transaction Signing

Transaction signing solutions are deployed to provide banking institutions the ability to use one-time passwords to conduct digitally signed online transactions with their business and consumer account holders. The same solutions can be used to authenticate users. The practice has gained traction in some European and Asian markets, but is relatively new to the U.S. Respondents acknowledge their lack of familiarity:

Have you deployed (or are you considering) a transaction signing solution to your corporate or retail customers to help prevent unauthorized user access?

- Don't know enough about transaction signing - 54%
- No - 26%
- Piloting a program now - 4%
- Yes - 16%

Mobile Banking

Mobile is another recurring theme in the survey results. Respondents are concerned about evolving threats (i.e. mobile malware) and increasing points of attack. They also point to what they perceive as a glaring oversight of the FFIEC guidance: Mobile. So, how are institutions helping to mitigate fraud in this growing channel?

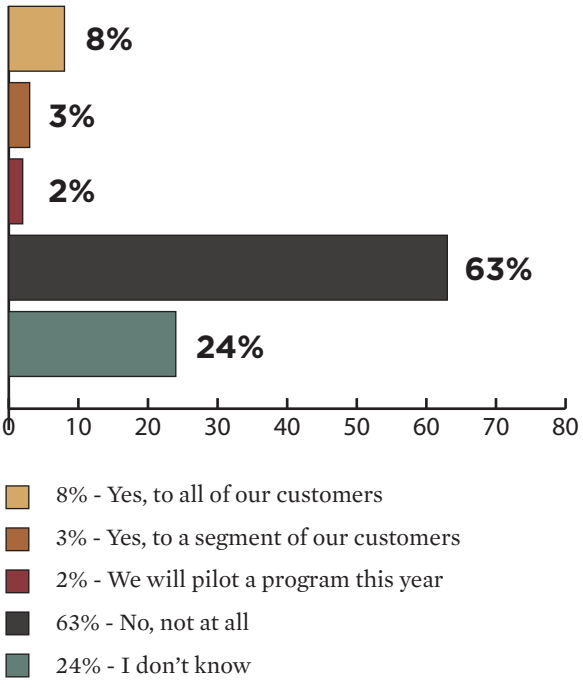
Mobile banking is increasingly prevalent – and so are fraud threats to mobile customers: How do you prevent/detect mobile banking fraud?

- Anomaly detection - 22%
- Customer education - 41%
- Device identification - 34%
- Transaction limits - 32%
- Transaction signing - 5%
- User authentication - 56%
- We do not offer mobile banking - 44%

EMV

The conventional mag-stripe payment card is approaching the end of its life span. Most global markets have made the move to the chip-and-PIN security method of the Europay Mastercard Visa (EMV) standard. This transition is slower in the U.S., where the mag-stripe remains the standard. But even some U.S. institutions are piloting EMV programs, particularly for customers who travel abroad to EMV markets. According to our results, the pilot programs are the exception, not the rule.

If your organization is a banking institution, does it offer payment cards compliant to the Europay Mastercard Visa (EMV) security standard?



Expert Insights

Q&A: Avivah Litan of Gartner Group on Banks' Fraud Investments

INFORMATION SECURITY MEDIA GROUP: How far along are banks in their conformance to the FFIEC guidance?

AVIVAH LITAN: On average, 50 percent done. They are in the middle of making improvements based on the risk assessment. So, it is an ongoing process; you can't change banking systems overnight. There is a lot to be done, for example, if you're moving from simple challenge questions to out-of-band authentication. You have to spend a lot of time just getting the phone numbers of your customers up to date. That is not always so easy, especially if you are a business customer. So that could take six months to a year alone - maybe even more than that.

ISMG: Are institutions focusing too much attention on customer education?

LITAN: It depends on who you ask. I have seen the results of the survey that demonstrate the smaller [institutions] think security and fraud should be solved by their customers. So, for the ones that think it's the customer's issue, yes, I think they are putting too much weight on it.

But I do think, assuming that everybody takes equal responsibility for the problem, customer awareness is very important because it can help avoid a lot of mishaps. Certainly some of the fraud that we're seeing from sophisticated Trojans, you can't expect the customer to see that on their desktop. But at least if you make them aware of security issues, they'll call in right away if something is unusual, or they may not fall for a phishing attack.

So, it is important to share responsibility across customers and banks, but definitely not rely on your customer for your entire fraud strategy.

Avivah Litan is a fraud expert and analyst with Gartner.

Fraud Agenda

"What One Factor ...?"

Anticipate Threats. Verbatims. Action Items.

At the conclusion of the 2012 Faces of Fraud survey, we ask respondents a simple, open-ended question:

"What one factor could make the greatest difference in your organization's efforts to improve detection and prevention of fraud?"

Among the 200-plus responses, there are common themes captured by these verbatim answers:

- "Better customer awareness;"
- "Cooperation between processors and financial institutions;"
- "Cross-channel fraud detection;"
- "Losing the 'it'll never happen to us' attitude;"
- "Secure the call center."

These responses echo many of the topics discussed in this report – evolving fraud threats, regulatory compliance, layered security solutions and greater awareness.

They also help to inform our fraud-fighting agenda. Based on the survey results and expert analysis, these six items emerge as priorities for the fraud-fighting agenda (see next page).

Expert Insights

George Tubin, Fraud Analyst, on Securing Resources

Banks tend to have a rearview mirror approach. They look at the amount of fraud they had last year, and a fraud manager may say: "As long as I stay within that percentage or don't go over a certain threshold, I'm doing okay."

Now, as volume increases or the market changes, sometimes people don't look at absolute fraud numbers. You may still be within your limits when the actual amount of fraud has gone up significantly. That sometimes is one of the problems – this sort of siloed view, where "As long as I'm OK within my silo, everything's OK." There's not enough looking across all the different payments types and delivery channels.

It's not easy to get investments in something that you expect to happen, or that could have been an anomaly. For instance, maybe you had a slight increase in fraud in a certain area, but what's to say it's not going to come back down? How do you try to prove that there's going to be a continued threat and a continued need to have enhanced protection in a certain area?

It's important for the fraud organization to look forward and really think out of the box about what all the benefits are to implementing better fraud detection and prevention technology. Then they must report this perspective to senior management, so that the rest of the organization understands the value that's being brought to bear.

George Tubin, formerly a researcher with Tower Group, is CEO of GT Advisors.

Action Items

1. Improve Cross-Channel Fraud Detection

It is unacceptable that, 82 percent of the time, institutions first learn of a fraud incident when their customers notify them. Fraudsters are pursuing financial accounts through every available channel – simultaneously. Institutions, then, must invest not just in the tools to detect anomalous activity across all channels, but also in the processes that will finally break down the communications barriers that keep the individual channels and their stakeholders siloed.

2. Treat the FFIEC Authentication Guidance as a Starting Point

There is no good excuse for failing to understand regulators' expectations or for not knowing whether your own institution is in conformance. Risk assessments, layered security programs and customer awareness are minimum expectations that must be met now. And they must be improved upon over time, as threats evolve. The fraudsters have not called time-out to wait for conformance questions to be answered. Neither should banks.

3. Prepare for Mobile

It is time to recognize that mobility is no longer an emerging channel - it's here. And even in the absence of specific mobile guidance, institutions must act. As more banks and customers move into mobile, so will the fraudsters. Anticipate their schemes by investing in mobile security technologies that fight malware, authenticate users and transactions and maximize mobile as an out-of-band security control.

4. Prioritize Anti-Fraud Investments

A majority of institutions expect additional fraud-fighting resources in 2012, yet far too few are prepared to conform to the FFIEC Authentication Guidance. Survey results dictate that institutions must start with investments in risk assessments, layered security programs and improved customer awareness. But conformance is a beginning, not a destination. Anti-fraud investments must be prioritized over the coming year – and beyond – to match the sophistication and cross-channel nature of the evolving threats.

5. Perform Due Diligence

Survey results convey a mixed message about technology vendors. On one hand, institutions have confidence in the vendors' FFIEC conformance. But then institutions rate low the effectiveness of vendors' technologies. Institutions and vendors must engage in open discussions about compliance, security and emerging threats. It is the vendor's responsibility to provide good answers, but first, the institutions must ensure they are asking the right questions.

6. Raise Fraud Awareness: Starting Within

Awareness is not just about the customer. To ensure sufficient resources and buy-in for effective anti-fraud solutions, banking/security leaders also must educate their bosses and board members to the changing threat landscape, regulatory mandates and the potential costs of a breach. Hard costs are one component, but do not forget to discuss loss of productivity and reputation. These are the items that will quickly raise awareness levels and ensure support for anti-fraud activities.

Resources

Want to learn more about the 2012 Faces of Fraud survey results and analysis? Please check out these additional resources:

Webinar:

2012 Faces of Fraud Survey: Complying with the FFIEC Guidance

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:

- A look at 2012's top fraud threats;
- How banking institutions are countering these threats;
- Top security investments to fight fraud and conform to the FFIEC Authentication Guidance.

http://www.bankinfosecurity.com/webinars/fraud-survey-2012

Interviews:

FFIEC: How Well Do Banks Conform?

How well do banks conform to the FFIEC's updated Authentication Guidance? Gartner analyst Avivah Litan says most have made progress, but they still struggle with the details.

http://www.bankinfosecurity.com/interviews/ffiec-how-well-do-banks-conform-i-1537

How to Prioritize FFIEC Fraud Investments

When it comes to the FFIEC Authentication Guidance, Aite analyst Shirley Inscoe fears too many banking institutions are investing only in achieving compliance – not ongoing security.

http://www.bankinfosecurity.com/interviews/how-to-prioritize-ffiec-fraud-investments-i-1540

Fighting Fraud: The Bank's Perspective

Banking institutions expect significant increases in fraud-fighting resources in 2012. But in which solutions should they invest? Banking CTO Michael Wyffels has some prioritized suggestions.

http://www.bankinfosecurity.com/interviews/fighting-fraud-banks-perspective-i-1543

From Our Sponsors:

Phishing: New and Improved

Phishing - it's the classic scheme that never goes away. In fact, it evolves. Amy Blackshaw of RSA offers insights on how to respond to this and other trends identified in the 2012 Faces of Fraud survey.
http://www.bankinfosecurity.com/interviews/phishing-new-improved-i-1523

Fraud Fighting: How to Engage the Customer

When it comes to fighting financial fraud, Peter Tapling of Authentify says banking institutions are chronically underestimating and under-utilizing one key resource: Their own customers.
http://www.bankinfosecurity.com/interviews/fraud-fighting-how-to-engage-customer-i-1534

The Anti-Fraud Evolution

When Joseph Bognanno of Wolters Kluwer Financial Services examines 2012's financial fraud trends, all he sees is more – more of everything, from schemes to new guidance. How can banks stay ahead?
http://www.bankinfosecurity.com/interviews/anti-fraud-evolution-i-1546

The Hidden Costs of Fraud

Dollars lost of fraud are one measure of an incident's impact. But the "soft" costs – loss of reputation and productivity – are the ones that most get the attention of Terry Austin of Guardian Analytics.
http://www.bankinfosecurity.com/interviews/hidden-costs-fraud-i-1551

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

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

ISMG
INFORMATION SECURITY
MEDIA GROUP

4 Independence Way • Princeton, NJ • 08540 • www.ismgcorp.com