2017 FACES OF FRAUD SURVEY

MOBILE EXPLOITS COME OF AGE,
AND FOCUS TURNS TO
IMPROVING CUSTOMER EXPERIENCE

VASCO®
TRUST FOR THE DIGITAL WORLD

iSMG
INFORMATION SECURITY
MEDIA GROUP

Tom Field
Senior Vice President, Editorial

2017 Actionable Threat Intelligence Survey

Only 38 percent of banking/security leaders have high confidence in their organization’s ability to detect and prevent fraud. Meanwhile, 66 percent say the number of fraud incidents has stayed steady or risen in the past year, and 58 percent say financial losses have remained the same or increased.

These are some of the findings of the 2017 Faces of Fraud Survey. Roughly 250 banking/security leaders participated in this survey, which was conducted to determine:

- The top forms of fraud afflicting financial organizations in 2017;
- The biggest gaps in organizations' efforts to detect and prevent fraud;
- What organizations are doing to counter the surge in mobile exploits, while at the same time attempting to preserve a frictionless customer experience.

Ninety-eight percent of respondents expect the same or increased budget for fraud prevention in 2018. Their top investment priorities are staff training, new anti-fraud tools and customer awareness. Are these the smartest investments they can make? That is the key question to be answered in this report.

Read on for full survey results, as well as expert analysis of how to put this information to use to improve your organization’s ability to detect and respond to financial fraud.

Best,

Tom Field
Senior Vice President, Editorial
Information Security Media Group
tfield@ismg.io

About this survey: This survey, conducted online in the summer 2017, generated more than 250 responses from banking institutions of all sizes, primarily in the U.S. Roughly one-third of respondents are from institutions with more than $2 billion in assets under management.

About VASCO:

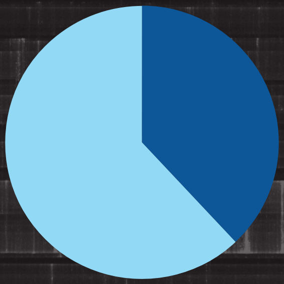
VASCO is a global leader in delivering trust and business productivity solutions to the digital market. VASCO develops next-generation technologies that enable more than 10,000 customers in 100 countries in financial, enterprise, government, healthcare and other segments to achieve their digital agenda, deliver an enhanced customer experience and meet regulatory requirements. More than half of the top 100 global banks rely on VASCO® solutions to protect their online, mobile and ATM channels. VASCO's solutions combine to form a powerful trust platform that empowers businesses by incorporating identity, fraud prevention, electronic signatures, mobile application protection and risk analysis.

https://www.vasco.com

VASCO
THE AUTHENTICATION COMPANY

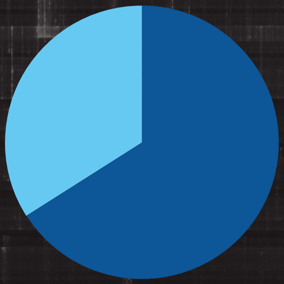
By the Numbers

Some statistics that jump out from this study:



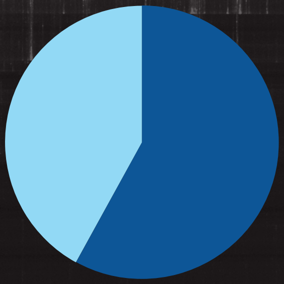
38%

of banking/security leaders have high confidence in their organization's ability to detect and prevent fraud.



66%

say the number of fraud incidents has stayed steady or risen in the past year.



58%

say financial losses have remained the same or increased.

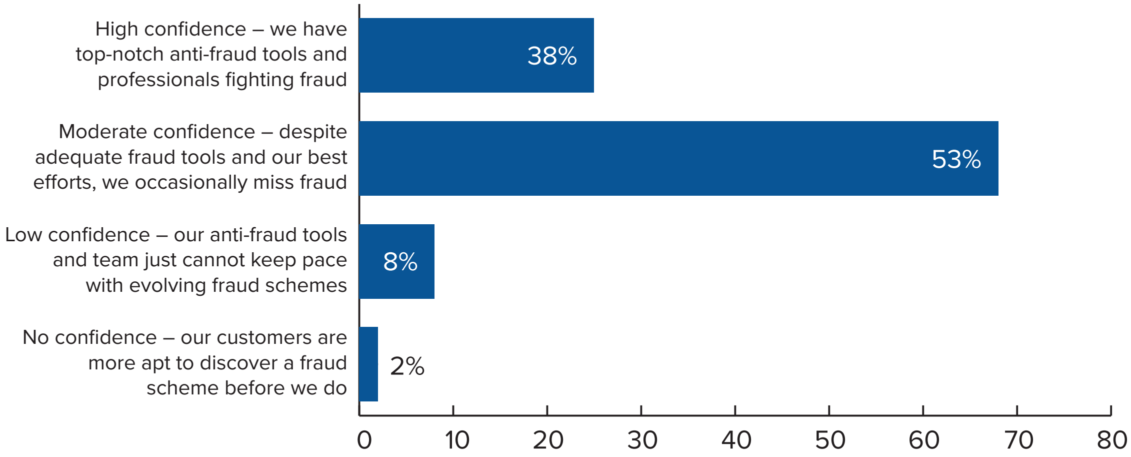
Baseline Fraud Defense

This opening section of the report takes the pulse of the respondent base, reviewing their gut feelings about the current fraud environment. To hammer home the key message from these statistics:

Only 38 percent of respondents have high confidence in the tools and staff that make up their organization's ability to detect and prevent fraud.

Read on for other baseline responses.

What is your level of confidence in your organization's ability today to detect and prevent fraud before it results in serious business impact on your enterprise or your customers?

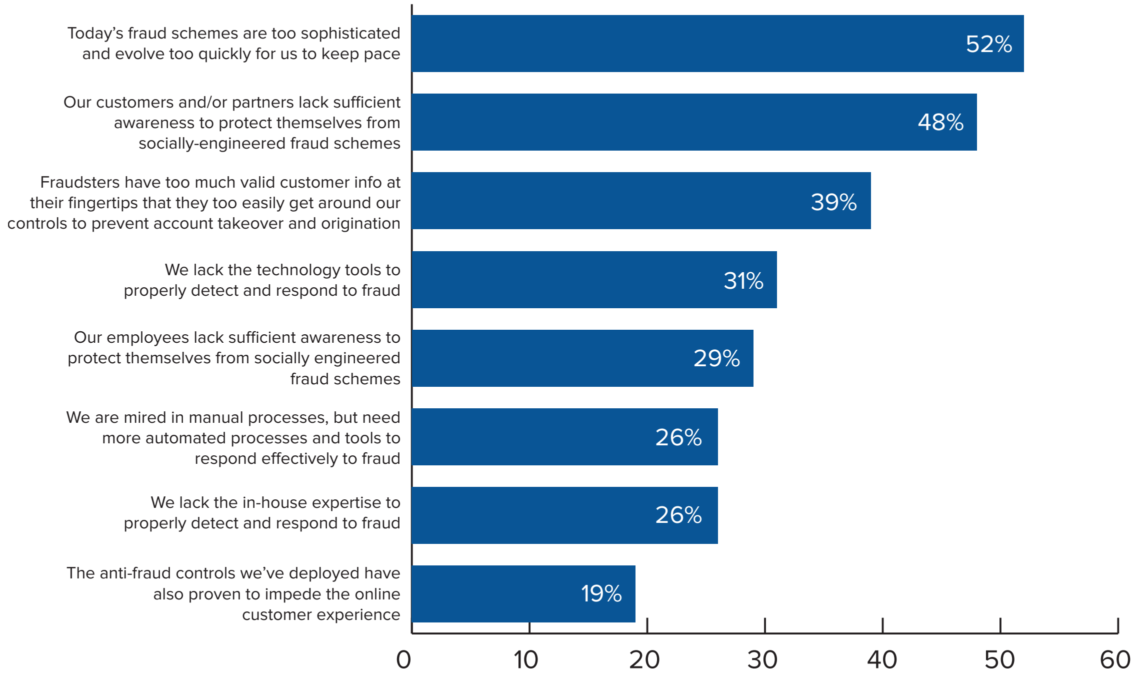


It is a daunting statement to start the review of survey results with the reality that barely over one-third of respondents have high confidence in their anti-fraud tools.

In contrast, not quite 10 percent report low or no confidence in their abilities to fight fraud. But at a time when fraud incidents and losses continue to grow, only 53 percent of banking/security leaders say they have even moderate confidence in their anti-fraud controls and staff.

At a time when fraud incidents and losses continue to grow, only 53 percent of banking/security leaders say they have even moderate confidence in their anti-fraud controls and staff.

What do you believe to be the top three vulnerabilities in your fraud defenses? (select three that apply)

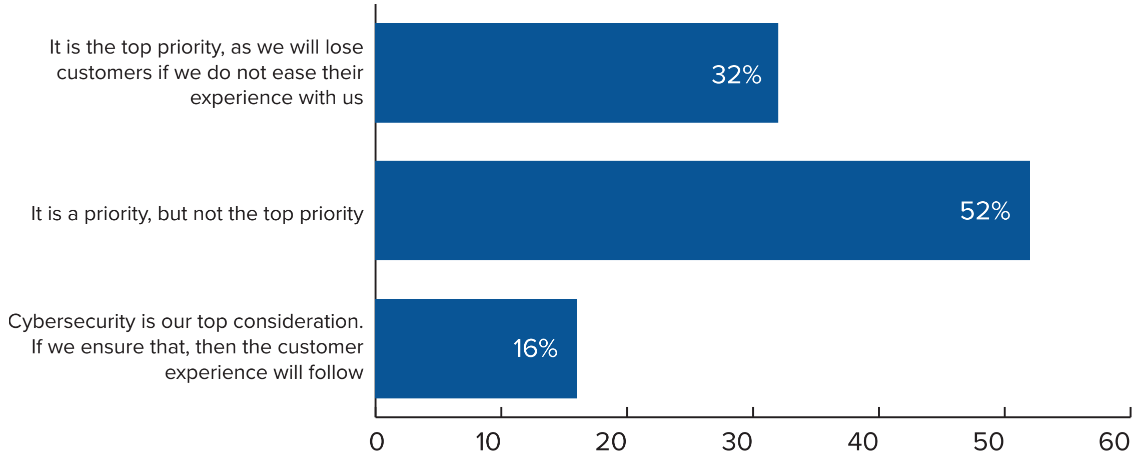


Asked to list their top three vulnerabilities in fraud defenses, 52 percent of respondents say today's schemes are too sophisticated and evolve too quickly for them to keep pace. Other top responses: Customers and/or partners lack sufficient awareness to protect themselves from socially engineered fraud schemes, and fraudsters have too much valid customer information at their fingertips that enables them to easily get around controls to prevent account takeover and origination.

Note: This survey was completed before the September announcement of the Equifax breach, in which 143 million US consumers saw their account data compromised—an incident that down the road could impact statistics related to account takeover and origination.

Fifty-two percent of respondents say today's schemes are too sophisticated and evolve too quickly for them to keep pace.

How does “frictionless customer experience” rate as a priority for your organization as you roll out new anti-fraud controls?



“Frictionless customer experience” is one of the most frequently used terms of 2017, as organizations struggle to find that balance between true security and ease of use. How big of a priority is this “frictionless customer experience” for survey respondents? Roughly one-third say it is their top priority because they will lose customers if they do not ease that experience. Just over half say it is a priority, but not the top priority. Sixteen percent say cybersecurity trumps customer experience.

The next section of the report delves into the specific 2017 faces of fraud to see which forms are causing the most trouble for financial institutions – and how they are responding.

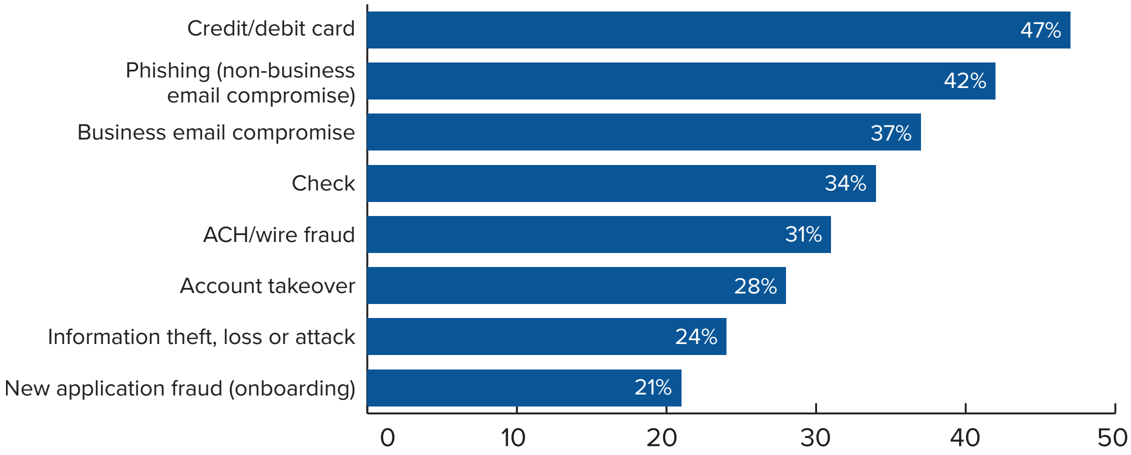
> ***‘Frictionless customer experience’ is one of the most frequently used terms of 2017 as organizations struggle to find that balance between true security and ease of use.***

2017 Faces of Fraud

Top forms of fraud, fraud rates, detection and mobility – these topics are all part of this Faces of Fraud section. Some key statistics to consider upfront:

- 47 percent of respondents say payment card fraud remains a top concern.
- 35 percent say they have helped secure the mobile channel by deploying multifactor authentication.
- 55 percent say lack of productivity is their biggest nonfinancial loss suffered because of fraud.

Overall, which types of fraud has your organization experienced in the past year? (check all that apply)



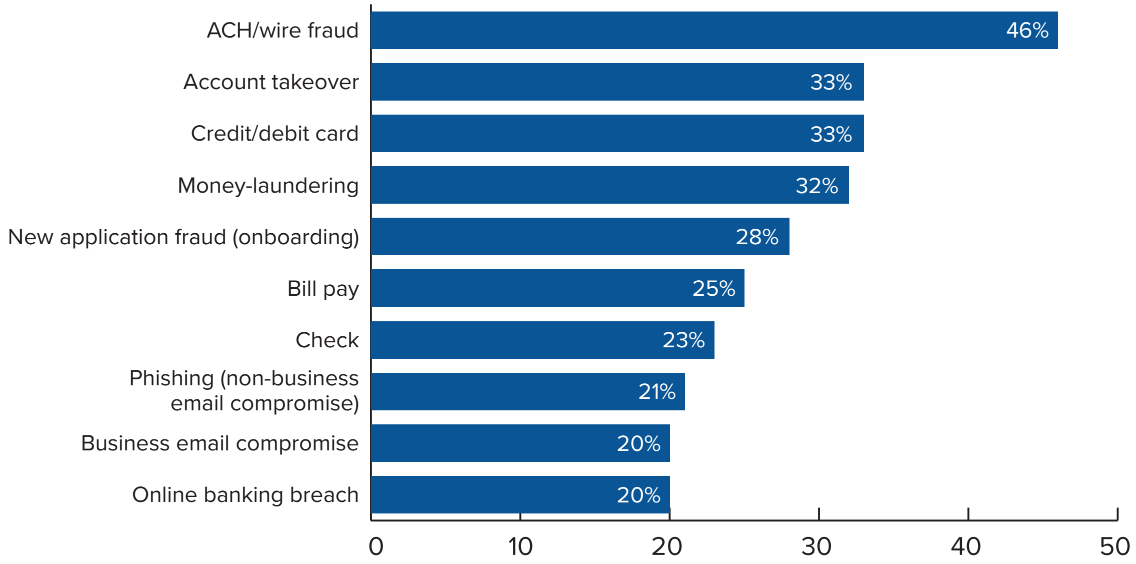
No surprise, given the continued headlines about payment card breaches and business email compromise: When asked to report the top forms of fraud their organizations have experienced in the past year, respondents say their top three are:

- Credit/debit card fraud – 47 percent;
- Phishing (non-business email compromise) – 42 percent;
- Business email compromise – 37 percent.

As for what forms of fraud they believe their organizations are best prepared to prevent and detect ...

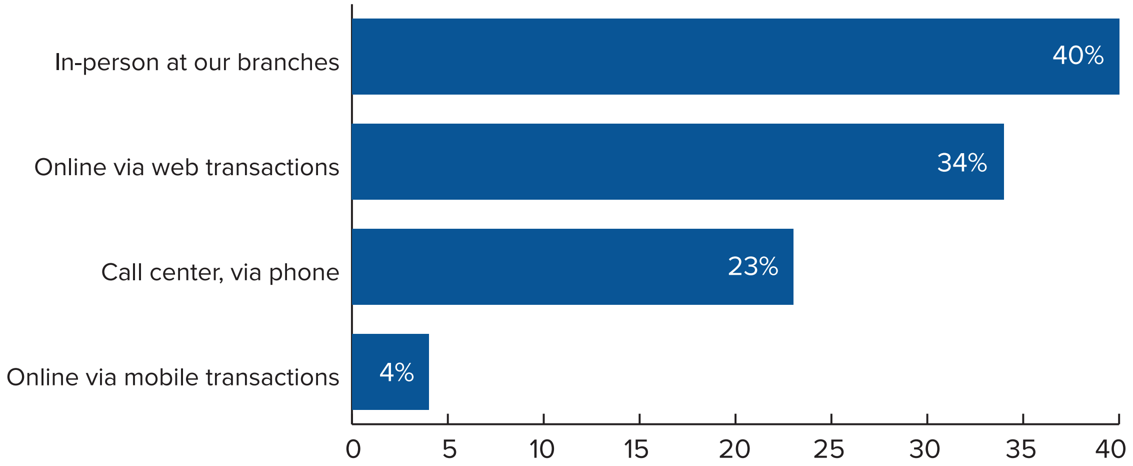
Forty-seven percent of respondents say payment card fraud remains a top concern.

Which types of fraud do you feel your organization is currently best prepared to prevent and detect? (check all that apply)



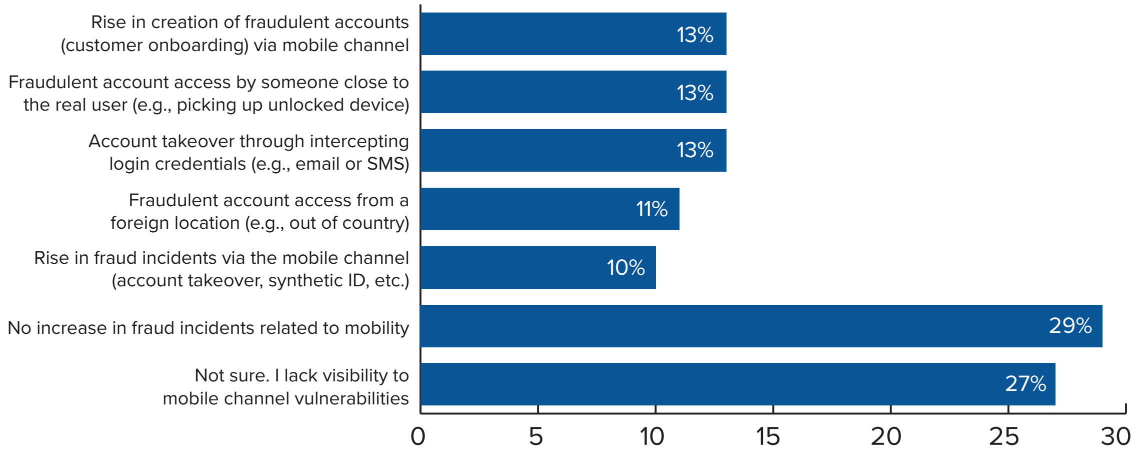
ACH/wire fraud and account takeover take the top two spots, followed closely by payment card fraud and money laundering. No surprise again: These defenses tie most closely to the areas upon which banking regulators focus most closely.

What today is your customers' primary channel for conducting business with your institutions?



Despite the rise of online and especially mobile banking, 40 percent of respondents say their physical branches are still the primary channel for conducting business. Online via web transactions is a close second at 34 percent, while online via mobile is only 4 percent.

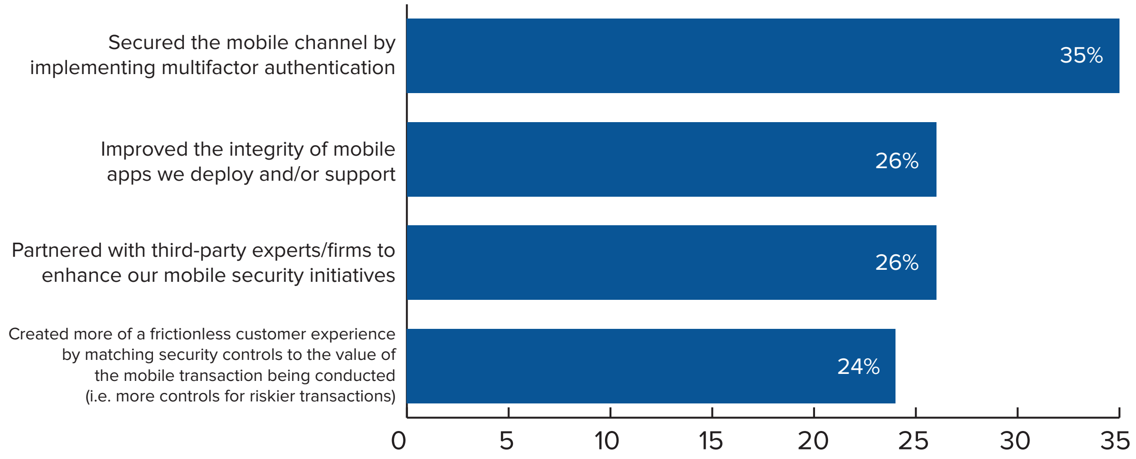
In the past year, have you experienced any of the following fraud incidents specifically related to mobility? (check all that apply)



Asked what types of fraud their institutions have experienced via the mobile channel, 29 percent of respondents say they see no increase in fraud related to mobility, while 27 percent say they lack visibility into the mobile channel. Top forms of fraud reported:

- Rise in creation of fraudulent accounts;
- Fraudulent account access by someone close to the user;
- Account takeover through intercepting credentials.

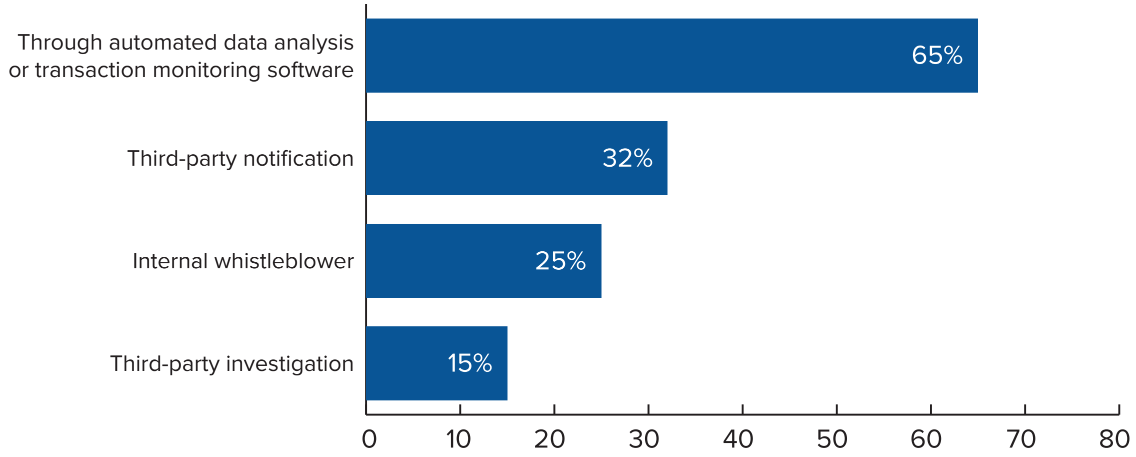
As a result of these incidents related to mobility, how has your organization responded? (check all that apply)



Despite the relatively low number of fraud incidents identified as being tied to mobility, organizations still are taking significant steps to secure the channel. Among these steps:

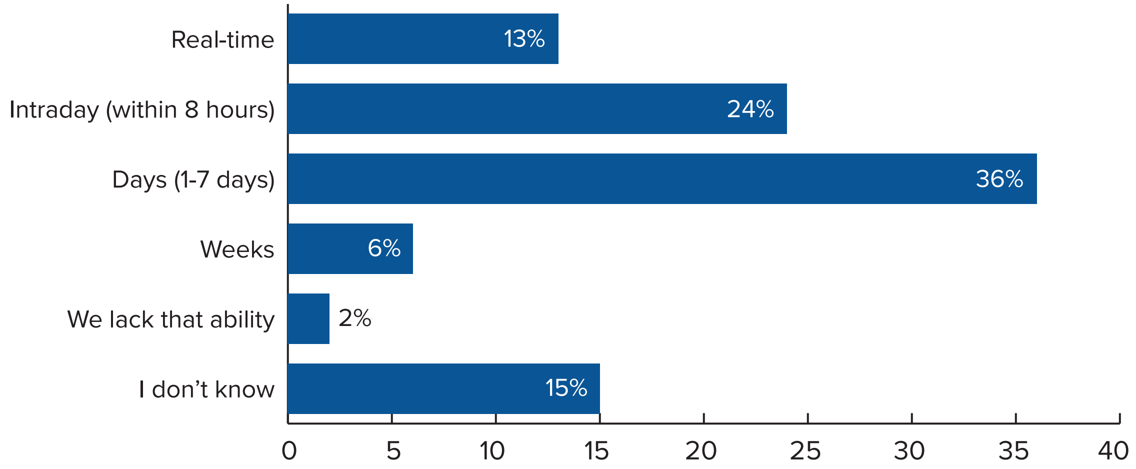
- Implementing multifactor authentication (35 percent);
- Improve integrity of mobile apps (26 percent);
- Partner with third-party experts/forms to enhance mobile security (26 percent).

How is a fraud incident involving your organization typically detected? (check all that apply)



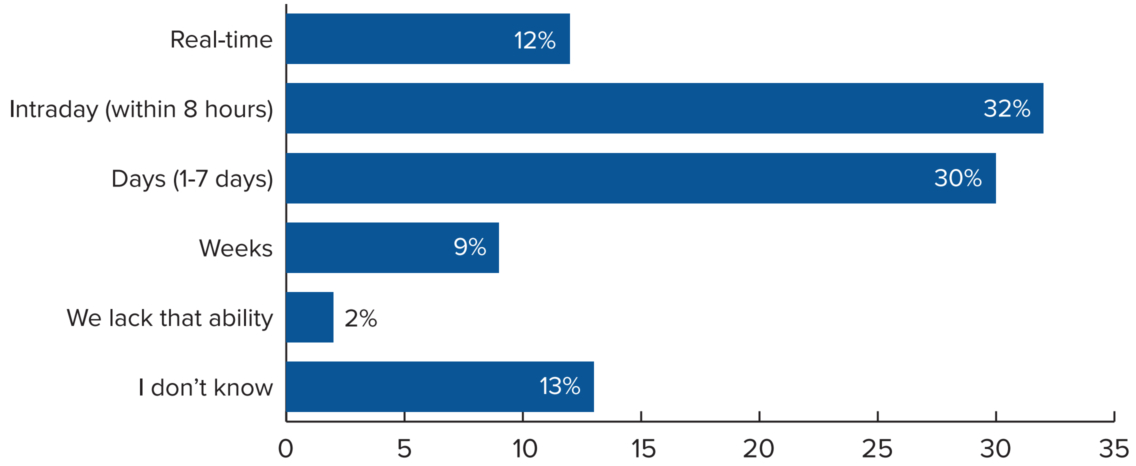
Fraud detection is an area that has improved significantly in recent years. Not long ago, one of the top responses to "When is fraud detected?" was "When a customer notifies us." This year's top response: Through automated data analysis or transaction monitoring software (65 percent).

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



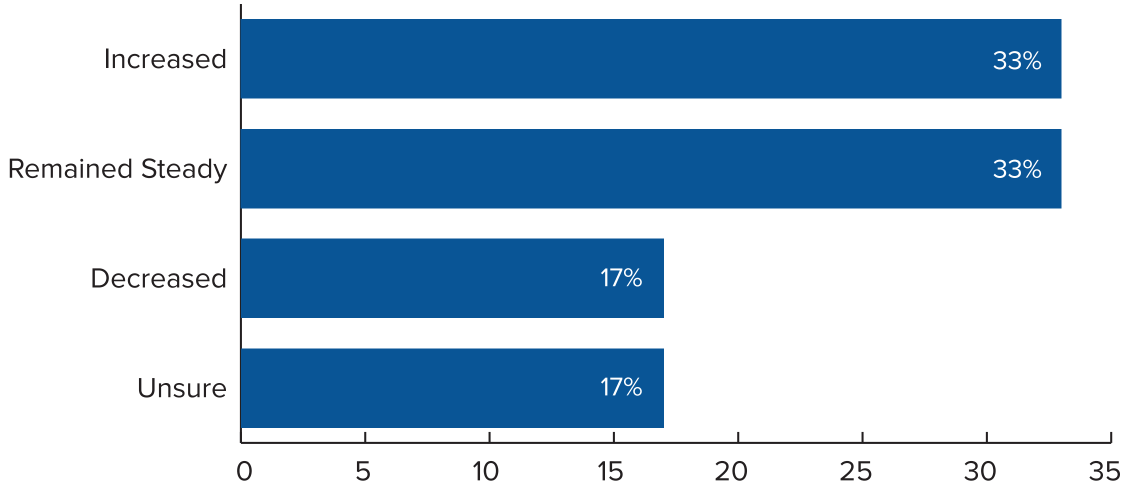
But how long does it take for institutions to uncover fraud once it occurs? Thirty-six percent of respondents say it takes one to seven days. Only 13 percent report real-time detection.

On average, how long do you estimate it takes your organization to mitigate a vulnerability once fraud is detected?



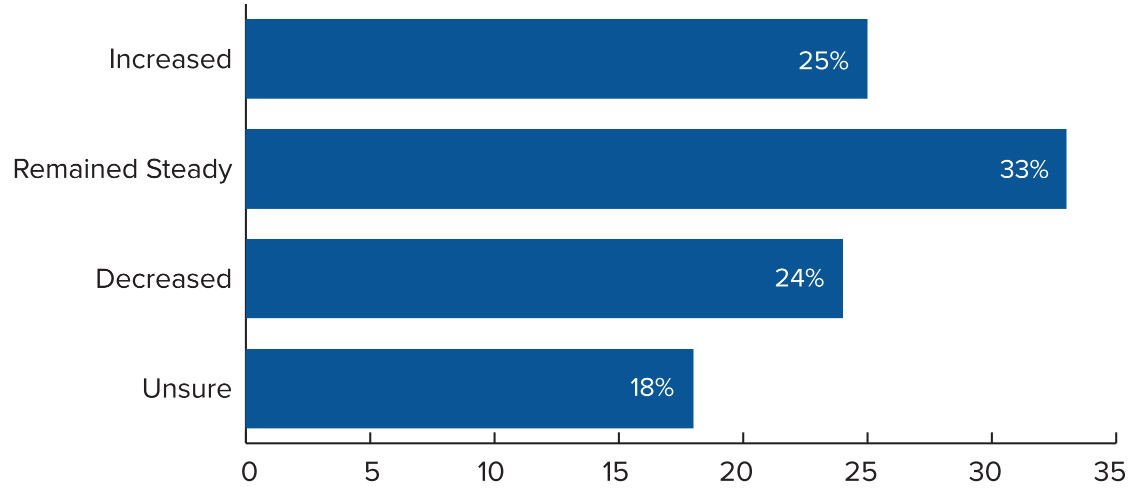
Once detected, how long does it take to mitigate a fraud vulnerability? Only 12 percent report real-time, while 32 percent say they can do so within a business day.

Has the number of fraud incidents involving your organization increased, decreased or stayed steady in the past year?



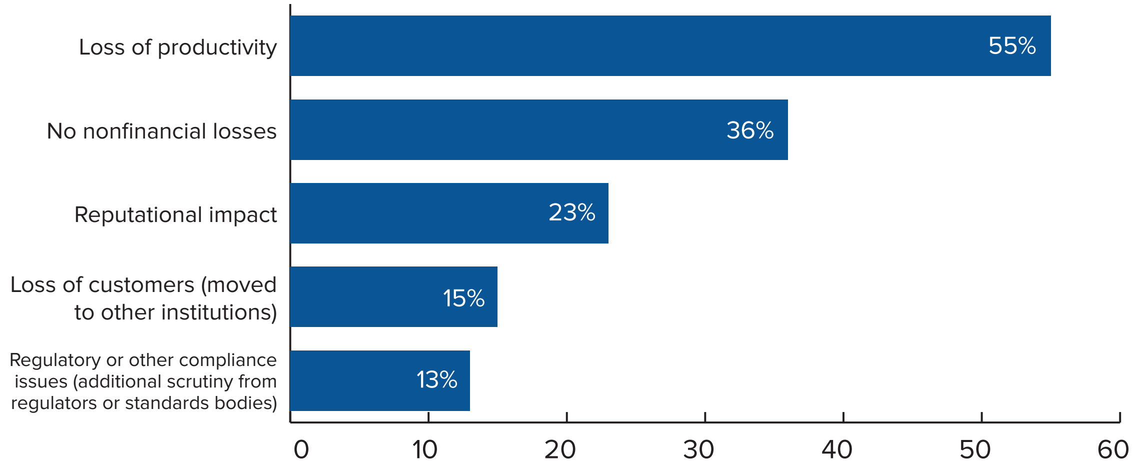
Despite the regulations, controls and staff thrown at fraud in recent years, 66 percent of respondents still say incidents have either remained steady or increased in the past year.

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



And despite efforts to improve detection and response, 58 percent say financial losses to fraud have increased or remained steady. Only 24 percent report a decrease.

Beyond the financial toll from the fraud incidents, what nonfinancial losses did your organization suffer from fraud incidents? (check all that apply)



Beyond financial losses, of course, there are other tolls. Respondents say their top nonfinancial fraud losses are loss of productivity (55 percent) and reputational impact (23 percent).

Next, the report looks at what organizations are doing to improve enterprise fraud prevention.

Aite's Julie Conroy on Mobility

In light of survey responses on mobility and fraud, Aite Group Research Director **Julie Conroy** was asked to weigh in on fraud trends via the mobile channel. Here is what she had to say:

Q: What growth are you seeing in fraud incidents via the mobile channel in 2017?

Conroy: We're not yet seeing a huge increase in losses solely attributable to mobile, but we're absolutely seeing a rise in cross-channel fraud. Some of this is an increase in criminal cross-channel tactics, but we also see that FIs are better leveraging their data assets, and so they're gaining more visibility into the scope of the cross-channel problem.

Q: What are the primary forms of fraud you see via mobile?

Conroy: The primary issue I hear at this point is related to mobile remote deposit capture - that was cited as a major pain point in a recent survey we did of large North American FIs. While account takeover is also an issue, we see that still impacting online more heavily since there is greater transactional capability there.

Q: How are institutions responding most effectively to fraud via mobile?

Conroy: We are seeing FIs deploying layered techniques to verify mobile device ownership, bind the device to the customer either via deep device fingerprinting or PKI-based solutions, and through behavioral analytics. Properly fortified, a well-protected mobile app can be used not just to protect transactions in the mobile channel, but that device can also then be used to enable security for other channels as well.

Q: What are your greatest concerns re: fraud via mobile as we head into 2018?

Conroy: The continued progress toward faster payments introduces new opportunity for fraudsters, especially given the fragmented approach in the U.S. Expect to see criminals capitalize on this with routines that target faster payments across all channels, including mobile. ■

Julie Conroy, research director, Aite Group

> *"Properly fortified, a well-protected mobile app can be used not just to protect transactions in the mobile channel, but that device can also then be used to enable security for other channels as well."*

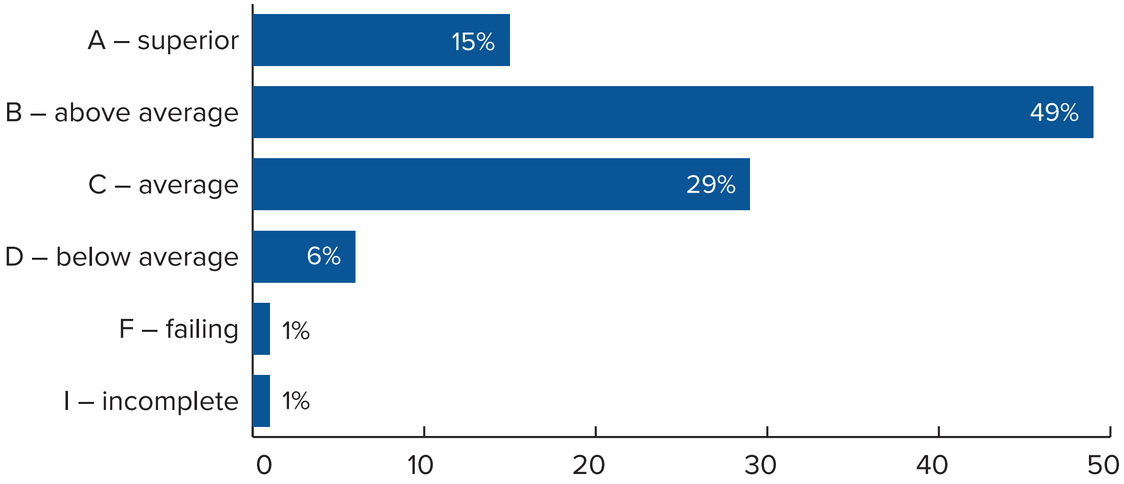
Enterprise Fraud Prevention

What are the relative strengths and weaknesses of organizations' current enterprise fraud prevention efforts?

- 64 percent of respondents say the efficacy of their current anti-fraud controls is above average or superior.
- 48 percent say they are hindered by technical barriers—their controls do not "talk" to each other.

See the full results below.

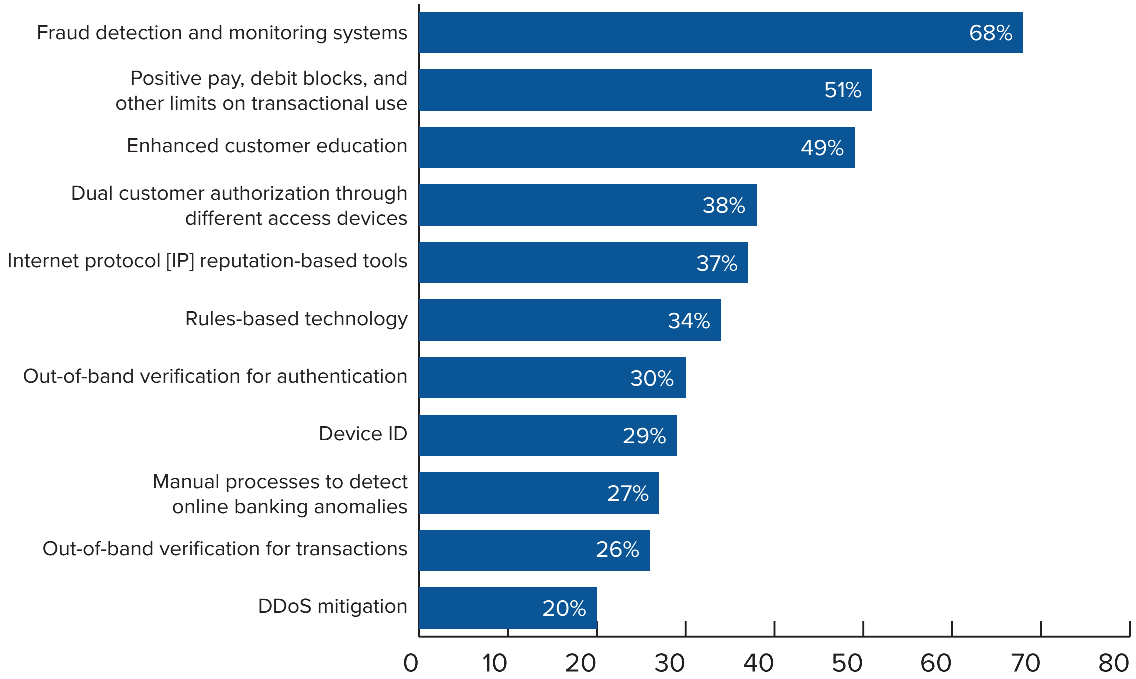
What grade would you give the efficacy of your organization's current anti-fraud controls?



Asked to grade the efficacy of their organization's current anti-fraud controls, nearly 50 percent give themselves a B, or above average. Only 15 percent rate their controls as superior, while 35 percent say average or below.

Sixty-four percent of respondents say the efficacy of their current anti-fraud controls is above average or superior.

Which of these anti-fraud controls has your organization already deployed? (check all that apply)

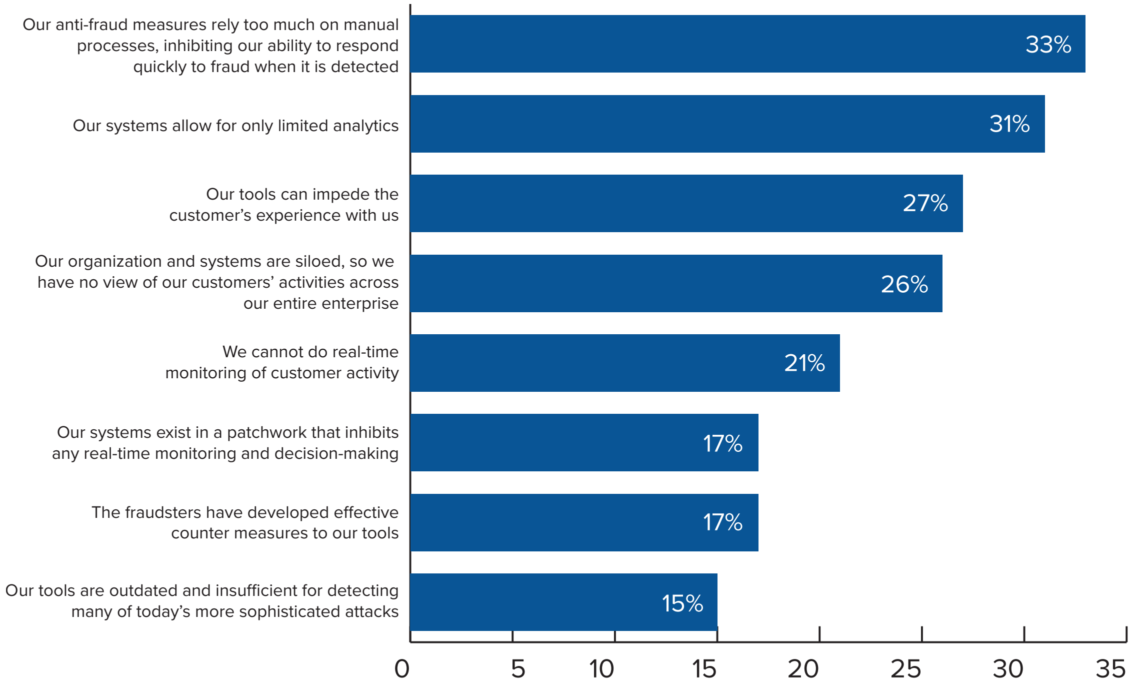


Organizations have deployed a plethora of anti-fraud controls—many of them a result of regulatory mandates or guidance. The current top three controls:

- Fraud detection and monitoring systems (68 percent);
- Positive pay, debit blocks and other transaction limits (51 percent);
- Enhanced customer education (49 percent).

Organizations have deployed a plethora of anti-fraud controls, many of them as a result of regulatory mandates or guidance.

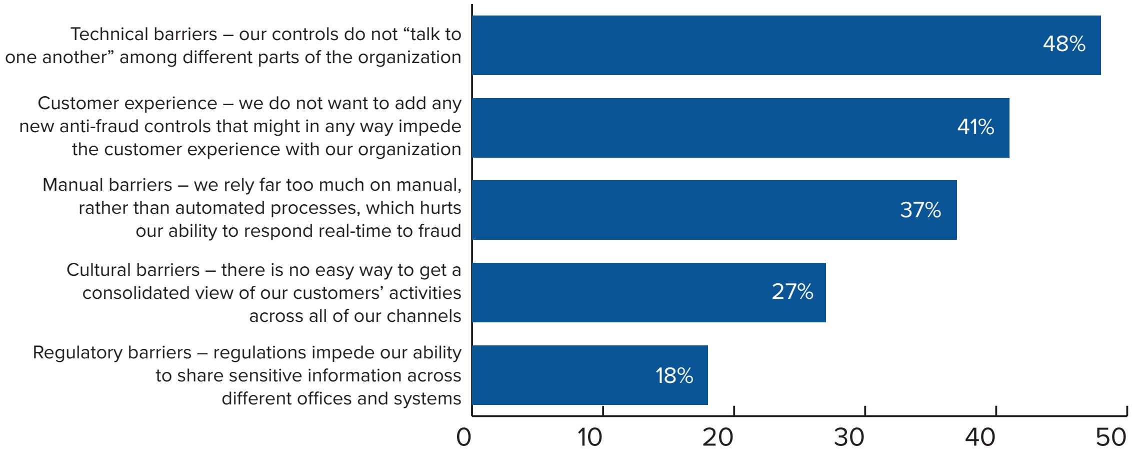
What do you find most lacking in your enterprise's current anti-fraud tools? (check all that apply)



Asked what they find most lacking in their enterprise's current anti-fraud tools, respondents say:

- Our anti-fraud measures rely too much on manual processes, inhibiting our ability to respond quickly to fraud when it is detected (33 percent).
- Our systems allow for only limited analytics (31 percent).

What are your organization’s top two barriers to improving enterprise fraud prevention?



Then, asked to name the top two barriers to improving enterprise fraud prevention, respondents said:

- Technical barriers – our controls do not “talk to one another” among different parts of the organization (48 percent);
- Customer experience – we do not want to add any new anti-fraud controls that might in any way impede the customer experience with our organization (41 percent).

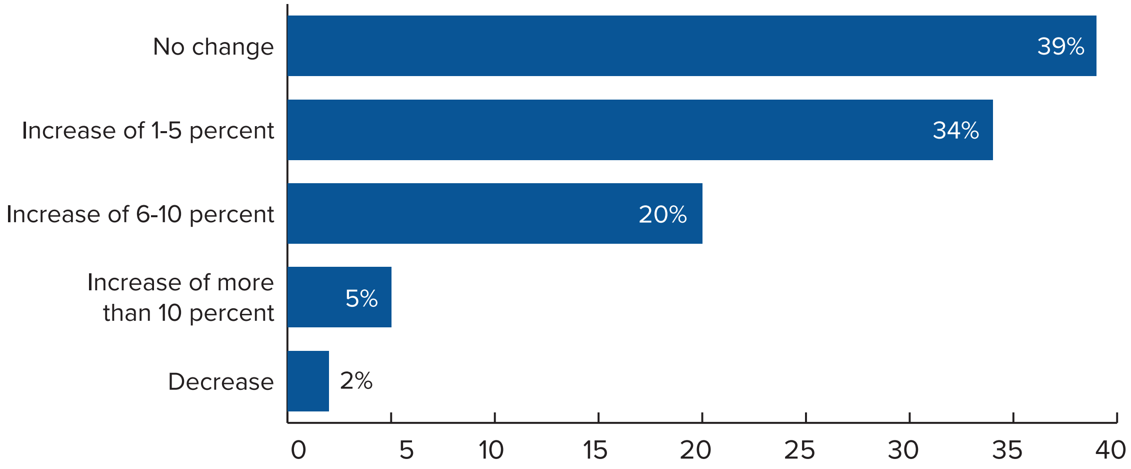
Next: The anti-fraud agenda for 2018

The inability of controls to ‘talk to one another’ is a top barrier to improving enterprise fraud prevention.

2018 Fraud Agenda

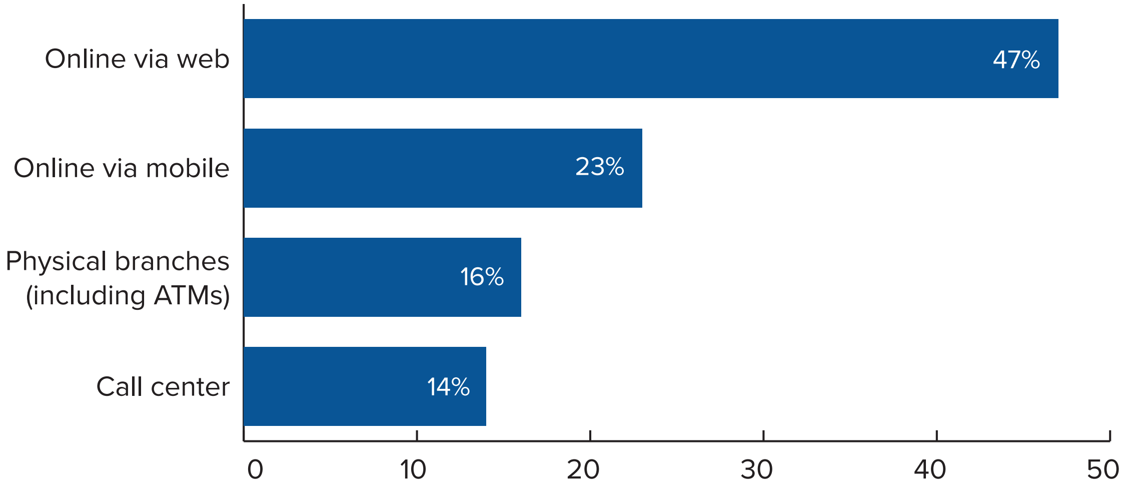
Ninety-eight percent of respondents expect to receive the same or increased budget to fight fraud in 2018. How will they invest these resources? The answers follow.

How do you expect your budget dedicated to fraud prevention to change in the next year?



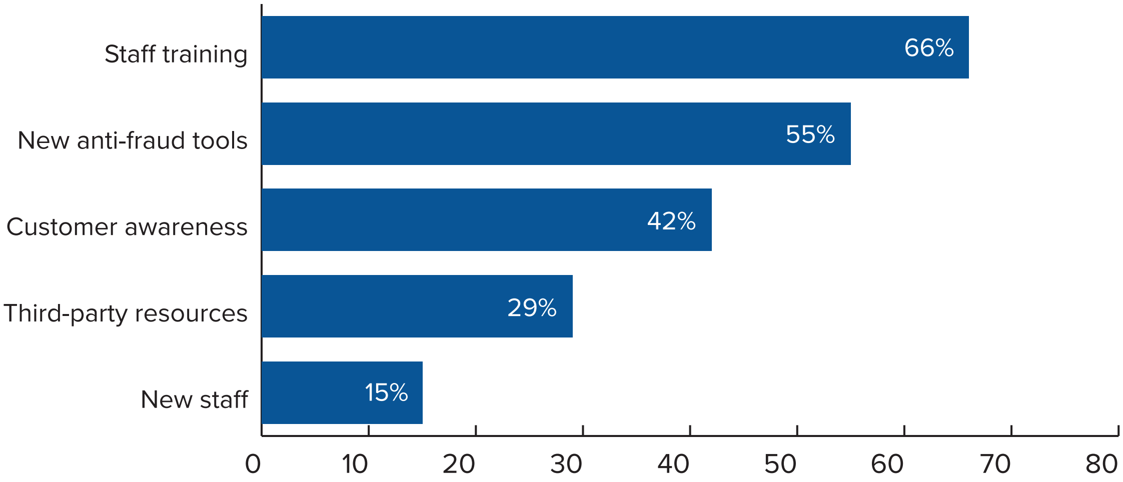
Budgets are always tight, and it is never an easy discussion to ask for increased resources to fight fraud. Yet, all but 2 percent of respondents say they will receive the same or more funds for fighting fraud in 2018. In fact, 54 percent expect increases ranging from 1 percent to 10 percent.

Which of these banking channels will be your top priority for improving cybersecurity in the next year?



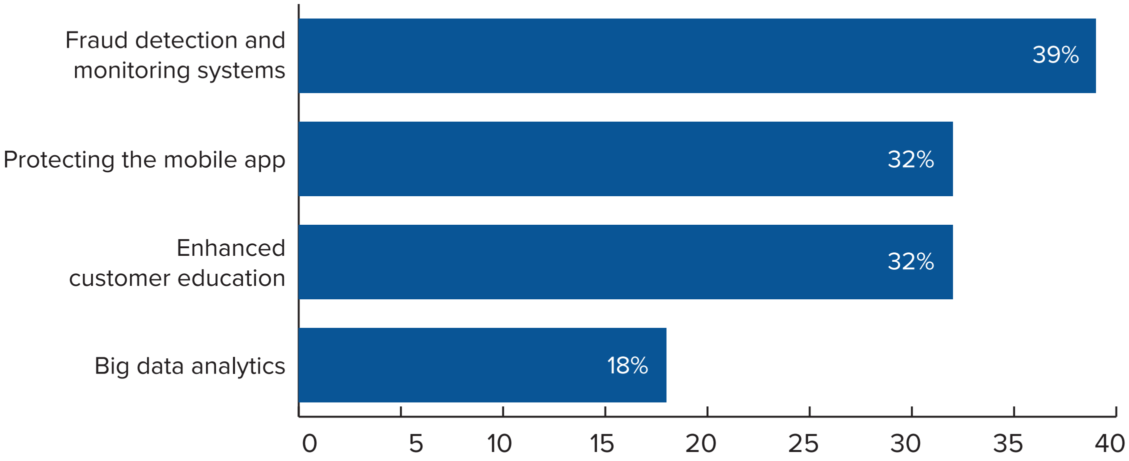
The top priority banking channel for improving security in 2018: online via the web, according to 47 percent of respondents. Twenty-three percent say their will enhance the mobile channel.

Where do you expect to make key investments? (select all that apply)



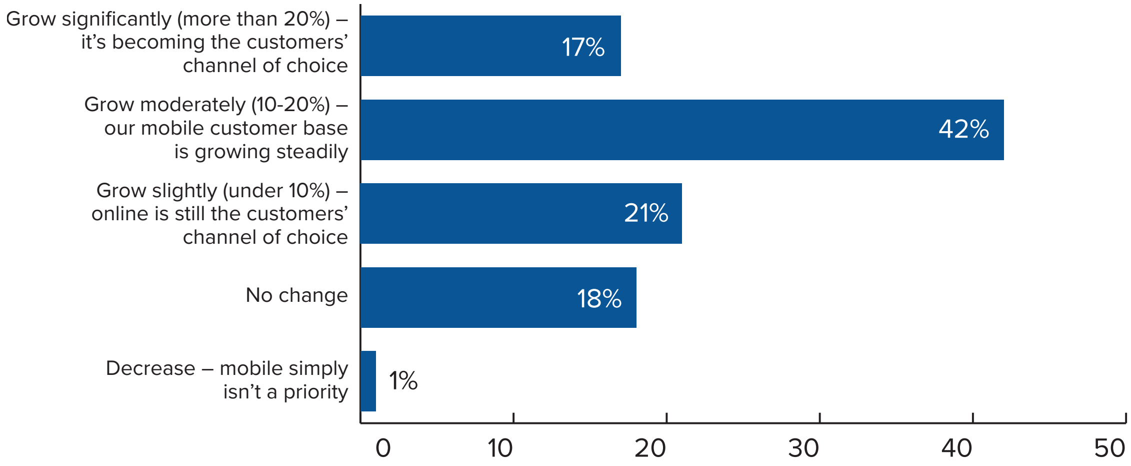
What are the investment priorities for the new year? Staff training for 66 percent of respondents; 55 percent will purchase new anti-fraud tools.

Which specific anti-fraud technology investments do you plan to make within the next 12 months? (select all that apply)



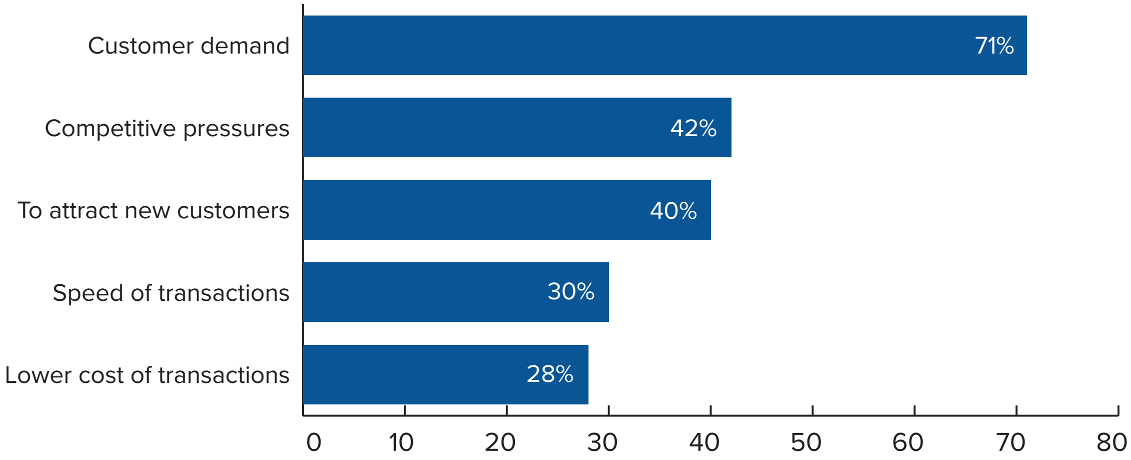
As for which tools to invest in, 39 percent say they will purchase new fraud detection and monitoring systems, while 32 percent eye protecting the mobile app and enhancing customer education.

How do you expect your organization's mobile channel to grow in 2018?



Forty-two percent of respondents expect moderate (10 percent to 20 percent) growth in the mobile channel in 2018, while 21 percent project slight (under 10 percent) growth.

What are your organization's biggest drivers for mobile channel growth? (check all that apply)



As for the biggest drivers for growing the mobile channel, 71 percent say it is because of customer demand, while 42 percent say it is in response to competitive pressures.

What do all these results mean? That question will be answered in the next two sections, which include the survey results conclusions and the expert analysis by John Gunn, CMO of survey sponsor VASCO Data Security.

Gartner's Avivah Litan on Fraud, Customer Experience

In light of survey responses on mobility and fraud, Gartner VP and distinguished analyst Avivah Litan was asked to weigh in on emerging anti-fraud controls and the push for a "frictionless customer experience." Here is what she had to say:

Q: What are the emerging anti-fraud controls that encourage you the most?

Litan: I'm encouraged by the advances in and fine-tuning of machine learning models and other forms of advanced analytics being applied to the fraud use case, and the use of mega global sets of shared data to inform those models.

I'm also encouraged by continuous behavioral biometric authentication, along with other continuous identity assessment measures, that raise confidence in a user's legitimacy. We need this - especially in an era of heavily compromised PII data.

Q: How important is the "frictionless customer experience" in securing the organization (and customer) from fraud?

Litan: Frankly, this is not a new priority. There has always been a tug of war between marketing and customer service managers who want a frictionless customer experience and security managers who want strong security that can often create a lot of friction for the customer.

Luckily, in my opinion, frictionless security also provides the strongest security. Frictionless by default means the user cannot easily 'see' the security measures, for example strong biometric authentication, since they run transparently in the background. But that also means the criminals can't see these security measures and therefore can't develop workarounds for them.

It's much harder for a bad guy to beat a system he or she cannot easily see. An unseen fraud control is much harder to map out for the purpose of circumventing it later. Of course, fraudsters can run test transactions through applications to try and ascertain their 'unseen' or transparent fraud logic, but this is difficult to do without getting caught.

The truth is "harder is not better – it doesn't keep the bad guys out and only inconveniences the good ones". ■

Avivah Litan, VP and distinguished analyst, Gartner

"It's much harder for a bad guy to beat a system he or she cannot easily see."

Conclusions

In bringing this survey report to a close, it is relevant to return to some of the statistics used to open this discussion of the 2017 Faces of Fraud:

- Only 38 percent of banking/security leaders have high confidence in their organization's ability to detect and prevent fraud.
- 66 percent say the number of fraud incidents has stayed steady or risen in the past year.
- 58 percent say financial losses have remained the same or increased.

With these statistics in mind, and having reviewed each of the other survey results, the report offers these conclusions:

Improving Fraud Detection and Prevention in 2018 is About Improving:

Confidence

It's a problem that barely one-third of respondents have high confidence in their organizations' abilities to detect and prevent fraud before it causes serious damage. This sentiment speaks to the increase in fraud incidents and losses, and it accounts for organizations' inabilities to detect and respond to fraud incidents in anything close to real time. The message is clear: Traditional anti-fraud controls are not sufficient for stopping today's determined fraud efforts. The controls, how they communicate with one another and how people respond to alerts all need to be up for review in order to build greater confidence in defenses.

Customer Experience

Upfront, respondents said that the "frictionless customer experience" is more of a priority, but not *the* priority. Yet, when asked about top barriers to improving enterprise fraud prevention, "customer experience" was near the top of the list. As the banking experience transitions more from the branch and the laptop to the mobile device, the institution has to be increasingly mindful of the customer experience and ensuring the customers can do business with you via convenient channels. To do so requires deployment of authentication and transaction controls that are at once effective and efficient—which leads to the next conclusion.

Convenience

Banking customers have more options than ever before, and if your security controls are perceived as a barrier to customers conducting transactions ... then they will move on to another institution or seek a work-around to duck the security controls. Organizations say they have improved multifactor authentication and the integrity of their mobile apps. But they also say they are seeing account takeover and bogus account creation. In the survey analysis that follows, John Gunn of survey sponsor VASCO Data Security makes the point clearly: We are seeing incredible innovation in mobile attacks, and a plethora of consumer data is readily available—especially in the wake of the Equifax breach. Those banking institutions that can deliver a convenient and secure user experience will likely win more customers, sell more services and suffer fewer losses.

Next: John Gunn's survey analysis and how to put these results to work to improve fraud detection and prevention.

An Annual Checkup on the Battle Against Hackers

Survey Analysis by John Gunn of VASCO Data Security

NOTE: In preparation of this report, ISMG Senior Vice President Tom Field sat down with John Gunn, CMO of survey sponsor VASCO Data Security, to analyze the results and discuss how security leaders can put these findings to work in their organizations. Following is an excerpt of that conversation.

Reviewing Survey Results

TOM FIELD: So, John, if you take a look at the survey results overall, what's your gut reaction to what we've collected?

JOHN GUNN: It's kind of like an annual checkup on the state of the battle against hackers. And it's very insightful. To me, it really underscores that in spite of the fact that financial institutions have really gone all in, we're not seeing big reductions in the amount of fraud. What I mean is, if you look at [what is spent], their budgets have increased every year. And the technology that vendors like VASCO and others bring to market keeps advancing. So it's a little worrisome, maybe. And kind of a "where do you go from here?"

Surprising Stats

FIELD: What do you find specifically surprised you in these results?

GUNN: A couple things just jumped out at me. One of them was the fact that only a little more than one-third of the respondents have a high confidence [in their abilities to detect and prevent fraud]. And when you consider the amount spent, the amount of resources, just the investment, and these are really smart people making really good decisions about how to defend themselves … maybe it's disappointing that only a third have high confidence in the progress they're making. Ultimately, it should be 99 percent of financial institutions feel good about the results and the progress they're making.

John Gunn

"In spite of the fact that financial institutions have really gone all in, we're not seeing big reductions in the amount of fraud."

Mobile Fraud Trends

FIELD: John, one of the major subthemes of our survey was looking at the impact of mobility on financial institutions. So again, based on your experience with the customers you deal with, where do you see the growing impact of mobility on institutions and on the types of fraud that they're facing?

GUNN: That's a great question, because we see that first-hand. We work with not only some of the largest banks in the U.S. and around the globe, but we work with every size financial institution. And whether they're your regional bank or one of the world's largest, they all are experiencing a big increase in attacks on their mobile banking. And we expect that to continue,

“As more users come on and more services are offered, mobile just becomes a bigger target for hackers.”

as they do as well. Just the more volume that’s there, the more opportunity, the more users—you know, in rough numbers you’ve got 80 percent of financial institutions’ customers doing online banking. A few years ago, it was 40 percent doing mobile, and now it’s eclipsed 50 percent and it continues to grow. So as more users come on and more services are offered, [mobile] just becomes a bigger target for hackers. And you have as a backdrop to that: Financial institutions see the benefit of mobile customers. Mobile customers are more sticky. They buy more products. That’s where a financial institution makes their money.

The Frictionless Customer Experience

FIELD: John, for years now you’ve been talking about the customer experience, but it’s only really in the last year that the industry has started talking about this balance between security and the so-called frictionless customer experience. My question for you is, how critical is this balance? If you ask our survey respondents up front, they would say it’s a factor but not the most important factor. Yet, consistently as we talked to them about roadblocks they talked about the risk of impeding the customer experience.

GUNN: Part of that is that, over the last five years or 10 years, so many financial institutions have just accepted that if they are going to have an acceptable level of security, they’re also going to have some customer inconvenience, some hassle.

But the best news is that with newer solutions that we’ve got and that others have got … it shouldn’t be an either/or. It should be a matter of “how does the financial institution deliver the absolute best customer experience to attract more customers from the very initial process of establishing an account all the way through the services they want to sell and not have to compromise security?” It shouldn’t be a trade-off—and that’s really where the direction of the solutions is going.

Faces of Fraud

FIELD: John, we’ve delivered this survey for several years now, and I can’t help but stop to think of how it’s changed. When we did the first survey and asked institutions about the types of fraud that concerned them, it was still a lot about check fraud. It was about ATM. It was about corporate account takeover. You’ve been in this industry for a long time. How do you see the faces of fraud evolving with financial institutions?

GUNN: There are several factors that are driving that. The biggest … is just the sophistication that hacking organizations have. Whether it’s five years or 10 years ago, the attacks were much more simple, much easier to identify, much easier to mitigate. The losses were much smaller. I mean, you look at the tools that we have now to fight fraud—they’re so sophisticated, but the hackers are still just every bit as sophisticated in their attacks. So it continues to evolve; it continues to grow in scope and scale and sophistication; and it’s a never-ending battle. But our customers, the financial institutions—they don’t have a choice. We have to win that battle. The business depends on it.

Defensive Gaps

FIELD: Again, if I go back to when we first started conducting this survey years ago, you found that anti-fraud controls tended to be right in line with what the regulators asked the financial institutions to do. So they were strong against money laundering. They were strong with fighting check fraud, ATM fraud. How do you see defensive gaps being addressed today to keep pace with the shift in fraud and the sophistication you talked about a few moments ago?

GUNN: You touched on a key point that relates to that, and that is regulation. Because the regulation was what drove a lot of anti-fraud solutions in the past, but most solutions now have eclipsed that to where banks, for the most part, have met all their regulatory requirements. But as we’ve seen, they still have significant losses to fraud. When you look at the close to a billion dollars of loss at the ATM, it’s not because financial institutions

"You look at the tools that we have now to fight fraud - they're so sophisticated, but the hackers are still just every bit as sophisticated in their attacks."

are not meeting regulations. Regulations couldn't possibly keep pace with the sophistication and the evolution of new attacks. So it's that economic argument we talked about, and it's about the new tools, the next generation and what's coming. And that is: unified tools, tools that work with each other that are easier to implement.

And fraudsters have a real advantage. If you look at game theory, there's always an advantage to being the attacker because you can pick that one point of vulnerability when you find it. Whereas financial institutions or their vendor partners, such as VASCO, have to cover a thousand potential points of vulnerability. So it's a monumental task, and it requires coordination, collaboration and staying on the front end of new technologies.

Mitigating Mobile Vulnerabilities

FIELD: What do you find to be the most effective means to both assess and remediate today's mobile vulnerabilities?

GUNN: There are some fundamentals that most financial institutions have now that are a key part of that. We view it as three elements: the individual who is attempting the transaction, the device that they are trying to do it on and then the transaction itself. So it's having the tools to assess each of those.

Who is this individual? We can look now at the device they're using, the history of the device, how long they've had the device, the reputation of the device, the status of the device. We can look at the individual, the history of that individual, how well they're known not only to the financial institution, but through other channels. And then the transaction itself: Is this a typical transaction where you can look at the behavior of that transaction?

For example, if you normally bank on Fridays when you get paid, and you normally send funds to a child you have at a university, you have these patterns. And we're getting more and more sophisticated tools to identify these patterns in real time.

One of the survey responses that surprised me was that only 13 percent of financial institutions feel they're effective in stopping fraud in real time. That means that 87 percent of the fraud is probably not blocked, and those are losses. And if we can move that to where 90 percent plus of fraud is identified in real time, using the techniques and tools I just discussed, then we'll be able to make some serious progress in reducing the losses to fraud.

2018 Agenda

FIELD: John, one point I found encouraging is how many institutions are getting increases in their anti-fraud budgets, or at least maintaining the same level of funding that they have this year. If you look at investments, what do you see as the must-have anti-fraud controls for institutions as they go into 2018?

GUNN: A lot of it is an expansion of tools they already have—keeping those tools updated, getting more sophisticated tools. And they really relate to the tools that put less burden on their users. We use the terms "frictionless" or "seamless" or "transparent." And those are the tools that are going be most effective because it serves that dual purpose of allowing financial institutions to offer more services to more customers and increase what they're really in business to do without taking greater risk, while reducing those frauds.

"Regulations couldn't possibly keep pace with the sophistication and the evolution of new attacks."

The risk analysis engines are getting more sophisticated. They're moving to machine learning and ultimately going to move to artificial intelligence. And you'll hear a lot of people talk about that in the coming year.

Behavioral biometrics is a solution that we offer that's very valuable. It looks at things such as the way you type numbers on a keypad—the cadence, your normal patterns and then an expansion of different anti-fraud controls.

We give our financial institutions a powerful engine to be able to allow more transactions to go through without any friction and then provide a larger toolbox of new ways to authenticate people in the background. And in those few cases where you have to, you can step up and say, "OK, you know, we need some biometrics. We want to do a facial authentication" ... methods that users are accustomed to that they readily accept. So those are the new tools that we see financial institutions moving to in 2018 and beyond.

Customer Education

FIELD: Now consistently, when we ask organizations how they intend to invest their resources in the year ahead, you always see a strong percentage that want to focus on customer education. You have very strong feelings about an overemphasis on improving customer education. Could you talk about that a bit, please?

GUNN: There's nothing wrong with improving customer education. I just think the impact is somewhat limited. And in some ways that places the burden on the customer. And with the newest solution that we have that we're offering financial institutions, there shouldn't be any burden on their customer to participate. It should all take place in the background. It should all be very effective, and all the customers experience is this great relationship with their financial institution that makes them want to do more business. ...

Consider the fact that the average user ... has more than 60 apps on their phones. And when you consider the massive amount of time that people spend on their social media apps, then the amount of time that a financial institution has to interact with that user is really limited. And the impact of the enhanced awareness effort isn't going to be very great. And there are so many individuals, so many organizations, so many groups that try to educate consumers. But I don't think financial institutions are going to make much of a dent.

Our strategy is to give financial institutions the security that's effective, so if they want to educate customers they can educate them on their solutions, on new offerings they have—things that will generate more revenue for that financial institution. That's where I disagree with the notion of educating customers about safety and security. That should be baked in, and the new solutions we have should allow financial institutions to do that.

VASCO's Solutions

FIELD: Well, John, what is VASCO bringing to the table to help institutions fight fraud better in the year ahead?

GUNN: That's the most exciting part of all of this. We have this great legacy of stopping fraud. And we have hundreds of millions of instances out there of individuals using our solutions. What really matters is where the industry is going. And where it's really going to is ... being able to deliver solutions that are easy to implement.

It shouldn't take two weeks for financial institutions to implement a new solution in their stack. That limits what they can do. It limits their ability to defend themselves. So the next generation of solutions have easy interoperability—and not just among our solutions, but among our competitors or third parties. The solution has to become more of a hub where the bank has much greater flexibility, and instead of taking weeks to implement, it should take hours to do that. So our goal is to always provide that full bundle—the best of breed in every area.

We also recognize that financial institutions may have different needs, or they may want those needs serviced by somebody else. And they shouldn't have to choose a single vendor to the exclusion of others. So new solutions will integrate much easier. But beyond that ... what we really focused on in developing our new solutions is having the sum be more than the total of the components of it.

Banks have a lot of different solutions now that aren't always easy to implement, aren't always easy to use. So we're taking big strides in making them easy to implement, easy to use. But more important, they have to talk to each other and they have to have been designed from the ground up in a manner that allows each component to perform at a higher level. We've got some announcements coming up later this year and in the spring of next year where we'll introduce our new platform that combines all of those features. ■

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANKINFO SECURITY® CUINFO SECURITY® Just for Credit Unions GOVINFO SECURITY® HEALTHCAREINFO SECURITY®

infoRisk® TODAY CAREERSINFO SECURITY® ~~Data Breach~~. Prevention. Response. Notification. TODAY

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io