appgate

iSMG INFORMATION SECURITY MEDIA GROUP

Faces of Fraud 2023

The Evolution of Online Fraud in 2023 and Best Practices to Plug the Gaps

Author: ISMG

Table of Contents

About this survey:

This survey was conducted by Information Security Media Group and Appgate in Q2 2023. In all, more than 150 financial institutions, primarily from the U.S. and Canada, participated in this study.

About Appgate:

Appgate is a secure access company that empowers how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Appgate helps organizations and government agencies worldwide start where they are, accelerate their Zero Trust journey and plan for their future. Learn more at Appgate.com.

Introduction

Welcome to our report summarizing the *2023 Faces of Fraud* survey. We are most grateful to our industry contributors who answered our questions frankly to enable us to provide a snapshot of the frauds causing most concern for financial services in 2023. We are also able to see how the industry as a whole is being affected and enable you to see how your peers are prioritizing ways to protect themselves.

These include identifying where today's financial institutions are focusing investments on fraud prevention technologies in the coming year.

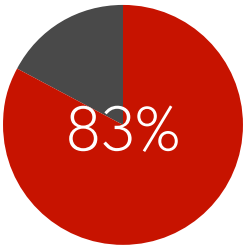
When it comes to threats, every new technology begets new frauds as attackers evolve and innovate, but our cyber defenses are evolving, too. So, what should we be looking out for in the year ahead – and how should we respond?

The data shared in this report will help inform your fraud prevention strategy for the year ahead, not only in relation to the threats you face and the technology you deploy to prevent them – but also for benchmarking what you should realistically be aiming to achieve.

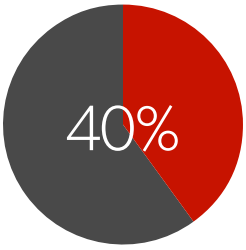
Best regards,

TONY MORBIN
Executive Editor, EU
Information Security Media Group
Tmorbin@ismg.io

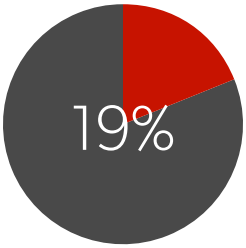
By The Numbers



83% of respondents say today's fraud schemes are evolving too quickly for them to keep pace.



Only 40% of organizations have the visibility needed to identify the impact of a phishing attack.



Just 19% of organizations have the capabilities to identify fraud in real time.

Executive Summary

Fraud is a perennial problem, and attackers see every advance in technology as an opportunity to exploit increased complexity, expanding threat surfaces and potential new gaps in our defenses.

Case in point? As soon as generative AI became widespread, fraudsters began to exploit it to identify vulnerabilities, speed new attacks and create more convincing lures, including deepfakes. They also used it as a lure buzzword. And threat actors continue to exploit complexities created by scattered IT infrastructures, digitization, cloud migration, and a shift to remote and hybrid workforces and BYOD.

Concern about the impact of rapid change is reflected in this year's *Faces of Fraud* survey results, where financial services respondents say the top vulnerability is that today's fraud schemes are evolving too quickly for them to keep pace. While the pace of change has annually been an issue in this *Faces of Fraud* series, the number of respondents who see it as their top concern has almost doubled, from 43% in 2019 to 83% this year.

One obvious vulnerability enabling such frauds is the lack of visibility that organizations have to be able to identify the impact of a phishing attack, with 55% saying they had limited visibility, and 5% admitting they had none. Fewer than half – just 40% – claim to have the detailed visibility needed to identify the impact of a phishing attack, suggesting this remains a target area for improvement.

The Perception Gap

In this year's survey, contradictory perceptions are very enlightening when comparing respondent answers to different questions. For example, when rating their financial organization's ability to identify and mitigate fraud, 60% of respondents say it is above average or superior; 37% say they are average; and 3% rate it below average.

But while 97% of respondents say they have an average or above ability to detect and mitigate fraud, only 19% say they can identify a fraud attack in real time. Even fewer, 11%, say they can mitigate in real time. Twenty percent of organizations who take more than a week to identify fraud either lack the ability to do so or don't know if they have the ability. Twenty-nine percent of organizations taking more than a week to mitigate fraud also say they lack the ability to do so or do not know if they have that ability. Particularly concerning is that the mitigation times have increased compared to previous surveys in this series; the percentage of those able to do so in real time is down 3% from 2020. Even allowing for any statistical margin of error, clearly the situation is not improving.

It is therefore no surprise that a perception gap between how strong an organization's security stance against fraud is versus what the organization believes it to be. The gap has been remarkably consistent across the survey series with confidence in abilities remaining high In the 2021 Faces of Fraud survey, nearly three-quarters of survey respondents said they were confident or very confident that their C-suite understood the investment needed to counter and mitigate growing fraud threats. And nearly three-quarters of 2020 survey respondents said they were confident or very confident that their C-level executives "got it" with regard to anti-fraud investments. Yet in both cases, nearly half of institutions surveyed stated that they had limited or no visibility in identifying the impact of such an attack.

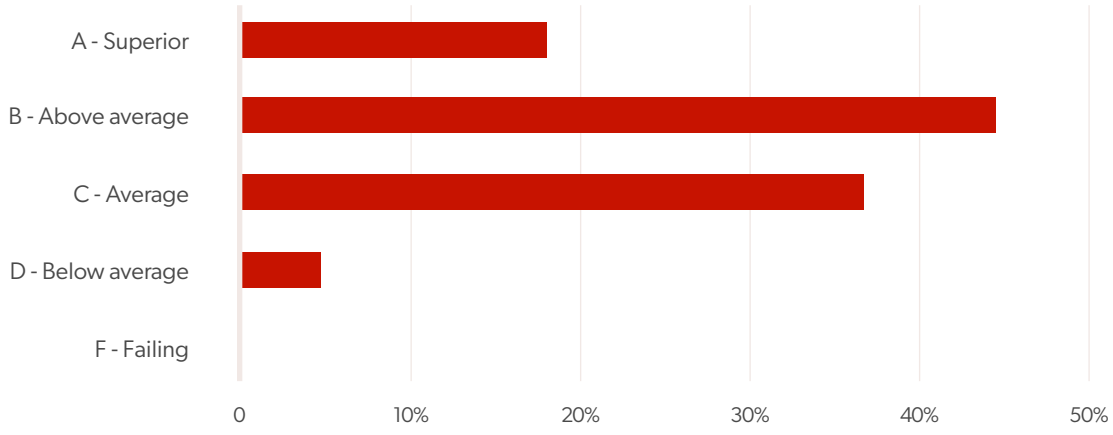
Awareness vs. Willingness

Another disconnect is that while 57% of respondents say that fraud intelligence detection and monitoring systems have the most significant impact on preventing fraud losses, only 43% of respondents say they plan to invest in fraud intelligence detection and monitoring systems over the next 18 months. The inference is that awareness of the benefit of modern fraud prevention tools exceeds a willingness or ability to commit to spending on those same tools.

It may also be that financial organizations are taking too siloed an approach to fraud tooling, because 80% of respondents say their controls do not talk to one another in different parts of the organization. There is also a persistent complacency in the belief that organizations are already doing enough to prevent fraud, even though the evidence suggests otherwise.

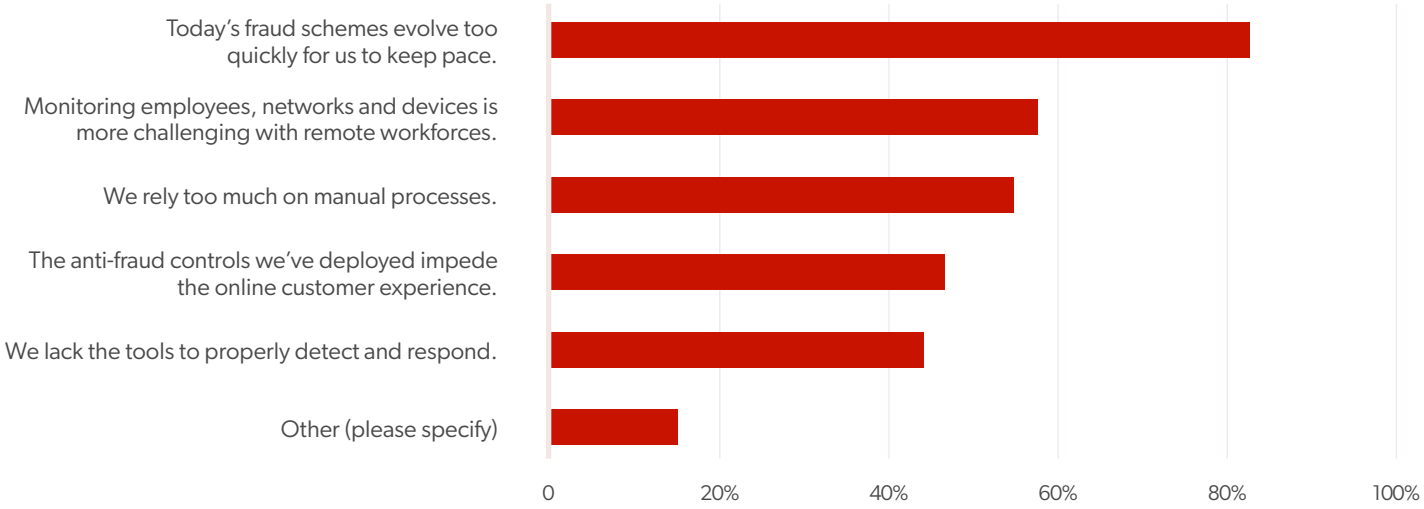
2023 Faces of Fraud Survey Results

What grade would you give your organization's ability to identify and mitigate fraud?



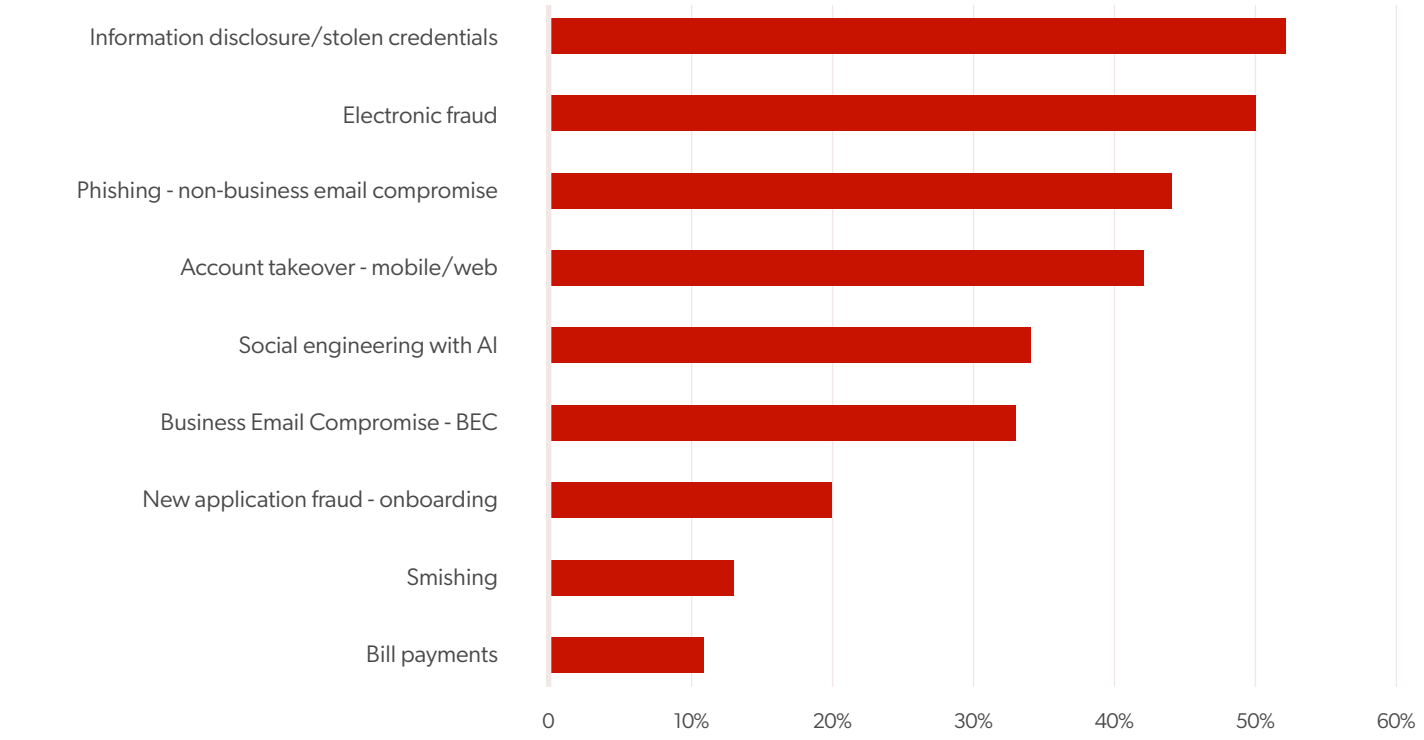
Unsurprisingly, most respondent, 60%, think their ability to identify and mitigate fraud is above average or superior, while 37% say they are average and just 3% say they are below average.

What do you believe to be the top three greatest vulnerabilities in your fraud defenses?



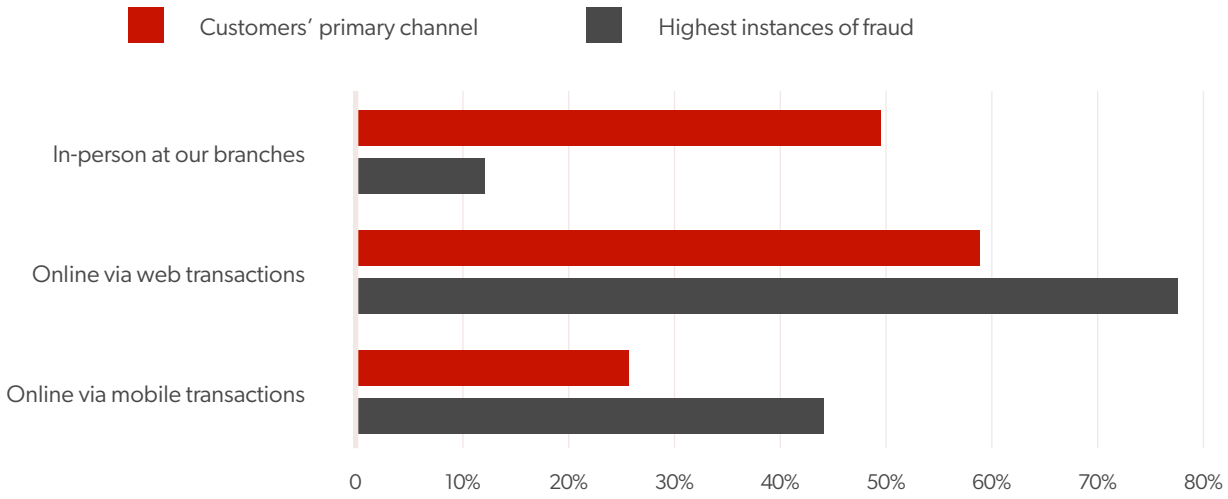
The top vulnerability for respondents is that today's fraud schemes are evolving too quickly for them to keep pace, at 83%. In second place, at 57%, is the related issue of how monitoring employees, networks and devices has become more challenging with remote workforces. And 55% of respondents say that they are concerned about an overreliance on manual processes.

Please select the top three most concerning fraud schemes for your institution this upcoming year.



The most concerning fraud scheme for institutions for the rest of 2023 and into 2024 is information disclosure/stolen credentials at 52%, closely followed by electronic fraud at 50%. Phishing (non-business email compromise) comes next at 44%, followed by account takeover (mobile/web) at 42%.

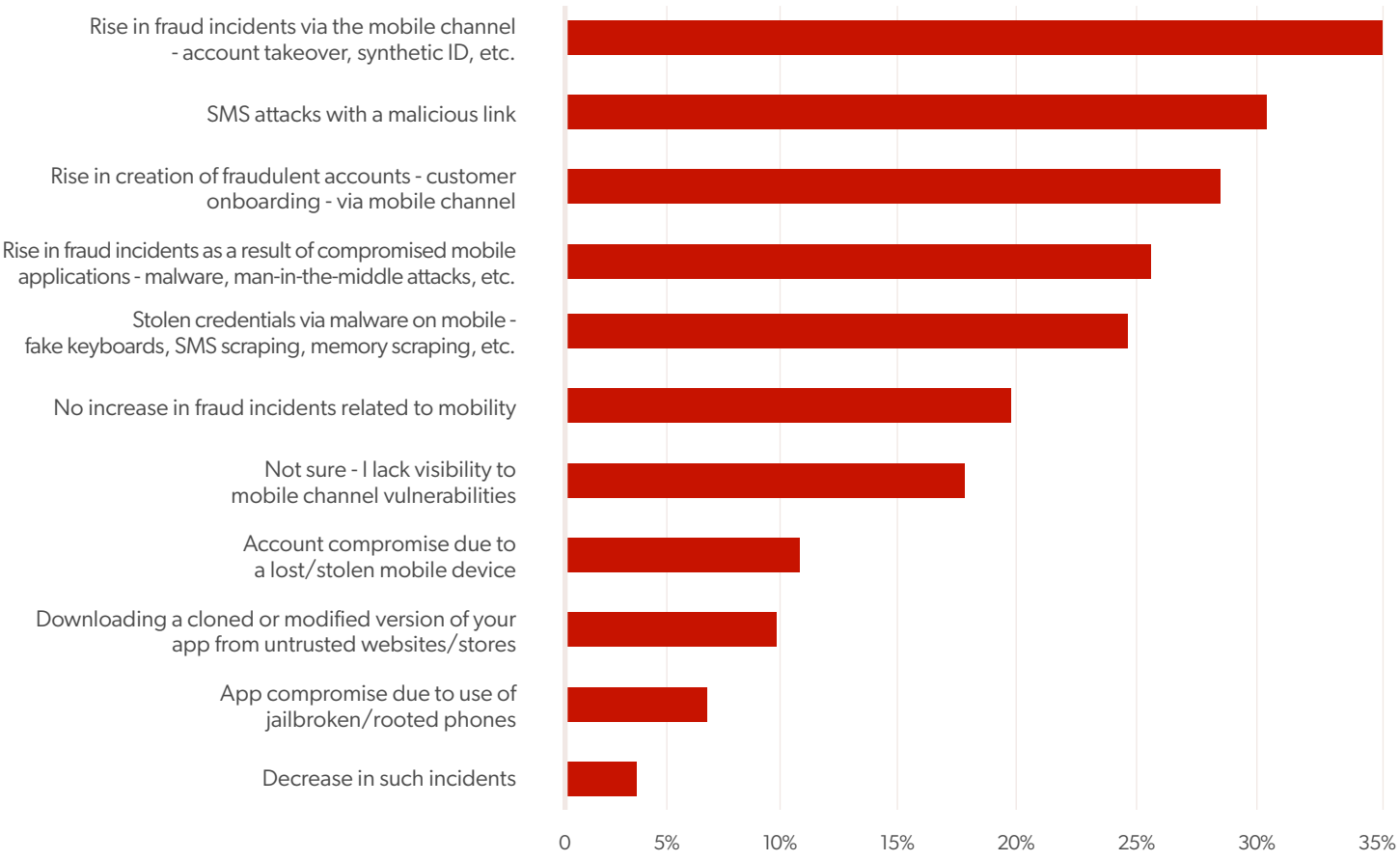
Today, what is your customers' primary channel for conducting business with your institutions? Which channel has the highest incidence of fraud?



Respondents say customers' primary channel for conducting business with their organization is online transactions, at 44%. They also say this channel has the highest incidence of fraud, at 58%, which far exceeds usage. It seems that risk managers – whether they know it or not – are accepting the potential for higher levels of fraudulent activities in return for increased volumes of business via online channels.

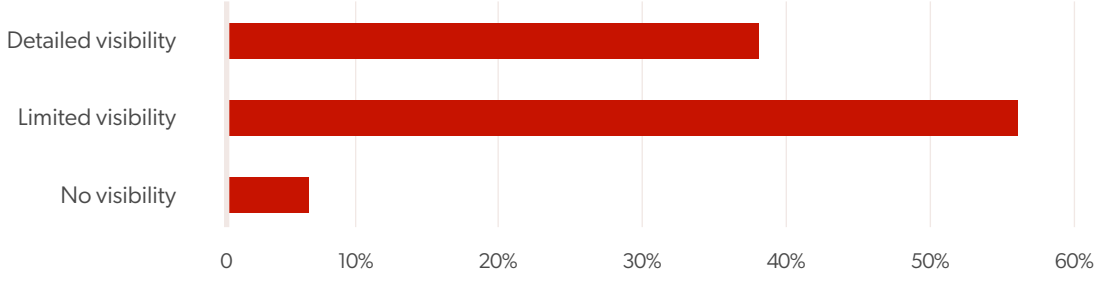
In contrast, respondents say in-person business at branches accounts for 37% of use but just 9% of fraud. Mobile transactions are third in usage terms at 19% but second-highest in fraud at 33%.

In the past year, have you experienced any of the following fraud incidents specifically related to the mobile channel?



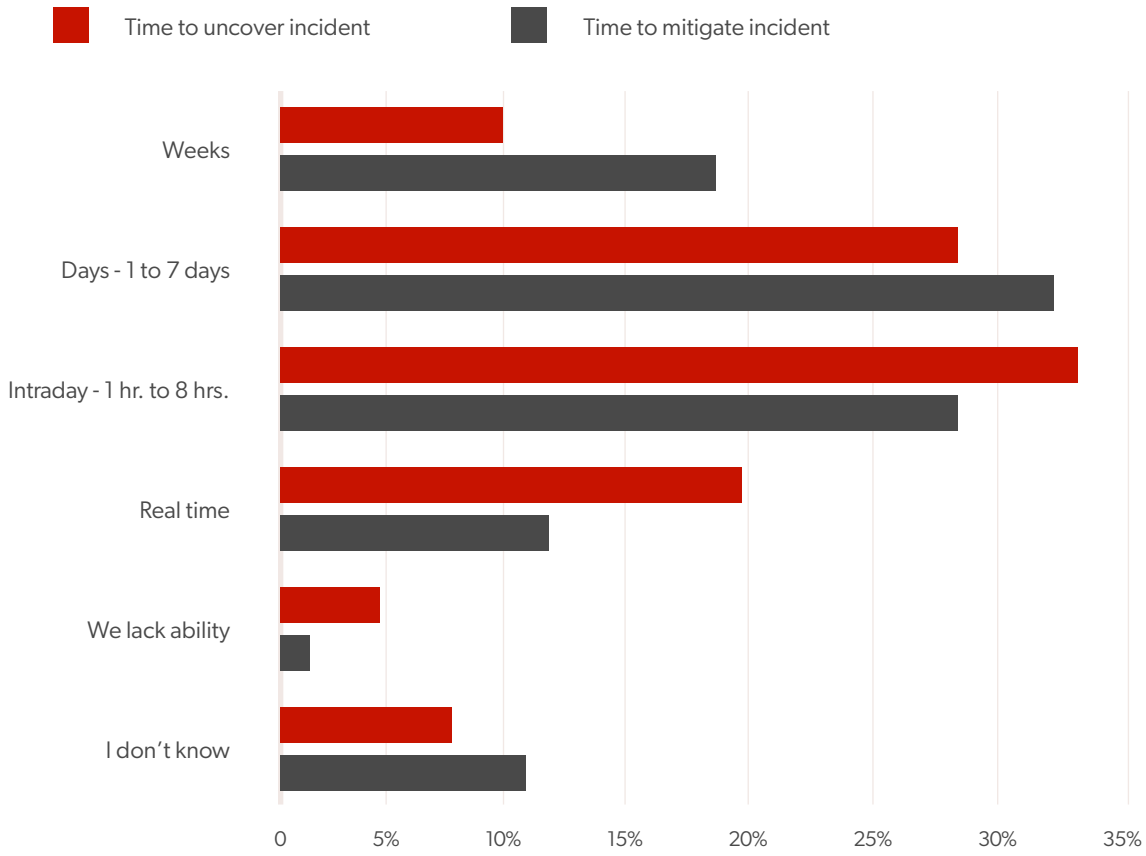
Although there was no one standout attack method, 35% of respondents report a rise in fraud incidents via the mobile channel (account takeover, synthetic ID, etc.), 30% say SMS attacks with a malicious link are on the rise, and 28% report a rise in the creation of fraudulent accounts (customer onboarding) via the mobile channel.

How much visibility does your organization have when it comes to identifying the impact of a phishing attack?



Most organizations, 62%, say they have limited or no visibility when it comes to identifying the impact of a phishing attack, and just 38% claim to have detailed visibility. The results suggest that this remains a target area for improvement.

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

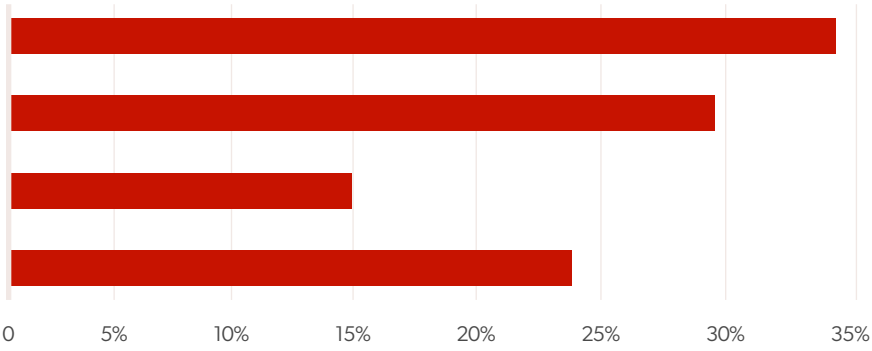


Nineteen percent of respondents say they can uncover a fraud incident in real time. That's a 7% increase from 2019 and a 3% decrease from 2020. Eleven percent of respondents say they can mitigate fraud in real time.

Almost half of the respondents say it takes over a day to identify fraud. While the percentages for intraday and 1-7 days dropped, the "over a week" numbers increased from 2019 and 2020. Also, when evaluating mitigation times from prior years overall, the mitigation times increased, meaning it is taking institutions longer.

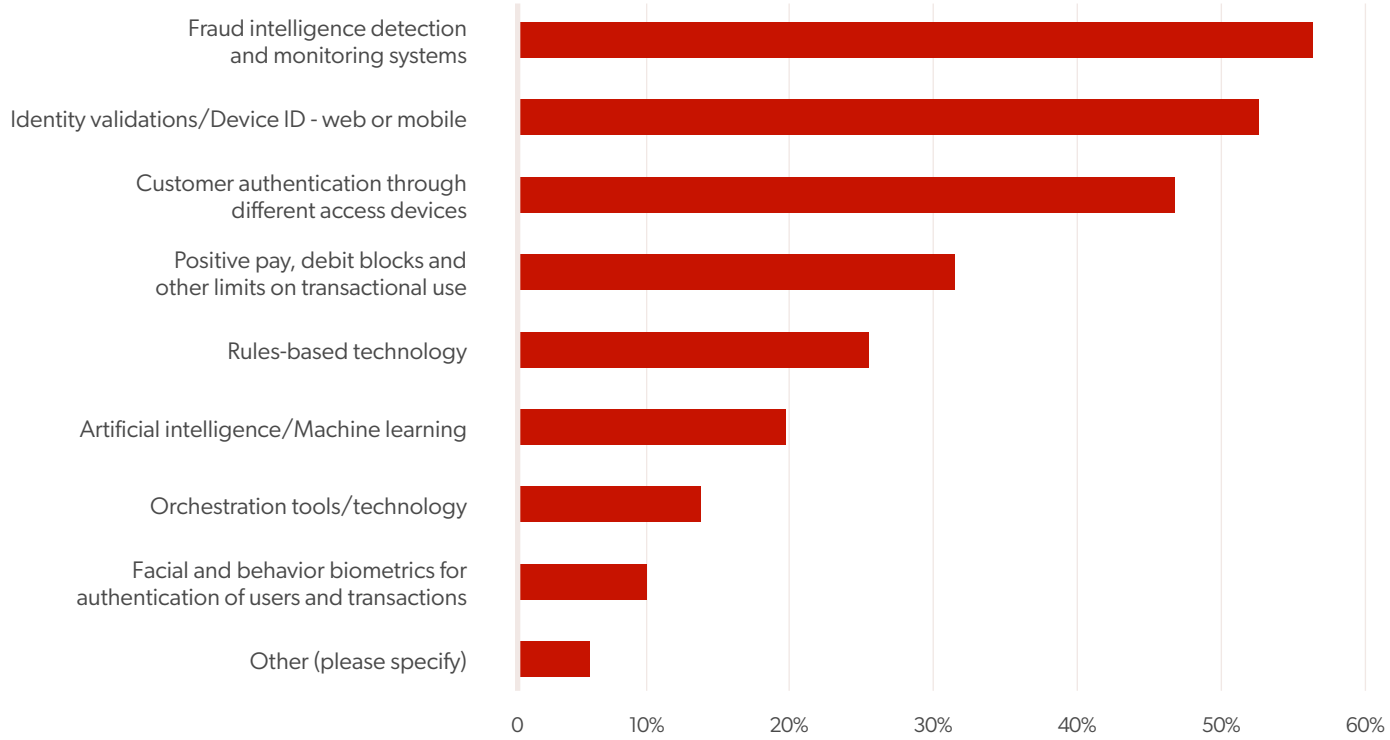
Yet 97% of respondents say their ability to detect and mitigate fraud is average or above. So, there is a disconnect between their perceptions and reality.

Considering the last 12 months regarding fraud losses, and your current fraud posture, how do you see your monetary fraud losses during the next 12 months?



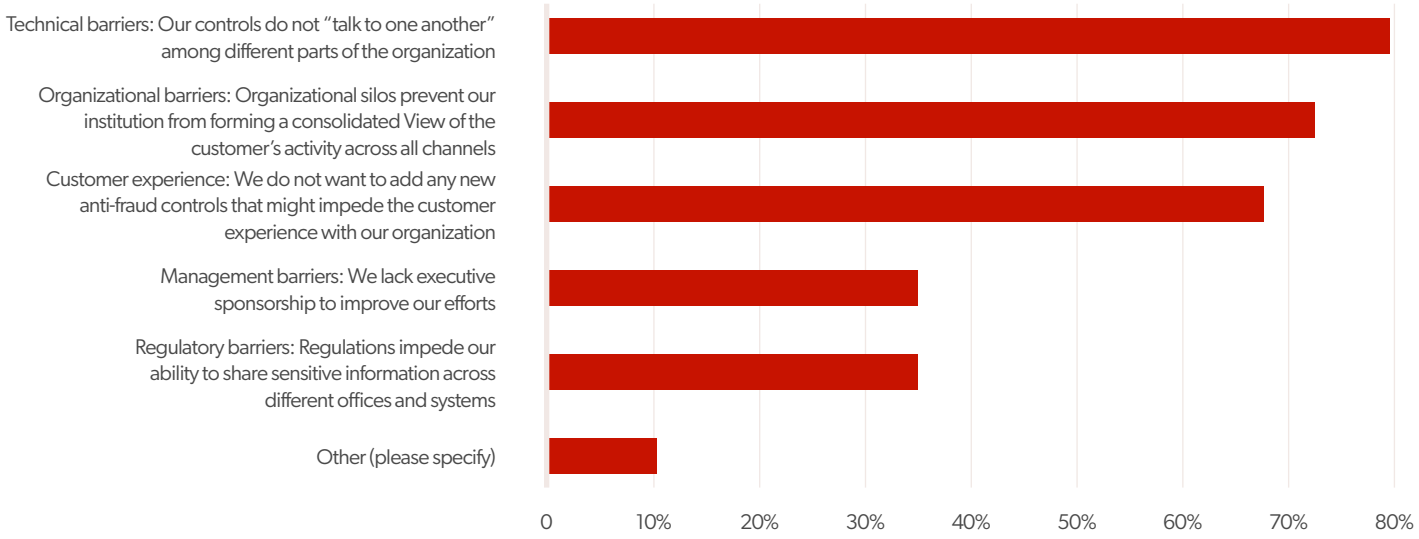
Thirty-four percent of respondents expect monetary fraud losses to increase during the next 12 months, while 29% expect them to remain steady and just 14% forecast a decrease.

Which technologies had the most significant impact on preventing fraud losses?



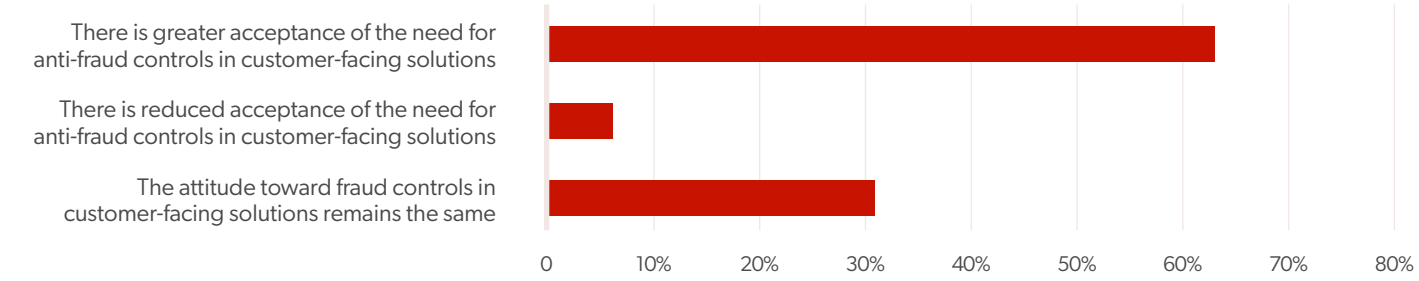
Fraud intelligence detection and monitoring systems top the list of technologies that have the most significant impact on preventing fraud losses, at 57%. Identity validations/device ID (web or mobile) is second at 53%, and customer authentication through different access devices is third at 47%.

Please select your organization's top three barriers to improving fraud prevention.



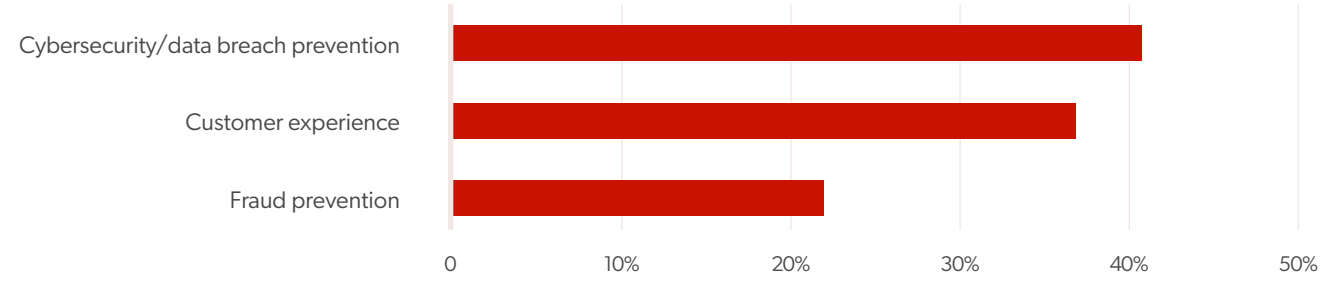
The top barrier to improving fraud prevention is technical barriers, 80% of respondents say. This is followed by organizational barriers at 73%, and customer experience at 68%.

In your institution, how has the attitude toward anti-fraud controls compared to customer experience changed?



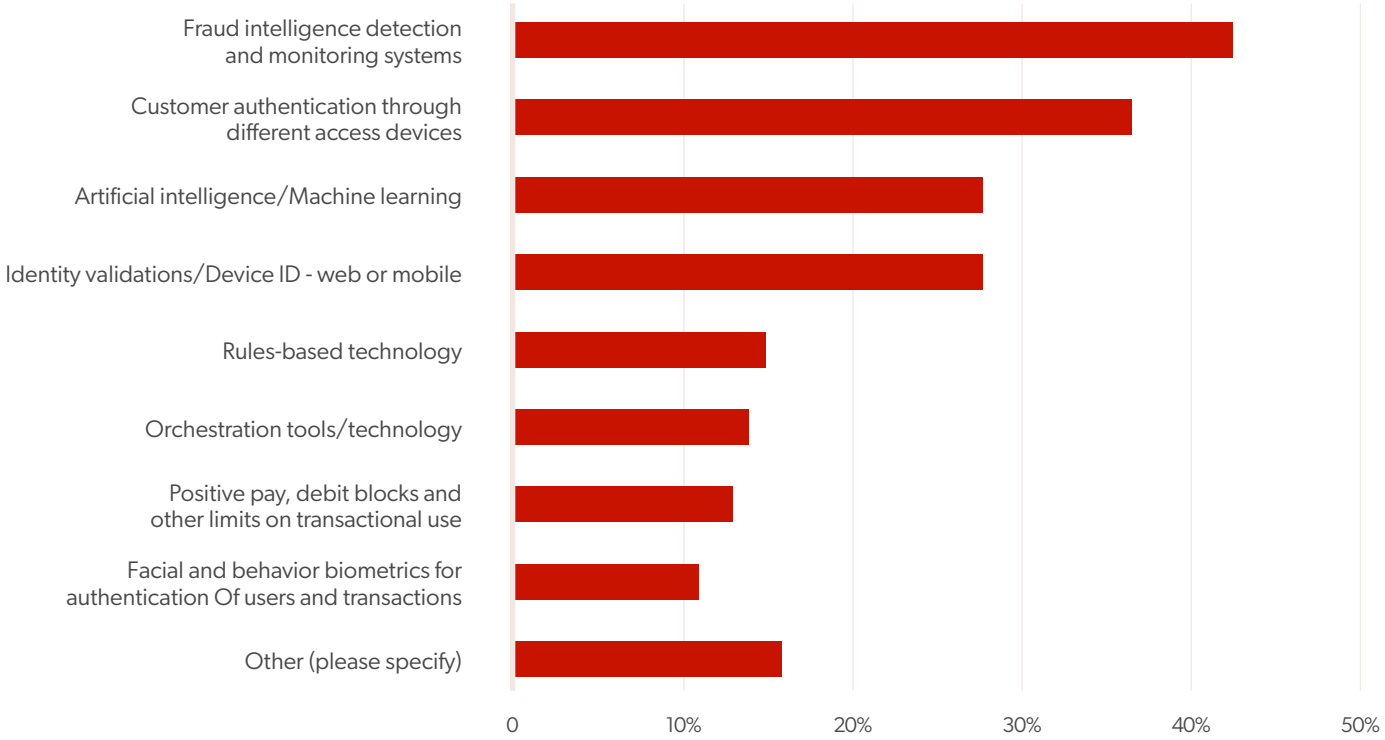
The majority of respondents, 63%, say there is greater acceptance of the need for anti-fraud controls in customer-facing solutions, compared to 31% who say the attitude remains the same and just 6% who say there is reduced acceptance.

In your opinion, which of these have the greatest priority for your institution in customer-facing solutions today?



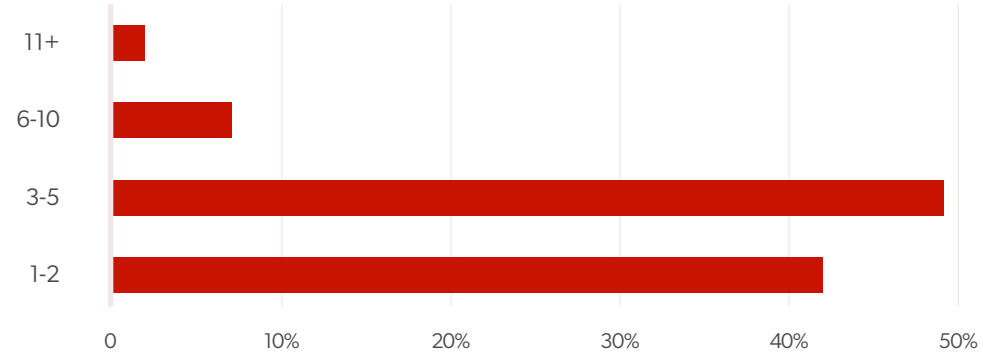
When asked what the greatest priority for your institution in customer-facing solutions is today, 41% of respondents say cybersecurity/data breach prevention. Customer experience is next at 37%, followed by fraud prevention at 22%.

Which of the following technologies are you planning to invest in within the next 18 months?



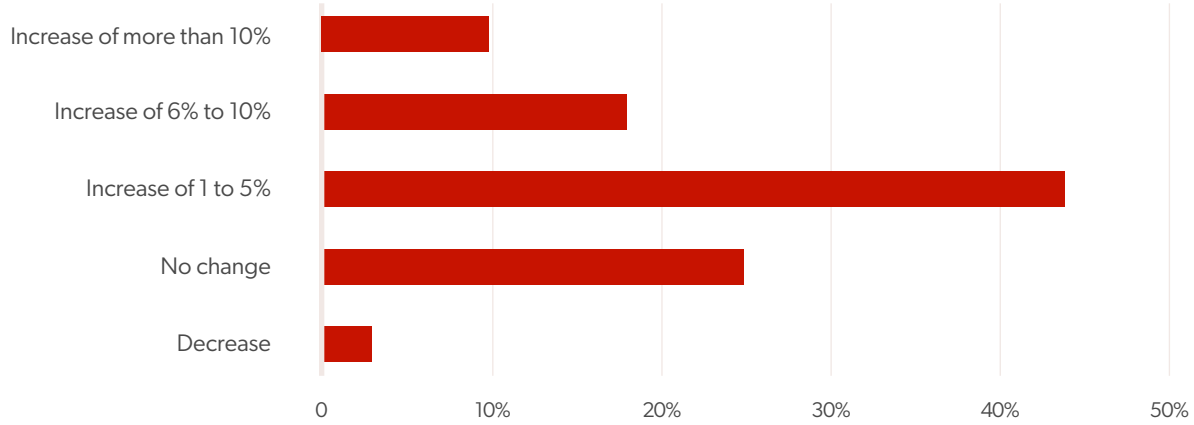
Forty-three percent of respondents say they plan to invest in fraud intelligence detection and monitoring systems within the next 18 months. This is followed by customer authentication through different access devices at 37% and identity validations/device ID (web or mobile) and artificial intelligence/machine learning, both at 28%.

How many separate providers do you purchase from to achieve your anti-fraud needs?



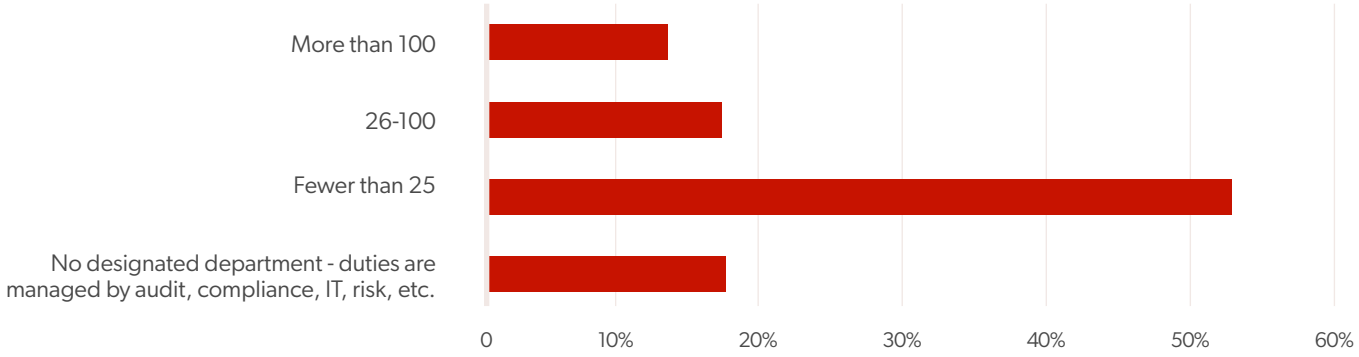
Forty-nine percent of respondents say they use three to five vendor providers, and 42% say they use one to two. Only 9% say they use six or more.

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



Forty-four percent of respondents say their budget dedicated to fraud prevention will increase by 1% to 5% in the next year. Twenty-five percent forecast no change, 18% expect an increase of 6% to 10%, and 10% expect an increase of more than 10%. Only 3% expect a decrease.

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



Most respondents, 53%, say their department assigned to fraud prevention and detection consists of fewer than 25 people. Seventeen percent say they have no designated department, 17% report having 26 to 100 people, and just 13% say they have more than 100 people.

Conclusions

Visibility

The biggest concern from the data is that only 19% of respondents achieve real-time identification of the impact of a phishing fraud, and the response times are increasing. That means companies are getting slower in their ability to identify that they have been affected by fraud. Real-time mitigation is even less, at just 11%.

A significant contributory factor is that 56% of respondents say they have limited visibility when it comes to identifying the impact of a phishing attack, and 6% admit they have no visibility.

Tooling and Silos

The respondents recognize the benefits that can be obtained through deployment of fraud intelligence detection and monitoring systems – which top the technologies that have the most significant impact on preventing fraud losses, at 57%. But only 43% of respondents actually plan to invest in fraud intelligence detection and monitoring systems over the next 18 months.

Another problem is that the implementation of tooling appears to be happening in a piecemeal manner, since 80% say their controls do not talk to one another – the top barrier to improving fraud prevention. A holistic approach is required.

Entities need to work through their technical and organizational barriers. This has been a consistent trend in the report dating back to 2020. Silos are preventing institutions from taking a multilayer approach. Without that, it becomes very difficult to keep up with the speed at which the fraud landscape evolves.

Concern about manual processes, which implies the need for automation, continues to grow, but this can be seen as a positive development that is likely to drive automation going forward.

A Holistic Approach

We need to take a holistic approach to fraud. We cannot look at the parts or components involved in isolation. Organizations need to be encouraged to leverage the sensors they have from each of the parts – user, device, transaction/event – to create a singular, continuous assessment of the session.

While a time lag between solution awareness and implementation is to be expected, the gap between perception of performance and evidence of performance is a persistent feature of this survey series. There appears to be a lack of awareness/benchmarking of peer performance and a certain amount of complacency.

Hopefully, readers of this survey will recognize how expectations of high-performing fraud prevention have continued to increase, and if they see they are falling behind best practices, they will rise to the occasion by targeting real-time identification of the impact of phishing and taking a holistic approach to implementing fraud prevention technologies.

Survey Analysis

Appgate Faces of Fraud Survey Discussion With Mike Lopez, Senior Vice President, Appgate

MIKE LOPEZ
Senior Vice President, Appgate

Perception vs. Reality

TONY MORBIN: What stood out for you in the survey results, and how does that compare with what you're finding in the market generally?

MIKE LOPEZ: One of the things that stood out to me was the responses around the time frames for identifying and mitigating fraud. Only 19% of the respondents said that they can identify fraud in real time. Not only does that statistically stand out to me, but the overwhelming majority of the respondents said that they believe that their ability to identify and mitigate fraud is either average or above average. That is a trend that we have consistently seen since we've done this with ISMG for over five years now. It's a disconnect between the perceived effectiveness of the fraud posture of the organization and reality in terms of the actual ability to identify and mitigate fraud.

The Biggest Challenge

MORBIN: How do the respondents' answers to what they see as the greatest vulnerabilities in their fraud defenses align with what you're seeing?

LOPEZ: Since 2019, the biggest challenge that the respondents see is the speed at which fraud is evolving and the rate at which the attackers are modifying their attacks to keep pace with the emerging technologies being implemented by financial institutions. This year, 83% of the respondents said that is their biggest vulnerability. That is up from 55% in 2020, and it is something that the financial institutions need to look at.

There are multiple reasons why that is a problem, and it's embedded in the responses. One is the fact that there's still an abundance of manual processes being run by financial institutions. The second piece, which is the largest contributor to this, is the lack of orchestration between not only the technologies that are implemented by financial institutions and the

> *"There are still significant silos being created between these components that are forcing manual processes to be run, and that is allowing the fraudsters and the adversaries to stay just one step ahead of the institutions themselves."*

respondents, but also the business units themselves. There are still significant silos being created between these components that are forcing manual processes to be run, and that is allowing the fraudsters and the adversaries to stay just one step ahead of the institutions themselves.

A Holistic Approach

MORBIN: When it came to the attacks that concerned the respondents, do you agree with their priorities?

LOPEZ: The biggest threat right now from a respondent's perspective is definitely the online channel. But part of the problem is that the silo aspect of the data is preventing institutions from effectively making appropriate decisions. They consistently highlight the balance between anti-fraud mitigating controls versus the customer experience. And in that process, they're focusing on those silos, and it is creating ineffective programs that directly affect the user experience. They should be taking a holistic approach.

Better Orchestration

MORBIN: I was surprised at the reported lack of visibility for identifying the impact of a phishing attack. Were the respondents particularly poor in this regard?

LOPEZ: Typically, with either smaller credit unions or larger financial institutions, there is a split between who's responsible for fraud and who's responsible for cyber. And the anti-phishing controls typically fall under the cyber side. That information is not being passed over to the fraud unit so that they can correlate their fraud losses. That's problematic.

Automation and AI

MORBIN: The respondents reported which technologies they believe have the most significant impact on preventing fraud losses. Have they got it right?

LOPEZ: Ultimately, technology is the way to go. You need to continue to invest in automation and be able to ingest as many data points as possible. The orchestration needs to be considered. You can't look at individual factors or sensors in isolation. You need a holistic approach. If you're going to stay ahead of the adversaries, you can't have singular points for detection. You need to look at the user's patterns, the device patterns and the transactional patterns collectively to effectively move toward a program that is going to be effective. You need to invest in automation, artificial intelligence and behavioral biometrics. Those will definitely help solidify your posture.

> *"If you're going to stay ahead of the adversaries, you can't have singular points for detection. You need to look at the user's patterns, the device patterns and the transactional patterns collectively to effectively move toward a program that is going to be effective."*

A Collective Risk Score

MORBIN: Did you see those needs reflected in what the companies reported as technologies that they were going to invest in over the next 18 months?

LOPEZ: They're nailing everything that they should be investing in. They are looking at detection monitoring systems. That was 43% of the response. They're looking at customer authentication and identity validation, whether on the user side or the device side. That was 37%. The remaining percentage is in the artificial intelligence/machine learning, so they're looking at everything correctly. The key point is how they take each one of those components and get them to talk to each other. They need to get a collective risk score that incorporates the device risk, the user risk, the user identity and artificial intelligence or machine learning around the transaction or sessions themselves to collectively have just one risk score as opposed to looking at each one of those components again in isolation.

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 36 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.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® · CU INFO SECURITY® (Just for Credit Unions) · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

infoRisk TODAY · CAREERS INFO SECURITY® · Data Breach TODAY (Prevention. Response. Notification.) · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

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