Sponsored by

Guidehouse

EXECUTIVE SUMMARY

Staying Ahead of the Fraud Curve

Solid Risk Assessment Is the Foundation of a Best-in-Class Fraud-Control Program

Fraud is on the rise, and the COVID-19 pandemic has raised the stakes for financial institutions intent on staying ahead of criminals. More people are working from home and doing business digitally—from purchasing goods to managing their financial lives. Meanwhile, cybercriminals are staying busy: The FBI's Internet Crime Complaint Center reported a record number of complaints from the American public in 2020 tied to losses of more than $4.1 billion.[1]

Nevertheless, banks largely feel confident in their ability to detect, prevent and mitigate fraud, according to a new survey conducted by American Banker/Arizent Research, in partnership with Guidehouse. Their ability to continue to assess and prioritize fraud risk will be a key factor in determining whether they will feel equally confident in the coming years.

Fraud remains a high priority for financial institutions

The vast majority of financial institutions (FIs) have grown more concerned about fraud over the past 12 months. Regional and community banks and credit unions report increased concerns at a higher rate (95%) than national banks (73%) or broker-dealers (72%).

That discrepancy is not surprising, according to Sandra Desautels, a partner in Guidehouse's Global Investigations and Compliance practice. Larger national banks tend to have mature fraud prevention programs and share intelligence via global forums, giving them a broader perspective on criminal activity than more locally focused regional banks. Much of the fraud in the past year has been related to government relief programs, and benefits and unemployment payments, which may have impacted the customer base of some banks more than others. Criminals also are aware that large banks tend to have more fraud controls in place, so it's likely that criminal activity is trickling down to smaller markets.

[1] FBI, "Internet Crime Report, 2020," https://www.moneylaundering.com/wp-content/uploads/2021/03/FBI.Report.IC3_.032121.pdf.

EXECUTIVE SUMMARY

As fraud cases rise, FIs are increasingly worried about the potential business risks that can accompany fraudulent activity. The most commonly cited risks include hits to profitability (41%), brand reputation (40%) and customer satisfaction (38%), with national banks expressing a higher level of concern than other FIs about negative impacts on profitability. For their part, regional and community banks and credit unions are generally more worried about increased costs tied to rising customer reimbursements than national banks or broker-dealers (58% versus 27% and 16%).

This discrepancy may suggest an area of focus for smaller banks, according to Desautels. Because community banks have historically dealt with people from their local communities, they may not have developed the type of robust, formalized know-your-customer (KYC) processes that national FIs have instituted. "As a community bank, we do a good job of knowing our customers and how they conduct business," says an executive manager at a community bank. Absent strong authentication and education processes, however, this viewpoint could mask a weakness that criminals could target with increasingly sophisticated impersonation schemes.

As fraud cases rise, FIs are increasingly worried about the potential business risks that can accompany fraudulent activity, including hits to profitability, brand reputation and customer satisfaction.

The dangers of complacency

Despite their concerns, most leaders at FIs believe they are doing a good job managing fraud prevention and mitigation. Most (70%) rate their organization's strategy as proactive, and nearly 80% are confident in their ability to assess and prioritize key fraud risks, with national banks reporting the most confidence in these abilities. But it's important to note that as fraud continues to evolve, today's proactive fraud strategies could quickly become obsolete and organizations must remain on alert and at the ready to make changes and implement new tactics. Proactive efforts also can be ineffective if they don't target the areas where organizations need the most help. "If your resources aren't going toward the places you're currently weakest in terms of your risk exposure, you end up trying to put out the wrong fires," Desautels warns. It's critical that organizations keep risk assessments up to date so that they align their resources with their needs as efficiently as possible.

Alex Shea, director of Global Investigation and Compliance at Guidehouse, notes that it can be easy for organizations to become complacent, because the categories of fraud against which they need to defend remain more or less the same. FIs say that identity theft (63%) and security breaches (54%) are the most significant risks to their organizations. National banks, which attract more varied types of attacks due to their reputations for having stronger controls in place, are three times more likely than broker-dealers to see significant risk in social engineering attacks seeking entry to their systems via contact center agents.

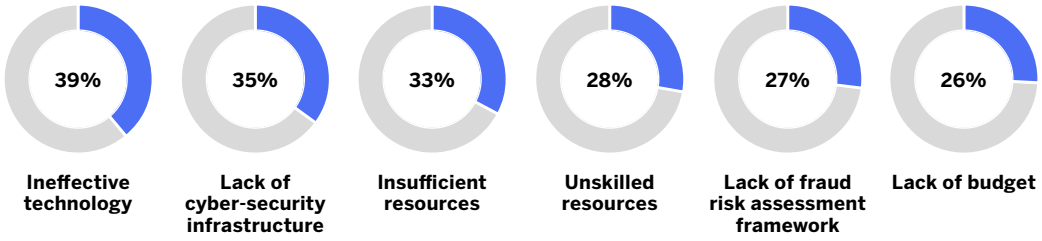
Some FIs may have also become overconfident because they don't fully grasp the changing attacks used by criminals. For instance, smaller banks may be less aware of newer fraud schemes because they have not been targeted as heavily in the past, says Desautels. The increased scale and sophistication of fraud attempts make it possible for more criminals to attack more targets in more ways. "It's critical that institutions guard against complacency," Desautels says.

EXECUTIVE SUMMARY

Addressing gaps and challenges

While most organizations say they are effective at assessing and prioritizing key fraud risks, FIs note their many challenges in actively doing so. In particular, they cite ineffective technology, a lack of cybersecurity infrastructure and insufficient resources. (See Figure 1.)

Figure 1: **Challenges in Assessing and Prioritizing Fraud Risks**



Source: Arizent Research/American Banker, February 2021

Shea says an objective risk assessment is a critical tool when building an effective and proactive fraud prevention and mitigation strategy. But more than one in four FIs report a lack of a risk assessment framework as one of their biggest challenges. Without such a framework, organizations may direct resources into the wrong areas. A firm, for example, may invest money to address an issue highlighted by a regulatory advisory—even if that issue isn't one that poses a considerable risk to that particular institution.

Fraud prevention program best practices

Taking these factors into consideration, Desautels suggests organizations take a hard look at their activities to be sure they truly are proactive. An efficient way to do this is to hire an objective third party to review your program to assess whether the institution's risk prevention and mitigation efforts align with actual fraud risks to which it is currently exposed.

More importantly, Desautels urges organizations to treat risk assessments as a fluid exercise, since risks are always changing. The dynamic nature of the threat puts a premium on ongoing training and testing to ensure both employees and customers are aware of risks and acting appropriately. "There's been a lot of effort put into safeguarding systems since COVID," she says. "Companies benefiting from that now may feel proactive—but in two or three months they could find themselves reacting to something they could have prepared for with a different risk assessment strategy in place."

"If your resources aren't going toward the places you're currently weakest in terms of your risk exposure, you end up trying to put out the wrong fires."

—Sandra Desautels,
Guidehouse

Methodology

The online survey was conducted by Arizent Research/American Banker in February 2021 among 102 respondents that work at financial institutions or technology providers. Qualified respondents are employed in manager level–plus roles and have at least a moderate level of responsibility or oversight into fraud prevention/mitigation at their organization.

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology, and risk consulting. We help clients address their toughest challenges and navigate significant regulatory pressures with a focus on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that prepare our clients for future growth and success. www.guidehouse.com

About Arizent Research

Arizent delivers actionable insights through full-service research solutions that tap into their first-party data, industry SMEs, and highly engaged communities across banking, payments, mortgage, insurance, municipal finance, accounting, HR/employee benefits and wealth management. They have leading brands in financial services including American Banker, The Bond Buyer, PaymentsSource, Financial Planning, National Mortgage News, and in professional services, such as Accounting Today, Employee Benefits News, and Digital Insurance. For more information, please visit www.arizent.com