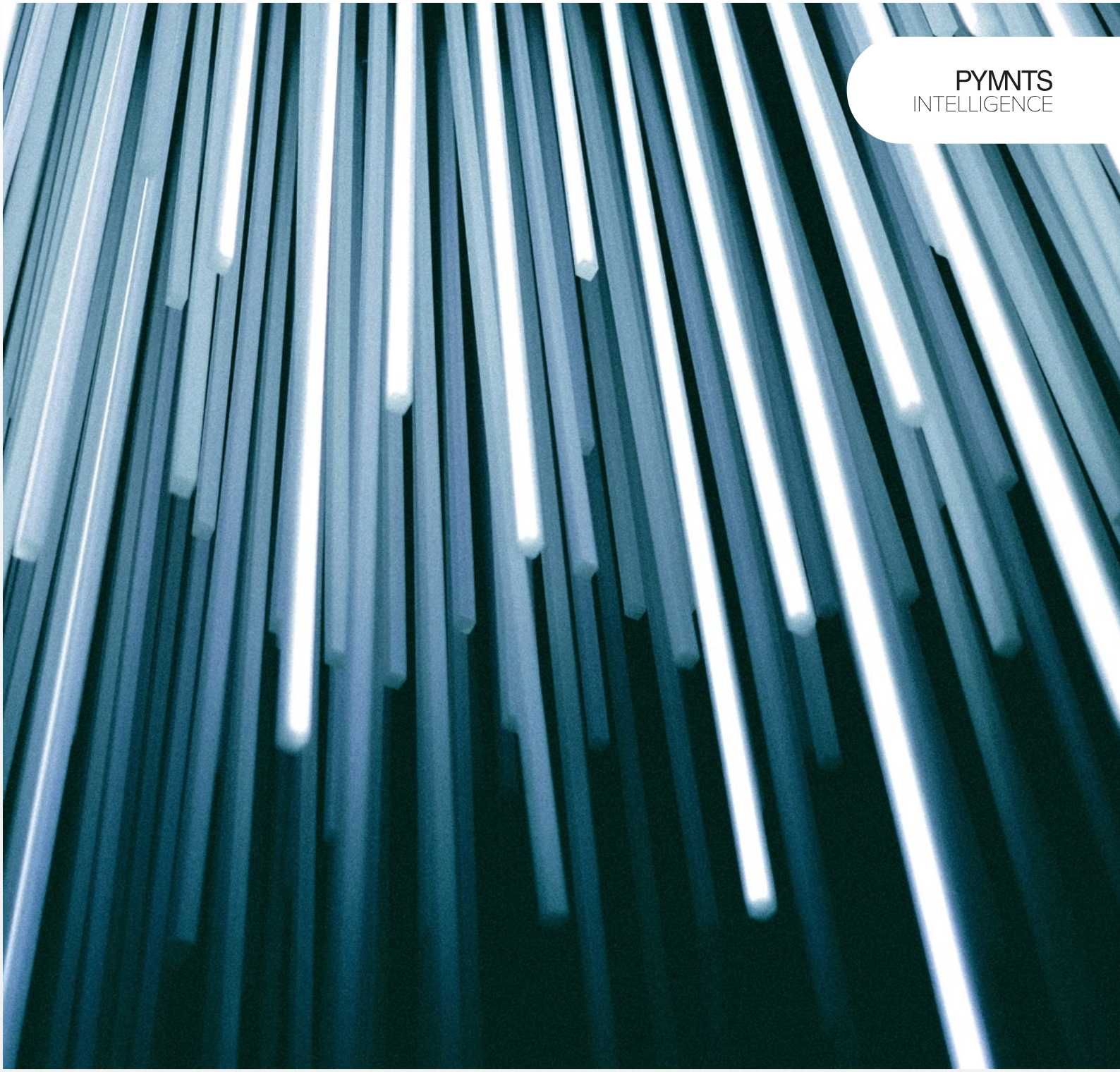


PYMNTS
INTELLIGENCE

THE STATE OF **FRAUD AND FINANCIAL CRIME IN THE U.S. 2024:** WHAT FIs NEED TO KNOW

November 2024 Report

THE STATE OF **FRAUD AND FINANCIAL CRIME IN THE U.S. 2024:** WHAT FIs NEED TO KNOW

PYMNTS INTELLIGENCE

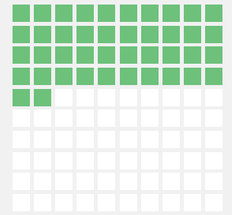
The State of Fraud and Financial Crime in the U.S. 2024: What FIs Need To Know is a PYMNTS Intelligence report.

TABLE OF CONTENTS

WHAT'S **AT STAKE**

As transactions have moved more digital, financial institutions (FIs) have invested heavily in shoring up their defenses against fraudsters who seek to exploit the digital shift. Those efforts have paid off, as fraud related to more routine digital payments has decreased markedly over the last three years.

But there is a new fraudster in town — or a new type that weaponizes different skills and new tool — and FIs find themselves fighting this new fraud threat. In a way, it's as if fraudsters have become more customer-centric, in that they turn to social engineering to deceive consumers into sending funds or providing access to their bank accounts to perpetrate fraud. Tools designed to detect fraudsters doing bad things with stolen credentials are little match for transactions that consumers are tricked into sending from their own accounts. This has resulted in an increase in fraud year over year.



42%

Share of FIs that **saw their overall fraud rate increase** in the last 12 months

In 2024, we find that the volume of fraudulent transactions and dollars lost to fraud grew at a faster rate than in 2023. This uptick in fraud is largely attributable to shifts in fraudsters' strategies, as the share of fraud stemming from scams rose 56% in the last year. Worse, the share of dollars lost to fraudsters because of scams rose by 121%. Now, scams are now the most common form of fraud reported by banks, at 23% of all fraudulent transactions.

FIs understand the stakes and the complexity of the fight. More than one-quarter (26%) added behavioral analytics to their anti-fraud toolkits in the past year — a technology that is quickly becoming table stakes for effective fraud prevention in a world where fraudsters have the tools to mimic or to trick consumers into acting on their behalf.

Moreover, 76% of FIs are either in the process of adding new technologies now or planning to do so in the next year, suggesting a broad upswing in such investments since our prior survey is on the way. The largest FIs in our sample (those with more than $25 billion in assets) have a head start over smaller competitors in this initiative, with nearly one-third already in the process of adding these technologies, whereas it is more common for FIs with between $1 billion and $25 billion in assets to have plans to add these technologies in the next six to 12 months.

56%

Increase in the share of fraudulent transactions that are scams

These are just some of the findings detailed in The State of Fraud and Financial Crime in the U.S. 2024: What FIs Need To Know, a PYMNTS Intelligence special report. This study examines the dynamic fraud environment for FIs and how they are responding, with a focus on fraud prevention technologies. It draws on insights from a survey of 200 executives working at 200 different FIs in the United States with at least $1 billion in assets conducted from Sept. 9 to Sept. 30.

This is what we learned.

KEY **FINDINGS**

01

CHANGING TARGETS

Fraudsters have shifted away from digital payments fraud to social engineering tactics that exploit the trust of their victims.

27%

Share of FIs' total dollar losses to fraud attributable to either relationship or trust scams or product or service scams

02

FINANCIAL DAMAGES

A higher share of FIs report increases in dollars lost to fraud relative to 2023.

40%

Share of FIs whose dollar losses to fraud grew in the last 12 months

03

INNOVATIVE DETECTION

FIs are turning to newer anti-fraud technologies that support them in identifying social engineering strategies.

26%

Share of FIs that implemented behavioral analytics technology in the last year

04

COST MATTERS

Although cost is a key barrier to innovating fraud technology, worsening fraud losses highlight the ROI of sophisticated fraud detection tools that can outsmart fraudsters using their own upgraded tools.

83%

Share of FIs that cite cost as a factor that makes it difficult to upgrade their fraud prevention solutions

THE FULL STORY

Fraudsters are evolving their strategies faster than FIs can adapt their detection technology, leaving customers vulnerable.

Fraudsters have shifted away from digital payments fraud to social engineering tactics that exploit the trust of their victims.

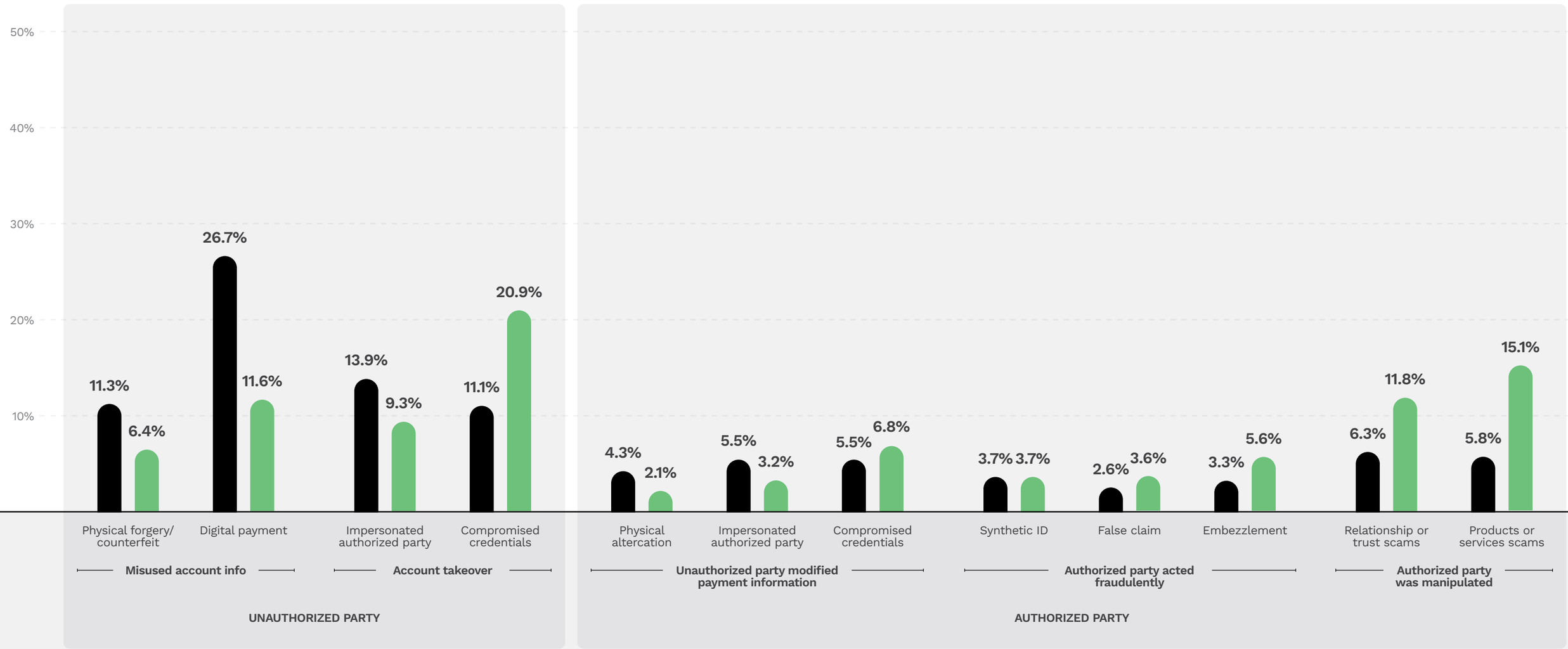
One of the reasons fraud management can be an uphill battle is that fraudsters constantly change their tactics. More transactions are now digital, and in recent years, banks have made large strides in reducing digital payment fraud, which was the leading type of fraud just last year. Fraudsters adapted in response, and now focus more on exploiting a less protected vulnerability: people. The share of fraud stemming from scams — which manipulate authorized individuals — rose 56% in the last year, making scams the most common type of fraud.

These trends reflect a fundamental shift in fraud patterns. In 2023, digital payment fraud accounted for 27% of dollar losses and 22% of fraudulent transactions. In 2024, these shares fell by 57% and 37%, respectively, as anti-fraud systems and strategies improved in this area.

FIGURE 1

Key types of fraud

Share of total dollar losses, by select categories of fraudulent activities and year



Source: PYMNTS Intelligence

The State of Fraud and Financial Crime in the U.S. 2024, November 2024

N = 200: Whole sample, fielded Sep. 9, 2024 – Sep. 30, 2024

Conversely, in 2024, scams accounted for 27% of dollar losses: product or services scams at 15% and relationship or trust scams at 12%. Digital payment scams, meanwhile, fell all the way down to 12% from 27%. Also notable this year is the sharp rise in compromised credential fraud, in which fraudsters use deception to make victims hand over account details. Taken together, today's fraudsters can be seen as more customer-centric, leveraging social engineering to strike away from FIs' fortresses of security.

The rapid increase in scams that manipulate victims directly is particularly worrisome, as only 44% of FIs are willing to reimburse these customers. FIs lost 121% more to scams in 2024 than in the previous year in terms of the share of total dollars lost to fraud.

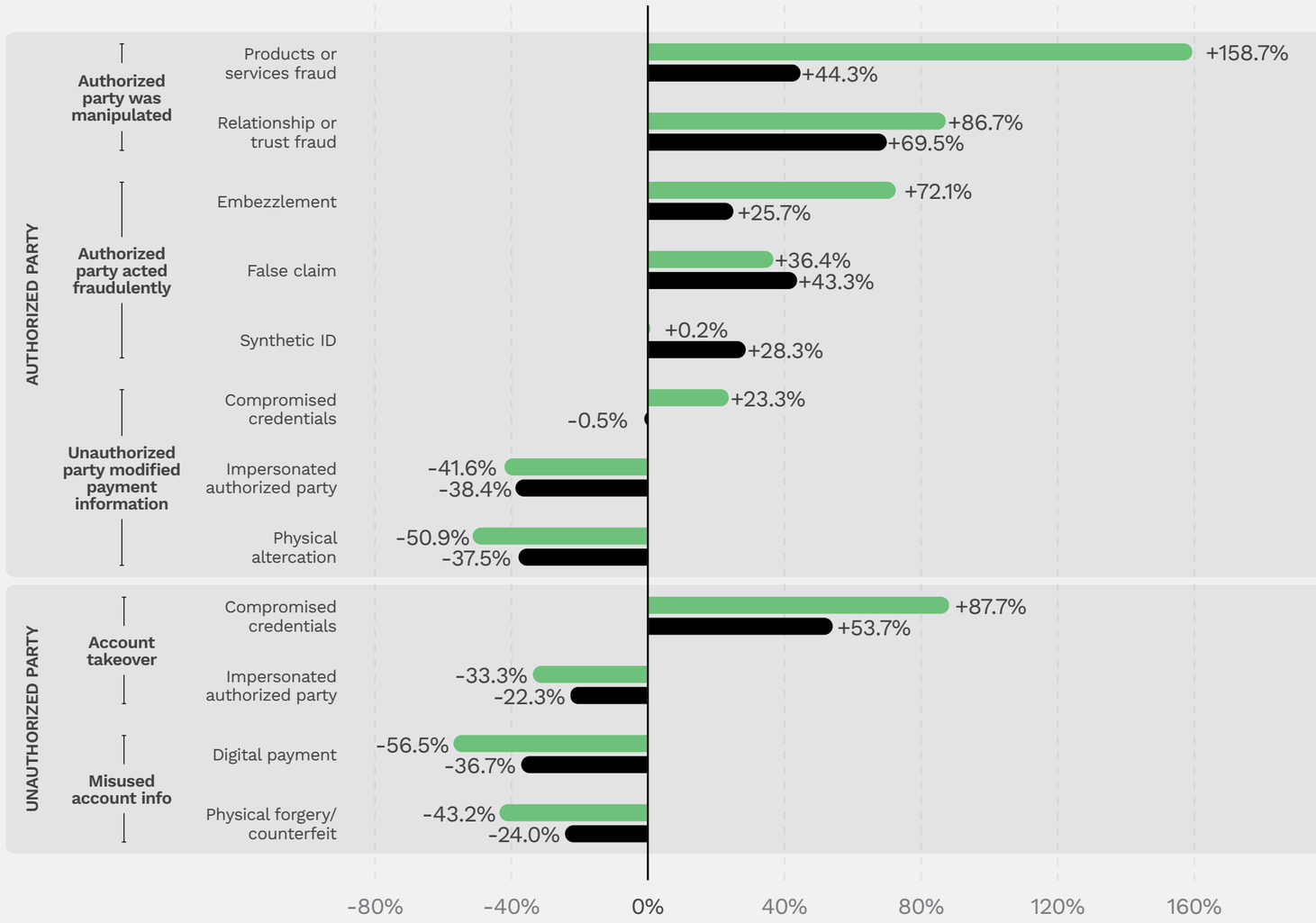
Not only is this form of fraud growing more common but it is also growing more effective. While the share of total fraud attributed to scams and compromised credentials rose, the dollar value of these scams rose even more.

Our recent work on consumer experiences of scams finds only 56% of scam victims report the scam to their bank, indicating the impact of scams on bank customers is largely under-captured. It also found that customer satisfaction takes a major hit even when victims are reimbursed, so FIs should consider protecting customers from social engineering to be paramount.

FIGURE 2

Fraudsters' shifting tactics

Change in share of total dollar losses and number of fraudulent transactions, by select categories of fraudulent activities



Source: PYMNTS Intelligence

The State of Fraud and Financial Crime in the U.S. 2024, November 2024

N = 200: Whole sample, fielded Sep. 9, 2024 – Sep. 30, 2024

A higher share of FIs report increases in dollars lost to fraud relative to 2023.

The shift to scam tactics has proven effective — and lucrative — for fraudsters. Forty percent of FIs lost more money to fraudulent transactions in the last 12 months than in the preceding year. Similarly, 38% reported a higher volume of fraudulent transactions in the same time frame. These are substantially higher shares than those that reported improvements, both at 23%. Our previous edition of this study, published in 2023, confirms these upward trends. Last year, 32% said they suffered higher dollar-value losses and 29% experienced more fraudulent transactions than in the preceding year — much lower rates than reported this time around.

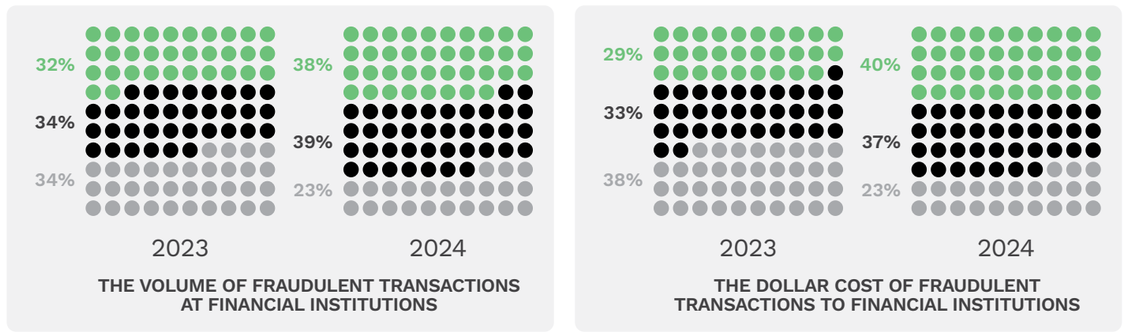
38%

Share of FIs that **reported an increase in the volume of fraudulent transactions** in the last year

FIGURE 3

Increases in fraudulent activity

Share of FIs citing an increase in select metrics in the last 12 months versus the preceding 12 months



- Increased
- Stayed about the same
- Decreased

Source: PYMNTS Intelligence
The State of Fraud and Financial Crime in the U.S. 2024, November 2024
N = 200: Whole sample, fielded Sep. 9, 2024 – Sep. 30, 2024

FIs turn to newer anti-fraud technologies that support them in identifying social engineering strategies.

Of course, FIs are not blind to their financial losses from fraud. A closer look at the fraud prevention technologies FIs currently have in place sheds light on the complex cost-benefit dynamics at work — and why companies that hold back investment for too long will likely regret their decisions. Nearly all FIs already implemented older technologies that excel at blocking simple unauthorized transactions more than one year ago. These include transaction alerts, device fingerprinting and fraud-prevention application programming interfaces (APIs), among others. This helps explain why digital payment fraud is declining, as discussed previously.

Meanwhile, many are now adopting key newer technologies that mirror fraudsters' shift in focus. At the time of the survey, only 45% of FIs had implemented behavioral analytics for more than a year, while 26% rolled this out in the last 12 months. This technology is proven to excel at defeating scams involving the manipulation of human targets — and it is one of the technologies where the largest FIs have an edge. All surveyed FIs with $25 billion in assets or more report using behavioral analytics; 88% of FIs with between $5 billion and $25 billion in assets also use the tool. Among the smallest FIs in our sample, those with between $1 billion and $5 billion in assets, 64% use behavioral analytics, meaning more than one-third of these smaller FIs are missing out.

71%

Share of FIs that

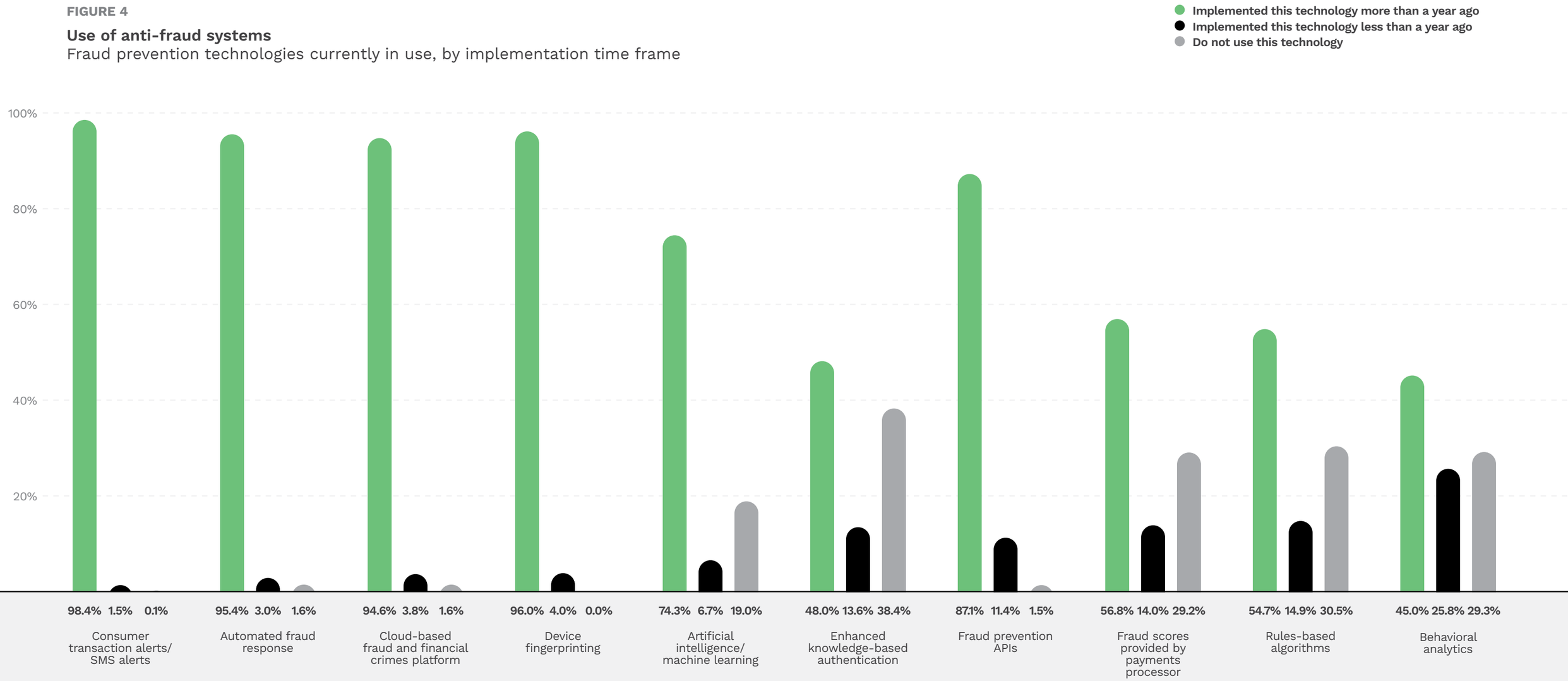
have deployed fraud score solutions

Other key technologies follow these trends. Similarly, only 71% of FIs overall had deployed fraud scores — a powerful new screening tool that leverages the massive transaction datasets available to payment processors — for more than a year; 14% more added this into their anti-fraud arsenal in the last 12 months. Larger FIs again lead their smaller counterparts in implementing this technology; 91% of those with more than $25 billion in assets have implemented it, with 68% of the smallest FIs in our sample following suit. We expect more FIs to roll out these and other new technologies as they respond to recent jumps in fraudulent transaction losses.

FIGURE 4

Use of anti-fraud systems

Fraud prevention technologies currently in use, by implementation time frame



Source: PYMNTS Intelligence

The State of Fraud and Financial Crime in the U.S. 2024, November 2024

N = 200: Whole sample, fielded Sep. 9, 2024 – Sep. 30, 2024

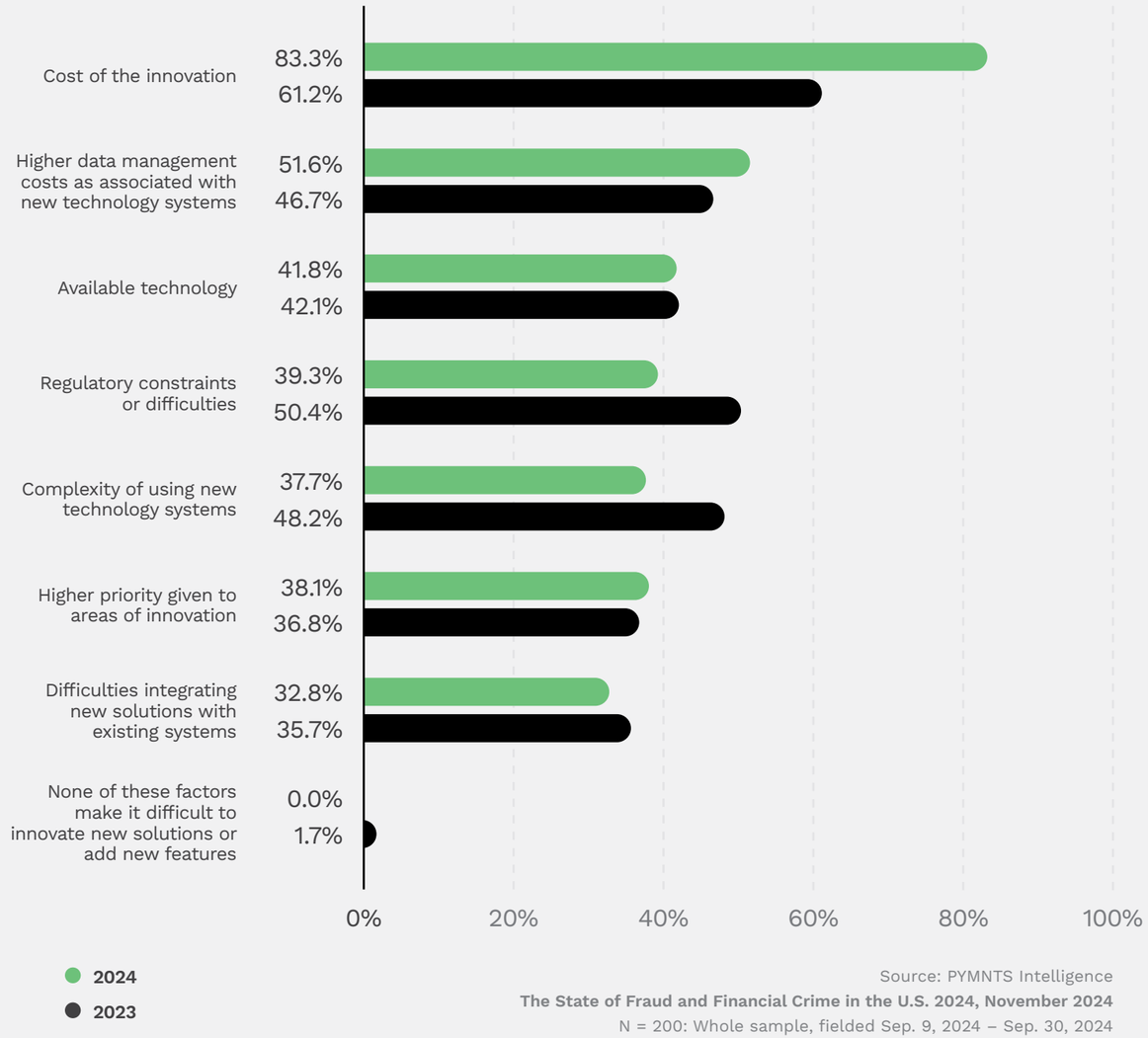
PYMNTS INTELLIGENCE

Although cost is a key barrier to innovating fraud technology, worsening fraud losses highlight the return on investment (ROI) of sophisticated fraud detection tools that can outsmart fraudsters using their own upgraded tools.

Cost plays a central role in whether FIs decide to upgrade their fraud prevention strategies and the extent to which they are willing to innovate. Eighty-three percent of FIs in our latest survey said the cost of innovation makes it difficult to add new features or improve existing solutions, up from 61% in our 2023 study. Higher data management costs also weighed more heavily in this year's survey than in the previous one, with 52% now naming these costs as a difficulty, up from 47%.

FIGURE 5

Roadblocks for innovation
Share of FIs indicating that selected factors make it difficult to add new solutions or features for fraud and financial crimes



Source: PYMNTS Intelligence
The State of Fraud and Financial Crime in the U.S. 2024, November 2024
N = 200: Whole sample, fielded Sep. 9, 2024 – Sep. 30, 2024

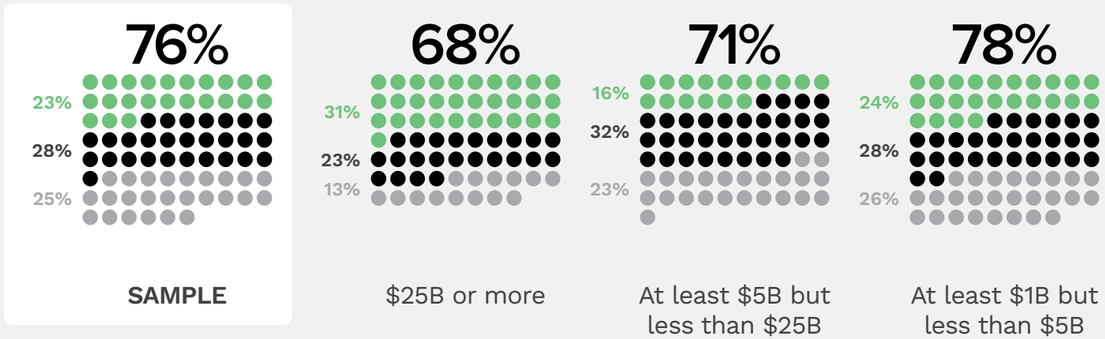
Two other frequently cited obstacles — the complexity of using new technology and the difficulty of integrating new solutions into existing systems — also partly relate to the cost of either management or implementation. For example, new technology can require new staff or training, and integration challenges can be expensive and time-consuming to solve or cause business disruptions.

The share of FIs currently innovating or planning to innovate in the next year shifted from 49% to 76% since 2023, indicating that while cost was a key barrier, the increased loss due to fraud is driving banks to see the ROI of cutting-edge fraud detection tools. Twenty-three percent of FIs surveyed have upgrades to their anti-fraud toolkits underway, compared to just 4% of FIs that said the same in the previous survey. Another 28% of our latest respondents plan to add new technologies in the next six months, and 25% in the next 12 months. In total, this means 76% of FIs are seeking more robust fraud solutions now or plan to do so in the next year.

An analysis of FI size reveals slightly conflicting trends. Overall, the smallest FIs in our sample — those with between $1 billion and $5 billion in assets — are the most likely to either be adding technology systems or planning to do so, at 78%. Although a smaller share of the largest FIs in our sample (those with $25 billion or more in assets) are planning to add or adding these systems, at 68%, they seem to be a step ahead of smaller competitors, with a leading 31% already innovating, rather than planning to innovate. In total, this suggests the grand majority of these FIs, regardless of size, understand these new systems could make a positive impact, but while the largest FIs have the resources to put these plans into immediate action, smaller FIs need more time to prepare.

FIGURE 6

Plans for new anti-fraud technology
Share of FIs that are currently adding or plan to add new technology systems, by asset size



Source: PYMNTS Intelligence
The State of Fraud and Financial Crime in the U.S. 2024, November 2024
N = 200: Whole sample, fielded Sep. 9, 2024 – Sep. 30, 2024

DATA FOCUS

Banks no longer worry that instant payments make it harder to prevent fraud.

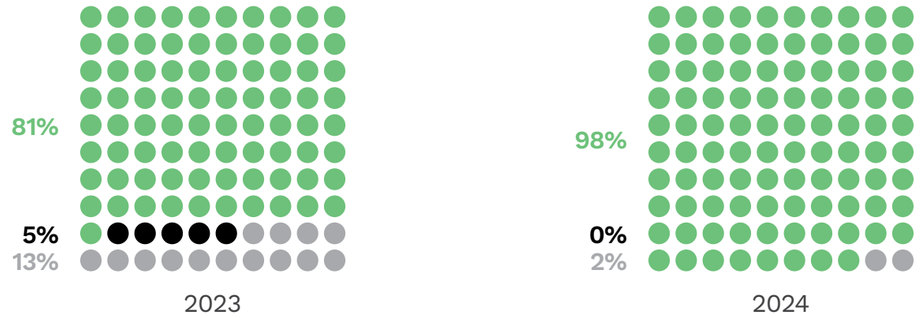
Ninety-eight percent of FIs now believe they can offer faster payments without compromising security.

Instant payments offer a range of advantages, including rapid clearance and secure transactions that cannot be reversed through mechanisms such as chargebacks. In the past, this combination of speed and irreversibility has caused FIs to worry that instant payments carry a higher risk of fraud than traditional payment methods. However, the latest survey finds FIs no longer have this concern: 98% said their organizations can support faster payments, including instant payments, without compromising security. In 2023, 19% of FIs surveyed still felt unable or unsure about their ability to do so.

FIGURE 7

Concerns about security

Share of FIs indicating select responses about their ability to use faster payments without compromising organizational or customer security, by year



- **Able**
- **Not sure**
- **Not able**

Source: PYMNTS Intelligence
The State of Fraud and Financial Crime in the U.S. 2024, November 2024
N = 200: Whole sample, fielded Sep. 9, 2024 – Sep. 30, 2024

2%

Share of FIs that **still have concerns about maintaining security** with faster transactions such as instant payments

ACTIONABLE INSIGHTS

01

Compared to the previous year, more FIs reported growing volumes of fraudulent transactions and greater resulting dollar losses. Innovators by nature, bad actors constantly seek new fraudulent exploits. FIs should regularly reevaluate their overall fraud management strategies to ensure they are innovating enough to stay ahead of fraudsters.

02

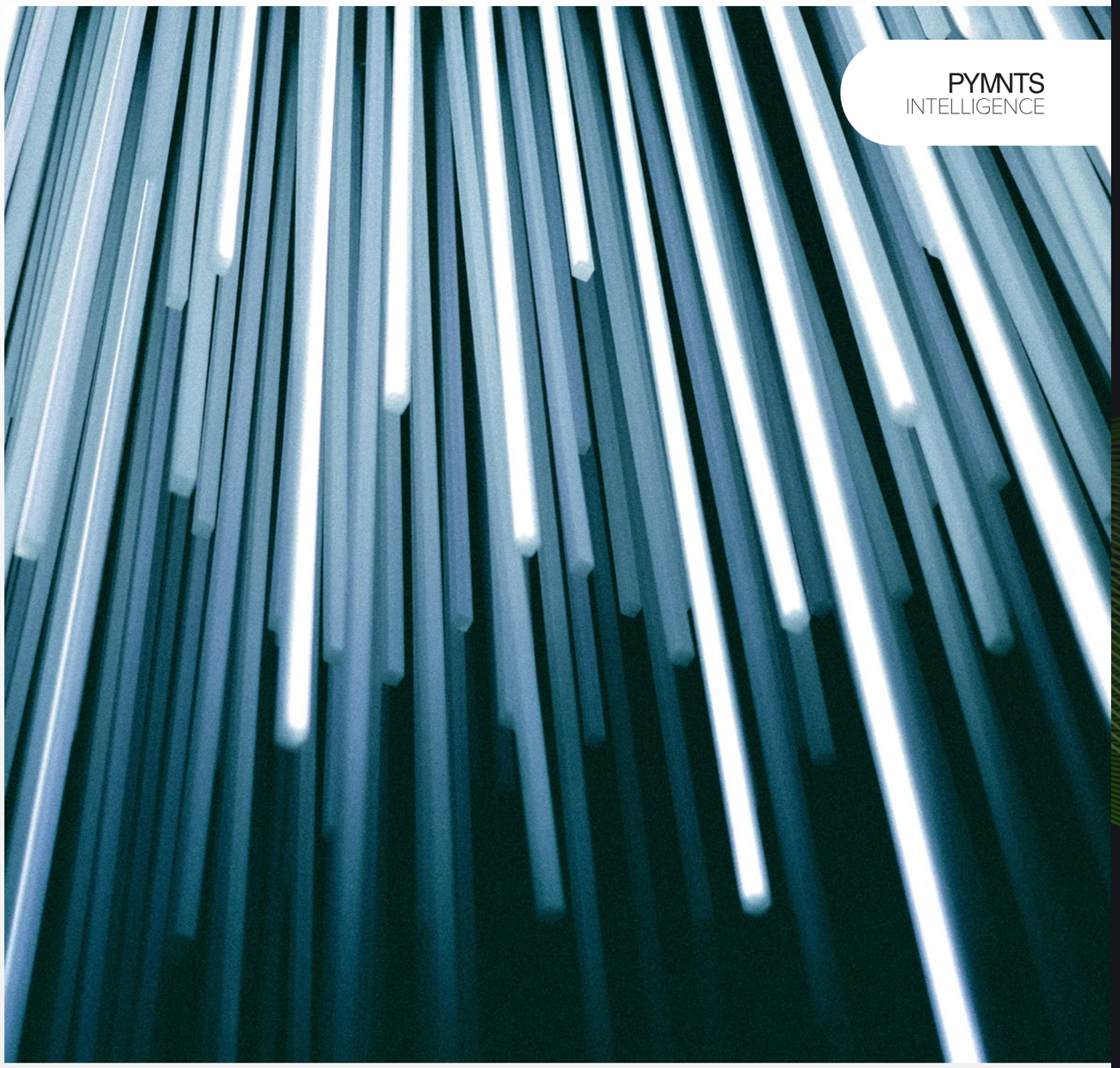
Fraudsters have centered a new target in their sights: FIs' customers. Becoming a victim of these scams can harm these consumers both financially and emotionally. With only 44% of FIs willing to reimburse these scam victims, such attacks can jeopardize victims' relationships with their FIs. To preserve customer loyalty, FIs should prioritize shoring up social engineering protections.

03

The complex cost-benefit dynamics of fraud prevention are difficult for FIs to navigate. FIs have almost universally implemented some older technologies, including consumer alert messages and device fingerprinting, that have effectively mitigated some types of fraud. However, FIs need to add newer technologies that are more effective at thwarting fraudsters as they focus more on manipulationg customers. Behavior analytics is one such area FIs should prioritize.

04

The theme of FIs needing to adapt as quickly as fraudsters extends to FIs' ongoing and planned near-term upgrades. Most FIs are investing in new fraud prevention technologies, with larger FIs already enacting their plans and smaller FIs more likely to be in the planning stages. Despite this upswing in demand, FIs remain highly sensitive to costs, not only for implementation but also ongoing management. Anti-fraud solutions providers should consider adjusting their service and pricing models to better fit their FI customers' needs and constraints.



PYMNTS INTELLIGENCE

THE STATE OF **FRAUD AND FINANCIAL CRIME IN THE U.S. 2024:** WHAT FIs NEED TO KNOW

November 2024 Report

METHODOLOGY

The State of Fraud and Financial Crime in the U.S. 2024 draws on insights from a survey of 200 executives working at 200 separate FIs in the United States with at least $1 billion in assets conducted from Sept. 9 to Sept. 30. The respondents were required to have deep knowledge and leadership responsibilities in fraud and risk operations, fraud strategy or fraud analysis.

THE PYMNTS INTELLIGENCE TEAM THAT PRODUCED THIS REPORT:

Karen Webster
CEO

Daniel Gallucci
Senior Writer

Story Edison, PhD
Senior Analyst

Matt Vuchichevich
Senior Content Editor,
Head of Reports

ABOUT

PYMNTS INTELLIGENCE

PYMNTS Intelligence is a leading global data and analytics platform that uses proprietary data and methods to provide actionable insights on what's now and what's next in payments, commerce and the digital economy. Its team of data scientists include leading economists, econometricians, survey experts, financial analysts and marketing scientists with deep experience in the application of data to the issues that define the future of the digital transformation of the global economy. This multi-lingual team has conducted original data collection and analysis in more than three dozen global markets for some of the world's leading publicly traded and privately held firms.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe, please email us at feedback@pymnts.com.