



THE STATE OF  
**FRAUD AND  
FINANCIAL CRIME**  
IN THE U.S. 2023

---

September 2023 Report

---

PYMNTS  
INTELLIGENCE



# THE STATE OF FRAUD AND FINANCIAL CRIME IN THE U.S. 2023

## TABLE OF CONTENTS

---

- What’s at Stake ..... 04
- Key Findings ..... 08
- PYMNTS in Depth ..... 12
- Data Focus ..... 34
- Actionable Insights ..... 38
- Methodology..... 41



The State of Fraud and Financial Crime in the U.S. 2023 was produced in collaboration with Hawk AI, and PYMNTS Intelligence is grateful for the company’s support and insight. [PYMNTS Intelligence](#) retains full editorial control over the following findings, methodology and data analysis.

# WHAT'S AT STAKE

---

**F**inancial institutions (FIs) continue to experience increasingly sophisticated fraud and financial crime. The rise of digital banking and ever-faster digital payment methods have accelerated this phenomenon. As a result, banks have had to elevate their systems and processes to find ways to stem the growth in fraudulent transactions — and the resulting uptick in financial losses. PYMNTS Intelligence finds that compared to 2022, 43% of FIs have experienced increased fraud. The average cost of fraud for FIs with assets of \$5 billion or more also increased by 65%, from \$2.3 million in 2022 to \$3.8 million in 2023.

To better identify and assess the types of fraud banks most commonly experience, we used the Federal Reserve's Fraud Classifier Model, which provides a standardized and holistic picture of fraud for all FIs. Misuse of account information is still



# 43%

of U.S. financial institutions reported increases in fraudulent transactions this year.

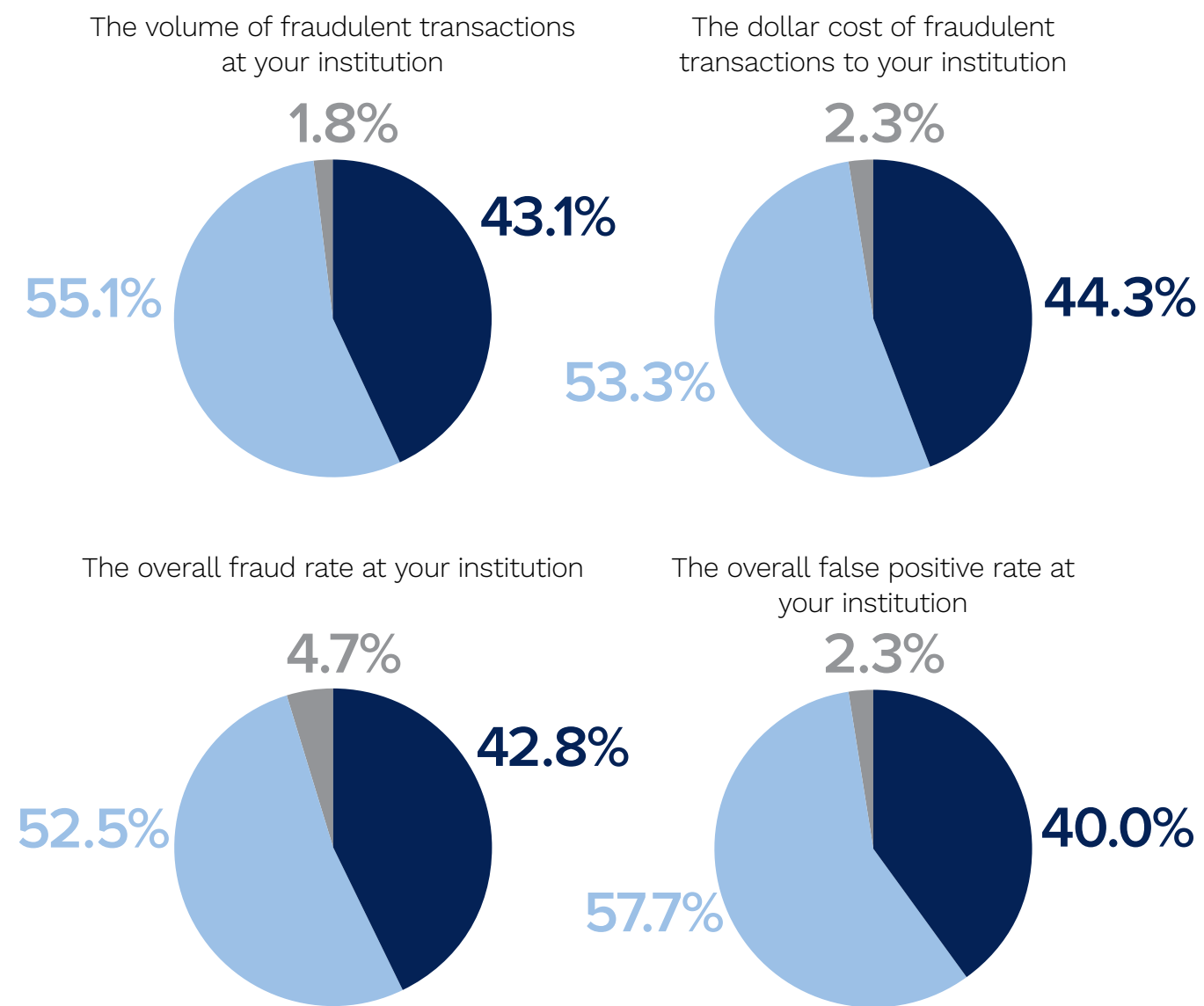
---

the leading source of fraud, accounting for 38% of fraudulent transactions. Digital wallets, such as Samsung Pay, Google Pay and Apple Pay, exhibited the most significant increases in fraud rates since 2022, as do same-day automated clearing house (ACH) and regular ACH payments. To combat growing fraud, FIs are increasing investments and deployments of machine learning (ML) and artificial intelligence (AI), which FIs already recognize as powerful tools in stemming fraudulent transactions.

**FIGURE 1:**  
**Changes in fraud**

Share of FIs with assets totaling more than \$5 billion that cite experiencing select changes in fraud and financial crime in 2023 versus 2022

- Increased
- About the same
- Decreased



Source: PYMNTS Intelligence

The State of Fraud and Financial Crime in the U.S. 2023, September 2023  
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

The State of Fraud and Financial Crime in the U.S. 2023, a PYMNTS Intelligence and Hawk AI collaboration, examines the state of fraud and financial crime FIs experienced in 2023 compared to 2022, including the rising costs of fraud and what actions they have taken to mitigate fraud. We collected 200 responses from executives working at FIs with assets of at least \$1 billion between March 29 and June 16. Respondents were also part of our 2022 survey on fraud FIs experienced. In 2022, all sampled FIs had assets totaling more than \$5 billion. In 2023, sampled FIs included 108 FIs with assets totaling more than \$5 billion and 92 FIs with assets between \$1 billion and \$5 billion. Respondents were executives with deep knowledge and leadership responsibilities in the following areas: fraud and risk operations, fraud strategy or fraud analysis.

**This is what we learned.**



# KEY FINDINGS

# 01

## MORE FRAUD

More than 40% of banks in the U.S. experienced an increase in fraud relative to 2022, resulting in more fraudulent transactions and fraud losses increasing by about 65%. Last year, 70% of FIs reported an increase in fraud relative to 2021.



# 55%

Share of FIs with assets of more than \$5 billion that saw no change in the volume of fraudulent transactions in 2023

# 02

## SCAM LOSSES

While account information misuse is still the leading type of fraud, each FI lost, on average, nearly half a million dollars related to scams in 2023.



# 12%

Share of fraudulent transactions from scams, with bank tech support impersonation and IRS scams most common

## 03

## ADVANCED TECH

FIs have invested in technologies such as ML and AI to address the increase in fraud, yet smaller FIs still lag in adoption.



# 66%

Share of FIs that currently use ML and AI technologies to combat fraud, up from 34% in 2022

## 04

## STEPPING UP

Most FIs are already adding or will add ML and AI technologies to combat fraud in the next year and are shifting from outsourcing to in-house solution development.



# 48%

Share of FIs that either are in the process of adding or will add new tech systems to combat fraud in the next year

# PYMNTS IN DEPTH

---

**Fraud and financial crimes are still rising, and FIs are increasing investments in advanced ML and AI technologies in response.**

**More than 40% of banks in the U.S. experienced an increase in fraud relative to 2022 figures — the uptick resulted in a higher number of fraudulent transactions and fraud losses increasing by about 65%.<sup>1</sup> Last year, 70% of FIs reported an increase in fraud relative to 2021.**

---

Fraud remains a top challenge, even as fraud rates have remained stable for many FIs in 2023 relative to 2022 figures — a year in which nearly three-quarters of FIs experienced increased fraud. Approximately 55% of sampled institutions report that all fraud measurements remained constant in 2023 versus 2022, while roughly 44% of FIs report that all fraud measurements increased in 2023. For example, 43% of FIs report experiencing an increase

<sup>1</sup> Our sample covers FIs in the United States with assets of at least \$1 billion, representing 15% of all FIs in the U.S. but covering 93% of banks' assets.

in fraudulent transactions in 2023 — and larger FIs are more likely to have experienced increases in the volume of fraudulent transactions. While 63% of FIs with assets of more than \$100 billion saw an increased volume of fraudulent transactions, just 30% of FIs with assets between \$1 billion and \$5 billion experienced this.

An increase in the volume of fraudulent transactions can correspond to a rise in the cost of these transactions, and our data finds that among FIs with assets of more than \$5 billion, the share of transactions resulting in fraud losses increased from 1.6 basis points in 2022 to 1.9 in 2023. Larger FIs experienced the highest increases.<sup>2</sup> The total losses for all FIs in our sample was \$3 billion, yet FIs with assets of at least \$5 billion each spend, on average, \$11 million combating fraud. Of this, \$3.8 million covers losses due to fraudulent transactions, up from \$2.3 million in 2022 — a 65% increase. FIs spent the rest of this total on investing in staffing and technological resources and outsourcing services to combat fraud.

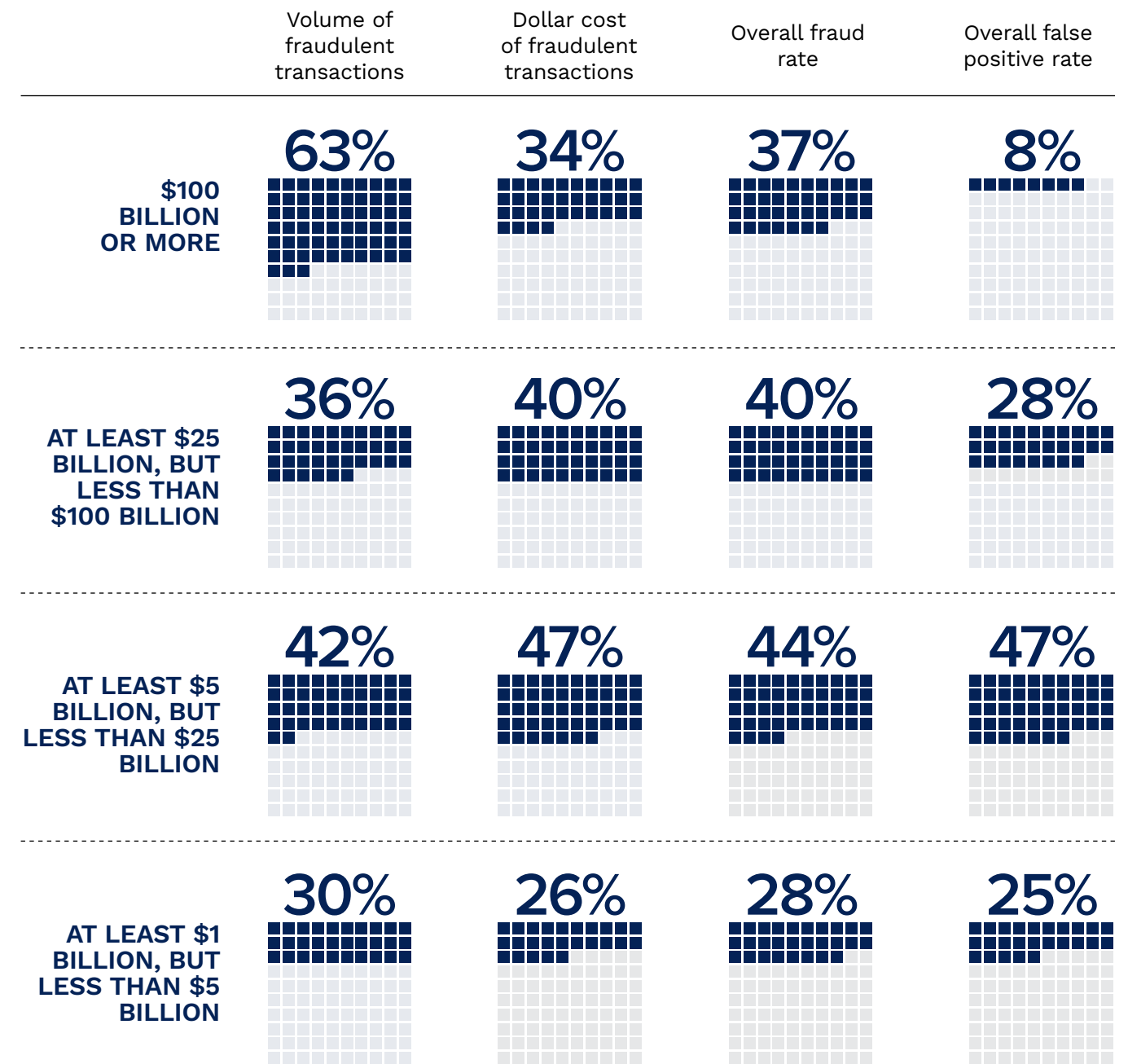
As there are 333 FIs in the U.S. with assets of at least \$5 billion, the total losses due to fraudulent transactions for these FIs added up to more than \$1.3 billion in 2023, nearly doubling the \$767 million lost in 2022. For the 1,053 FIs in the U.S. with assets between \$1 billion and \$5 billion, each lost \$1.4 million on average — a collective total of \$1.4 billion.

<sup>2</sup> Note: Data for FIs with assets between \$1 billion and \$5 billion is not included in time comparison charts.

**FIGURE 2:**

**Firms experiencing increasing fraud**

Share of firms that experienced an increase in select fraud metrics in 2023, by asset size



Source: PYMNTS Intelligence

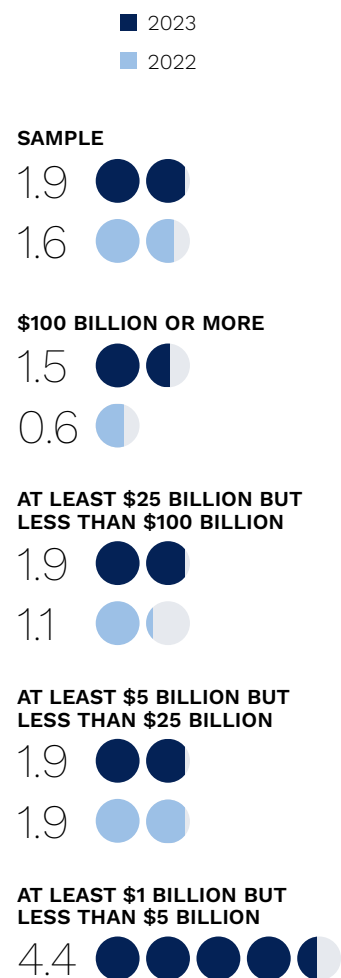
The State of Fraud and Financial Crime in the U.S. 2023, September 2023  
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023



**FIGURE 3A:<sup>3</sup>**

**Fraud losses**

Share of transactions (in basis points) resulting in fraud losses in the last 12 months among firms with assets totaling more than \$5 billion, by year

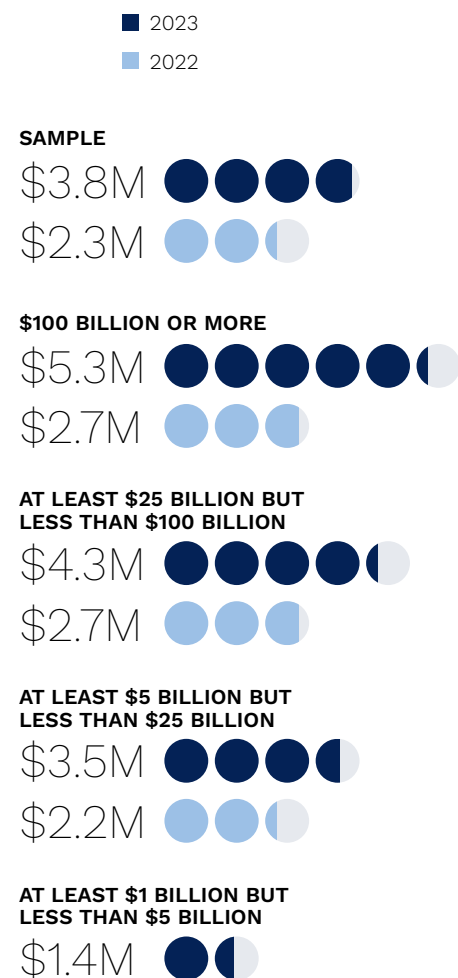


Source: PYMNTS Intelligence  
 The State of Fraud and Financial Crime in the U.S. 2023, September 2023  
 N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

**FIGURE 3B:**

**Fraud losses**

Average cost of fraud related to fraudulent transactions experienced among firms with assets totaling more than \$5 billion, by year

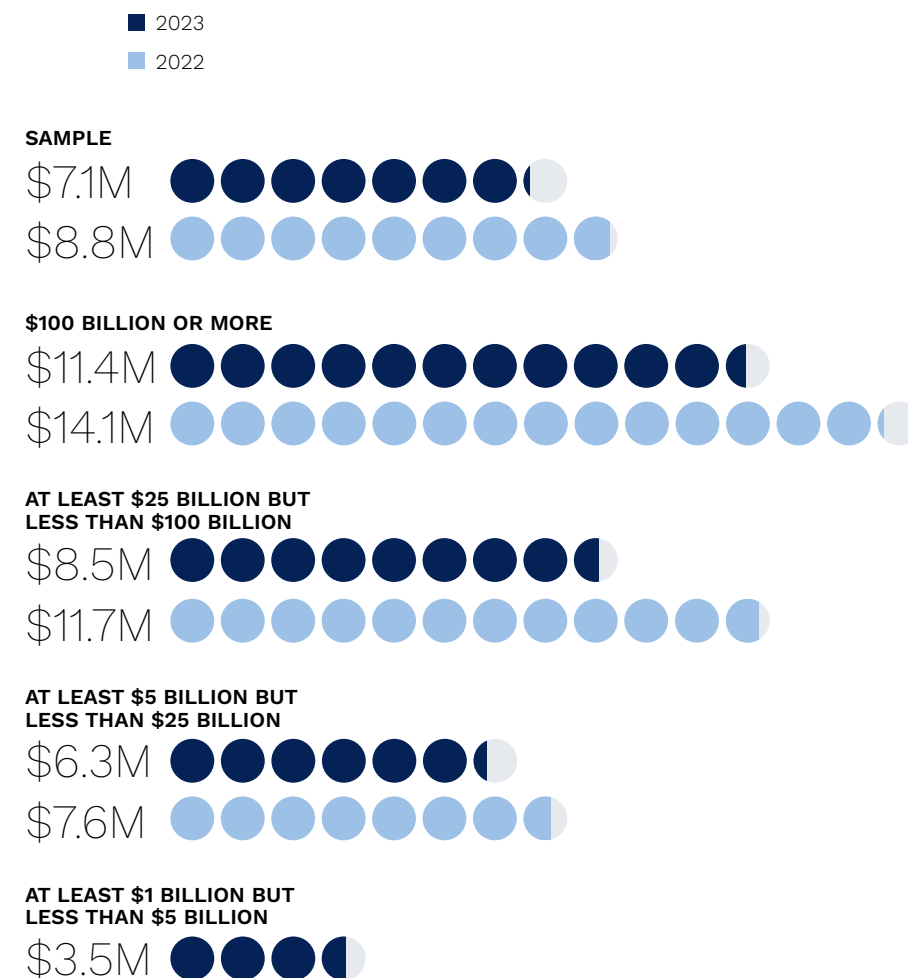


Source: PYMNTS Intelligence  
 The State of Fraud and Financial Crime in the U.S. 2023, September 2023  
 N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

**FIGURE 3C:**

**Fraud losses**

Average total cost of fraud not related to fraudulent transactions in the last 12 months experienced among firms with assets totaling more than \$5 billion, by year



Source: PYMNTS Intelligence  
 The State of Fraud and Financial Crime in the U.S. 2023, September 2023  
 N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

<sup>3</sup> When referring to time comparison data, we use data for FIs with assets of at least \$5 billion, representing 4% of all FIs in the U.S. but covering 85% of banks' assets.

## While misuse of account information is still the leading type of fraud, each FI lost nearly half a million dollars, on average, related to scams alone in 2023.

---

Using the Federal Reserve's Fraud Classifier Model, PYMNTS Intelligence finds that rates of unauthorized fraud surpass authorized fraud for all FIs, with 63% of fraudulent transactions coming from unauthorized party fraud — the type of fraud that occurs when external actors take over or compromise credentials to commit fraud. The misuse of account information — consisting of digital payment fraud and physical forgery — remains the leading source of fraud, with each FI losing an average of \$1.4 million to this scheme in the last year. Authorized fraud, in which bad actors manipulate internal individuals to commit fraud in the form of scams, including relationship, trust fraud and product or services fraud, represents just 12% of fraudulent transactions, yet each FI lost an average of nearly half a million dollars due to scams this year.

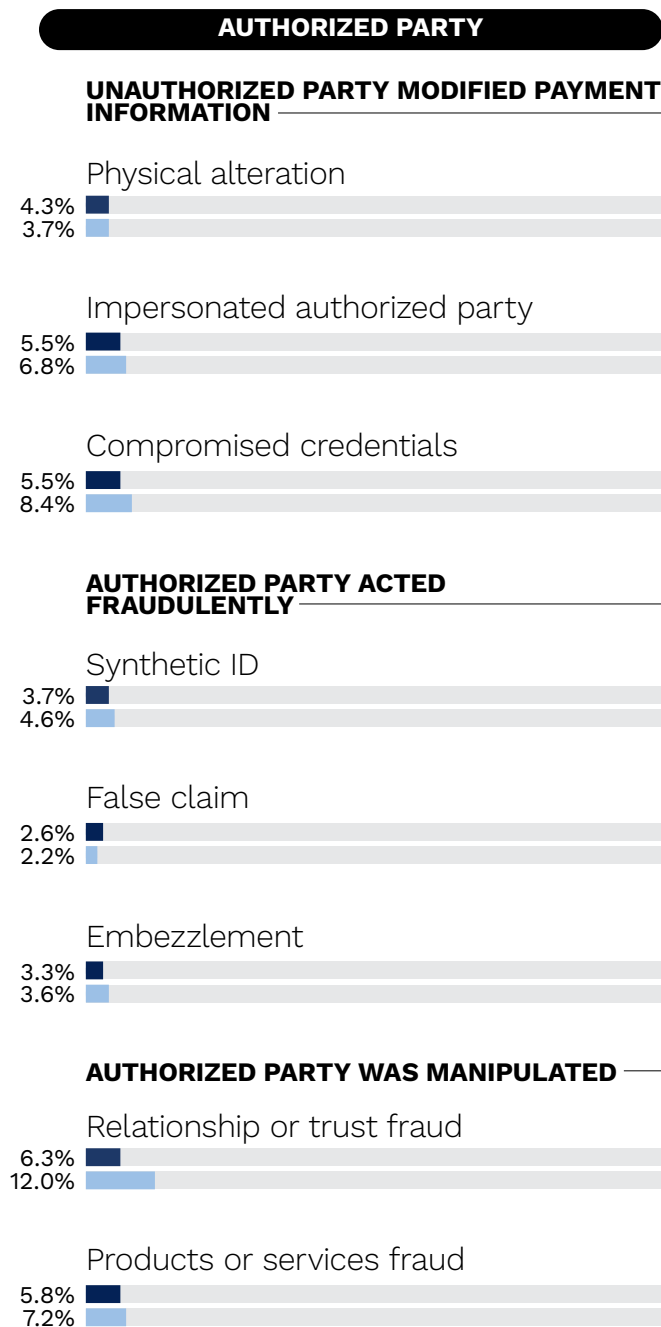
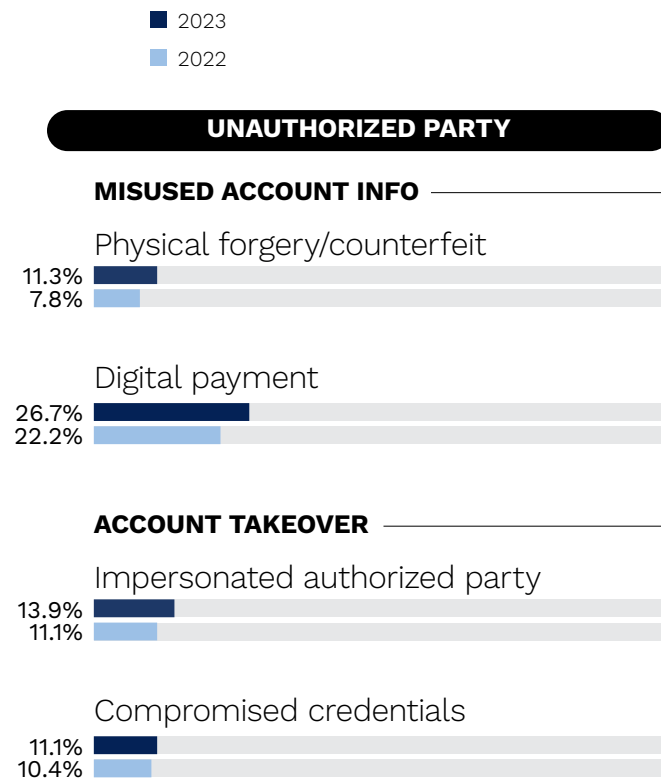
The most common scams of late have been IRS imposter scams, a form of relationship or trust fraud 22% of FIs experienced, and bank tech support impersonation, a form of product or services fraud 20% of FIs experienced in the past year. Relationship and trust fraud scams decreased to 6% in 2023 from 12% in 2022, suggesting that banks have found ways to mitigate this kind of scam.

Digital payment fraud rates rose with most payment methods accepted by FIs, and digital wallets such as Samsung Pay, Google Pay and Apple Pay exhibited the highest increases. For instance, 65% of FIs that accept Samsung Pay experienced increased fraud rates in 2023, up from 27% in 2022. Same-day ACH and regular ACH payments also experienced notable increases in fraud. From 2022 to 2023, the share of firms that experienced an increase in payments made via same-day ACH increased by 35 percentage points. The increased speed of payment transactions contributed to these dramatic increases in digital payment fraud.

FIGURE 4A:<sup>4</sup>

**Leading sources of fraud**

Fraud classifier model: Share of fraudulent transactions (based on total dollar value) among FIs with assets totaling more than \$5 billion, by year<sup>5</sup>

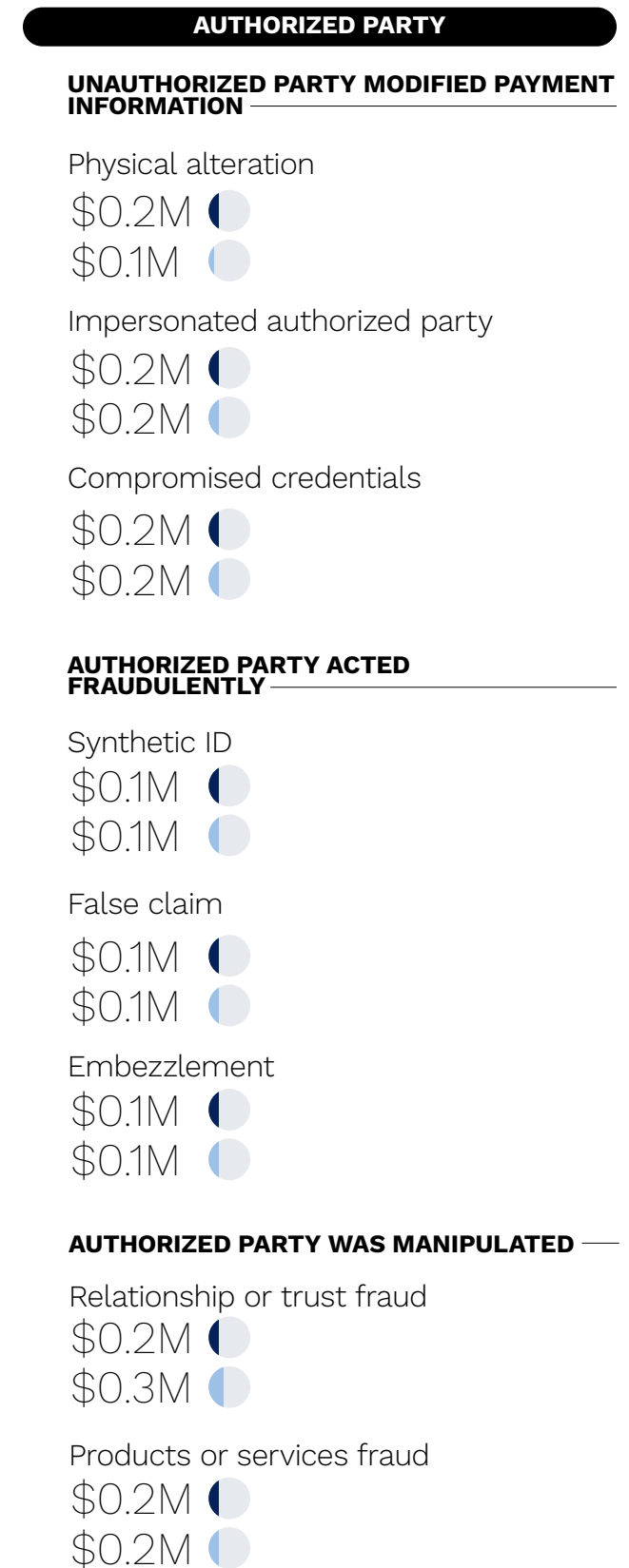
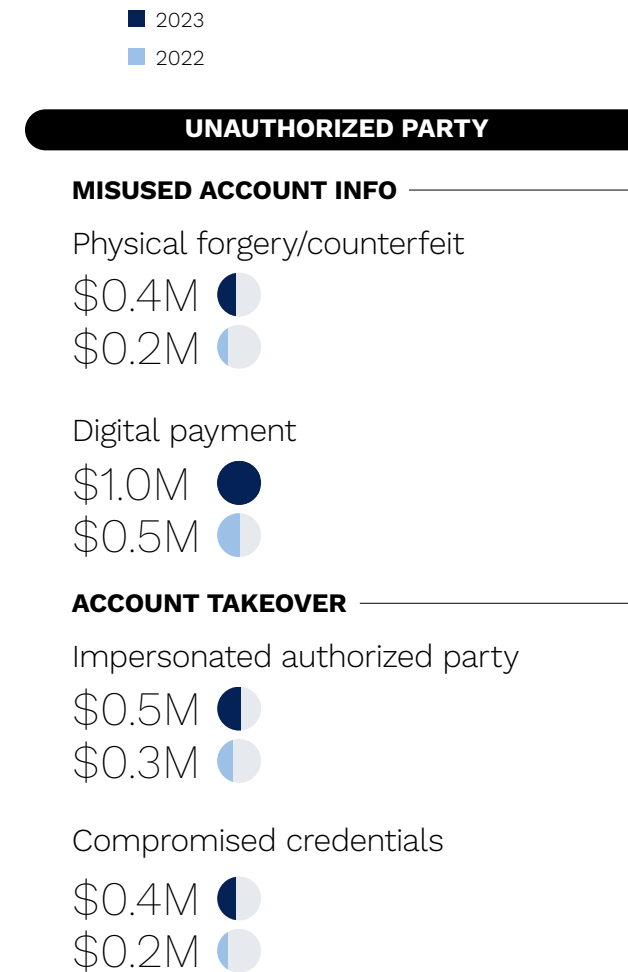


Source: PYMNTS Intelligence  
 The State of Fraud and Financial Crime in the U.S. 2023, September 2023  
 N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

FIGURE 4B:

**Leading sources of fraud**

Fraud classifier model: Average total losses (in millions) related to fraudulent transactions, based on total dollar value among firms with assets totaling more than \$5 billion, by year



Source: PYMNTS Intelligence  
 The State of Fraud and Financial Crime in the U.S. 2023, September 2023  
 N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

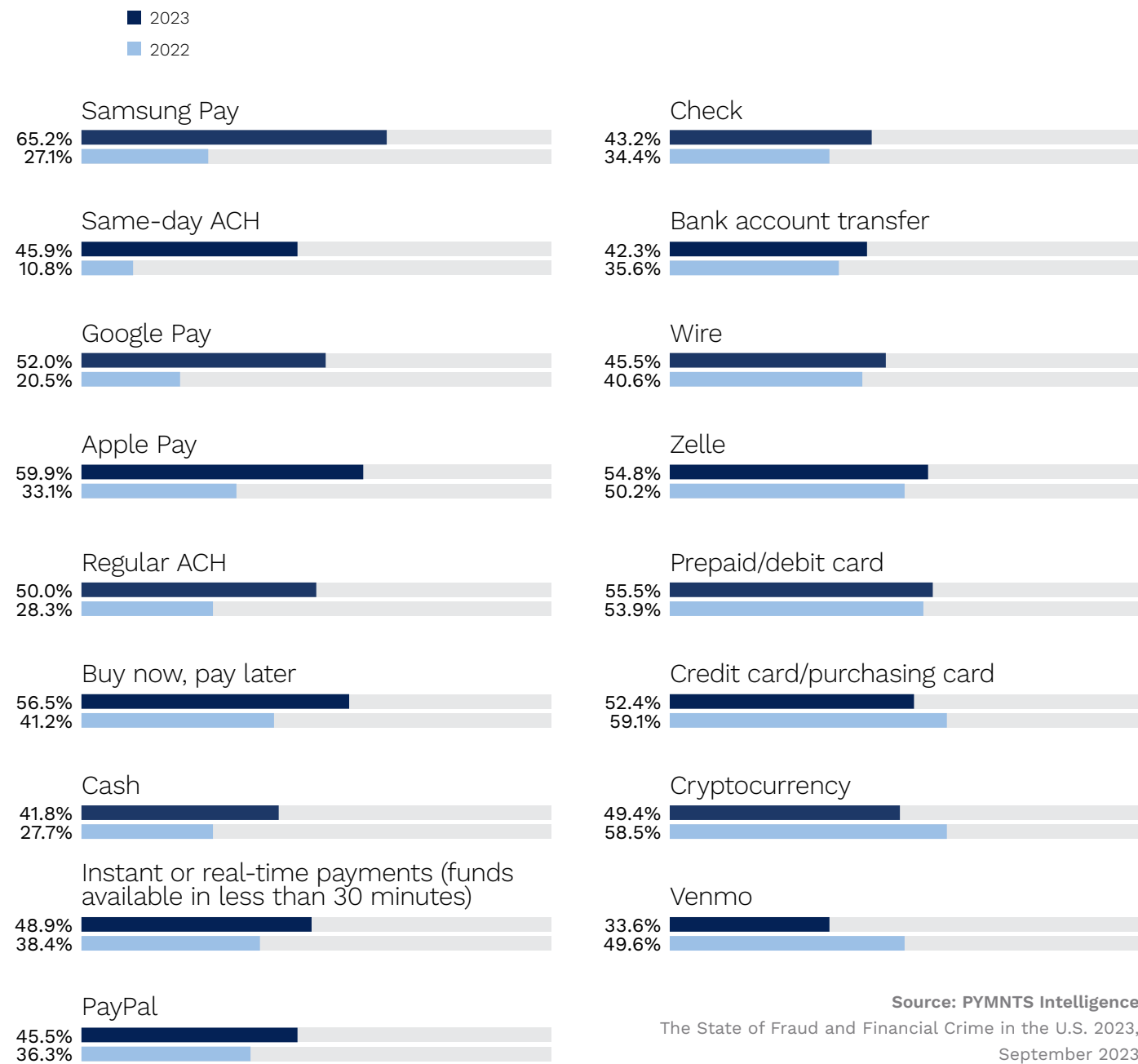
<sup>4</sup> Note: Data for FIs with assets between \$1 billion and \$5 billion is not included in time comparison charts.

<sup>5</sup> The Federal Reserve developed the Fraud Classifier Model to help address the industry-wide challenge of inconsistent classifications for fraud. The advantage of this model is the ability to classify fraud independently of payment type, channel or any other characteristics. This model starts with who initiated the payment, how they acted and the final type of fraud.

**FIGURE 5A:**

**Fraud and payment methods <sup>6</sup>**

Share of FIs with assets totaling more than \$5 billion experiencing increased fraud across payment methods, by year

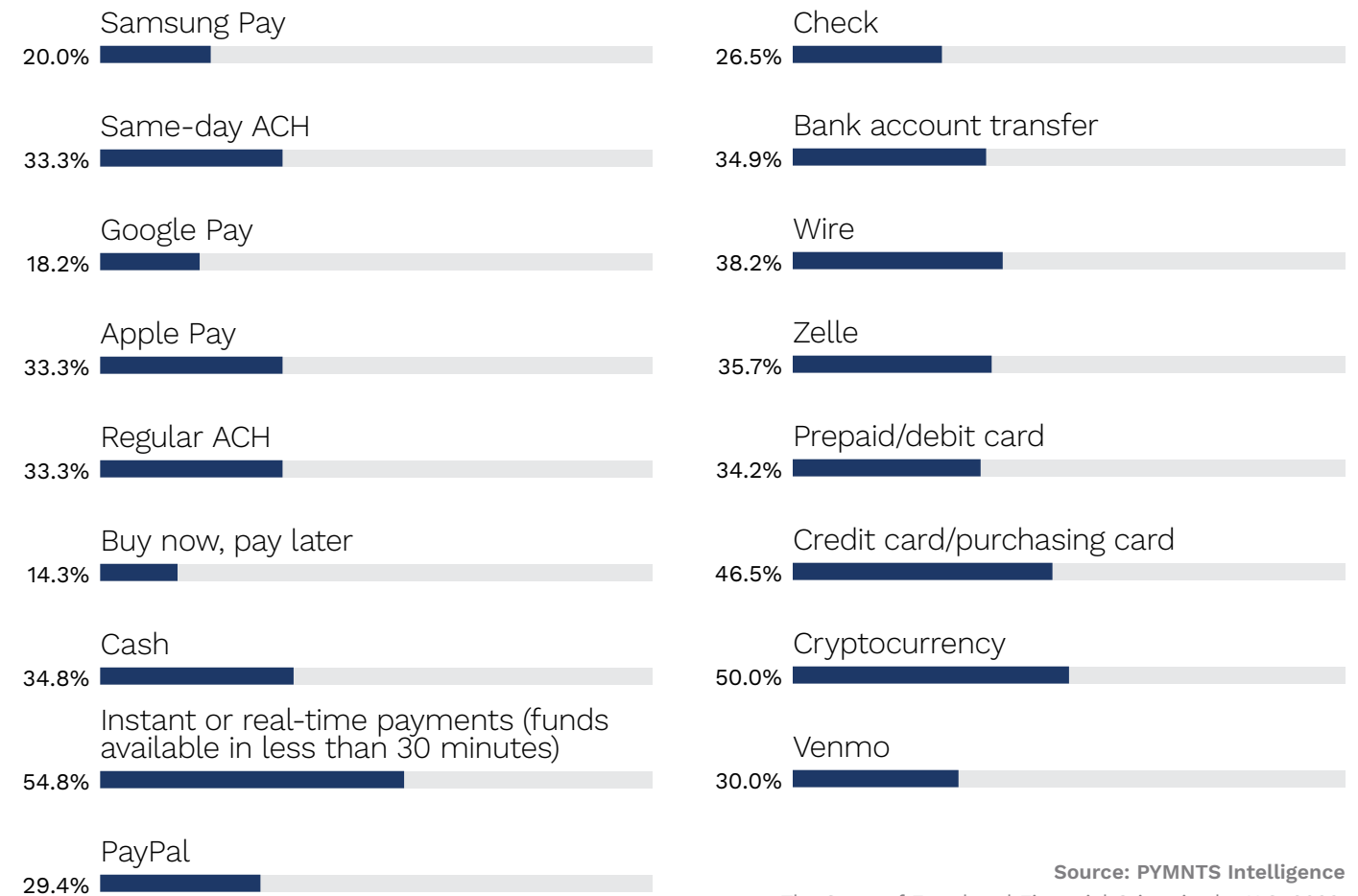


Source: PYMNTS Intelligence  
 The State of Fraud and Financial Crime in the U.S. 2023,  
 September 2023  
 N = 200: Complete responses,  
 fielded March 20, 2023 – June 16, 2023

**FIGURE 5B:**

**Fraud and payment methods**

Share of FIs with assets of up to \$5 billion experiencing increased fraud across payment methods, by year



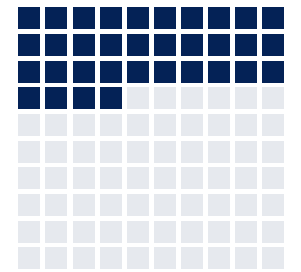
Source: PYMNTS Intelligence  
 The State of Fraud and Financial Crime in the U.S. 2023,  
 September 2023  
 N = 200: Complete responses,  
 fielded March 20, 2023 – June 16, 2023

<sup>6</sup> Note: Data for FIs with assets between \$1 billion and \$5 billion is not included in time comparison charts.

## FIs have invested in ML and AI to address the increase in fraud, yet smaller FIs lag in adopting these modern technologies.

Rules-based algorithms, ML and AI are the technologies most used to combat fraud, especially among larger banks. In 2023, 60% of FIs report using rules-based algorithms to combat fraud, up from 50% in 2022. At least 66% of FIs with more than \$5 billion in assets use ML and AI, exceeding the 44% of smaller FIs that do the same. Meanwhile, fraud scores and fraud prevention application programming interfaces (APIs) are falling out of favor, as fewer FIs now report using these technologies, at 50% compared to 65% in 2022. Approximately 4 in 10 banks with assets of more than \$25 billion currently use these APIs. Smaller FIs are hanging on, with 55% of FIs with less than \$5 billion in assets still utilizing these technologies.

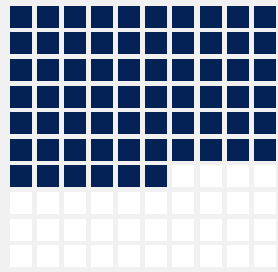
# 34%



Share of FIs not using ML/AI technologies that **faced increased fraud**

FIs using ML or AI also report lower rates of the two most common scams: 22% of FIs not using these technologies experienced bank tech-support impersonation scams, but just 18% of those using these ML or AI faced the same scams. Likewise, 24% of FIs not using the technology experienced IRS imposter scams, compared to 20% of FIs using them.

FIs that leverage ML/AI to combat fraud are significantly less likely to report that their overall fraud rate increased in 2023 than those not using these technologies. While 26% of FIs using these technologies faced increased fraud, 34% of FIs not using ML/AI reported the same.



66%

Share of FIs with assets over \$5 billion that are **using ML/AI technologies** in 2023

Advanced ML and AI technologies identify anomalies in authorized user profiles and block bad actors before they reach their targets, resulting in fewer fraud incidents. One drawback is that the expense of deploying these systems, even with fewer incidents, can increase the cost of fraud — at least in the short term.

FIGURE 6A

**Fraud-fighting technologies**

Share of FIs citing select technologies currently used to combat fraud and financial crimes, by size

	Sample	\$100 billion or more	\$100 billion or more	At least \$5 billion but less than \$25 billion	At least \$1 billion but less than \$5 billion
• Rules-based algorithm	59.9%	31.6%	81.8%	60.0%	59.8%
• ML/AI	48.8%	97.3%	45.5%	65.5%	43.5%
• Fraud prevention APIs	54.1%	40.7%	42.4%	52.7%	55.4%
• Cloud-based fraud and financial crimes platform	47.7%	52.7%	39.4%	34.5%	51.1%
• Fraud scores provided by payments processor	42.0%	23.7%	24.2%	14.5%	50.0%
• Rely entirely on manual processes	2.5%	0.0%	0.0%	0.0%	3.3%

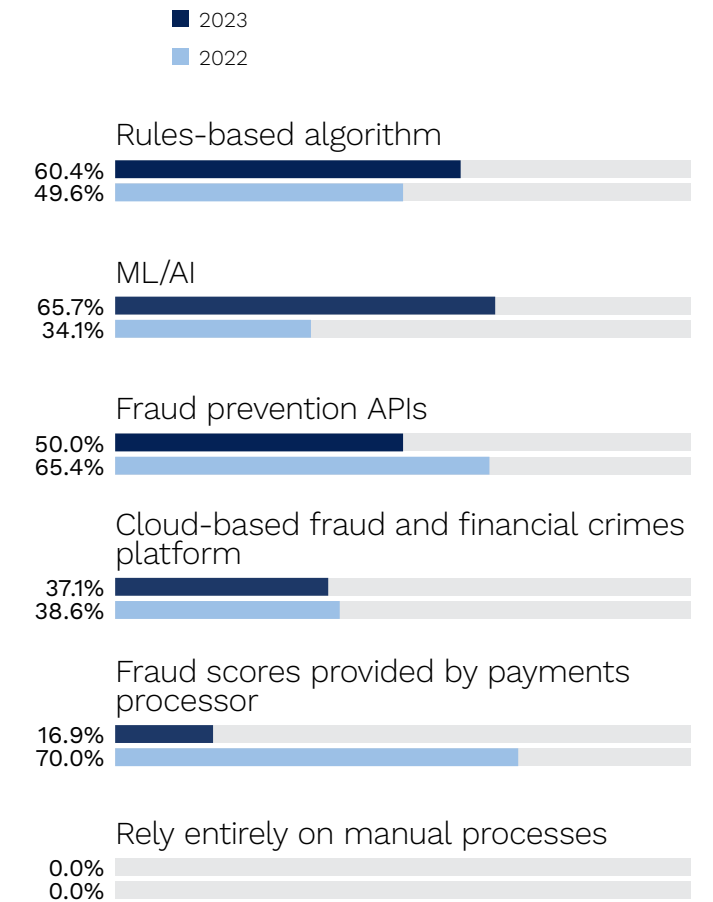
Source: PYMNTS Intelligence

The State of Fraud and Financial Crime in the U.S. 2023, September 2023  
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

FIGURE 6B:

**Fraud-fighting technologies<sup>7</sup>**

Share of FIs with assets of up to \$5 billion citing select technologies currently used to combat fraud and financial crimes, by year



Source: PYMNTS Intelligence

The State of Fraud and Financial Crime in the U.S. 2023, September 2023

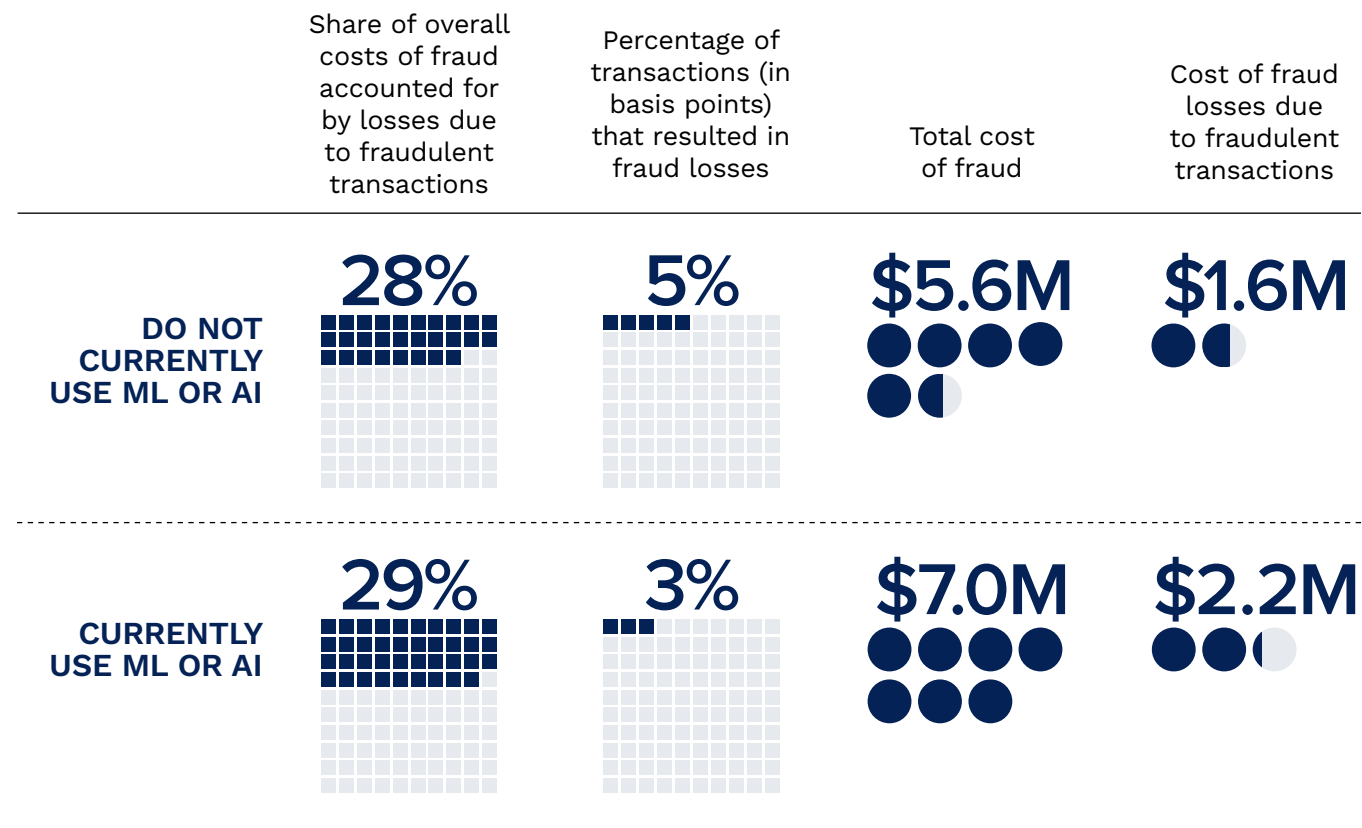
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

<sup>7</sup>Note: Data for FIs with assets between \$1 billion and \$5 billion is not included in time comparison charts.

**FIGURE 7A:**

**ML and AI technologies' fraud impact**

Average share of select fraud measures and costs, by use of ML and AI



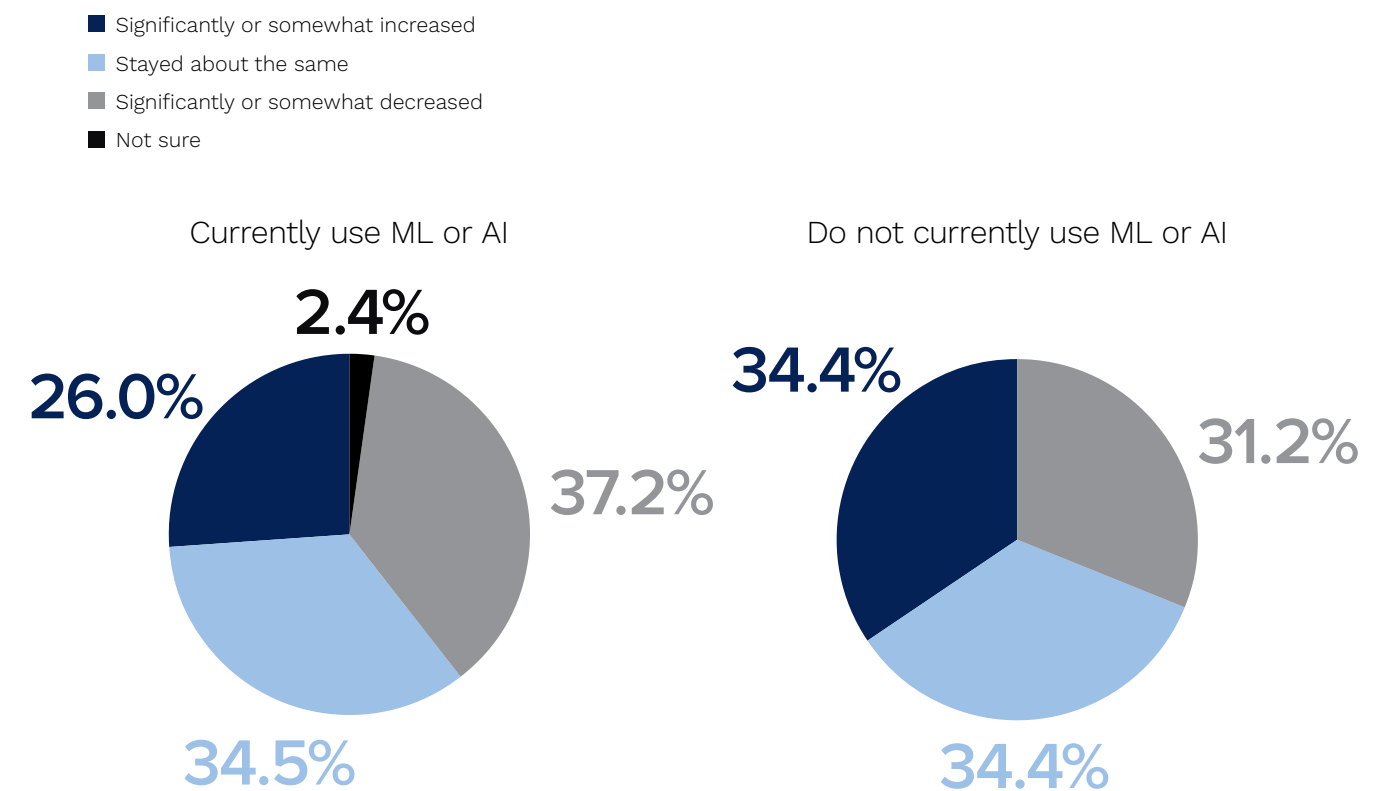
Source: PYMNTS Intelligence

The State of Fraud and Financial Crime in the U.S. 2023, September 2023  
 N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

**FIGURE 7B:**

**ML and AI technologies' fraud impact**

Share of FIs citing changes in overall fraud rate experienced in 2023 versus 2022, by use of ML and AI



Source: PYMNTS Intelligence

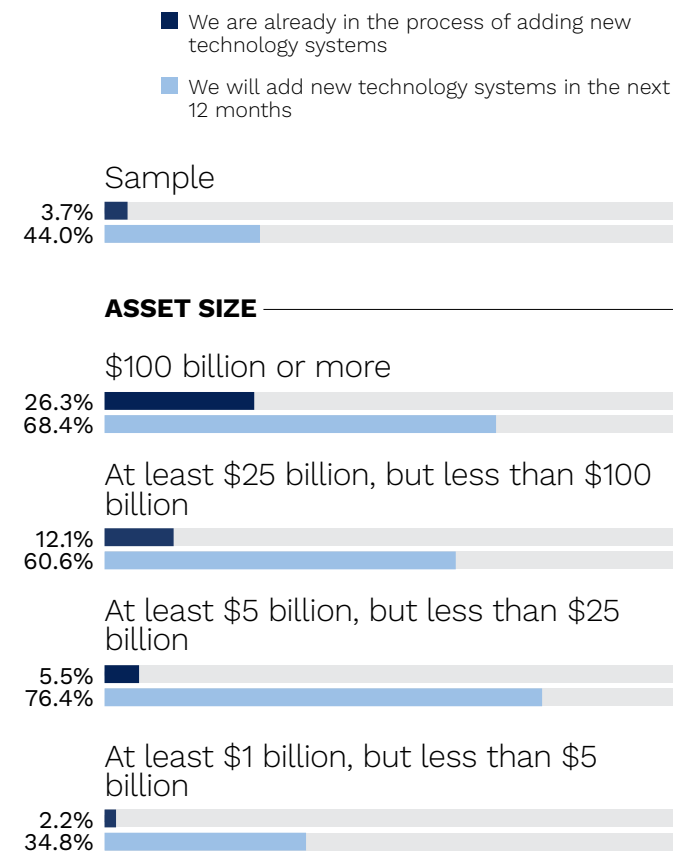
The State of Fraud and Financial Crime in the U.S. 2023, September 2023  
 N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

# Most FIs are adding or will add ML and AI technologies to combat fraud in the next year — and rather than outsourcing fraud detection and protection, they are moving to develop solutions in-house

The battle against rising fraud never ends, and banks of all sizes need more sophisticated tools to win the fight. Our study finds that 48% of FIs are either in the process of adding or will add new technology systems in the next year — especially the largest banks. Among FIs with assets of \$100 billion or more, 26% have begun adding new technologies, and 68% will do so in the next 12 months. In contrast, just 2.2% of FIs with assets of less than \$5 billion are adding new technologies, and 35% will do so in the next 12 months.

**FIGURE 8:**

**Improving existing technology solutions**  
Share of FIs planning to add new technologies, by asset size



**Source: PYMNTS Intelligence**  
The State of Fraud and Financial Crime in the U.S. 2023, September 2023  
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

Still, more FIs recognize ML and AI as the most effective technologies to combat fraud and mitigate fraud losses. This year, 56% of FIs with more than \$5 million in assets reported plans to initiate or increase their use of ML and AI to improve existing fraud solutions, whereas 36% had these plans in 2022.

Traditionally, FIs have outsourced their efforts to improve fraud detection and protection solutions. Our study finds that outsourcing is now the least popular option, with just small FIs interested in pursuing this path to improve existing solutions. While 42% of FIs with assets of less than \$5 billion plan to outsource to a third party, just 5.3% of FIs with assets of \$100 billion or more plan to do so. FIs are instead more apt to develop new in-house systems to combat fraud, with this share increasing significantly in the past year. In 2023,



**FIGURE 9A:**  
**How FIs plan to improve anti-fraud efforts**

Share of FIs planning select actions to improve existing fraud solutions, by size

	\$100 billion or more	At least \$25 billion, but less than \$100 billion	At least \$5 billion, but less than \$25 billion	At least \$1 billion, but less than \$5 billion
• Improved communication with customers	51.3%	60.6%	63.6%	68.5%
• Initiating or increasing the use of ML/AI models	71.0%	54.5%	54.5%	50.0%
• Initiating or increasing the use of cloud-based fraud and financial crimes platforms	25.0%	48.5%	58.2%	55.4%
• Developing new in-house systems for fraud and financial crimes	52.7%	45.5%	45.5%	43.5%
• Initiating or increasing the use of deep learning systems	69.7%	45.5%	43.6%	46.7%
• Outsourcing the detection and prevention of fraud and financial crimes to a third party	5.3%	21.2%	18.2%	42.4%
• Have no plans to improve our current solutions for fraud and financial crimes	1.3%	3.0%	0.0%	2.2%

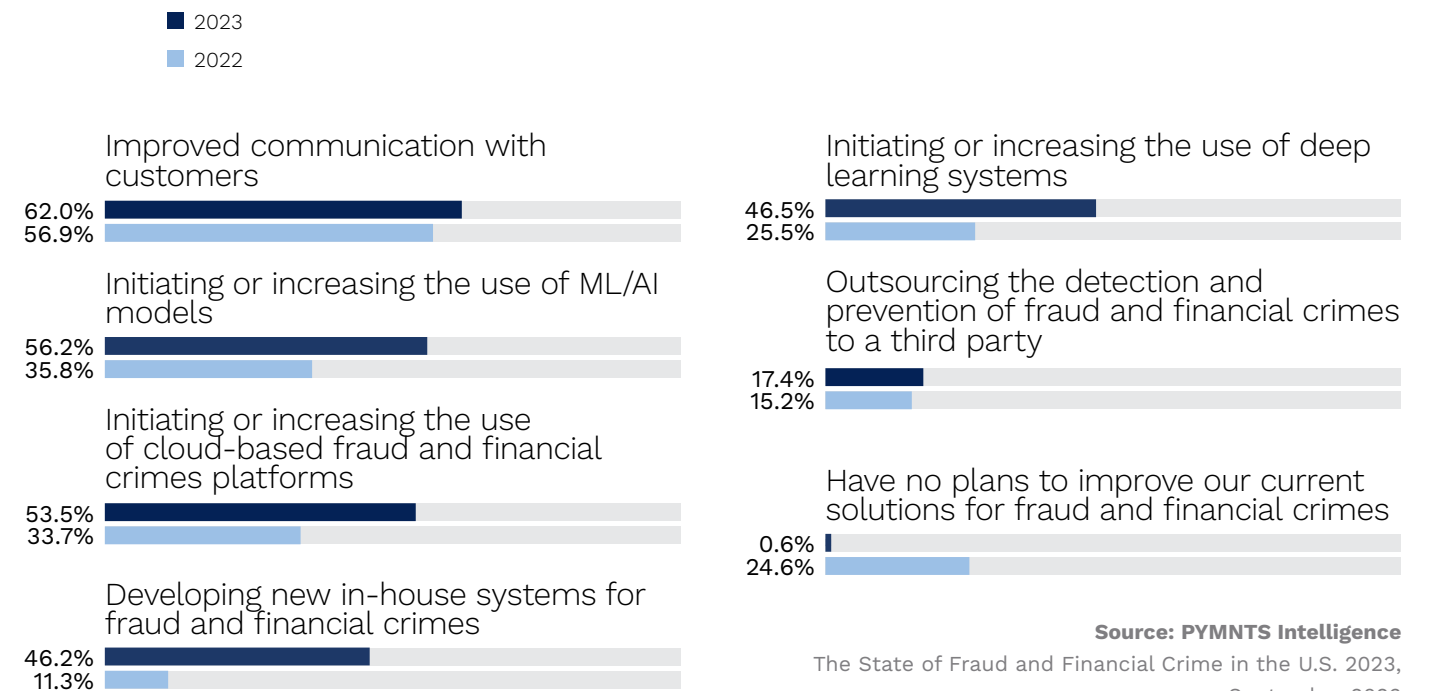
Source: PYMNTS Intelligence

The State of Fraud and Financial Crime in the U.S. 2023, September 2023  
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

**FIGURE 9B:**

**How FIs plan to improve anti-fraud efforts**

Share of FIs planning to add new technologies, by asset size



Source: PYMNTS Intelligence

The State of Fraud and Financial Crime in the U.S. 2023, September 2023  
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

46% of FIs with assets totaling more than \$5 billion cite developing new in-house systems to improve existing fraud solutions, compared to 11% in 2022. At 53%, FIs with assets of \$100 billion or more are the most likely to cite plans to develop new in-house systems to improve existing fraud solutions.

There are specific technologies and procedures that FIs tend to prefer to develop in-house with respect to fraud, such as ML/AI, adaptive authentication and transaction alerts, but not to the exclusion of inte-

grating third-party, cutting-edge solutions into the mix. For instance, FIs rely more on third-party fraud prevention APIs and two-factor or multi-factor authentication, and at least half of FIs want to improve their existing technologies and procedures by bringing in third-party developed technologies.

Additionally, FIs see third-party technologies as a way to enhance their in-house processes over the next three years. At least 60% of FIs will rely on third-parties to provide technologies such as cloud-based platforms and ML/AI to combat fraud.

# DATA FOCUS

**Data breaches, complex regulatory requirements and the increased speed of payments are FIs' biggest challenges in the face of rising fraud.**

## **FIs face more challenges when combating fraud, including fending off increasingly sophisticated cyberattacks, handling faster payment rails and a stiffer regulatory environment**

Data breaches, increased speed of payment and complex regulatory requirements are the top challenges FIs say they face when combating fraud. In particular, the share of FIs with assets totaling more than \$5 billion that mention data breaches and the increased speed of payments as their top challenges rose significantly in 2023 compared to 2022. In 2023, 16% of FIs cite cyberattacks and data breaches as a top challenge, doubling the 7.7% share that said the same in 2022. This year, 14% cited increased speed of payments as their top challenge, while just 3.7% said this in 2022.

The share of FIs citing complex regulatory requirements as their top challenge decreased significantly this year, as did the share of FIs citing the increasing sophistication and growing number of fraud and financial crimes. What dropped the most — from 16% in 2022 to 4.2% in 2023 — is the share of FIs citing the cost of deploying new technologies to combat fraud as their biggest challenge. This 74% decrease suggests that FIs increasingly recognize the necessity of adopting advanced anti-fraud solutions and are willing to make the investment. This may stem from the growing concerns FIs have about losing customers and revenue due to fraud and financial crime, with 9.3% of FIs citing loss of customers and revenue due to fraud and financial crime as their biggest challenge. Just 1.5% said the same in 2022.

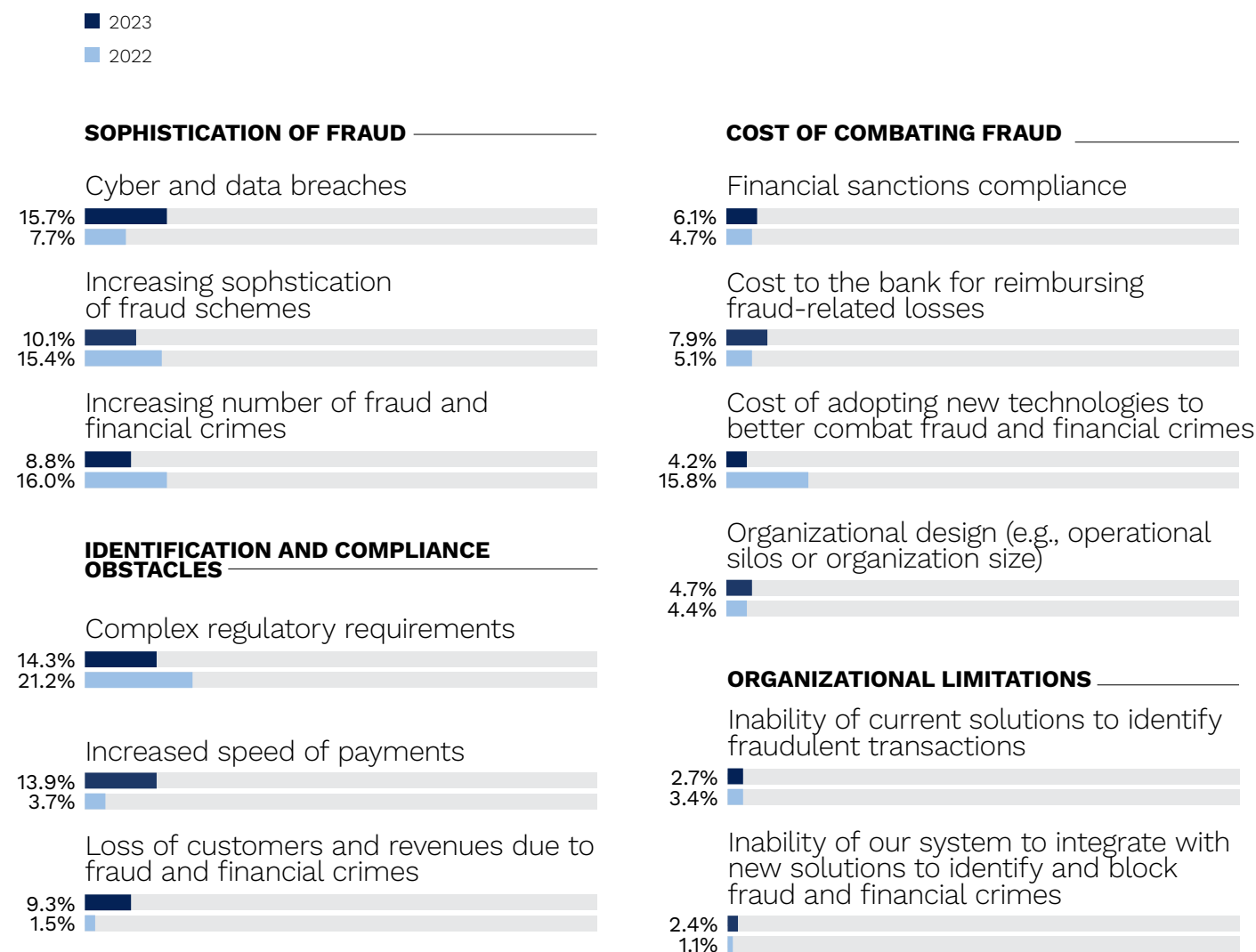


Share of FIs with assets over \$5 billion citing the **loss of customers and revenue** due to fraud and financial crime as their biggest challenge in 2023

FIGURE 10:<sup>8</sup>

**FIs' top fraud-fighting challenges**

Share of FIs with assets totaling more than \$5 billion that cite select challenges as their top challenge in combating fraud, by year



Source: PYMNTS Intelligence  
 The State of Fraud and Financial Crime in the U.S.,  
 September 2023  
 N = 200: Complete responses,  
 fielded March 20, 2023 – June 16, 2023

Source: PYMNTS Intelligence  
 The State of Fraud and Financial Crime in the U.S.,  
 September 2022  
 N = 200: Complete responses,  
 fielded April 29, 2022 – June 3, 2022

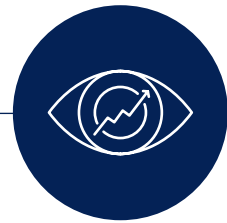
<sup>8</sup> Note: Data for FIs with assets between \$1 billion and \$5 billion is not included in time comparison charts.

# ACTIONABLE INSIGHTS



01

Misuse of account information is still the leading source of fraud, with each FI losing \$1.5 million in the last year to this type of fraud. These losses include increases in fraud related to digital wallets, same-day ACH and regular ACH payments, which can be attributed to the increasing speed of digital transactions. This suggests that FIs need to improve user authentication protocols and increase efforts to identify unauthorized users earlier — many with the help of ML and AI technology.



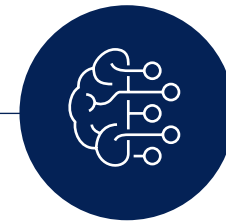
02

FIs are experiencing more challenges when combating fraud, with a significantly higher share of FIs with assets totaling more than \$5 billion citing the increased speed of payments as their biggest challenge this year than last, primarily due to the growing use of digital payment methods. FIs could benefit from payment authorization processes and advanced technology solutions that outrun bad actors, identifying fraudulent transactions as they happen.



03

Given the efficiency and success of ML and AI in combating fraud, most FIs are adding or will add these technologies to combat fraud in the next year. Outsourcing fraud detection is becoming less useful for FIs, and most plan to significantly reduce outsourcing in the next year. Instead, FIs are developing fraud solutions in-house, which tend to be more resource-intensive, and thus are employed primarily by larger FIs. Even these FIs could benefit — based on in-house resources and budget — from connections with technology solution providers with expertise in these advanced technologies.



04

FIs that currently use ML and AI technologies experienced 30% fewer transactions that resulted in fraud losses in the last 12 months compared to those that do not, an indication that banks of all sizes should increase investments in these advanced technologies to combat fraud and reduce losses.



# THE STATE OF FRAUD AND FINANCIAL CRIME IN THE U.S. 2023

September 2023 Report

PYMNTS  
INTELLIGENCE



## METHODOLOGY

**T**he State of Fraud and Financial Crime in the U.S. 2023, a PYMNTS Intelligence and Hawk AI collaboration, examines the state of fraud and financial crime FIs experienced in 2023 compared to 2022, including the rising costs of fraud and what actions they have taken to mitigate fraud. We collected 200 responses from executives working at FIs with assets of at least \$1 billion from March 29 to June 16. Respondents were also part of our 2022 survey on fraud FIs experienced. In 2022, all sampled FIs had assets totaling more than \$5 billion. In 2023, sampled FIs included 108 FIs with assets totaling more than \$5 billion and 92 FIs with assets between \$1 billion and \$5 billion. Respondents were executives with deep knowledge and leadership responsibilities in the following areas: fraud and risk operations, fraud strategy or fraud analysis.

# ABOUT

---

DISCLAIMER ■

**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.



Hawk AI helps banks, payment companies and FinTechs fight financial crime with AML and fraud surveillance. Powered by explainable AI (patent-pending) and cloud technology with a core focus on information sharing, Hawk AI improves the efficiency and effectiveness of anti-financial crime teams. Fully modular, cloud-native and enhanced with ML, Hawk AI makes customer and transaction surveillance more efficient and ensures regulatory compliance. Using traditional rules combined with AI to detect suspicious behavior in real-time, financial crime specialists can investigate true instances of suspicious activity. The solution drastically reduces false positive rates by over 70% compared to legacy AML/CFT solutions.

Founded in 2018 by experienced FinTech veterans, the company has scaled globally, processing billions of transactions across 60 countries. Hawk AI works with leading financial institutions and partners such as North American Bancard, Moss, Banco do Brasil Americas, Mambu, Visa and LexisNexis. For more information, please visit Hawk AI's website at [www.hawk.ai](http://www.hawk.ai).

## THE PYMNTS INTELLIGENCE TEAM THAT PRODUCED THIS REPORT

Karen Webster  
CEO

Paula Armendariz Miranda  
Senior Analyst

Scott Murray  
SVP and Head of Analytics

Margot Suydam  
Senior Writer

---

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](mailto:feedback@pymnts.com).

The State of Fraud and Financial Crime in the U.S. 2023 may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.

Components of the content original to and the compilation produced by PYMNTS is the property of PYMNTS and cannot be reproduced without its prior written permission.