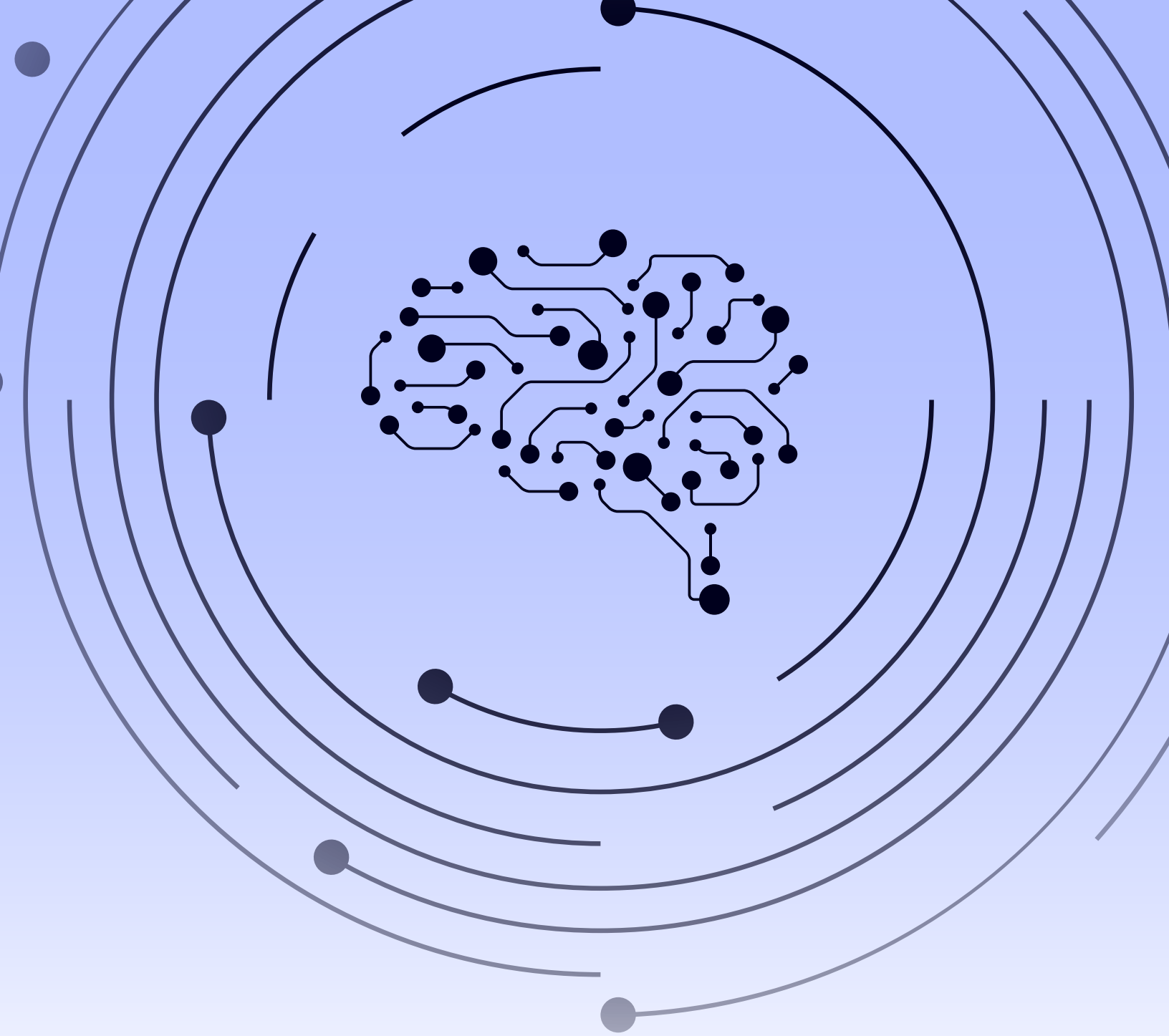


LEVERAGING AI AND ML TO **THWART SCAMMERS**

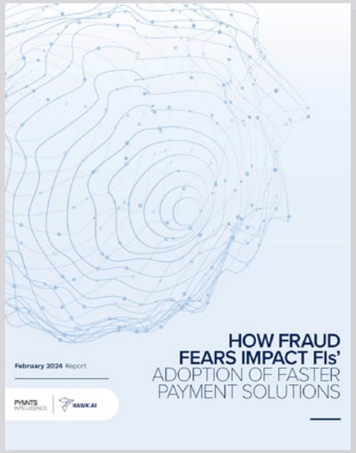
May 2024 Report

PYMNTS INTELLIGENCE | HAWK

LEVERAGING AI AND ML TO **THWART SCAMMERS**

TABLE OF CONTENTS

READ MORE



February 2024

How Fraud Fears Impact FIs' Adoption of Faster Payment Solutions

PYMNTS INTELLIGENCE | HAWK

Leveraging AI and ML to Thwart Scammers was produced in collaboration with Hawk, 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**

Despite ongoing efforts to educate consumers on how to protect themselves against financial crime, increasing instances of fraud and scams remain a financial nightmare for both banks and their customers. The Federal Reserve's FraudClassifier℠ model is an important resource in the battle against financial crime. Providing a standardized and holistic picture of payment fraud, this model segments fraud into two categories: authorized and unauthorized. Authorized fraud pertains to all fraud in which an authorized party initiates a payment, including when they are manipulated or deceived into making fraudulent payments (scams) or when an unauthorized party modifies information or instructions without the authorized party being aware. In contrast, unauthorized fraud happens when bad actors initiate or redirect a payment by taking over an account or by misusing account information to commit fraud.

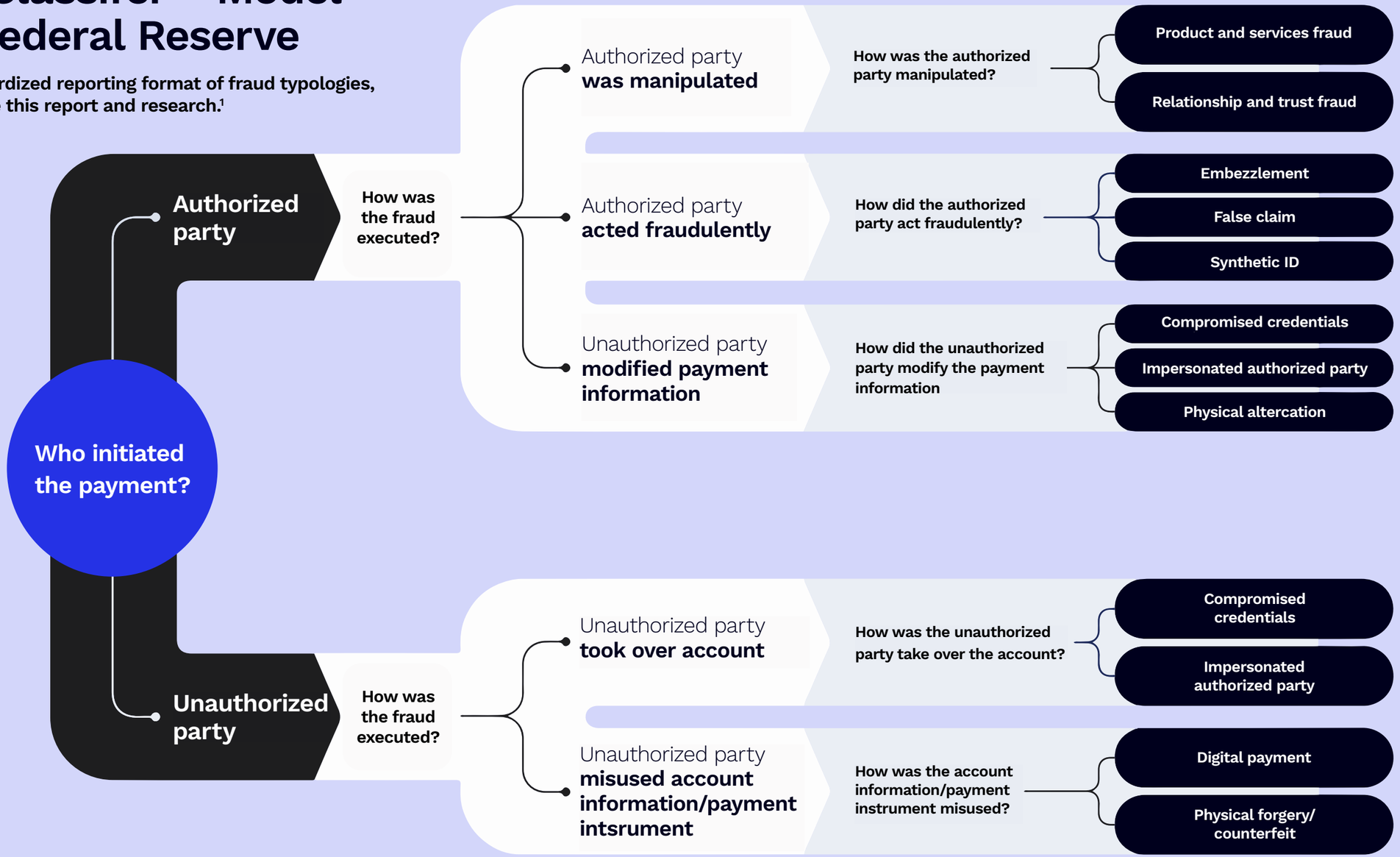
PYMNTS Intelligence finds that that 43% of the fraudulent transactions that financial institutions (FIs) have experienced are authorized fraud. Some customers or employees have had their credentials compromised, enabling bad actors to impersonate them, while others have been victims of a variety of product and services or trust/relationship scams. The result is financial loss. With fraud and financial crime an ever-growing reality for FIs of all sizes, adopting fraud prevention measures like machine learning (ML) and artificial intelligence (AI) models has helped increase FIs' confidence in their ability to protect their customers, employees and themselves from fraud-related financial losses.

Leveraging AI and ML to Thwart Scammers, a PYMNTS Intelligence and Hawk collaboration, details the impact of authorized fraud on FIs and their customers. We surveyed 200 U.S. FIs with more than $1 billion in assets between March 20, 2023, and June 16, 2023, to examine how they perceive the fraud risks and the impact of the technology solutions they use to mitigate fraud.

This is what we learned.

The FraudClassifer℠ Model from the Federal Reserve

This model is the standardized reporting format of fraud typologies, and it was used to frame this report and research.[1]



[1] Author unknown. FraudClassifier℠ Model. The Federal Reserve. 2022. https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/. Accessed April 2024.

Authorized fraud, which targets consumers, represents 43% of fraudulent transactions and accounts for 37% of dollars lost.

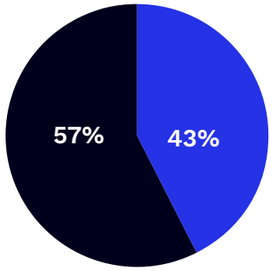
Typically, as FI size increases, authorized fraud rates rise as well. Authorized fraud peaks at 46% of fraud experienced by FIs with more than $100 billion in assets. The smallest FI respondents — those with between $1 billion and $5 billion in assets — are the exception to this rule, with the second-highest authorized fraud rate of 43%, suggesting these FIs may be targeted more than any but the largest firms.

Authorized fraud accounts for 43% of fraud volume, on average, but it represents just 37% of dollars lost, making the average dollar value of authorized fraud slightly lower than the amount lost to unauthorized fraud. The share of total dollars lost also increases with FI size, reaching a high of 44% for FIs with more than $100 billion in assets. Though authorized fraudulent transactions may cost slightly less than unauthorized fraud, customers often absorb these costs. Thus, addressing authorized fraud is central to customers' confidence and satisfaction with their financial services providers.

FIGURE 1A:

FI fraudulent transaction volume and cost

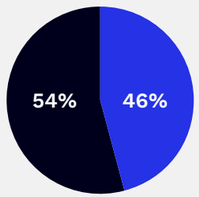
Share of the total volume of fraudulent transactions FIs experienced in select fraud types, by asset size



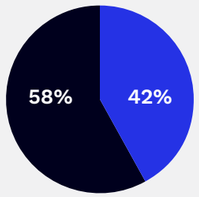
SAMPLE

- Instances of fraud initiated by an authorized party
- Instances of fraud initiated by an unauthorized party

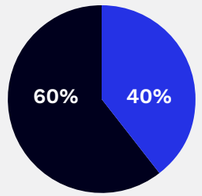
Asset size



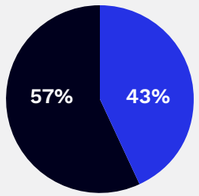
$100B or more



Between $25B and $100B



Between $5B and $25B



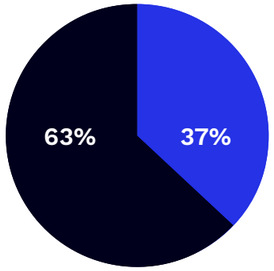
Between $1B and $5B

Source: PYMNTS Intelligence
Leveraging AI and ML to Thwart Scammers, May 2024
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

FIGURE 1B:

FI fraudulent transaction volume and cost

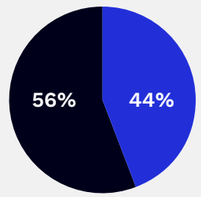
Share of the total dollar value of fraudulent transactions FIs experienced in select fraud types, by asset size



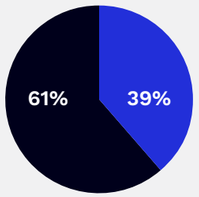
SAMPLE

- Instances of fraud initiated by an authorized party
- Instances of fraud initiated by an unauthorized party

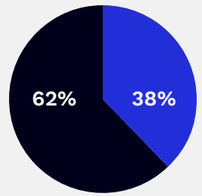
Asset size



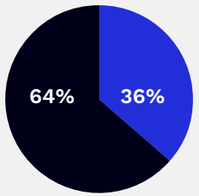
$100B or more



Between $25B and $100B



Between $5B and $25B



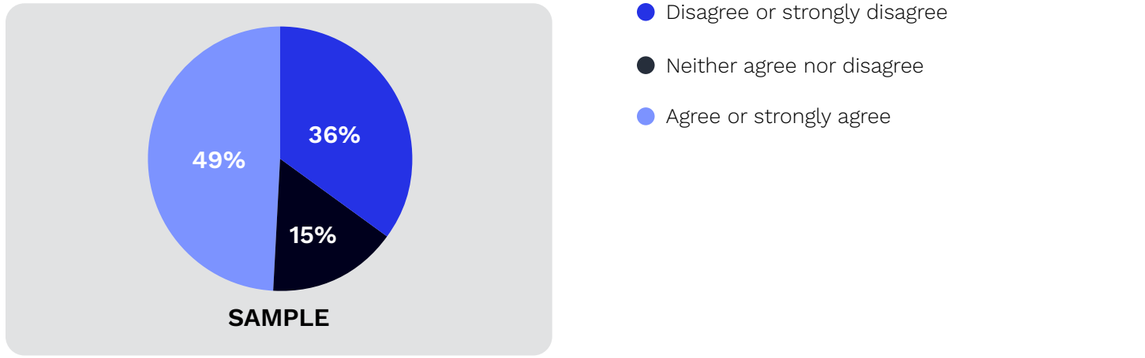
Between $1B and $5B

Source: PYMNTS Intelligence
Leveraging AI and ML to Thwart Scammers, May 2024
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

FIGURE 2:

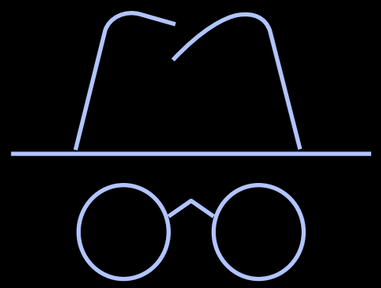
FIs' willingness to reimburse scam losses

Share of FIs citing their level of agreement with the idea that FIs should be responsible for reimbursing customers who were victims of authorized fraud, by asset size



Source: PYMNTS Intelligence
Leveraging AI and ML to Thwart Scammers, May 2024
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

Half of FIs agree that they should be responsible for reimbursing customers victimized by authorized fraud, highlighting the financial burden customers often face. In fact, the larger the FI, the more likely it is to reimburse its customers for charges stemming from authorized fraud. Even though larger FIs see a higher portion of scams, they are still more likely to refund customers, with 75% believing that customers should be reimbursed. This suggests that larger banks have the means to cover these transactions and may see doing so as a cost of doing business. Meanwhile, refunding customers may be too harmful to smaller FIs' bottom lines, with only 48% willing to do so. Since authorized fraud tends to harm customers more at small banks, smaller FIs that prioritize fraud prevention strategies could see increases in client retention and satisfaction.



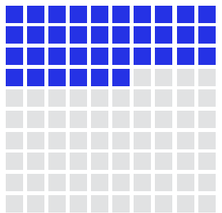
Scams, which represent one-third of authorized fraud, target consumer vulnerability, making them the type of fraud most harmful to consumers' experiences and finances.

The most common type of authorized fraud involves unauthorized parties modifying payment information or instructions, and this type of fraud accounts for 40% of all authorized fraudulent payments. The second-most common type are scams, where a fraudster manipulates or deceives the authorized party to make a payment, representing 34% of authorized fraud. Moreover, scams represent 14% of all fraudulent transactions in FIs with assets of $5 billion or more, making them a common occurrence.[2] Scams are particularly concerning because they negatively impact customer satisfaction and retention. Customers expect their FIs to protect them from fraud and may feel let down when they fail to do so. A customer who does not trust that that their FI can protect them from fraud is likely to take their business elsewhere.

[2] The State of Fraud and Financial Crime in the U.S. 2023. PYMNTS Intelligence. 2023. https://www.pymnts.com/study/increasing-fraud-heightens-need-for-newer-better-technologies/. Accessed April 2024.

A deeper dive into how customers get scammed reveals that 53% of the scams FIs report are product or services fraud, where what users pay for is never provided, and 47% are relationship or trust fraud, where customers are manipulated by a fraudster who eventually requests funds. Product or services fraud is the most common for the smallest FIs, while relationship fraud is most common for FIs with between $5 billion and $25 billion in assets.

More importantly, scams are among the hardest types of fraud to dispute, leaving customers vulnerable to financial losses. Even though many larger FIs are willing to reimburse scam victims, 36% of FIs believe they should not be responsible for reimbursing customers for money lost via authorized fraud. Preventing authorized fraud with technological solutions and consumer education remains a priority for many FIs.

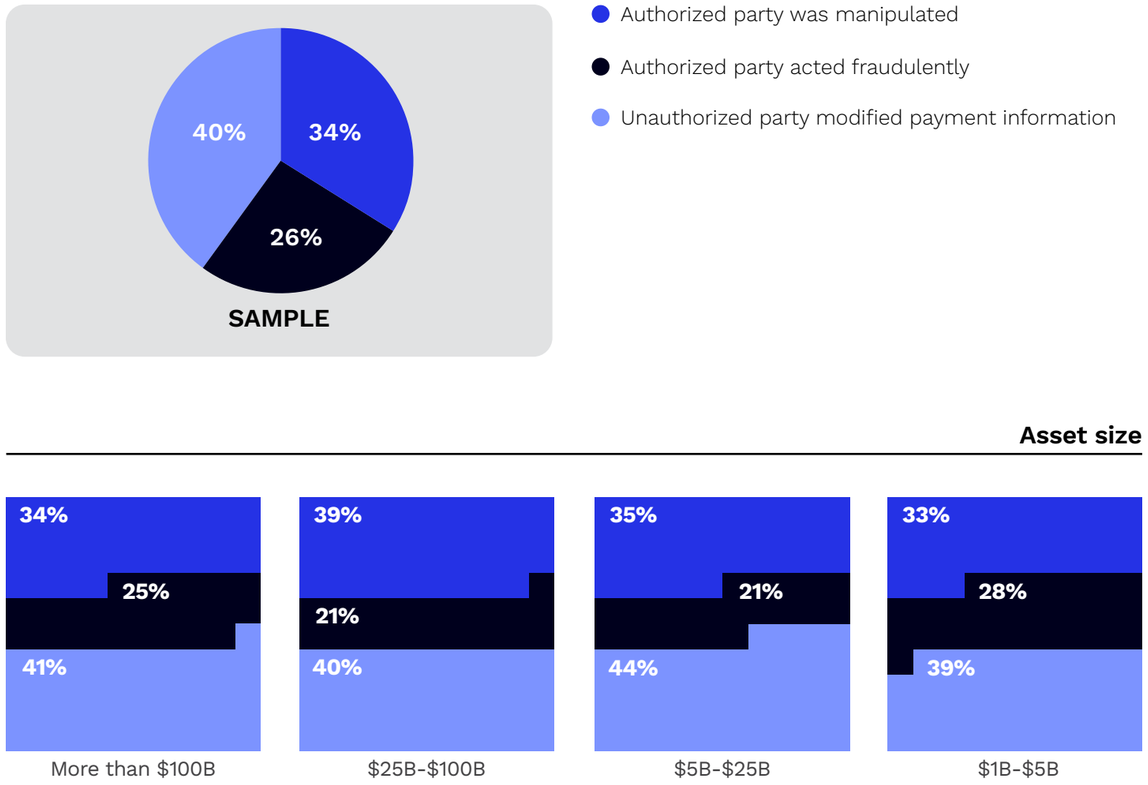


36%

Share of FIs that believe they should not be responsible for reimbursing consumers for money lost via authorized fraud

FIGURE 3:

Types of authorized fraud
Share of the total volume of authorized fraud transactions FIs experienced in select fraud types, by asset size

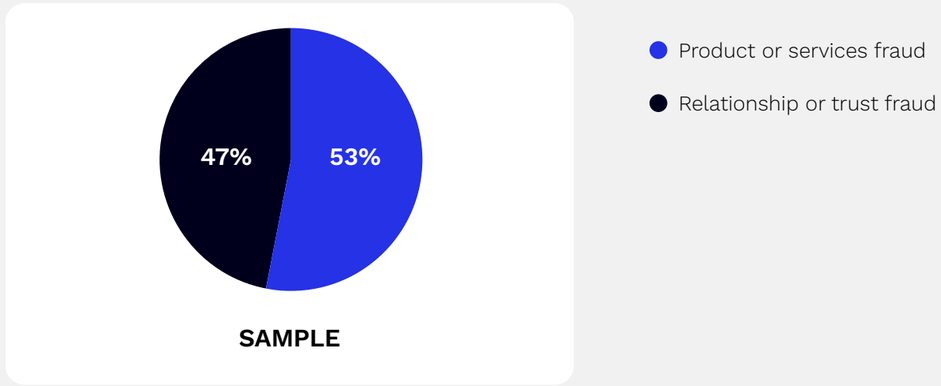


Source: PYMNTS Intelligence
Leveraging AI and ML to Thwart Scammers, May 2024
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

FIGURE 4:

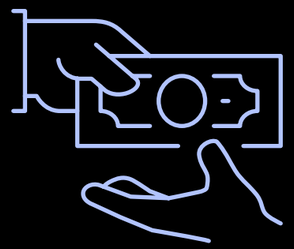
Types of scams FIs experienced

Share of the total volume of authorized fraud transactions FIs experienced in which the authorized party was manipulated, by asset size



Source: PYMNTS Intelligence
Leveraging AI and ML to Thwart Scammers, May 2024
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

Product or services fraud is the most common for the smallest FIs, while relationship fraud is most common for FIs with between $5 billion and $25 billion in assets.



Scammers disguised as a trusted service provider or promising monetary gain are the most likely to trick authorized users.

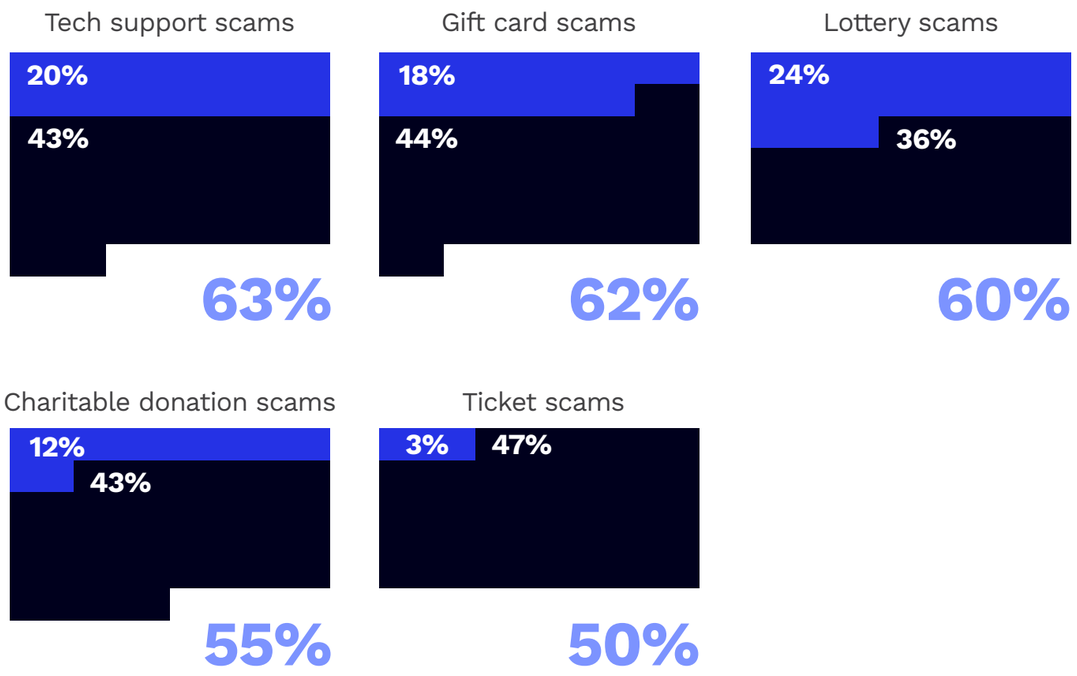
Scammers increasingly target vulnerable customers by making appealing offers or acting as a trusted service provider. Data shows that more than 63% of FIs reported incidents of tech support scams, making fictitious tech issues the most widespread risk for FIs in the product and services fraud category. This is followed by gift card scams and lottery scams, at 63% and 60%, respectively. Charitable donation scams and ticket scams are other prevalent forms of product and services scams. When looking at which scams FIs said they experienced the most, lottery scams take the lead, at 24%, followed by tech support scams, at 20%, and gift card scams, at 18%. In all cases, bad actors have enticed their victims to pay for products or services that will not be delivered, resulting in financial loss for the customer and possibly the FI as well.

When it comes to relationship and trust fraud, 65% of FIs reported incidents of utility company scams, with 14% saying this is the type of scam they experience the most. Meanwhile, 64% reported incidents of IRS imposter scams, with 22% citing it as the type of scam they experience the most. Fake debt collection scams and romance scams are also prevalent types of trust or relationship scams FIs reported, at 58% each. As these findings suggest, the most common scams come from bad actors posing as trusted sources for financial gain, thus identifying significant customer and FI employee vulnerabilities.

FIGURE 5:

Product or services fraud types

Share of FIs that experienced select types of product or services fraud, by level experienced

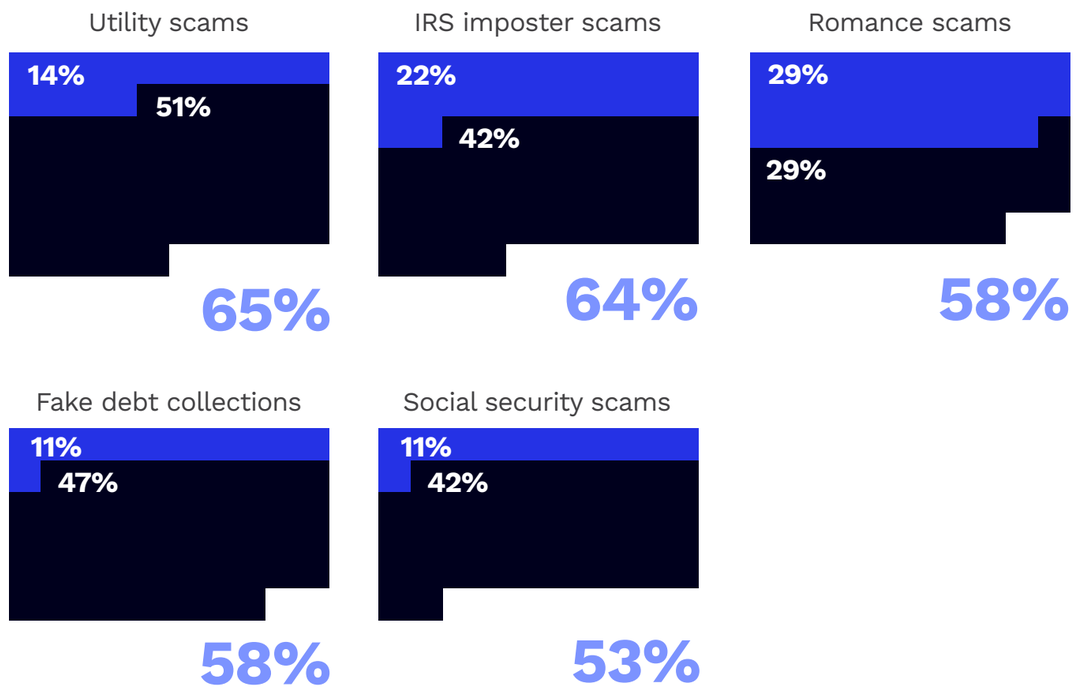


Source: PYMNTS Intelligence
Leveraging AI and ML to Thwart Scammers, May 2024
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

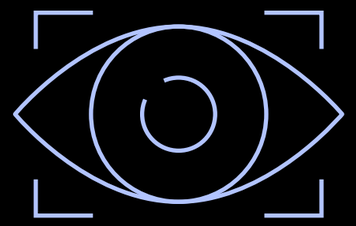
FIGURE 6:

Types of trust or relationship fraud FIs experienced

Share of FIs that experienced select types of trust or relationship fraud, by level experienced



Source: PYMNTS Intelligence
Leveraging AI and ML to Thwart Scammers, May 2024
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023



FIs that employ ML or AI fraud prevention models reported lower incidences of many of the most prevalent scams.

While educating customers on scams is an important fraud prevention strategy, FIs increasingly look to technological solutions such as ML or AI to mitigate fraud. The results look promising. For instance, tech support impersonation and IRS imposter scams are among the most frequently reported scams, yet FIs using AI or ML anti-fraud solutions were 17% less likely than those that do not use these technologies to report tech support scams as their biggest scam threat. Likewise, those employing AI or ML fraud prevention tools were 18% less likely to report IRS imposter scams as a top concern. FIs that use AI or ML technologies also reported lower rates of lottery, romance, utility and Social Security scams.

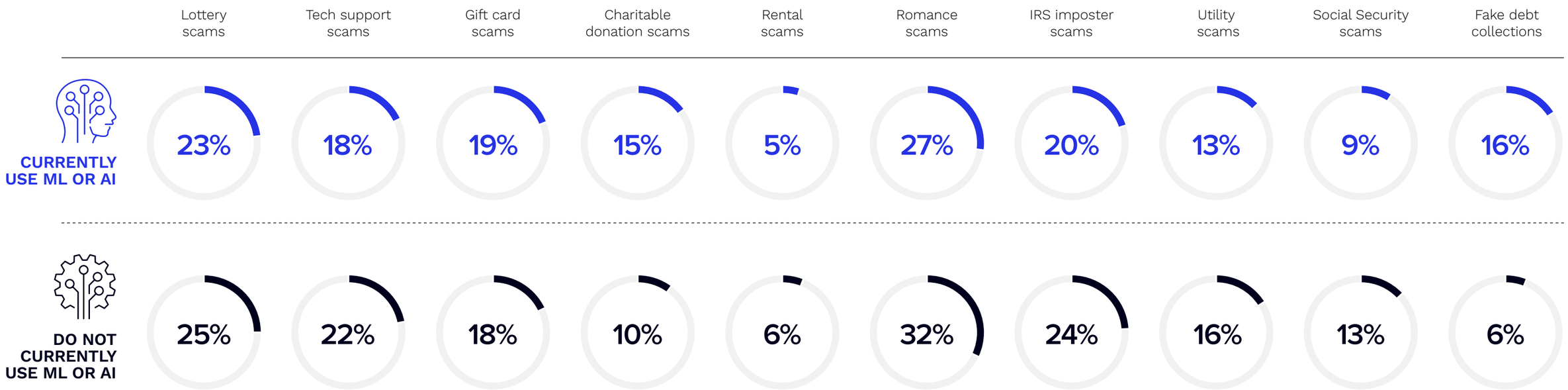
AI or ML solutions still have room for improvement in identifying charitable donation scams and fake debt collection scams, possibly because these scams remain less common. Alternatively, it could be that FIs added features addressing these scams more recently but they have yet to take effect.

There is good news for both FIs and customers in the battle against fraud. Data shows that 52% of FIs plan to implement or increase their use of AI or ML fraud prevention models. In fact, FIs currently using AI or ML are 17% more likely to have plans to implement additional AI or ML solutions than those that do not currently use AI or ML fraud prevention solutions. This suggests that many FIs see returns from using AI or ML fraud prevention.

FIGURE 7:

How AI/ML usage helps prevent leading scams

Share of FIs that experienced select types of scams the most in the last 12 months, by use of ML or AI



Source: PYMNTS Intelligence
Leveraging AI and ML to Thwart Scammers, May 2024
N = 200: Complete responses, fielded March 20, 2023 – June 16, 2023

CONCLUSION

As long as scammers continue to find ways to manipulate vulnerable customers, authorized fraud — whether based on exploiting trust and relationships or promising products or services without delivering — will result in significant financial losses for FIs and their customers. Efforts to make more consumers aware of scammers' tactics remain important. Yet, by adopting measures such as fraud prevention ML or AI models, FIs can stop bad actors before the damage is done while also increasing consumer confidence in their ability to protect them from such fraudulent transactions. Leveraging advanced technologies enables FIs to reduce financial losses while also providing customers with the trusted financial services they expect.

METHODOLOGY

Leveraging AI and ML to Thwart Scammers, a PYMNTS Intelligence and Hawk collaboration, details the impact of authorized fraud on FIs and their customers. We surveyed 200 U.S. FIs with assets of more than $1 billion between March 20, 2023, and June 16, 2023, to examine how they perceive the fraud risks and the impact of the technology solutions they use to mitigate fraud to increase consumer confidence and drive customer satisfaction.

THE PYMNTS INTELLIGENCE TEAM THAT PRODUCED THIS REPORT

Scott Murray
SVP and Head of Analytics

Story Edison, PhD
Senior Analyst

Margot Suydam
Senior Writer

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.

HAWK

Hawk is the leading provider of AI-supported anti-money laundering and fraud detection technology. Banks and payment providers globally are using Hawk's powerful combination of traditional rules and explainable AI to improve the effectiveness of their AML compliance and fraud prevention by identifying more crime, while maximizing efficiency by reducing false positives. Hawk's modular solution can either enhance or replace rules-based systems with AI-powered transaction monitoring, payment screening, pKYC and fraud prevention in real-time to deliver greater accuracy and reduced noise.

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.