SURVEY REPORT 2023

AI perspectives: Transaction fraud

brighterion by Mastercard | FINTECH NEXUS

Table of Contents

Introduction

The payments industry is changing.

Account-to-account (A2A) payments, transactions that move funds directly from one account to another, became increasingly popular during the 2020 digital banking disruption. Consumers are buying more goods and services online, increasing the risk of transaction fraud. The challenge of detecting and preventing fraud is becoming much broader.

Digital wallets surpassed credit cards in 2022, becoming the leading payment method among U.S. consumers shopping online, totaling 32 percent of e-commerce transactions. In total, FIS reports, A2A payments accounted for US $525 billion in 2022 global e-commerce transactions, estimating the market will reach nearly US $8.5 trillion in 2026.[1]

The problem with direct payments is customers are responsible for many of their own fraud losses, although larger banks may refund their customers to protect relationships. A2A is also attractive to money launderers as transactions are often untraceable. Fraudsters can just close their accounts once the money is received.

Direct payment methods have the attention of federal lawmakers who are calling for better account holder protection, particularly consumers. Simultaneously, the Federal Reserve has made faster B2B payments a major priority. Many banks want to provide seamless, secure e-transfer services, but face strict regulations on how they enable A2A transactions and who is responsibility for fraud losses.

Despite the rising popularity of A2A transactions, card sales, cash advances and cash withdrawals (from cardholder funds on deposit) totaled $48.955 trillion in total volume worldwide in 2021, an increase of 16.6% from 2020.

Global card fraud losses reached $32.34 billion in 2021, an increase of 13.8 percent over 2020, according to the Nilson Report. Over the next 10 years, the industry is projected to lose an accumulated $397 billion worldwide, with $165 billion coming from the US.

Fintech Nexus and Brighterion collaborated on a survey sent to financial institutions in the Spring of 2023 to understand how they are investing in technology in the face of rapid change. Specifically, we wanted to understand what organizations are thinking about using artificial intelligence (AI) for transaction fraud monitoring in this dynamic digital economic landscape.

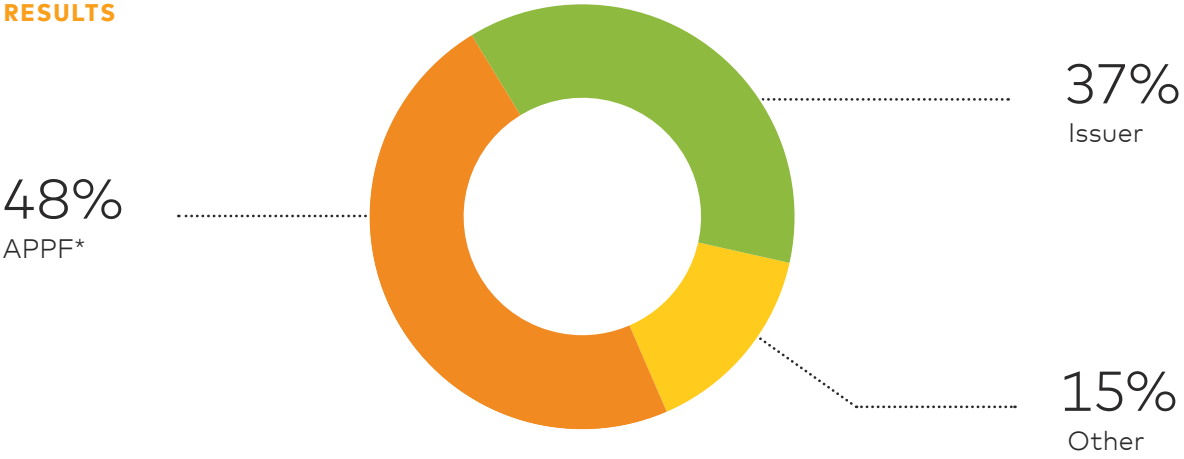
This report divides responses by the business categories that responded: acquirers, payment service providers, payment facilitators (grouped as "APPF"), issuers, and "other" organizations that process payment transactions.

1. FIS, "Account-to-Account Payments Set to Revolutionize Shopping, with E-commerce Payments Reaching $525 Billion Globally: Worldpay from FIS 2023 Global Payments Report," March 23, 2023.

QUESTION 1

Which of the following most closely defines your company?

RESULTS



**APPF: Acquirers, payment services providers and payment facilitators.*

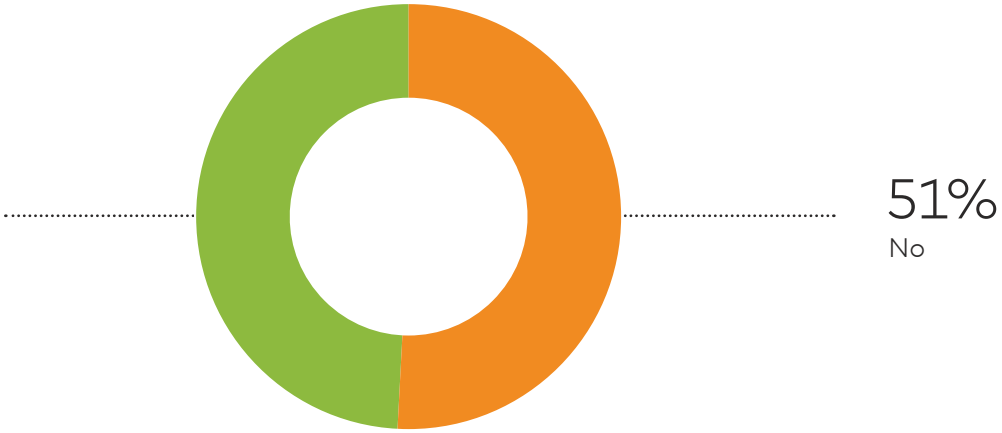
Key takeaways

Forty-eight percent of the survey respondents were acquirers, payment service providers and payment facilitators (APPF) and 37 percent were issuing banks. The remaining 15 percent represented a variety of organizations, including mobile money providers, lenders, and data analysts.

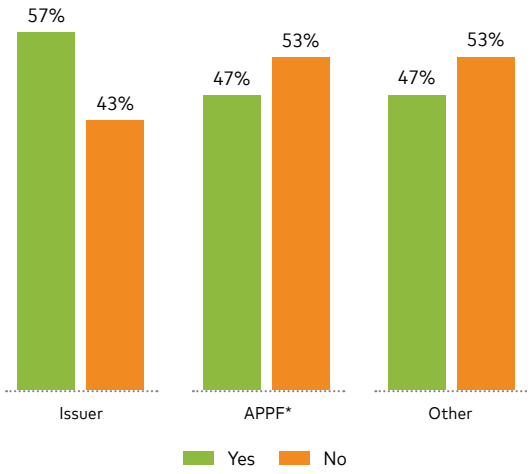
QUESTION 2

Does your organization use AI for fraud detection today?

RESULTS



BREAKDOWN



**APPF: Acquirers, payment services providers and payment facilitators.*

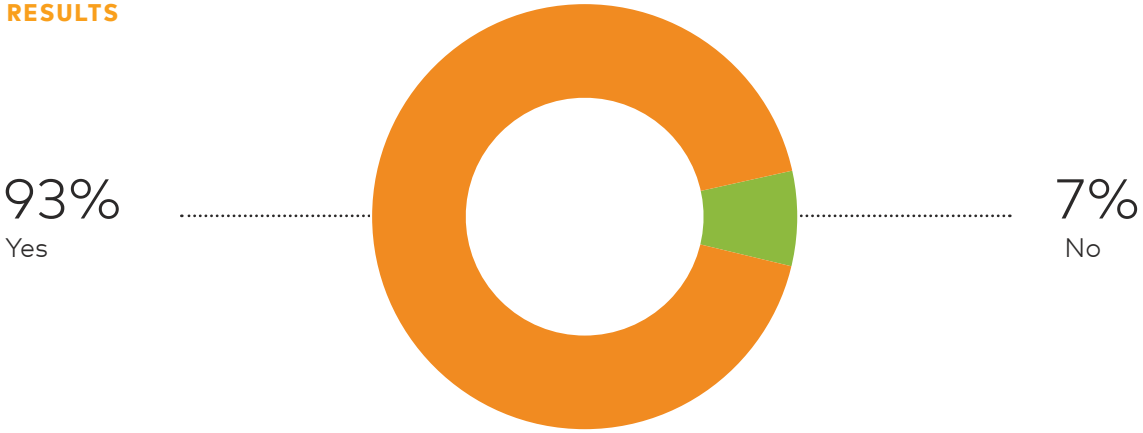
Key takeaways

Roughly half of the survey respondents from each financial business category reported using AI in their organizations to detect fraud.

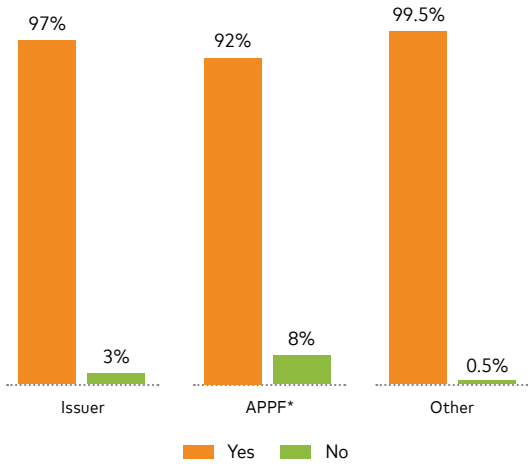
QUESTION 3

Does your organization plan to invest more in AI over the next 2–5 years?

RESULTS



BREAKDOWN



**APPF: Acquirers, payment services providers and payment facilitators.*

Key takeaways

Slightly less than half of the respondents used AI for fraud detection when surveyed, but an average 93 percent planned to invest in the next two to five years.

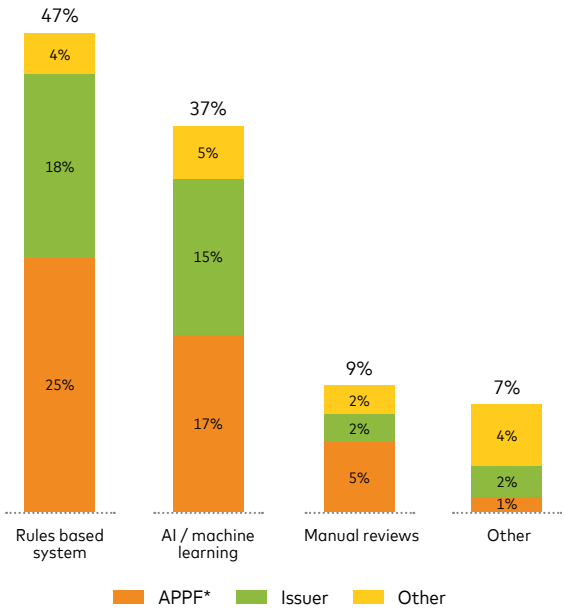
While 47% of APPF respondents were using AI, 97 percent planned to invest in AI solutions within the next five years, likely a reflection of increased e-commerce which drives a need for higher approval rates while increasing fraud detection. Those using AI may also be expanding their use of AI solutions in their businesses.

Issuers faced with account-to-account (A2A) fraud will need advanced detection solutions that are capable of identifying anomalies in frequently untraceable transactions. Issuers also need to comply with regulators who are seeking to hold them accountable for consumers' losses.

QUESTION 4

Which of the following technologies do you leverage today for fraud detection?

RESULTS



Respondents could select more than one answer.
**APPF: Acquirers, payment services providers and payment facilitators.*

Key takeaways

The greatest number of respondents reported using rules-based systems to detect fraud (47 percent), with AI and machine learning following closely behind at 37 percent.

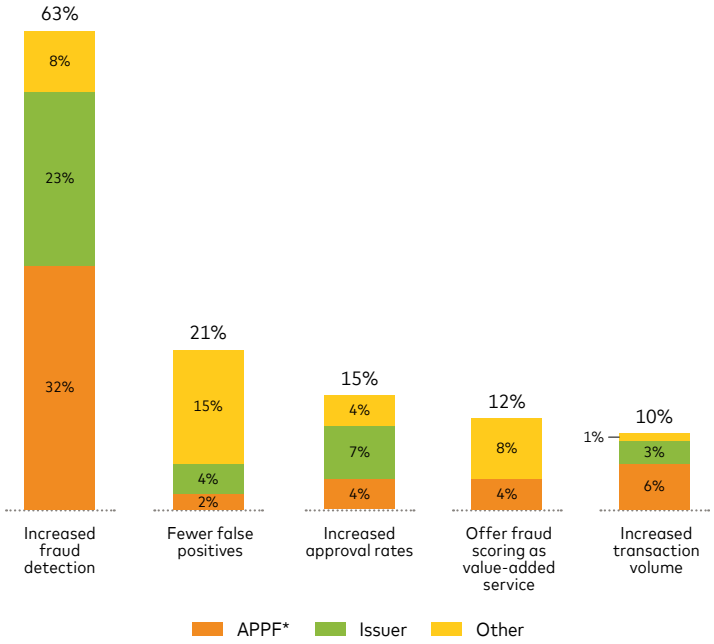
Manual review and other methods are also used to a lesser extent. While not reported as such, these may be combined with other technologies to ensure robust systems or to perform spot checks.

While rules-based solutions are still the most commonly used technology, when combined with AI their effectiveness is increased and the number of required rules is decreased. This results in simpler workflows and more efficient management. Fraud teams are freed up to investigate large cases and only conduct manual reviews for accuracy or to perform occasional audits.

QUESTION 5

What is the #1 need driving AI investment?

RESULTS



Answers do not total 100% as responses were ranked.
**APPF: Acquirers, payment services providers and payment facilitators.*

Key takeaways

Detecting fraud is clearly the top need expressed by the majority of survey respondents. "Increased fraud detection" was selected by 63 percent of the respondents, followed by "fewer false positives" by 21 percent as their most pressing need.

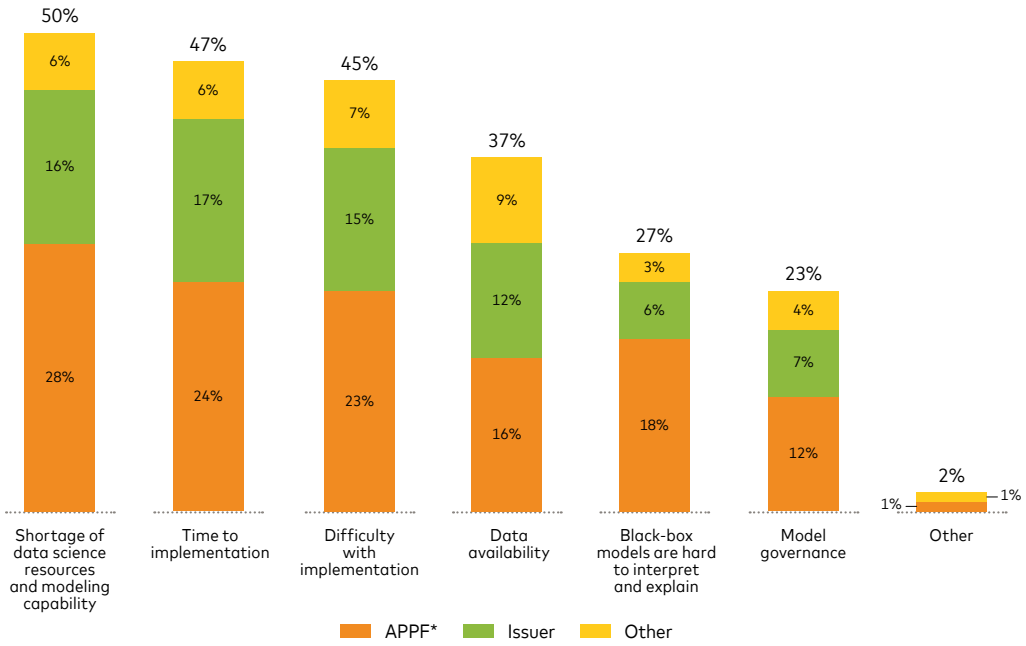
Increased fraud schemes and payment channels are leaving many financial institutions and their customers vulnerable. In 2022, consumers lost $8.8 billion to financial fraud in the U.S. alone.[2] According to the Nilson Report, payment card fraud losses worldwide exceeded $32 billion in 2021.

2. Federal Trade Commission, "New FTC Data Show Consumers Losing Nearly $8.8 Billion in Scams in 2022," (retrieved June 1, 2023).

QUESTION 6

What are the barriers to widely adopting AI to solve fraud and money laundering?

RESULTS



Respondents could select more than one answer.
**APPF: Acquirers, payment services providers and payment facilitators.*

Key takeaways

Respondents met a variety of barriers to widely adopting AI to meet the challenges of fraud and money laundering. Fifty percent of the respondents selected a shortage of data science resources and modeling capacity.

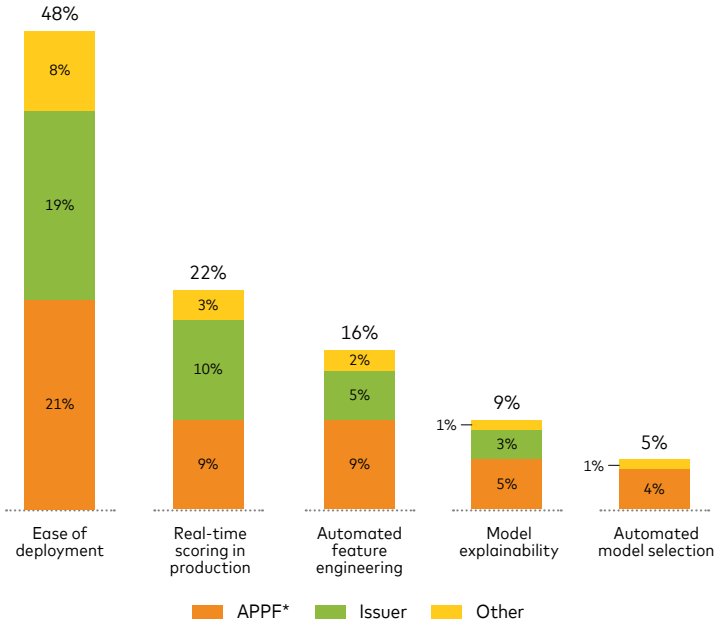
The time required for implementation was a barrier reported by 47 percent, while 45 percent reported the difficulties associated with implementation.

Data availability, explainability of outputs, and model governance were also cited as barriers.

These signal a need for outside resources and solutions with the capacity to address these barriers. In particular, the respondents show a need for AI implementation without having to recruit data scientists. They also require shorter timelines and production-ready models that include explainability layers and are guided by good model governance.

Importance of components on the success of your current/future AI infrastructure.

RESULTS



Answers do not total 100% as responses were ranked.
**APPF: Acquirers, payment services providers and payment facilitators.*

Key takeaways

Respondents were asked to rank the importance of various features of their AI infrastructure. Ease of deployment is the greatest barrier, cited by 48 percent of respondents. Research shows that deployment can take months, even years, to complete. New market-ready models are poised to solve this issue for all financial institutions.

Real-time scoring ranks second as the most important success factor, which is becoming even more critical for e-commerce and A2A transactions.

Automated feature engineering, model explainability and automated model selection follow, perhaps reflecting the shortage of data science resources and modeling capability cited in Question 6.

According to MIT Sloan Management Review, in a survey of 3,000 managers, they learned that only one in 10 companies successfully gained benefits from developing their own AI.[3] This is substantiated by CompTIA, which reports nearly 80 percent of AI projects don't scale beyond a proof of concept.[4]

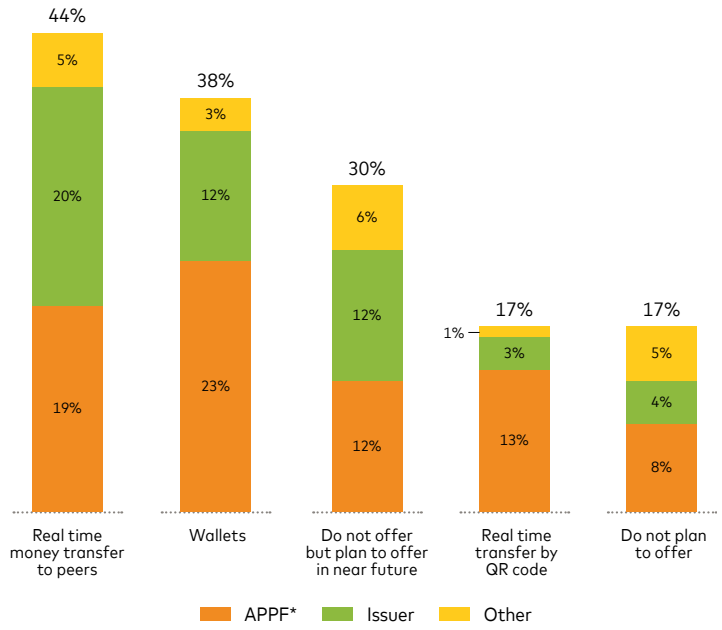
3. MITSloan Management Review, *Expanding AI's Impact With Organizational Learning*, October 2020.

4. CompTIA.org, "Artificial Intelligence in Business: Top Considerations Before Implementing AI," (retrieved June 26, 2013).

QUESTION 8

Which alternative payment methods (non-card) do you offer to your customers?

RESULTS



Respondents could select more than one answer.
**APPF: Acquirers, payment services providers and payment facilitators.*

Key takeaways

Real-time peer-to-peer (P2P) were the most common form of A2A payments offered by respondents (44 percent). In addition to e-transfers, this includes use of apps like PayPal, Zelle and others. Of note, only three percent of respondents that supported P2P payments were acquirers.

Digital wallets were also very popular amongst respondents, offered by 38 percent of respondents. Only 17 percent offered payment access through QR codes. Seventeen percent did not plan to offer non-card payments, while 30 percent planned to in the near future.

P2P payments is a quickly growing payment rail, expected to reach US $9.87 trillion globally by 2030, reports Precedence Research.[5] More than 5 billion people, or 60 percent of the world's population, will use digital wallets by 2026.[6] The Southeast Asian nations of the Philippines, Thailand and Vietnam are expected to see the fastest growth and Juniper predicts that 75 percent of these countries' populations will adopt digital wallets over the next four years.[7]

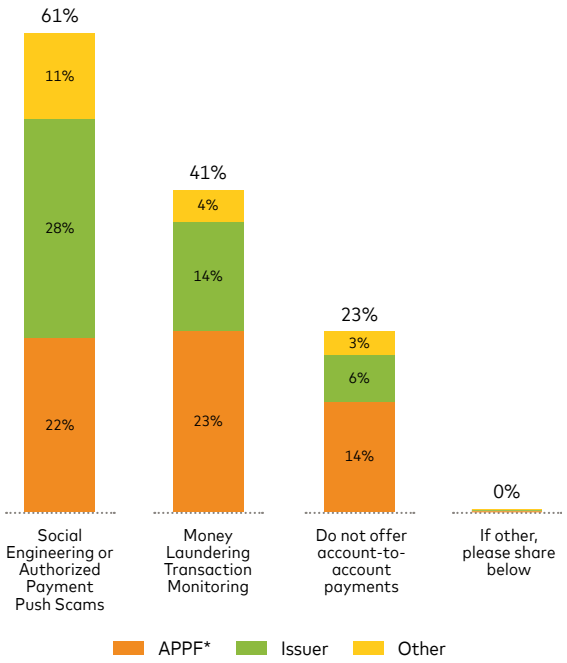
Digital wallets use strong encryption technology to protect users' information and transactions.[8] Despite this, they are still vulnerable to hacking or cyberattacks. Fraudsters may also hack into users' accounts to make unauthorized transactions. Financial institutions who support digital wallets will still need to monitor for anomalous behaviors that signal fraud.

5. GlobeNewsWire, "P2P Payment Market Size to Worth Around USD 9.87 Trillion by 2030," (retrieved June 1, 2023).
6. ComputerWeekly.com, "More than 60% of world population will use digital wallets by 2026," (retrieved June 1, 2023).
7. ComputerWeekly.com, "More than 60% of world population will use digital wallets by 2026," (retrieved June 1, 2023).
8. FinanceMagnates.com, "The Advantages and Risks of Moving Your Money to a Digital Wallet," (retrieved June 26, 2023.

QUESTION 9

Identify the top risks in real-time account-to-account payments.

RESULTS



Respondents could select more than one answer.
**APPF: Acquirers, payment services providers and payment facilitators.*

Key takeaways

Respondents felt that social engineering and authorized payment push scams (61 percent) were a higher risk than money laundering (41 percent) when considering fraud in A2A services. None stated another form of A2A fraud as being of higher concern.

In social engineering, fraudsters create scenarios to draw in their targets. Romance, grandparent and CEO scams are prevalent, preying on victims' vulnerabilities. Deep-fake AI is being used to mimic friends', family members' and colleagues' voices, gaining the trust of targets. Because P2P is the equivalent of giving someone cash, senders and their banks often can't trace the recipients who may have deleted the accounts once the funds were received.

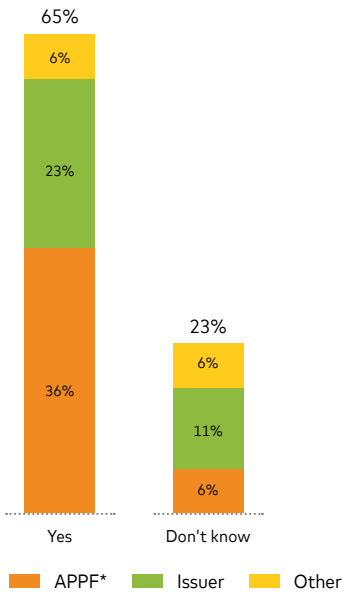
In authorized payments push scams, bad actors lure their targets to action. For example, the scammer advertises a product at a one-time trial price, but once they have their victim's payment information, they continue to withdraw funds, draining the account. As the customer authorized the withdrawals directly from their account, they may not be able to claim the loss from their bank. The second area of concern, money laundering, also benefits from the untraceable nature of transactions.

With legislation either enacted or being introduced by governments worldwide, banks face enforcement for not detecting these forms of fraud. Financial institutions need to find ways to detect anomalous transactions before they complete.

QUESTION 10

Can AI help solve the problem of social engineering and authorized payment push scams?

RESULTS



**APPF: Acquirers, payment services providers and payment facilitators.*

Key takeaways

The majority of respondents (65 percent) believed AI would be a useful tool in solving social engineering and authorized payment push scams.

One benefit of AI and machine learning is the technology evolves with changing data, learning new scams as they are identified. As the AI model matures, it becomes more effective unlike other technologies that become obsolete or need constant updating.

Conclusion

Almost half of the 100 financial institutions (FIs) surveyed were using AI at the time of responding, with 93 percent planning future investments in the following two to three years. Clearly not all respondents are using AI for fraud detection, as the greatest number of respondents reported using rules-based systems to detect fraud (47 percent), with AI and machine learning following closely behind at 37 percent.

Only 63 percent stated the number one reason they plan to use AI and machine learning is for fraud detection. The secondary reason follows at a distant 21 percent: fewer false positives.

Responses showed the challenges of implementation continued to be significant barriers to widely adopting AI for detecting fraud and money laundering:

- 50 percent of respondents cited a shortage of data science resources and modeling capacity
- 47 percent chose the time required for implementation
- 45 percent reported the difficulties associated with implementation
- Data availability (37 percent), lack of transparency (explainability) of outputs (27 percent), and model governance (23 percent)

These signal a need for outside resources and solutions with the capacity to address these barriers. In particular, the respondents show a need for AI implementation without having to recruit data scientists. They also require shorter timelines and production-ready models that include explainability layers and are guided by good model governance.

It will be no surprise, then, that almost half of the respondents (48 percent) said ease of deployment would be the most important success factor in choosing an AI solution, while a quarter were looking for real-time scoring, followed by automated features engineering. With the shortage of data science resources, limited modeling capacity and long deployment timelines, the data seems to reveal that many financial institutions want the promises of AI but are frustrated by the many barriers.

We also turned our attention to account-to-account transaction fraud, a rising problem faced by respondents (44 percent) from all categories we surveyed, although only three percent of acquirers were offering the service. There is a growing possibility that acquirers will be using A2A at some point and therefore see the potential for problems in their own businesses.

The most common A2A method supported by respondents was real-time peer-to-peer (P2P) payments which have been common for some time.

Digital wallets were also very popular amongst respondents, offered by 38 percent of respondents. Digital wallets use strong encryption technology to protect users' information and transactions. Despite this, they are still vulnerable to hacking or cyberattacks. Fraudsters may also hack into users' accounts to make unauthorized transactions. FIs that support digital wallets will still need to monitor for anomalous behaviors that signal fraud in real-time.

For other A2A services, 17 percent of respondents offered payment access through QR codes, 30 percent planned to offer non-card payments in the near future, while 17 percent do not plan to offer any direct payment services.

Respondents reported two primary areas of A2A payments fraud: social engineering and authorized payment push scams (61 percent) and money laundering (41 percent). Sixty-five percent believe AI will be useful in detecting social engineering and authorized payment push scams, signaling that if the technology becomes more accessible to them, they would be interested in applying it to this growing issue.

A benefit of AI and machine learning is that the technology evolves with changing data, learning new scams as they are identified. As the AI model matures, it becomes more effective unlike other technologies that become obsolete or need constant updating.

FIs clearly see the potential benefits of AI for fraud detection, but have been discouraged by lengthy deployment times, incomplete training data and a lack of resources to take the solution into production and maintain it throughout its lifetime.

There is a clear need for market-ready AI and machine learning solutions built with advanced training to identify evolving fraud that rules-based and other technologies can't identify or stay abreast of. Regulators around the globe are monitoring account-to-account payments with an eye to consumer protection. This new risk could result in restriction to financial institutions beyond the scope of their roles in these transactions. By investing wisely in advanced AI, FIs can prevent over-regulation while protecting their customers.

About Fintech Nexus

Fintech Nexus (formerly Lendit Fintech) is a diversified media company providing essential knowledge, connections and inspiration to the entire financial services industry, creating a link between traditional finance and the future of finance. Each year, we reach 200,000+ banking, fintech and investment professionals through our diverse portfolio of news, events, podcasts, webinars, whitepapers, newsletters and our credentialed education courses.

Like much of the economy today, financial services is experiencing a rapid upheaval. We are seeing a multi-decade transformation where fintech will take center stage as everything becomes digital. Fintech Nexus is there for you, reporting the news on a daily basis, and enabling real time discussion and insights via digital media and live events.

We immerse ourselves in all things fintech so we can be your trusted guide on this exciting journey.

About Brighterion

Brighterion, a Mastercard company, was founded in 2000 and acquired by Mastercard in 2017. Brighterion provides enterprise AI applications for payment service providers, financial institutions, healthcare payers and merchants. More than 2,000 companies worldwide and 74/100 of the largest U.S. banks use technology powered by Brighterion AI to protect against fraud and risk.

Brighterion's solutions offer value-added Mastercard network intelligence to further enhance performance beyond a client's own data. Using our full stack, state-of-the-art machine learning toolkit, we create off-the-shelf market models that are production-ready today and custom models in 6–8 weeks. With unrivaled deployment and scalability, customers can easily implement AI that delivers lightning fast response times and resiliency.

We are committed to responsible data innovation and product design that protects individuals' rights. Data responsibility lays the groundwork for best-in-class security and privacy, and built-in explainability.