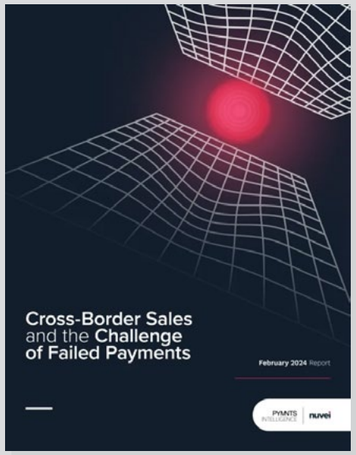
FRAUD MANAGEMENT IN **ONLINE TRANSACTIONS**

April 2024 Report

PYMNTS INTELLIGENCE | nuvei

FRAUD MANAGEMENT IN **ONLINE TRANSACTIONS**

READ MORE



February 2024

Cross-Border Sales and the Challenge of Failed Payments

PYMNTS INTELLIGENCE | nuvei

Fraud Management in Online Transactions was produced in collaboration with Nuvei, 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.

TABLE OF CONTENTS

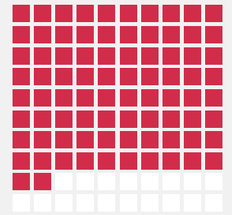
WHAT'S **AT STAKE**

Many eCommerce merchants in the United States serve international markets, making cross-border payments central to their operations. However, data breaches and failed payments disrupt smooth payments experiences for customers, erode revenue and undermine customer trust. Indeed, 8 in 10 large merchants with overseas sales confronted cyber or data breaches in the last year.

95%

Share of merchants that have recently enhanced their anti-fraud toolkits or plan to do so within the next year

82%



of merchants **experienced cyber or data breaches** in the last year.

PYMNTS Intelligence's latest study finds that nearly half of eCommerce merchants suffered financial losses and customer churn as a result of security issues. In the face of these challenges, merchants are eager to explore anti-fraud innovations in the next year. Among those that are already utilizing advanced anti-fraud measures, businesses partnering with specialized third-party providers have been particularly successful at reducing failed payment rates. Still, the widespread occurrence of security breaches and the prevalence of failed payments highlight the need for merchants to implement innovative solutions.

95%

of merchants are interested in innovating solutions to fight friendly and chargeback fraud within the next 12 months.

These are just some of the findings detailed in Fraud Management in Online Transactions, a PYMNTS Intelligence and Nuvei collaboration. This edition examines the state of play for U.S. eCommerce merchants in cross-border sales, focusing on the challenges they face in mitigating fraud and failed payments and their appetite for innovative solutions. It draws on insights from a survey of 300 heads of payments or fraud departments from international companies that operate in eCommerce conducted from Aug. 10, 2023, to Aug. 31, 2023.

This is what we learned.

KEY **FINDINGS**

01

CYBERSECURITY NEEDED

Most U.S. eCommerce merchants with international sales faced cyber and data breaches in the last year.

82%

Share of merchants that experienced cyber or data breaches in the last year

02

CUSTOMER EXPERIENCE ENHANCEMENTS

Anti-fraud tools have a significantly positive impact on customer satisfaction.

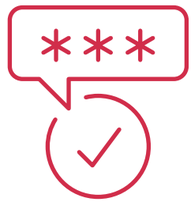
93%

Share of merchants reporting improved customer experiences after integrating anti-fraud technologies

03

2FA EFFICACY

Two-factor authentication (2FA) is highly effective for fraud prevention and reducing failed payments.



53%

Share of merchants using some form of 2FA as part of every transaction to combat fraud

04

OUTSOURCING WORKS

Outsourcing anti-fraud processes to third-party providers significantly lowers failed payment rates.

8.5%

Average failed payment rate for merchants outsourcing at least some of their anti-fraud processes, compared to 13% among those that do not outsource

PYMNTS
IN DEPTH

U.S. merchants that sell to international markets face significant challenges in cross-border payments, including high failed transaction rates.

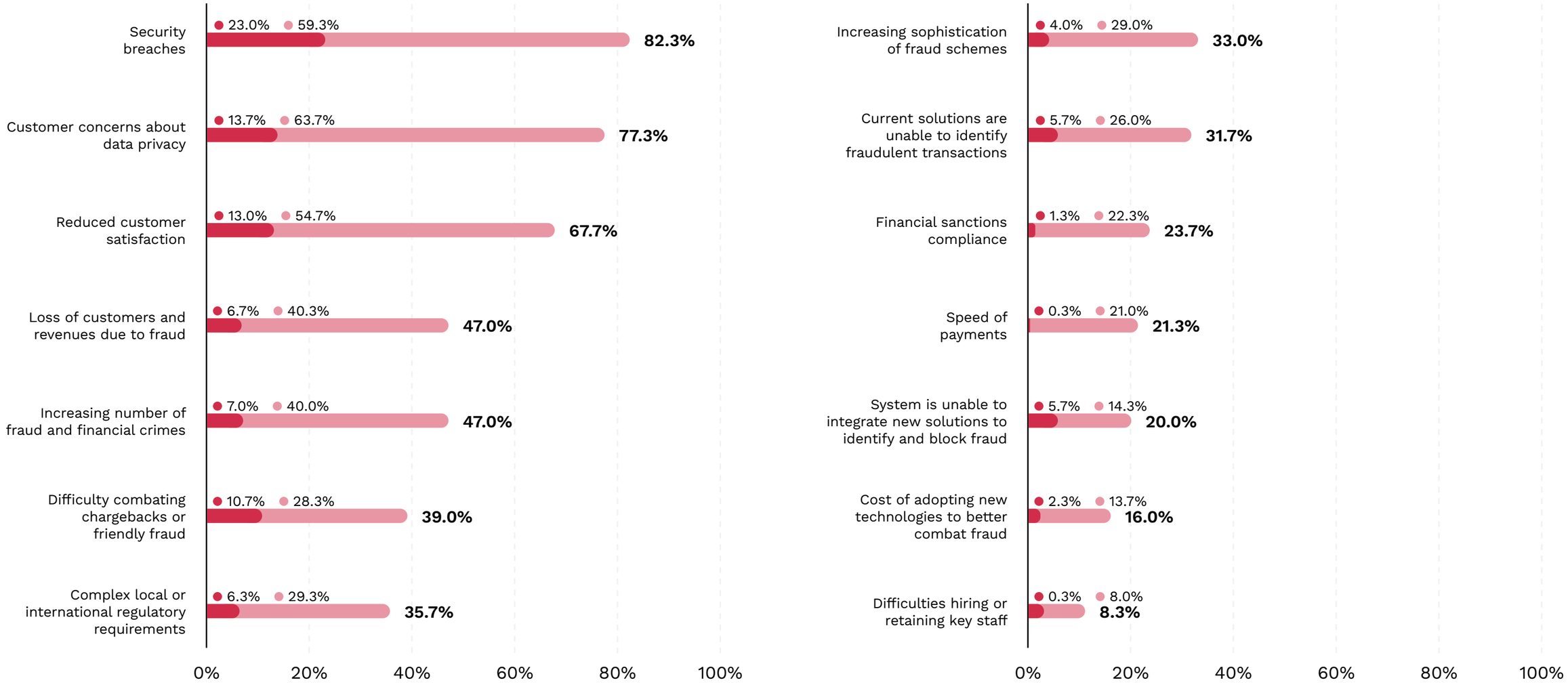
Security breaches widely impact U.S. eCommerce merchants, cutting into revenue and customer satisfaction.

PYMNTS Intelligence's research finds that 82% of U.S. eCommerce merchants with international sales suffered cyber or data breaches in the last year. These incidents often have direct financial impact, with 47% of businesses reporting lost customers and revenue as the result of fraud. Moreover, 68% of merchants experienced diminished customer satisfaction, clearly illustrating the link between security and customer retention. High-profile security breaches have ripple effects that cause more lasting reputational damage as well.

FIGURE 1:

Security challenges

Share of merchants citing select security management and fraud prevention process challenges experienced in the last 12 months, by level of challenge



Source: PYMNTS Intelligence
Fraud Management in Online Transactions, April 2024
N = 300: Complete responses, fielded Aug. 10, 2023 – Aug. 31, 2023

In response, 95% of merchants have started to enhance their anti-fraud capabilities or are planning to do so. Specifically, 41% have already begun bringing their anti-fraud toolkits up to speed, with another 54% planning to follow suit within the year. Merchants that focus on the sale of physical goods are the most proactive, with 45% currently upgrading their capabilities, versus 37% of digital services providers.

Across eCommerce businesses of different revenue sizes, the trends are broadly similar but uneven. Merchants generating between $100 million and $250 million in annual revenue are notably behind the curve, with only 31% actively upgrading their anti-fraud systems. Substantially larger shares of businesses in higher revenue brackets have anti-fraud upgrades underway, including 46% of those generating annual revenues of more than $1 billion. The stratified pace and scope of security investment likely reflects asymmetrical access to resources and expertise, with smaller merchants less willing or able to proactively invest in anti-fraud innovations.

FIGURE 2:

Merchants' anti-fraud innovation timelines

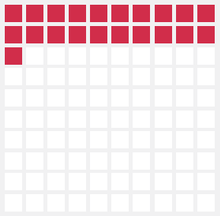
Share of merchants citing select plans about innovating tools or technologies to combat fraud

	Currently innovating	Will innovate in the next year	Will innovate, but not within the next year	Unsure or have no plans
• **Sample**	**41.0%**	**53.7%**	**4.7%**	**0.7%**
INDUSTRY				
• Digital services	37.1%	58.3%	4.0%	0.7%
• Retail	45.0%	49.0%	5.4%	0.7%
ANNUAL REVENUE				
• $1B or more	45.7%	49.3%	4.3%	0.7%
• $500M - $1B	39.0%	51.2%	9.8%	0.0%
• $250M - $500M	46.3%	51.2%	2.4%	0.0%
• $100M - $250M	30.8%	64.1%	3.8%	1.3%

Source: PYMNTS Intelligence
Fraud Management in Online Transactions, April 2024
N = 300: Complete responses, fielded Aug. 10, 2023 – Aug. 31, 2023

An effective anti-fraud toolkit does more than prevent fraud — it greatly enhances the customer experience.

Nearly every eCommerce business surveyed agreed that security innovations would enhance the customer experience, with 93% indicating positive impacts from employing these technologies. Notably, 82% of merchants identified increased consumer satisfaction as a key benefit of updating their anti-fraud toolkit, including 21% that named it the biggest advantage. This holds across businesses that focus on physical goods and digital services alike, and across revenue brackets with relatively little variation.



21%

Share of merchants citing increased **consumer satisfaction** as the biggest benefit from anti-fraud innovations

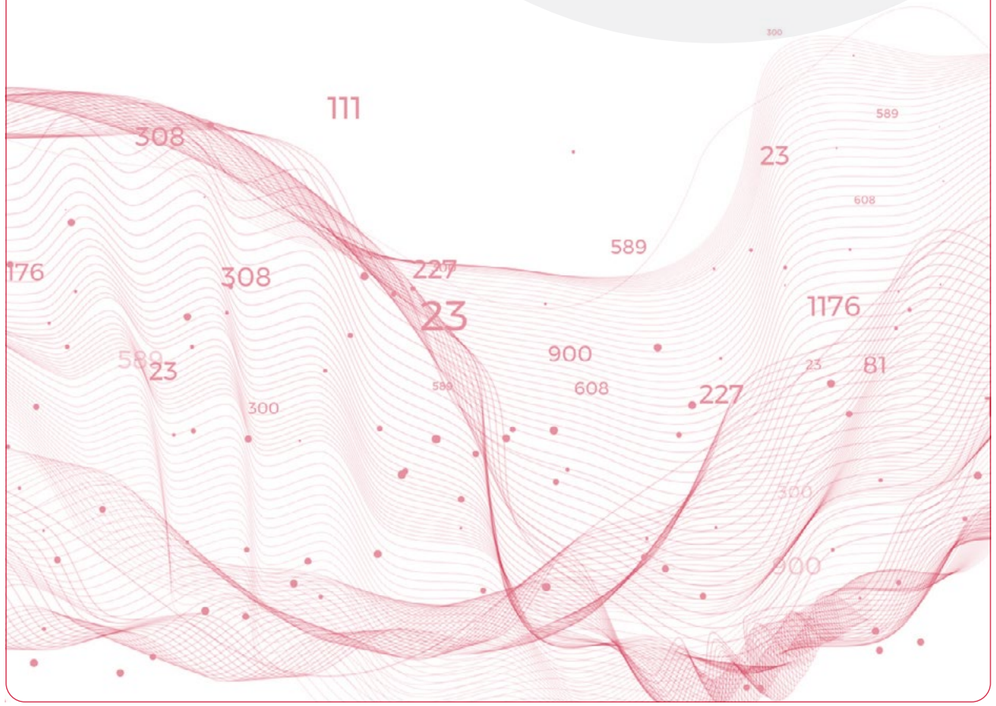
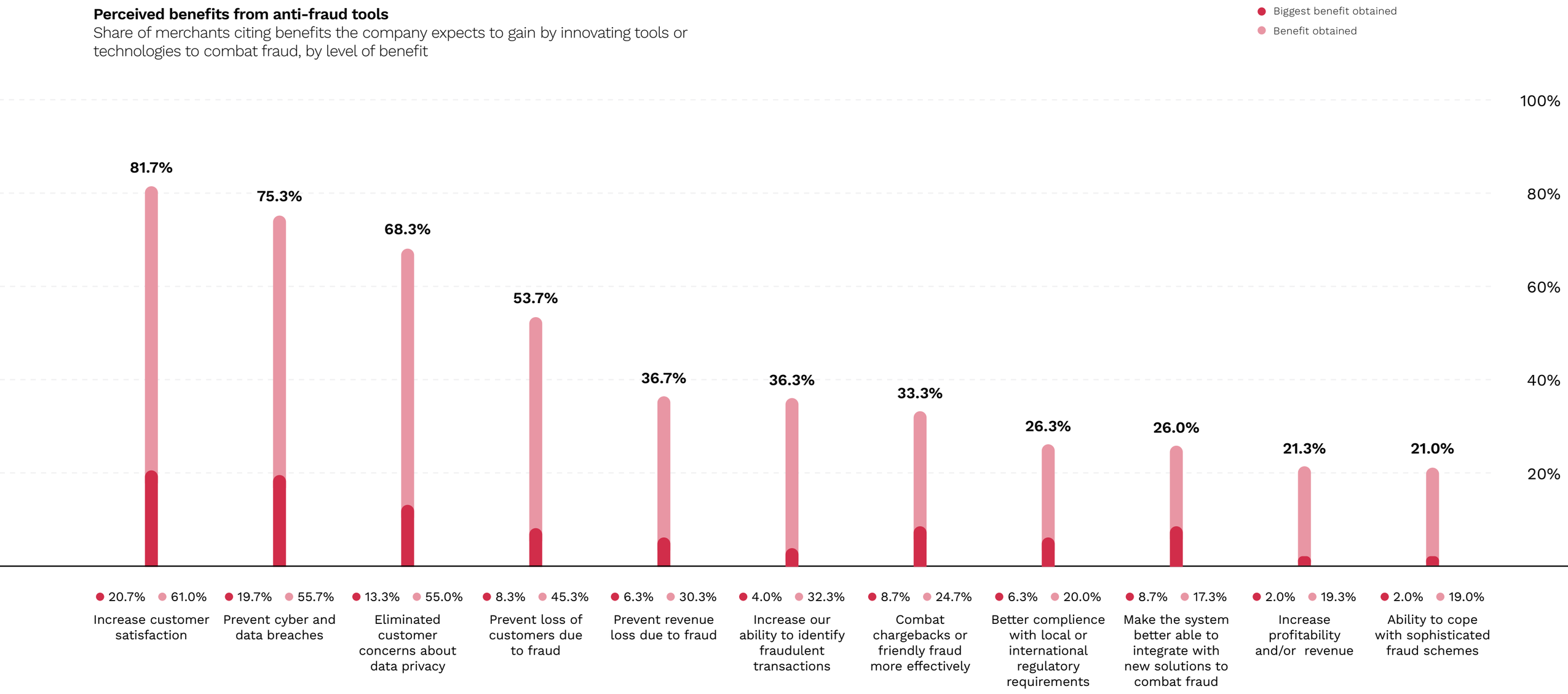


FIGURE 3:

Perceived benefits from anti-fraud tools

Share of merchants citing benefits the company expects to gain by innovating tools or technologies to combat fraud, by level of benefit



Source: PYMNTS Intelligence

Fraud Management in Online Transactions, April 2024

N = 300: Complete respondents, fielded Aug. 10, 2023 – Aug. 31, 2023

PYMNTS INTELLIGENCE | nuvei

Merchants widely point to numerous other customer experience advantages they expect to reap from anti-fraud innovations. For example, 68% cite the elimination of customer concerns about data privacy, with 13% naming it the most significant benefit. Additionally, 54% of merchants said that preventing customer loss due to fraud would be a key gain. However, the largest merchants were 11 percentage points more likely to hold this view than the smallest. While minimizing security threats is a compelling enough reason to upgrade anti-fraud technologies, the breadth of these additional benefits makes an even stronger business case for innovation.

FIGURE 4:

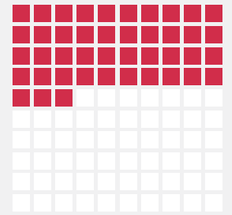
Top benefits of anti-fraud innovation
Share of merchants citing the top five benefits the company expects to gain by innovating fraud prevention tools or technologies, by annual revenue

	$100M - $250M	$250M - $500M	$500M - $1B	$1B or more
• Increase customer satisfaction	82.1%	80.5%	82.9%	81.4%
• Prevent cyber and data breaches	78.2%	80.5%	78.0%	71.4%
• Eliminate customer concerns about data privacy	73.1%	70.7%	73.2%	63.6%
• Prevent loss of customers due to fraud	47.4%	58.5%	46.3%	57.9%
• Increase our ability to identify fraudulent transactions	35.9%	41.5%	29.3%	37.1%
• Prevent revenue loss due to fraud	33.3%	34.1%	43.9%	37.1%
• Combat friendly or chargeback fraud more effectively	28.2%	34.1%	31.7%	36.4%
• Make the system better able to integrate with new solutions to combat fraud	24.4%	26.8%	17.1%	29.3%
• Better compliance with local or international regulatory requirements	25.6%	36.6%	19.5%	25.7%
• Increase profitability and/or revenue	11.5%	9.8%	31.7%	27.1%
• Ability to cope with sophisticated fraud schemes	17.9%	24.4%	34.1%	17.9%

Source: PYMNTS Intelligence
Fraud Management in Online Transactions, April 2024
N = 300: Complete responses, fielded Aug. 10, 2023 – Aug. 31, 2023

2FA for each transaction is not only the most effective anti-fraud method but also the one that delivers the lowest failed payments rates.

PYMNTS Intelligence consistently finds that 2FA is an effective security measure across different industries and use cases — but not all 2FA is equally potent. Merchants rank per-transaction 2FA, in which shoppers must authenticate each checkout, as the most effective security measure for preventing fraud of the 10 included in our survey. Among the businesses that have adopted per-transaction 2FA, 43% regard it as their most effective security method. Transaction confirmation notifications takes second place, at 37%, among those that use it. Notably, just 22% of merchants that implement 2FA at login rate this as their most effective method, reflecting the greater efficacy of requiring authentication with each purchase rather than just once per login, especially since users can often remain signed in across many sessions.



43%

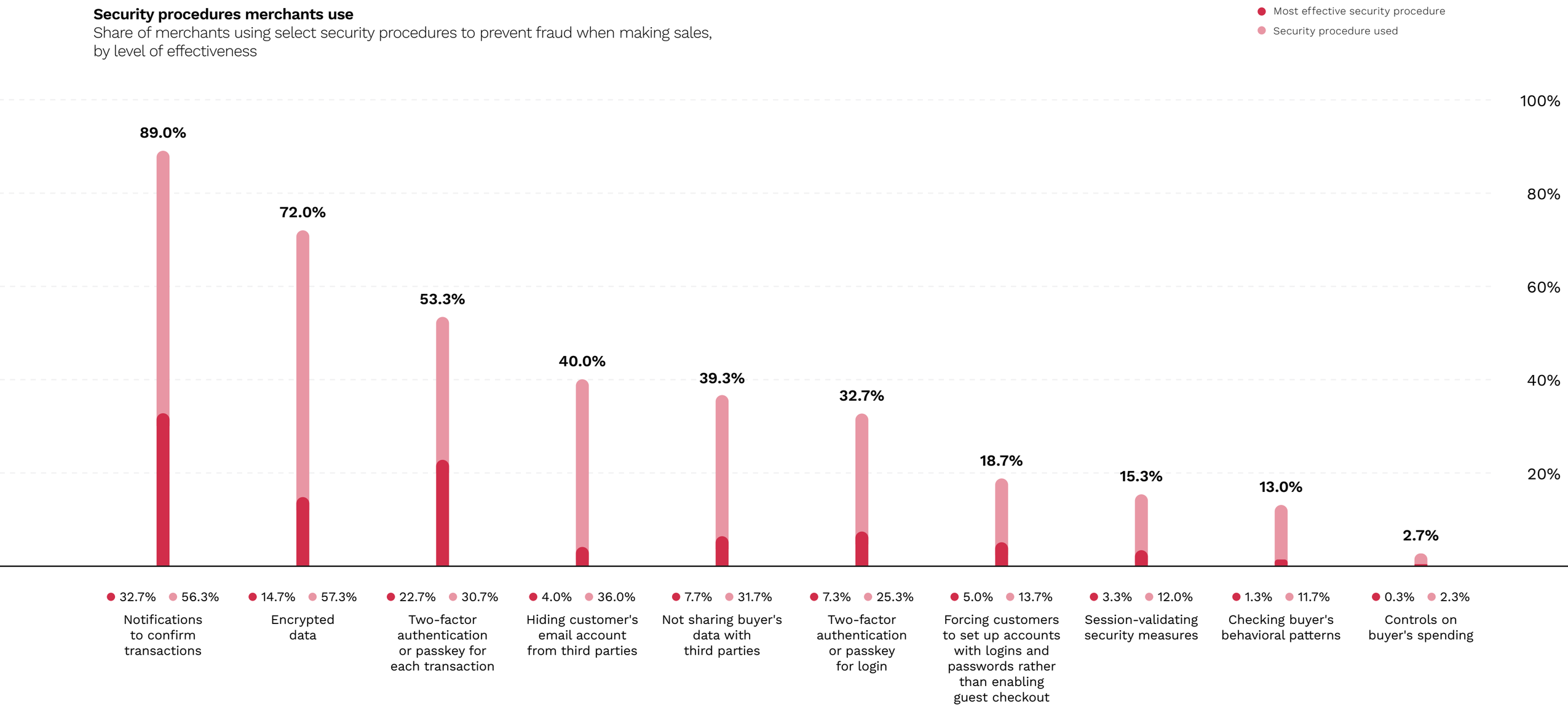
Share of merchants using **per-transaction 2FA** that identify it as their most effective security method

However, just 53% of merchants utilize per-transaction 2FA. Although it is the third-most common security method, nearly half of eCommerce businesses are not benefiting from this highly effective technology. Merchants that have not yet implemented per-transaction 2FA should evaluate its potential to significantly reduce fraud, enhance overall security and boost customer satisfaction.

FIGURE 5:

Security procedures merchants use

Share of merchants using select security procedures to prevent fraud when making sales, by level of effectiveness



Source: PYMNTS Intelligence
Fraud Management in Online Transactions, April 2024
N = 300: Complete respondents, fielded Aug. 10, 2023 – Aug. 31, 2023

PYMNTS INTELLIGENCE | nuvei

Per-transaction 2FA is not only the most effective fraud prevention measure but it is also the most effective measure for minimizing failed transactions. Merchants implementing 2FA for each transaction reported a failed payments rate of just 10.3% — the lowest among the 10 security methods in our survey. Even highly effective transaction confirmation notifications have a slightly higher failed payments rate of 10.8%. We also note that 2FA at the point of login does not yield the same results, with businesses using this method reporting much higher failed payment rates of 12%.

FIGURE 6:

Security procedures and failed payment rates

Average failed payment rate merchants using select security procedures reported

10.3%
2FA or passkey for each transaction

10.8%
Notifications to confirm transactions

11.0%
Forcing customers to set up accounts with logins and passwords rather than enabling guest checkout

11.4%
Session-validating security measures

11.6%
Hiding customers' email accounts from third parties

11.7%
Encrypted data

12.0%
2FA or passkey for login

12.5%
Not sharing buyers' data with third parties

12.7%
Controls on buyer's spending

12.9%
Checking buyer's behavioral patterns

Source: PYMNTS Intelligence
Fraud Management in Online Transactions, April 2024
N varies based on the number of merchants using each procedure, fielded Aug. 10, 2023 – Aug. 31, 2023

Outsourcing fraud prevention to third-party providers can be a powerful strategy for reducing failed payments.

Merchants use a variety of tools and strategies to combat fraud. Cloud-based platforms specifically designed to detect fraud and financial crimes lead the pack as the most popular security tool, with 63% of businesses surveyed leveraging these platforms. Models using either machine learning (ML) or artificial intelligence (AI) are also widely implemented, at 45%, as are deep learning systems, at 37%. Across all three technologies, merchants in higher revenue brackets generally tend to have higher implementation rates.

FIGURE 7:

Use of security tools and methods

Share of merchants citing tools or methods that the company currently use to combat fraud, by annual revenue

	SAMPLE	$100M - $250M	$250M- $500M	$500M - $1B	$1B or more
• Cloud-based fraud and financial crimes platform	63.3%	60.3%	73.2%	65.9%	61.4%
• ML or AI models	45.3%	34.6%	53.7%	41.5%	50.0%
• Outsourcing the process to third-party service providers	44.3%	48.7%	48.8%	53.7%	37.9%
• Deep learning systems	36.7%	32.1%	29.3%	24.4%	45.0%
• Manual processes and procedures developed in-house	17.0%	14.1%	9.8%	24.4%	18.6%
• SaaS or hosted service (without fully outsourcing the process)	14.0%	11.5%	17.1%	17.1%	13.6%
• Technology developed in-house	9.0%	2.6%	7.3%	4.9%	14.3%

Source: PYMNTS Intelligence
Fraud Management in Online Transactions, April 2024
N = 300: Complete responses, fielded Aug. 10, 2023 – Aug. 31, 2023

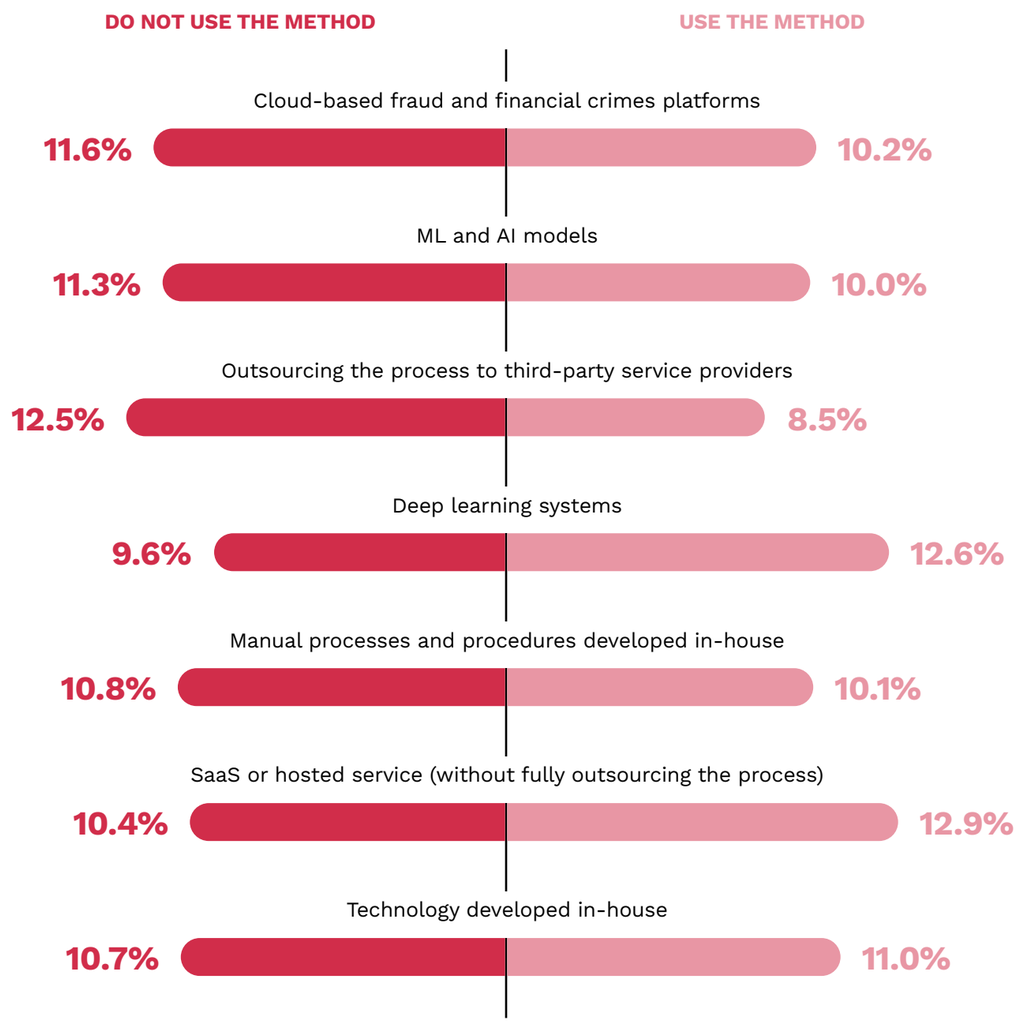
Importantly, PYMNTS Intelligence finds that leveraging external expertise results in lower rates of failed payments. Forty-four percent of merchants outsource at least a portion of their fraud prevention operations to specialized third-party providers. Those in this group report a dramatically lower average failed payment rate of just 8.5% — 32% lower than the 13% rate experienced by businesses that handle all their anti-fraud efforts internally.

Other variations in strategic approach appear to yield little or no benefit in terms of failed payments rates. For example, businesses that develop their own anti-fraud technology report an average failed payments rate of 11%, versus 10.7% for those that use only third-party tools. These findings highlight the need for eCommerce merchants to carefully review their anti-fraud strategies and leverage third-party expertise to maximize their capabilities.

FIGURE 8:

Failed payment rates of key security strategies

Average failed payments rate merchants reported, by whether they use select fraud prevention methods



Source: PYMNTS Intelligence
Fraud Management in Online Transactions, April 2024
N = 300: Complete responses, fielded Aug. 10, 2023 – Aug. 31, 2023

DATA FOCUS

Friendly and chargeback fraud are persistent challenges facing U.S. eCommerce merchants.

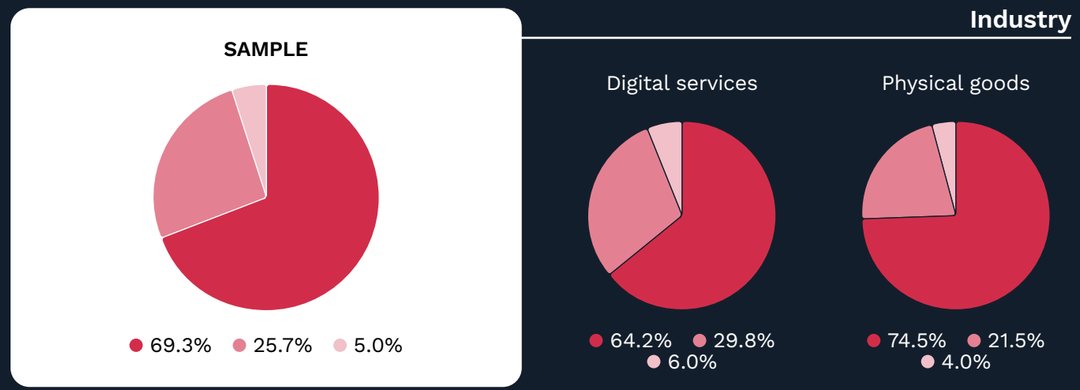
The majority of U.S. eCommerce merchants are ready for innovative solutions to tackle friendly and chargeback fraud.

PYMNTS Intelligence finds that nearly all U.S. eCommerce merchants with international sales want to improve their ability to combat friendly and chargeback fraud. Ninety-five percent are interested in innovating solutions in this area in the next 12 months, with 69% very or extremely interested. High levels of interest hold across merchants in all revenue brackets included in our study. Physical goods merchants demonstrate particularly strong interest: 75% say they are very or extremely interested, compared to 64% of their digital services counterparts who said the same. These trends signal an industrywide readiness to invest in more effective solutions to prevent friendly or chargeback fraud.

FIGURE 9:

Level of interest in innovating solutions

Share of merchants reporting how interested they are in innovating solutions to combat friendly or chargeback fraud in the next 12 months, by business demographic



Source: PYMNTS Intelligence

Fraud Management in Online Transactions, April 2024

N = 300: Complete respondents, fielded Aug. 10, 2023 – Aug. 31, 2023

ACTIONABLE INSIGHTS

01

Prioritize an immediate and comprehensive review of security measures to counteract the escalating threat of cyber and data breaches and make investments that address any gaps. By implementing a multifaceted approach that includes both upgrading existing anti-fraud capabilities and adopting new, innovative solutions, businesses can mitigate financial losses and customer churn, ultimately safeguarding their market position and customer trust.

02

Leverage anti-fraud technologies that also address consumer concerns about data privacy and transaction safety. Introducing user-friendly authentication methods or transparent data protection policies can create more engaging shopping experiences, fostering loyalty and encouraging repeat business. Indeed, embracing anti-fraud solutions as central to customer service and retention will maximize the impact of these efforts.

03

Implement 2FA for each transaction as well as at login, making this a cornerstone of fraud prevention. An audit of existing security processes and customer transaction data could help businesses pinpoint the optimal step in purchase journeys in which requiring 2FA would introduce minimal frictions, ensuring a balance between robust security and a smooth customer experience.

04

Consider partnering with specialized third-party providers that can deliver expert solutions. By doing so, eCommerce businesses can reduce failed payment rates and boost overall transaction security. This will have knock-on effects that improve operational efficiency and achieve greater customer satisfaction.

FRAUD MANAGEMENT IN ONLINE TRANSACTIONS

April 2024 Report

PYMNTS INTELLIGENCE | nuvei

METHODOLOGY

Fraud Management in Online Transactions, a PYMNTS Intelligence and Nuvei collaboration, is based on survey of 300 executives from eCommerce merchants selling both inside and outside the U.S. that generate annual revenues of more than $100 million and who have deep knowledge of their companies' payments systems. The survey was conducted from Aug. 10, 2023, to Aug. 31, 2023. This edition examines the ongoing challenges U.S. eCommerce merchants face when trying to mitigate fraud and failed payments in their cross-border sales as well as their appetite for innovative solutions to these challenges.

THE PYMNTS INTELLIGENCE TEAM THAT PRODUCED THIS REPORT

Scott Murray
SVP and Head of Analytics

Daniel Gallucci
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.

nuvei

Nuvei (Nasdaq: NVEI) (TSX: NVEI) is the Canadian FinTech company accelerating the business of clients around the world. Nuvei's modular, flexible and scalable technology allows leading companies to accept next-gen payments, offer all payout options and benefit from card issuing, banking, risk and fraud management services.

Connecting businesses to their customers in more than 200 markets, with local acquiring in 45+ markets, 150 currencies and 634 alternative payment methods, Nuvei provides the technology and insights for customers and partners to succeed locally and globally with one integration.

For more information, visit www.nuvei.com

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.