

# The Role of Fraud Screening in Minimizing Failed Payments

January 2024 Report

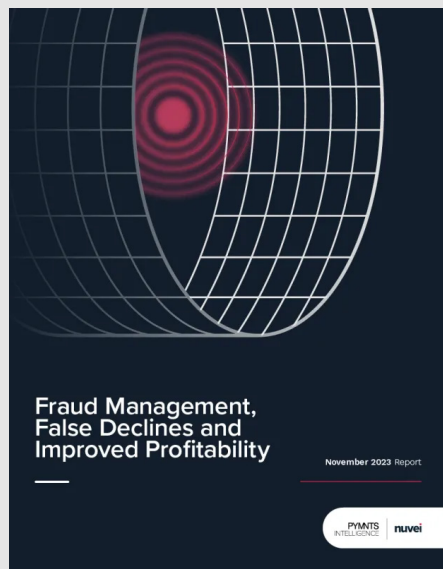
PYMNTS  
INTELLIGENCE

nuvei

# THE ROLE OF FRAUD SCREENING IN MINIMIZING FAILED PAYMENTS

---

READ MORE \_\_\_\_\_



■ November 2023

**Fraud Management, False Declines and Improved Profitability**



The Role of Fraud Screening in Minimizing Failed Payments 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.

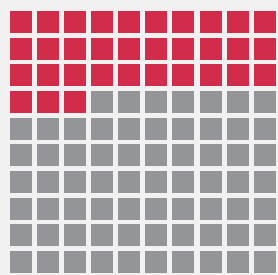
## TABLE OF CONTENTS

---

What’s at Stake . . . . .	04
Key Findings . . . . .	06
PYMNTS in Depth . . . . .	10
Actionable Insights . . . . .	22
Methodology . . . . .	25

# WHAT'S AT STAKE

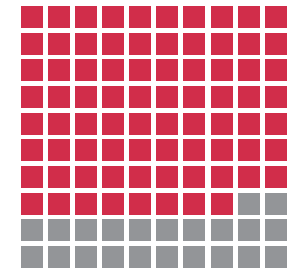
**M**any eCommerce merchants fail to connect the dots between fraud detection and failed payments. This oversight not only heightens the risk of lost sales but also signifies a missed opportunity for improving payment success rates, underscoring the urgency for a more comprehensive approach to fraud prevention. Despite the growing complexities of securely processing digital transactions, only one-third of merchants employ mechanisms that detect potential fraud as the cause of failed payments.



# 33%

of eCommerce merchants **utilize mechanisms to identify potential fraud** as the cause of failed payments.

# 78%



of merchants with minimal or no PSP collaboration are actively seeking **innovative solutions to combat friendly and chargeback fraud.**

PYMNTS Intelligence's latest study also highlights the critical role of collaboration between payment service providers (PSPs) and eCommerce merchants in deploying effective fraud prevention strategies. Merchants with greater levels of PSP collaboration show a markedly higher rate of adopting screening mechanisms that identify potential fraud as the cause of failed payments than do those with minimal or no collaborative involvement. These partnerships are crucial for balancing security with seamless customer experiences.

These are just some of the findings detailed in *The Role of Fraud Screening in Minimizing Failed Payments*, a PYMNTS Intelligence and Nuvei collaboration. This edition examines the efficacy of the fraud screening mechanisms eCommerce merchants use and draws on insights from a survey of 300 heads of payments or fraud departments from international eCommerce companies conducted from Aug. 10, 2023, to Aug. 31, 2023.

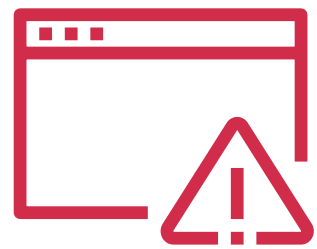
**This is what we learned.**

# KEY FINDINGS

## 01

### ADOPTION DISPARITIES

Smaller merchants generating revenues between \$100 million and \$250 million trail far behind their larger counterparts in the adoption of screening mechanisms to detect potential fraud as the cause of failed payments.



# 17%

Share of smaller merchants that utilize failed payment screening tools to detect potential fraud as the cause

## 02

### PSP COLLABORATION

Extensive collaboration with PSPs is a strong determinant of merchants' implementation of fraud screening mechanisms.



# 41%

Share of merchants collaborating extensively with PSPs that have adopted tools for identifying potential fraud as the cause of failed payments

## 03

## BALANCING SECURITY

Merchants strive to balance security with customer experience by encouraging reattempts on fraud-flagged transactions.



# 85%

Share of merchants that extensively collaborate with their PSPs and encourage customers to reattempt purchases even when they are flagged for fraud

## 04

## SEEKING FRAUD SOLUTIONS

Merchants' interest in innovative solutions to combat friendly fraud or chargeback fraud varies and is more pronounced among those that receive less PSP support.



# 78%

Share of merchants that collaborate minimally with PSPs but show high interest in innovative solutions for minimizing friendly and chargeback fraud

# PYMNTS IN DEPTH

**Most eCommerce merchants neglect the connection between potential fraud and failed payments, compromising both payment security and the customer experience.**

## Only 33% of merchants have systems to detect whether potential fraud is the cause of failed payments.

Despite heightened focus on preventing fraud, online merchants widely ignore the connection between this issue and failed payments. Just 33% of eCommerce merchants surveyed utilize mechanisms that screen for potential fraud as the cause of failed payments. In contrast, 79% have systems to identify data entry errors as the reason transactions fail. This suggests a pressing need for a more balanced approach that improves overall payment success rates.

We also see a substantial gap in the adoption of screening tools based on merchant size. Among smaller merchants, just 17% of those generating revenues between \$100 million and \$250 million had mechanisms in place to detect fraud as the cause of failed payments, compared to 39% of large merchants generating more than \$1 billion in revenue. This highlights not only the resource gap in fraud detection capabilities but also the need for scalable, accessible solutions for smaller merchants.

**FIGURE 1:**

**Screening for causes of failed payments**

Share of firms citing the use of screening mechanisms to identify whether a failed payment is due to potential fraud or a typo, by annual revenue

	Sample	\$1B or more	\$500M - \$1B	\$250M - \$500M	\$100M - \$250M
• Potential fraud	10.7%	7.9%	14.6%	17.1%	10.3%
• Potential typo	56.3%	60.0%	58.5%	51.2%	51.3%
• Both potential fraud and typos	22.3%	30.7%	24.4%	22.0%	6.4%
• Do not have a screening mechanism	10.7%	1.4%	2.4%	9.8%	32.1%

Source: PYMNTS Intelligence

The Role of Fraud Screening in Minimizing Failed Payments, January 2024

N = 300: Whole sample, fielded Aug. 10, 2023 – Aug. 31, 2023

## Why should merchants care about what causes failed payments?



**Increased failed payments recovery:**

Merchants that know why payments fail can better target recovery methods.



**Analytics for improvement:** Data on the causes of failed payments can reveal gaps in product design, payment systems or security policies.



**Customer retention and loyalty:** Failed payments cause frictions that can affect customer satisfaction, risking loyalty and retention.



**Resource allocation:** Merchants that know why payments fail can better allocate resources and reduce internal strain.



**Revenue loss:** Failed payments can cause revenue loss if consumers abandon the transaction and take their business to other merchants.

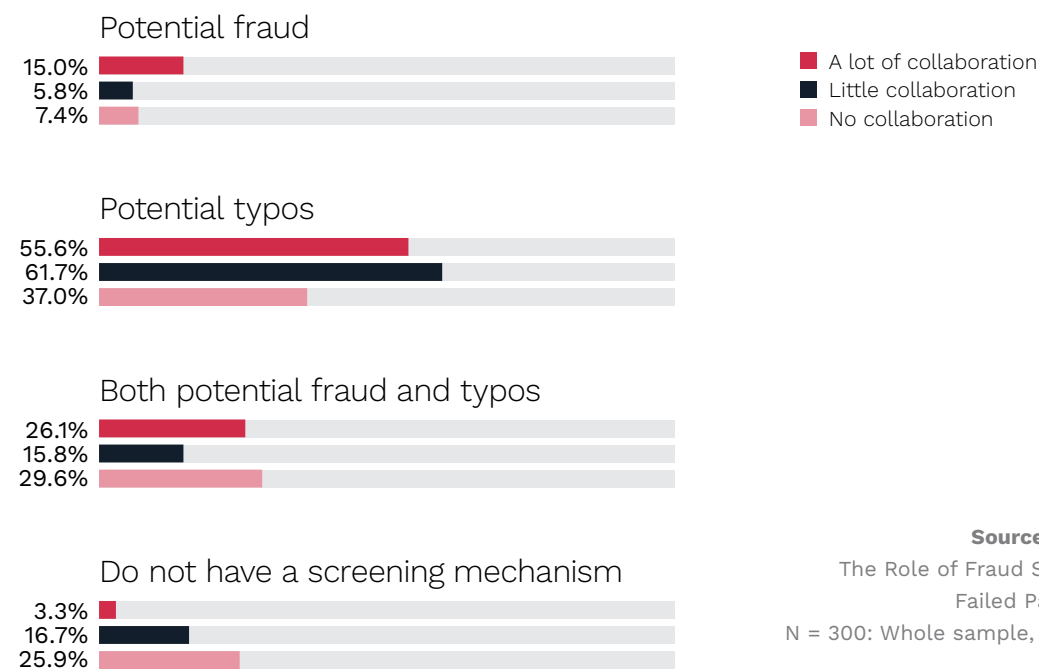
# Collaboration with PSPs helps merchants optimize their fraud prevention efforts to reduce failed payments.

The role of PSPs in enhancing fraud detection is increasingly crucial. Forty-one percent of merchants that collaborate extensively with their PSPs have implemented screening mechanisms to detect potential fraud as a cause of failed payments — higher than the 37% of those with no PSP collaboration and significantly higher than the 22% of those that minimally collaborate. PSPs play a pivotal role in enabling merchants to navigate online payment security complexities as well as failed payment prevention and recovery.

FIGURE 2:

## Collaboration and types of failed payment screening mechanisms

Share of merchants with select screening mechanisms, by level of PSP collaboration



Source: PYMNTS Intelligence  
The Role of Fraud Screening in Minimizing Failed Payments, January 2024  
N = 300: Whole sample, fielded Aug. 10, 2023 – Aug. 31, 2023





# Merchants balance transaction security with the customer payment experience when handling transactions flagged as fraudulent.

To prevent lost sales, merchants can encourage customers to reattempt purchases using the same payment method initially flagged as potentially fraudulent. The right screening strategy will minimize resulting friction and maximize recovered transactions. Eighty-five percent of merchants with deep levels of collaboration with PSPs engage in this practice, while just 70% of those with minimal or no PSP collaboration do so. The merchants with high PSP collaboration are also much less likely to enforce increased security checks on these customers — much lower than the 70% of merchants lacking any collaborative relationship with their PSPs that do the same. This indicates that PSP collaboration helps merchants find the right balance between fraud prevention and blocked transactions.

**FIGURE 3:**

### Responses to potentially fraudulent transactions

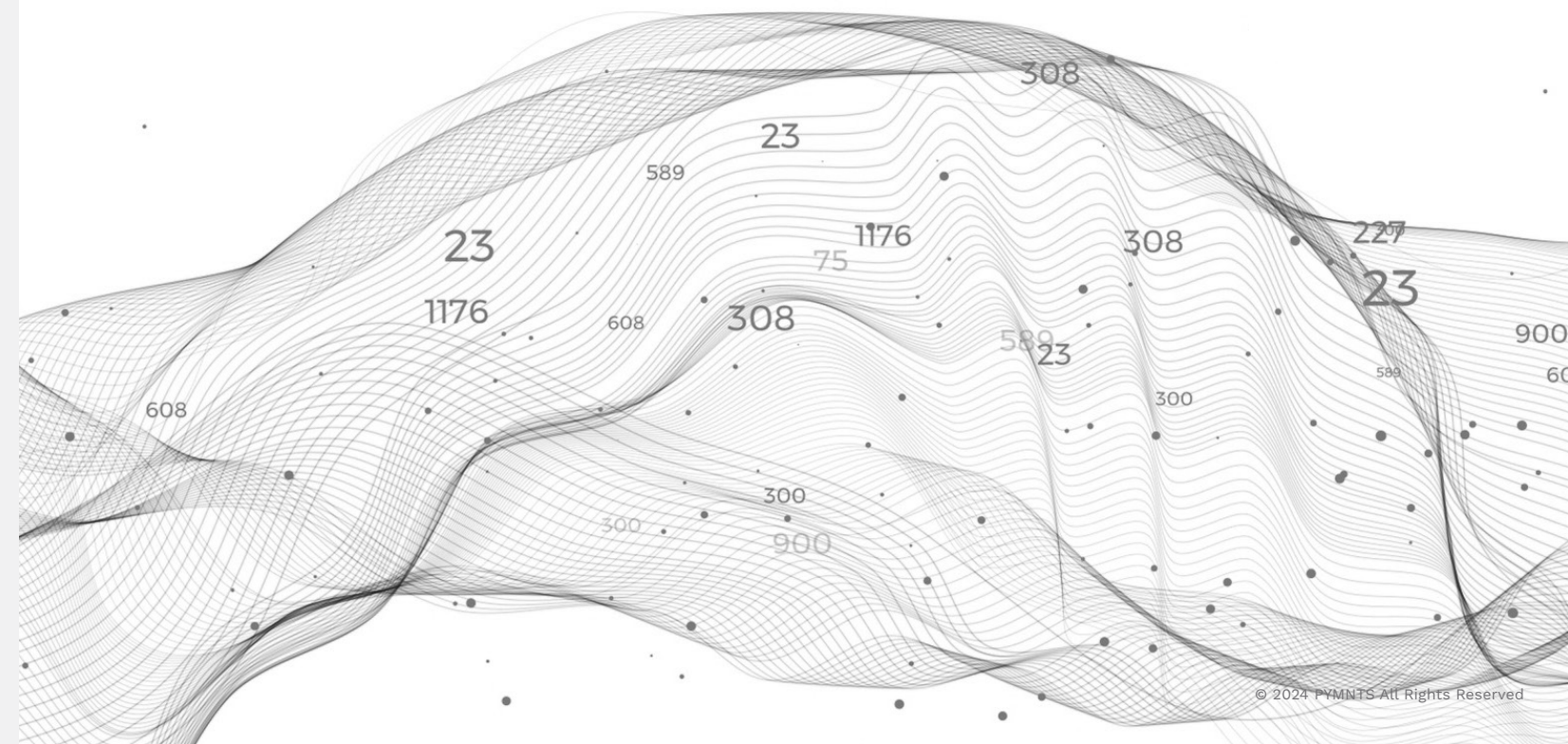
Share of firms that take select actions when failed payments are flagged as potentially fraudulent, by level of PSP collaboration

	Sample	A lot of collaboration	Little collaboration	No collaboration
• Encourage the customer to purchase again using the same payment method	79.6%	84.8%	70.4%	70.0%
• Increase security level and ask customer to purchase again	41.7%	37.9%	40.7%	70.0%
• Unilaterally cancel the transaction	11.7%	7.6%	18.5%	20.0%
• Discourage the customer from trying the transaction again	5.8%	4.5%	3.7%	20.0%

Source: PYMNTS Intelligence

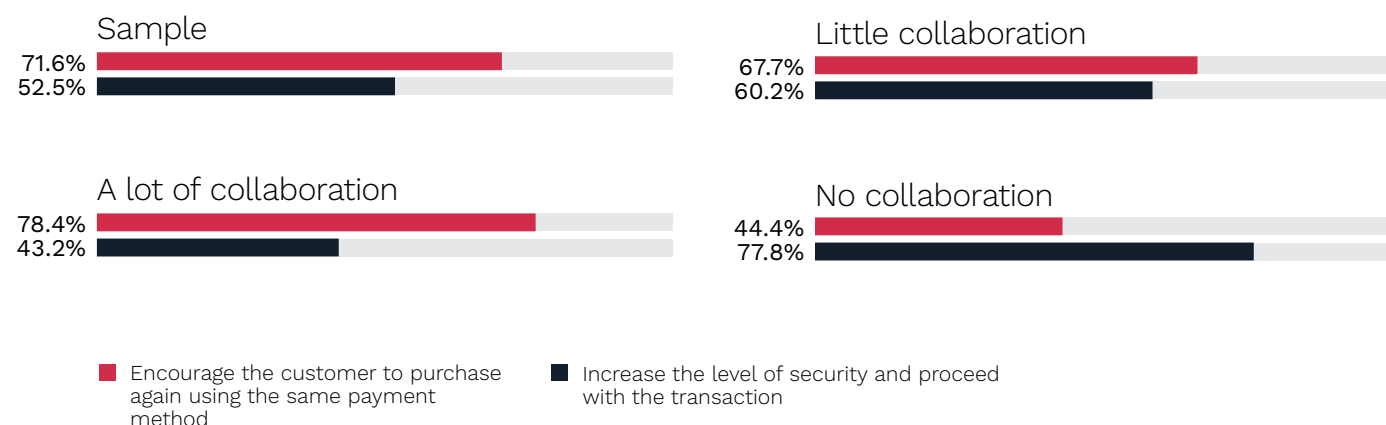
The Role of Fraud Screening in Minimizing Failed Payments, January 2024

N = 105: Firms that have a screening mechanism for potential fraud, fielded Aug. 10, 2023 – Aug. 31, 2023



A similar pattern plays out for input errors. Among merchants collaborating extensively with their PSP, 78% encourage consumers to reattempt failed payments flagged as potentially caused by a typo. This share declines to 68% for those with minimal collaboration and plummets to 44% for merchants reporting no collaborative relationship with their PSPs. The data reveals a significant difference in strategy: PSP-collaborating merchants lean toward enhancing customer convenience and reducing friction, while non-collaborators appear more inclined to prioritize security measures, even at the expense of lost sales and frustrated consumers.

**FIGURE 4:**  
**Responses to transactions flagged as typos**  
 Share of firms citing which actions they take in cases of failed payments caused by input errors, by level of PSP collaboration



Source: PYMNTS Intelligence

The Role of Fraud Screening in Minimizing Failed Payments, January 2024

N = 238: Firms that have a screening mechanism for potential typos, fielded Aug. 10, 2023 – Aug. 31, 2023

**78%**

of merchants collaborating extensively with PSPs encourage customers to reattempt failed payments potentially caused by a typo.

## Merchant interest in solutions to fight friendly fraud varies by intensity of PSP collaboration.

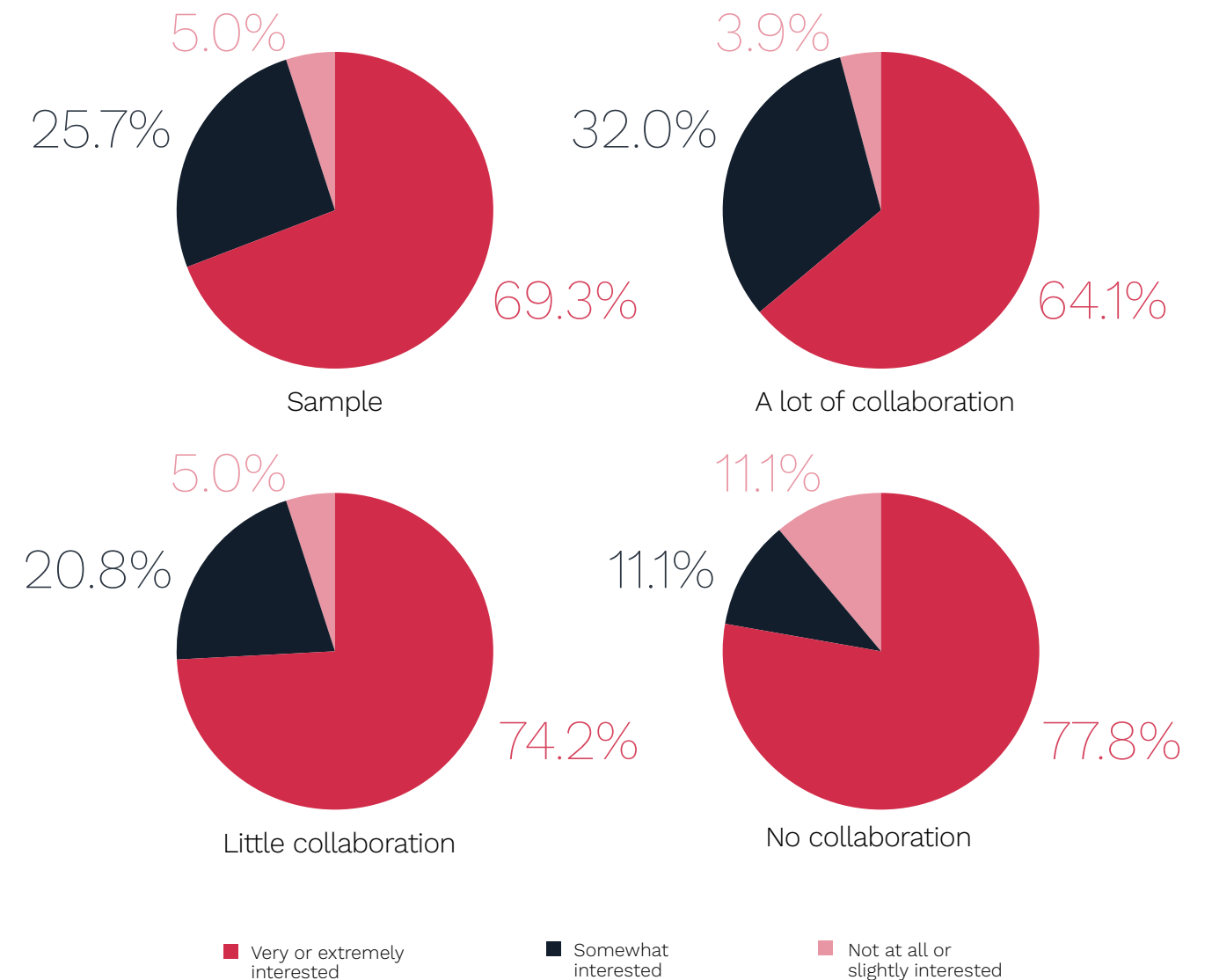
Approximately 70% of merchants show significant interest in innovative solutions to combat friendly and chargeback fraud. This interest is more pronounced among merchants with minimal or no PSP collaboration, at 74% and 78%, respectively. This indicates a pressing demand for fraud prevention technologies, particularly among merchants operating without extensive PSP support.

Conversely, only 64% of merchants that collaborate extensively with PSPs expressed strong interest in innovating solutions to minimize such fraud. This relatively tepid demand suggests that these merchants already benefit from comprehensive fraud management tools provided through their existing PSP relationships.

**FIGURE 5:**

### Interest in solutions to fight friendly and chargeback fraud

Share of firms interested in innovating solutions to combat friendly or chargeback fraud in the next 12 months, by level of PSP collaboration



Source: PYMNTS Intelligence

The Role of Fraud Screening in Minimizing Failed Payments, January 2024

N = 300: Whole sample, fielded Aug. 10, 2023 – Aug. 31, 2023

# ACTIONABLE INSIGHTS



## 01

For smaller merchants, investing in scalable fraud screening tools is critical. These solutions not only harden payment security but also are likely to improve conversion rates — especially important for merchants aiming to better compete in the digital economy.



## 02

Strengthening collaboration with PSPs is vital for enhancing fraud detection. Merchants should actively seek partnerships with PSPs to access advanced fraud screening tools and expertise. Collaboration can significantly improve a merchant's ability to manage online payment security and prevent fraud, which will ultimately benefit their bottom line.



## 03

Merchants need to balance transaction security with customer experience, particularly for transactions flagged as potentially fraudulent. Prioritizing strategies that reduce payment friction, such as allowing reattempts on flagged transactions, can enhance customer satisfaction. However, this should be coupled with robust security protocols, especially for merchants with limited PSP collaboration, to maintain an optimal balance between security and customer convenience.



## 04

Merchants with minimal PSP support should actively seek partnerships with technology providers that specialize in advanced fraud detection and prevention. These collaborations can help merchants gain insights into fraud prevention best practices and access to the latest tools. Doing so will help them stay ahead as digital payment and lost payments recovery technologies and strategies continue to evolve rapidly.

# The Role of Fraud Screening in Minimizing Failed Payments

January 2024 Report

PYMNTS  
INTELLIGENCE | nuvei

## METHODOLOGY

**T**he Role of Fraud Screening in Minimizing Failed Payments, a PYMNTS Intelligence and Nuvei collaboration, is based on survey conducted from Aug. 10, 2023, to Aug. 31, 2023, of 300 executives from eCommerce firms selling both inside and outside the U.S. that generate annual revenues of more than \$100 million and who have deep knowledge of their company's payments systems. This edition examines the efficacy of the fraud screening mechanisms eCommerce merchants use.

### The PYMNTS Intelligence Team That Produced This Report:

**Scott Murray**  
SVP and Head of Analytics

**Jimena Ferraro, PhD**  
Senior Analyst

**Daniel Gallucci**  
Senior Writer

# 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.

**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](http://www.nuvei.com)

The Role of Fraud Screening in Minimizing Failed Payments 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.

---

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).