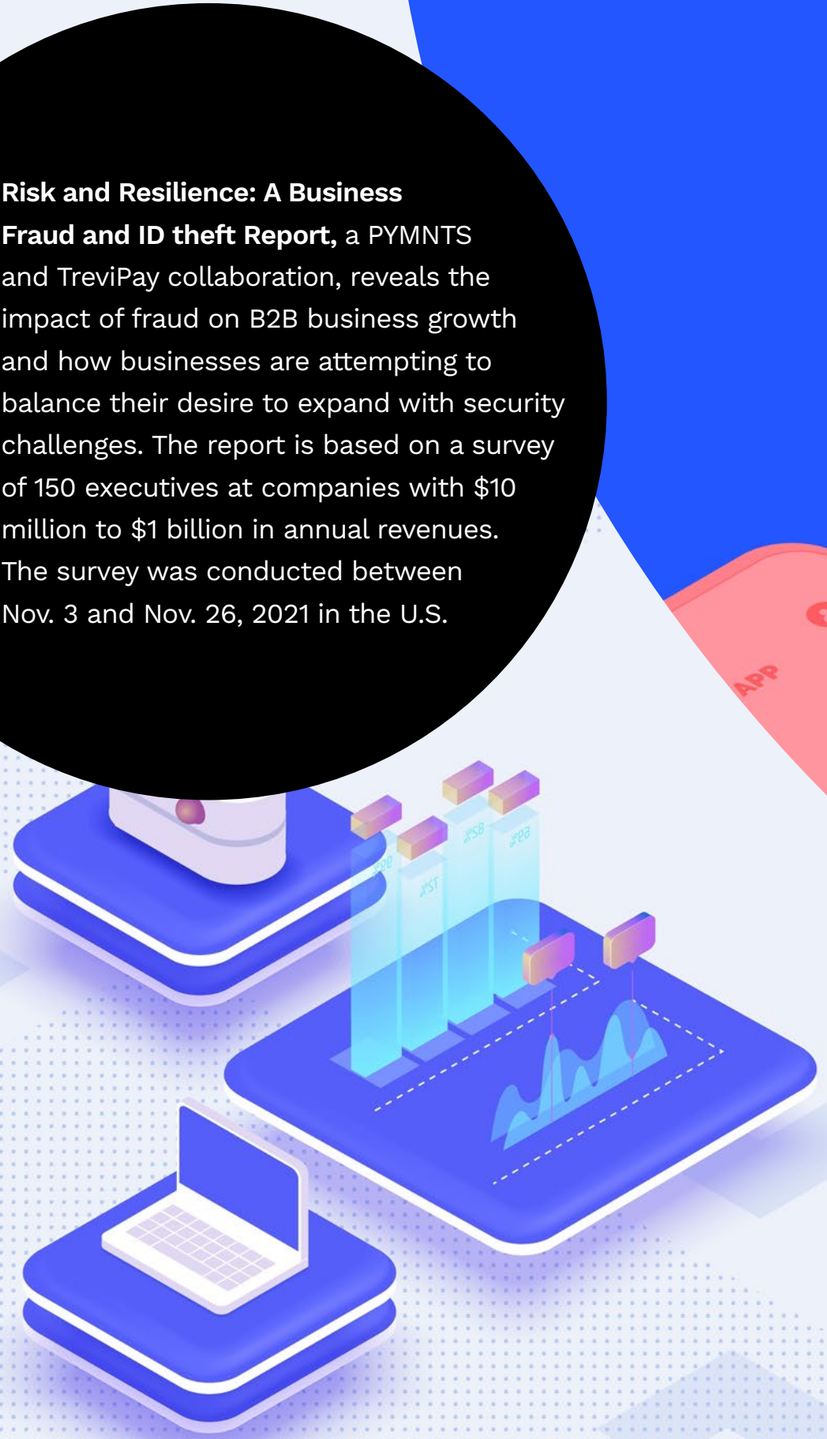
RISK AND RESILIENCE

A BUSINESS FRAUD AND ID THEFT REPORT

Risk and Resilience: A Business Fraud and ID theft Report, a PYMNTS and TreviPay collaboration, reveals the impact of fraud on B2B business growth and how businesses are attempting to balance their desire to expand with security challenges. The report is based on a survey of 150 executives at companies with $10 million to $1 billion in annual revenues. The survey was conducted between Nov. 3 and Nov. 26, 2021 in the U.S.



PYMNTS.com | trevi pay

RISK AND RESILIENCE

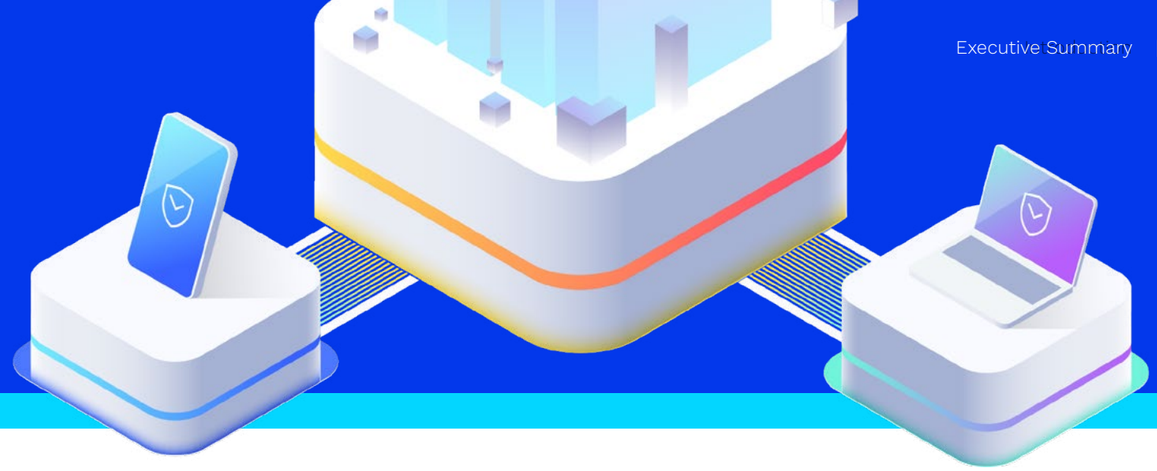
A BUSINESS FRAUD AND ID THEFT REPORT

PYMNTS.com | trevi pay

Risk and Resilience: A Business Fraud and ID Theft Report was produced in collaboration with TreviPay, and PYMNTS is grateful for the company's support and insight. **PYMNTS.com** retains full editorial control over the following findings, methodology and data analysis.

TABLE OF CONTENTS

EXECUTIVE SUMMARY



The pandemic inspired a wave of digital innovation as retailers, manufacturers and marketplaces adopted digital tools to make it easier for consumers and business-to-business (B2B) clients to pay and receive funds online. With payments modernization came risk: many businesses were inexperienced in the eCommerce space and lacked the technical and human resources to enact a comprehensive anti-fraud strategy.

In addition, many also were unable to find the right third-party technical solution before they went to market, meaning as their businesses scaled, their vulnerability, especially to scams such as ID theft, increased.[1] B2B businesses in particular have faced increased risks as they make new digital payment options available. Notably, cybercriminals' fraud attack volumes have increased by more than 150% in 2021 alone.[2] PYMNTS' research also shows that 98% of businesses experienced financial losses as a result of successful fraud attacks last year.

Fraud is a universal issue in the eCommerce space and causes significant harm to businesses, especially to those ill-prepared to face it. PYMNTS' research reveals that the average impact of fraud equals 3.5% of a B2B business's annual revenue, with many of them suffering even greater losses. The problem is not only that many businesses are inadequately equipped to react to fraud attacks either. Many organizations also have been unable to anticipate and rectify vulnerabilities, such as inadequate onboarding tools or the inability to accurately verify business data in real time.

The recent proliferation of fraud has resulted in tangible negative outcomes for many businesses. Our researchers found that nearly half (47%) of businesses surveyed were unable to onboard clients due to a fear of fraud and a belief that their existing anti-fraud measures would be insufficient. Still, other businesses fail to grow because their anti-fraud approaches flag legitimate business contacts or transactions as fraudulent, thereby preventing them from doing business.

PYMNTS' research finds that 71% of retailers, manufacturers and marketplaces want this to change. They plan to implement better tools to detect fraud, improved safeguards against false flags and solutions that make onboarding and data management less problematic.

Risk and Resilience: A Business Fraud and ID Theft Report, a PYMNTS and TreviPay Collaboration, examines how fraud inhibits B2B business growth and how businesses are searching for innovative ways to protect themselves from revenue loss as they scale. The report is based on a survey of 150 executives, 20% at small businesses (annual revenue between $10M and $50M) and 80% at mid-market businesses (annual revenue between $50M and $1B). Retailers, manufacturers and marketplaces each account for one-third of the sample. The survey was conducted between Nov. 3 and Nov. 26, 2021 in the United States.

This is what we found.

[1] PYMNTS.com Digital Connectivity Increases Efficiencies. https://www.pymnts.com/news/payment-methods/2021/as-digital-business-payments-become-the-norm-new-use-cases-emerge/. Accessed February 2022.

[2] Author unknown. Global Cybersecurity Outlook 2022. The World Economic Forum. 2022. https://www.weforum.org/reports/global-cybersecurity-outlook-2022. Accessed February 2022.

01

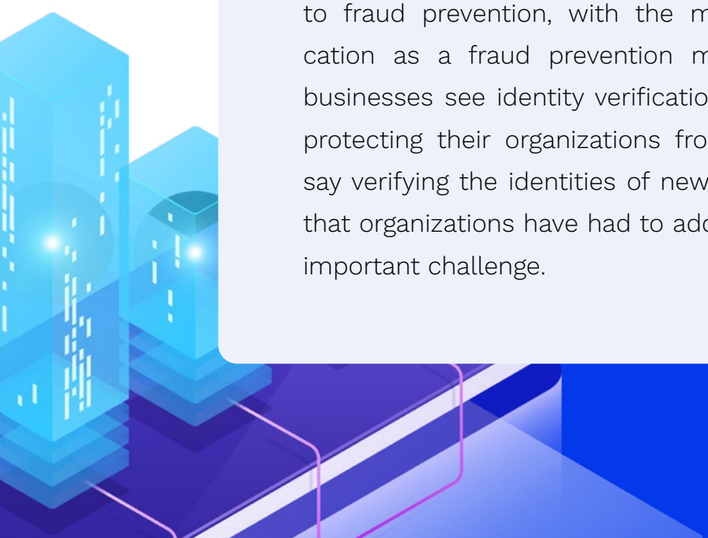
NEARLY ALL RETAIL, MANUFACTURING AND MARKETPLACE BUSINESSES HAVE SUFFERED REVENUE LOSSES BECAUSE OF FRAUD, WITH AN AVERAGE OF 3.5% OF THEIR ANNUAL SALES LOST FROM SELLING TO FRAUDULENT BUSINESSES OR MISTAKENLY FLAGGING LEGITIMATE BUSINESSES AS FRAUDULENT.

Our survey finds that 98% of retailers, manufacturers and marketplaces have been victims of fraud or have missed opportunities to transact with firms that were later revealed to be legitimate. While retailers, manufacturers and marketplaces that experienced fraud lost an average of 3.5% of their annual sales revenues, small businesses lost as much as 5% due to fraud-related occurrences, such as sales to fraudulent businesses. Organizations from these three sectors that implemented proactive and automated anti-fraud solutions lost less revenue (2%) to fraud-related occurrences, whereas those that reacted to instances of fraud using reactive and manual solutions lost 4.5% of their annual revenues.

02

IDENTITY VERIFICATION IS ONE OF THE TOP THREE CHALLENGES FACING RETAILERS, MANUFACTURERS AND MARKETPLACES.

Nearly half of these firms are actively addressing challenges related to fraud prevention, with the majority using payment card verification as a fraud prevention method. Approximately one-fifth of businesses see identity verification methods as equally important to protecting their organizations from fraud. Nearly half of executives say verifying the identities of new business customers is a challenge that organizations have had to address and 16% consider it their most important challenge.



03

MORE THAN HALF OF RETAILERS AND NEARLY HALF OF MANUFACTURING FIRMS AND MARKETPLACES SAY THEIR INABILITY TO FLAG FRAUDULENT BUSINESSES HAS CONSTRAINED GROWTH.

Organizations using manual and reactive anti-fraud methods experienced greater negative impacts on their growth due to fraud than those using proactive and automated solutions. Organizations that wait until evidence of fraud emerges or use manual solutions may naturally see greater revenue loss due to human error or slow and inefficient identity verification or vetting procedures.

04

OUR RESEARCH FINDS THAT 68% OF MARKETPLACES AND ORGANIZATIONS IN THE RETAIL AND MANUFACTURING SECTORS ARE NOT VERY SATISFIED WITH THE SYSTEMS THEY USE TO DETECT FRAUDULENT BUSINESSES.

Seventy-one percent of organizations plan to implement new digital solutions to prevent fraud, and 49% say finding a better digital solution for fraud prevention is their primary fraud prevention plan. Those that have reported success in implementing automated, digital anti-fraud solutions show the highest levels of satisfaction with their current anti-fraud strategies.

How Fraud Is Hindering B2B Business Development

PYMNTS' research finds that companies with the highest levels of fraud loss are also slow to onboard new customers/clients, compared to organizations with lower levels of fraud-related revenue loss. At least 30% of organizations that have lost more than 5% of their annual revenues to fraud take approximately one month or more to onboard new businesses. This could reflect PYMNTS' finding that businesses that use proactive, automated anti-fraud solutions tend to see fewer fraud impacts, as automated anti-fraud technology tends to increase onboarding efficiency and speed.

PYMNTS.com | trevipay

RISK AND RESILIENCE

A BUSINESS FRAUD AND ID THEFT REPORT

30%

OF BUSINESSES **HAVE LOST 3.5% OR MORE** OF THEIR AVERAGE ANNUAL SALES TO FRAUD

TABLE 1:

BUSINESSES' REPORTED LOSSES DUE TO FRAUD AND FALSE FLAGS

Portion of average annual sales lost due to select types of fraud-related issues

	Failed to sell to legitimate businesses	Sold to business that did not pay their bills	TOTAL
AVERAGE	1.6%	1.9%	**3.5%**
SIZE			
• Mid-market businesses	1.4%	1.7%	**3.1%**
• Small businesses	2.2%	2.9%	**5.1%**
INDUSTRY			
• Manufacturing	1.8%	2.1%	**3.9%**
• Retailers	1.6%	1.9%	**3.5%**
• Marketplace	1.3%	1.9%	**3.1%**
DIGITAL FRAUD SOLUTION			
• Proactive and automated	1.1%	1.2%	**2.3%**
• Proactive and manual	1.2%	1.4%	**2.6%**
• Reactive and automated	1.5%	2.1%	**3.5%**
• Reactive and manual	2.0%	2.5%	**4.5%**

N = 150; Complete responses

Source: PYMNTS | TreviPay

Risk and Resilience: A Business Fraud and ID Theft Report

TABLE 2:

FRAUD'S IMPACT ON BUSINESSES AND THEIR ONBOARDING TIMES

Average number of days and time required for organizations to onboard new businesses before they can place their first orders

	TIME REQUIRED					AVERAGE NUMBER OF DAYS
	Less than one week	About one week	A few weeks	About one month	More than one month	
AVERAGE	16.7%	36.7%	34.7%	11.3%	0.7%	**13**
SIZE						
• Mid-market businesses	15.0%	35.8%	39.2%	10.0%	0.0%	**13**
• Small businesses	23.3%	40.0%	16.7%	16.7%	3.3%	**12**
INDUSTRY						
• Manufacturing	0.0%	18.0%	58.0%	22.0%	2.0%	**19**
• Retailers	22.0%	48.0%	22.0%	8.0%	0.0%	**11**
• Marketplace	28.0%	44.0%	24.0%	4.0%	0.0%	**10**
DIGITAL FRAUD SOLUTION						
• Proactive and automated	15.4%	35.9%	33.3%	15.4%	0.0%	**14**
• Proactive and manual	8.3%	50.0%	37.5%	4.2%	0.0%	**12**
• Reactive and automated	28.6%	32.1%	28.6%	10.7%	0.0%	**12**
• Reactive and manual	15.3%	33.9%	37.3%	11.9%	1.7%	**14**

N = 150; Complete responses
Source: PYMNTS | TreviPay
Risk and Resilience: A Business Fraud and ID Theft Report

Our research shows that 54% of retailers and 44% of manufacturers and marketplaces fail to accept new customers due to fraud concerns. In addition, 54% of organizations implementing manual and reactive anti-fraud solutions fail to accept new customers due to fraud concerns, compared to 31% of those using automated and proactive technology.

Although fraud concerns and their impacts significantly hamper growth for many retailers and marketplaces, this does not indicate that organizations remain passive when confronting security challenges. Businesses use an array of methods ranging from traditional approaches, such as card verification, to modern, proactive methods that automate digital identity and transaction review to authenticate potential business partners' identities.

54%

OF RETAILERS **HAVE FAILED TO ACCEPT NEW BUSINESS** DUE TO FRAUD CONCERNS

The Shift Toward Automated Digital Identity Verification

The largest share of organizations surveyed cite the verification of new business partners' identities as their most significant security and operations challenge after managing a remote workforce. Seventy-three percent of organizations use a common method of identity authentication — payment card verification — as an anti-fraud measure when doing business online. Payment card verification appears to be the top method for smaller companies, with 53% of mid-market (with annual revenue between $50M and $1B) and 50% of small businesses (with annual revenue between $10M and $50M) relying on it as their most important anti-fraud approach.

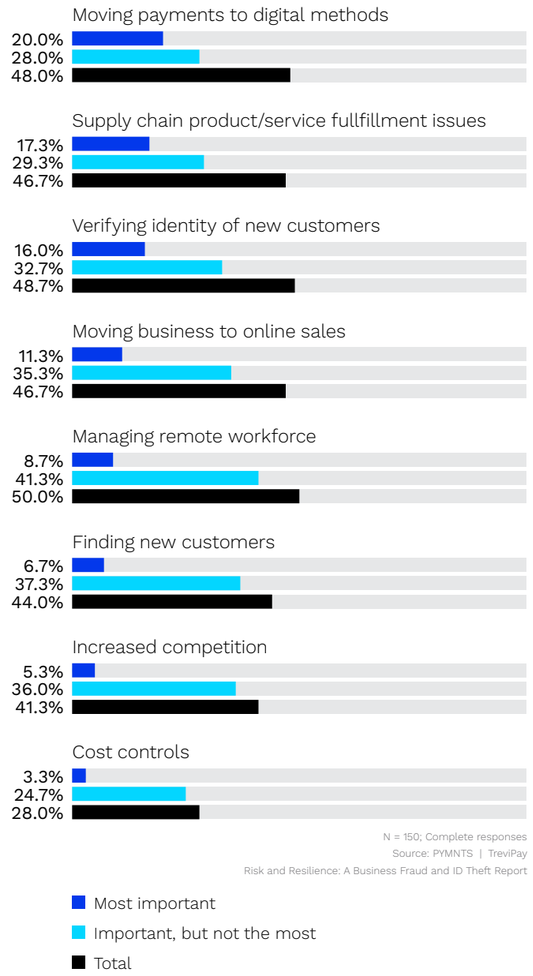
Many businesses nevertheless are adopting modern, proactive approaches to fighting fraud that involve automating anti-fraud measures. Fifty-five percent of respondents report that they use automated alerts for transaction anomalies, 47% are using automated web monitoring and 34% are using automated underwriting systems to manage fraud risk. Organizations using proactive and automated anti-fraud methods were the most likely to consider all available anti-fraud methods as equally important to their security against fraud at 36%, compared with 19% of all businesses.

How organizations feel about their approaches to combating fraud is indicative of how they evaluate their current methods' success and the urgency of their need to address fraud. At a time when the industry is defined by uncertainty, sustainable growth is imperative for businesses — and fraud has exacted a significant toll on the viability of many.

FIGURE 1:

BUSINESSES' MOST CITED CHALLENGES TO THEIR OPERATIONS

Share of businesses noting select challenges to their operations, by level of importance



N = 150; Complete responses
Source: PYMNTS | TreviPay
Risk and Resilience: A Business Fraud and ID Theft Report

49%

OF MERCHANTS FACE IMPORTANT CHALLENGES **VERIFYING THE IDENTITIES OF NEW CUSTOMERS**

PYMNTS.com | trevipay

RISK AND RESILIENCE

A BUSINESS FRAUD AND ID THEFT REPORT

16%

OF BUSINESSES USE **AUTOMATED ALERTS FOR TRANSACTION ANOMALIES** MOST AS PART OF THEIR ANTI-FRAUD STRATEGY

TABLE 3:

BUSINESSES' USAGE OF ANTI-FRAUD AND IDENTITY VERIFICATION METHODS
Share of businesses using select digital identity and fraud prevention methods when doing business online, by method and size

	METHOD			SIZE	
	Most used method	Used, but not the most	TOTAL	Mid-market businesses	Small businesses
• Payment card verification service	52.7%	20.0%	**72.7%**	53.3%	50.0%
• Automated alert for transaction anomalies	16.0%	38.7%	**54.7%**	17.5%	10.0%
• Automated web monitoring	8.7%	38.0%	**46.7%**	8.3%	10.0%
• Address verification services	7.3%	40.0%	**47.3%**	5.8%	13.3%
• Document and identity authentication	3.3%	34.7%	**38.0%**	2.5%	6.7%
• Automated underwriting systems	3.3%	30.7%	**34.0%**	4.2%	0.0%
• Payments innovation	6.0%	26.7%	**32.7%**	6.7&	3.3%
• Purchase amount filters	1.3%	20.7%	**22.0%**	0.8%	3.3%
• Solutions from third-party providers	1.3%	11.3%	**12.7%**	0.8%	3.3%
• Velocity filters	0.0%	8.7%	**8.7%**	0.0%	0.0%

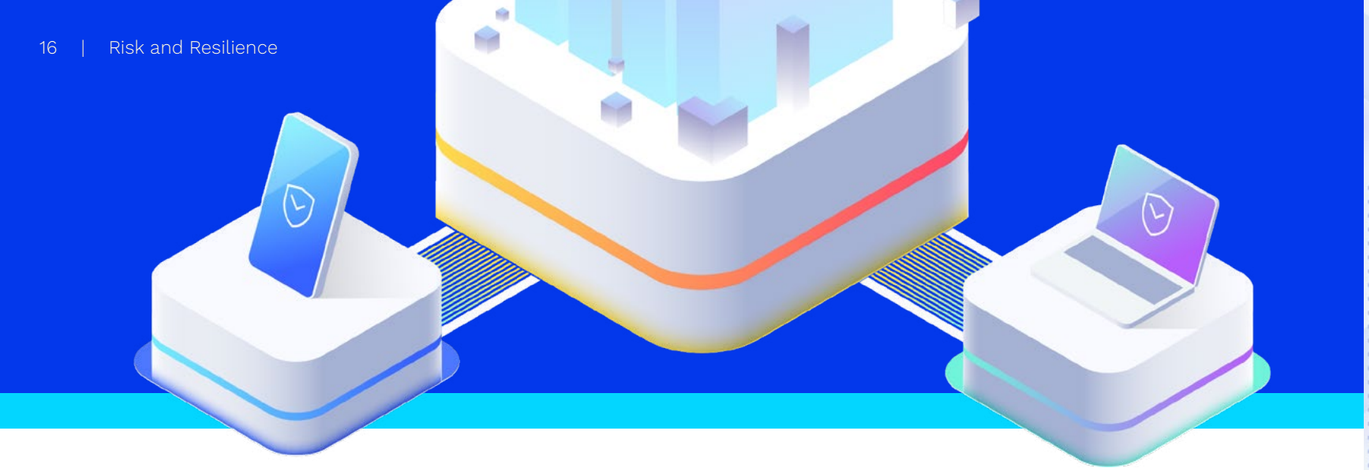
N = 150; Complete responses
Source: PYMNTS | TreviPay
Risk and Resilience: A Business Fraud and ID Theft Report

TABLE 4:

BUSINESSES' USAGE OF ANTI-FRAUD AND IDENTITY VERIFICATION METHODS
Share of businesses using select digital identity and fraud prevention methods when doing business online, by type of solution

	TYPE OF SOLUTION			
	Proactive and automated	Proactive and manual	Reactive and automated	Reactive and manual
• Payment card verification service	30.8%	66.7%	60.7%	57.6%
• Automated alert for transaction anomalies	20.5%	4.2%	17.9%	16.9%
• Automated web monitoring	15.4%	16.7%	0.0%	5.1%
• Address verification services	5.1%	4.2%	10.7%	8.5%
• Document and identity authentication	2.6%	0.0%	3.6%	5.1%
• Automated underwriting systems	7.7%	4.2%	3.6%	0.0%
• Payments innovation	12.8%	0.0%	3.6%	5.1%
• Purchase amount filters	2.6%	0.0%	0.0%	1.7%
• Solutions from third-party providers	2.6%	4.2%	0.0%	0.0%
• Velocity filters	0.0%	0.0%	0.0%	0.0%

N = 150; Complete responses
Source: PYMNTS | TreviPay
Risk and Resilience: A Business Fraud and ID Theft Report



19%

OF MERCHANTS RELY ON
MULTIPLE VERIFICATION METHODS FOR NEW PARTNERS

TABLE 5:

BUSINESSES' VERIFICATION METHODS FOR NEW PARTNERS
Businesses' usage of select methods to verify that new partners are valid businesses, by level of importance and type of solution

VERIFICATION METHODS	IMPORTANCE			TYPE OF SOLUTION			
	Most important	Important, but not the most	TOTAL	Proactive and automated	Proactive and manual	Reactive and automated	Reactive and manual
• Check the company through its employer identification number	14.7%	29.3%	**44.0%**	7.7%	16.7%	17.9%	16.9%
• Use search engines or websites to check the company's address and phone number	14.7%	40.0%	**54.7%**	5.1%	12.5%	17.9%	20.3%
• Use due diligence firms that perform automated KYC/AML compliance	14.0%	38.0%	**52.0%**	23.1%	12.5%	0.0%	15.3%
• Review court records in the jurisdiction in which the business is registered	9.3%	32.0%	**41.3%**	10.3%	12.5%	14.3%	5.1%
• Check the validity of companies' official business addresses	8.0%	34.0%	**42.0%**	0.0%	8.3%	17.9%	8.5%
• Check for membership or accreditation through community groups	7.3%	31.3%	**38.7%**	5.1%	8.3%	10.7%	6.8%
• Request a credit report through firms that provide reports on business	4.7%	36.0%	**40.7%**	7.7%	4.2%	3.6%	3.4%
• Subscribe to third-party databases that provide business and credit information	4.0%	15.3%	**19.3%**	5.1%	4.2%	3.6%	3.4%
• Review reports from the U.S. Department of Commerce	1.3%	25.3%	**26.7%**	0.0%	0.0%	0.0%	3.4%
• Check the reference or reviews on companies' own websites and contact them	1.3%	20.0%	**21.3%**	0.0%	0.0%	0.0%	3.4%
• Review filings using government database	1.3%	18.7%	**20.0%**	0.0%	4.2%	0.0%	1.7%
• Request trade or banking reference	0.0%	19.3%	**19.3%**	0.0%	0.0%	0.0%	0.0%
• All of these are equally important	—	—	**19.3%**	35.9%	16.7%	14.3%	11.9%

N = 150; Complete responses
Source: PYMNTS | TreviPay
Risk and Resilience: A Business Fraud and ID Theft Report

Fraud's Impact on Consumer Experiences And Business Operations

Fraud harms more than just businesses' revenues: Slow and inefficient anti-fraud methods also impact customer experience. We find that 46% of organizations using manual anti-fraud solutions report that fraud has a negative impact on customer experience, causing delays and other issues for their customers. As a result, these organizations say customers found it hard to work with them. Our research also finds that businesses with a rapid onboarding process report fewer customer experience issues than those with a lengthier onboarding procedure. Twenty eight percent of firms that spent less than a week onboarding new customers say fraud-related concerns cause issues that make it difficult for their customers to work with them. By contrast, 59% of firms that spent an average of at least one month onboarding new customers say their customers experience issues that make working with them difficult. Retailers and manufacturers are the hardest hit by customer experience issues due to fraud concerns, at 48% and 50%, respectively.

PYMNTS.com | trevipay

RISK AND RESILIENCE

A BUSINESS FRAUD AND ID THEFT REPORT

Our research also shows that businesses that used automated anti-fraud solutions proactively fare better than those that do not use them when it comes to customer experience. Only 26% of those businesses using automated anti-fraud solutions say their organizations have customer experience issues because of fraud-related concerns.

Just 5% of businesses that use proactive, automated approaches report that fraud limits their international growth, compared to 36% of reactive organizations using manual methods that say the same. The gap in efficiency between the two approaches naturally impacts how these organizations feel about their current solutions. Many organizations are displeased with poor results from their existing anti-fraud strategies and are actively seeking to improve outcomes.

TABLE 6:

BUSINESSES' FRAUD-RELATED CHALLENGES
Share of organizations that cite select fraud-related concerns as having a "very" or "extremely" large impact on their businesses

● Higher than average

	Failed to accept new customers	Difficult for customers to work with	Prevented or limited international expansion
AVERAGE	**47.3%**	**39.3%**	**26.0%**
SIZE			
• Mid-market businesses	**47.5%**	**40.0%**	24.2%
• Small businesses	**46.7%**	36.7%	**33.3%**
INDUSTRY			
• Manufacturing	44.0%	**48.0%**	**30.0%**
• Retailers	**54.0%**	**50.0%**	26.0%
• Marketplace	44.0%	20.0%	22.0%
DIGITAL FRAUD SOLUTION			
• Proactive and automated	30.8%	25.6%	5.1%
• Proactive and manual	**50.0%**	**45.8%**	20.8%
• Reactive and automated	**53.6%**	39.3%	**39.3%**
• Reactive and manual	**54.2%**	**45.8%**	**35.6%**

N = 71; Failed to accept new customers | N = 59; Difficult for customers to work with | N = 38; Prevented or limited international expansion
Source: PYMNTS | TreviPay
Risk and Resilience: A Business Fraud and ID Theft Report

A Call to Action: How Businesses Plan to Address Fraud

Organizations that use automated solutions show significantly higher rates of satisfaction than those that do not. Approximately 50% of organizations that implement automated solutions for digital identity verification and fraud prevention are “very” or “extremely” satisfied with their current solutions, whereas just 17% of organizations using manual solutions say the same.

Finding a better way to fight fraud is even more important for organizations that are unsatisfied with their current anti-fraud strategies and/or losing revenue because of these strategies. Sixty-three percent of organizations that are “slightly” or “not at all” satisfied with their current anti-fraud approaches report that the implementation of new, automated anti-fraud methods is their primary anti-fraud strategy.

PYMNTS.com | trevipay

RISK AND RESILIENCE

A BUSINESS FRAUD AND ID THEFT REPORT

FIGURE 2:

BUSINESSES’ SATISFACTION WITH THEIR CURRENT ANTI-FRAUD METHODS

Share of businesses that report select levels of satisfaction with their current digital identity verification and fraud prevention methods

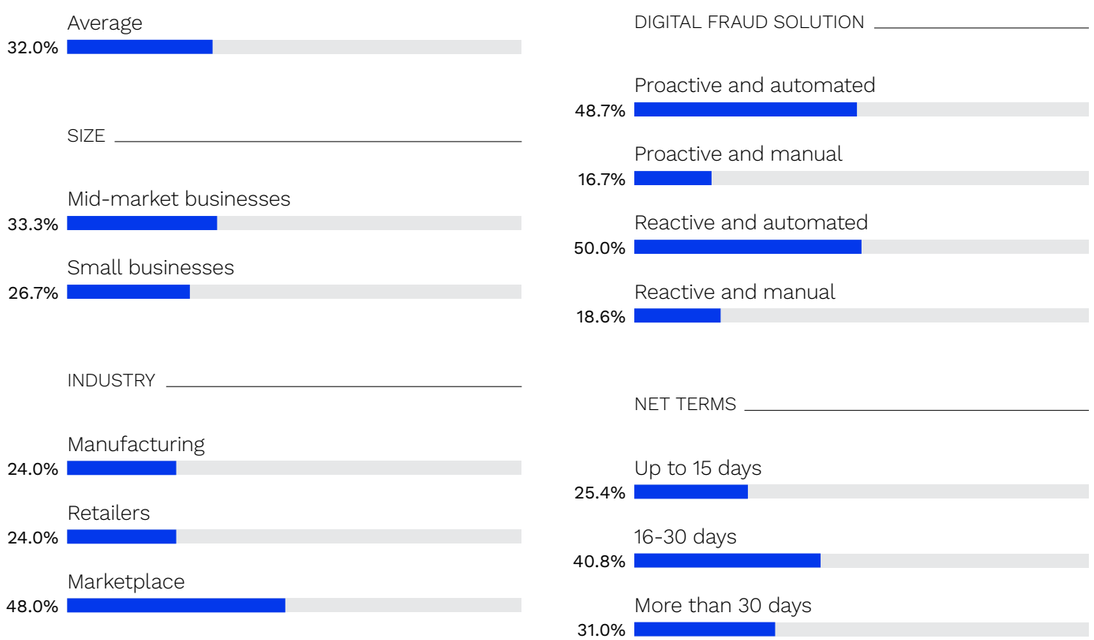
N = 150; Complete responses
Source: PYMNTS | TreviPay
Risk and Resilience: A Business Fraud and ID Theft Report

Businesses adopting automated anti-fraud solutions show higher rates of satisfaction, but there is still room for improvement. As B2B eCommerce sales increase, organizations face two types of financial risk: fraud and the hesitance to expand due to fraud that limits growth.

FIGURE 3:

BUSINESSES’ SATISFACTION WITH THEIR CURRENT ANTI-FRAUD METHODS

Share of businesses that report being “very” or “extremely” satisfied with their current digital identity verification and fraud prevention methods



N = 47; Executives who are “very” or “extremely” satisfied with their organizations’ current digital identity verification and fraud prevention solutions
Source: PYMNTS | TreviPay
Risk and Resilience: A Business Fraud and ID Theft Report

CONCLUSION

B2B eCommerce organizations are experiencing significant financial losses due to fraud, and the impact of that fraud reaches nearly all aspects of their operations. Although they had to completely revamp the way in which they do business to pursue growth during the early days of the pandemic, some have reached an impasse. Many are halting or missing new business opportunities due to the inadequacy of their existing solutions or their propensity to create false flags. Unsurprisingly, most businesses are not satisfied with their current anti-fraud methods, and 71% are searching for better solutions — either by attempting to improve on existing tools or by partnering with a powerful third-party solution provider. Proving and authenticating a business's digital identity is and will continue to be among the biggest challenges for organizations as well as an important driver of business growth.

METHODOLOGY

Risk and Resilience: A Business Fraud and ID Theft Report is based on survey responses from 150 executives from small businesses, those with annual revenues between $10 million and $50 million, and mid-market businesses, those generating revenues between $50 million and $1 billion, working in customer underwriting and compliance/risk management. Businesses surveyed had at least 75% of their sales classified as B2B transactions. The survey was conducted from Nov. 3 to Nov. 26, 2021.

RISK AND RESILIENCE

A BUSINESS FRAUD AND ID THEFT REPORT

ABOUT

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

TreviPay is a global B2B payments company, facilitating transactions for customers in over 190 countries. We take care of our clients by taking care of their customers. As a result, this past year alone we processed $6 billion in transactions in over 27 countries and 18 currencies. TreviPay helps businesses reach new heights by entering new markets, expanding their footprints and globalizing their opportunities while streamlining payments and improving cash flow.

TreviPay is disrupting the credit industry by enabling companies access to robust payment and credit solutions, sophisticated managed services and expert-driven integrations to power global commerce. Our high-performance culture has been the catalyst for continued success in the ever-changing world of technology. We embrace constant innovation with internal accelerators and technology investments to help businesses reach their full potential that drives deeply into geo-specific business processes and payments.

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.

DISCLAIMER