PYMNTS.com | trevipay

THE NEW B2B AUTHENTICATION STANDARD

THE SHIFT TOWARD AUTOMATED DIGITAL IDENTITY VERIFICATION

The New B2B Authentication Standard: The Shift Toward Automated Digital Identity Verification, 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 B2B companies generating $10 million to $1 billion in annual revenues. The survey was conducted between Nov. 3, 2021, and Nov. 26, 2021, in the U.S.

■ JULY 2022

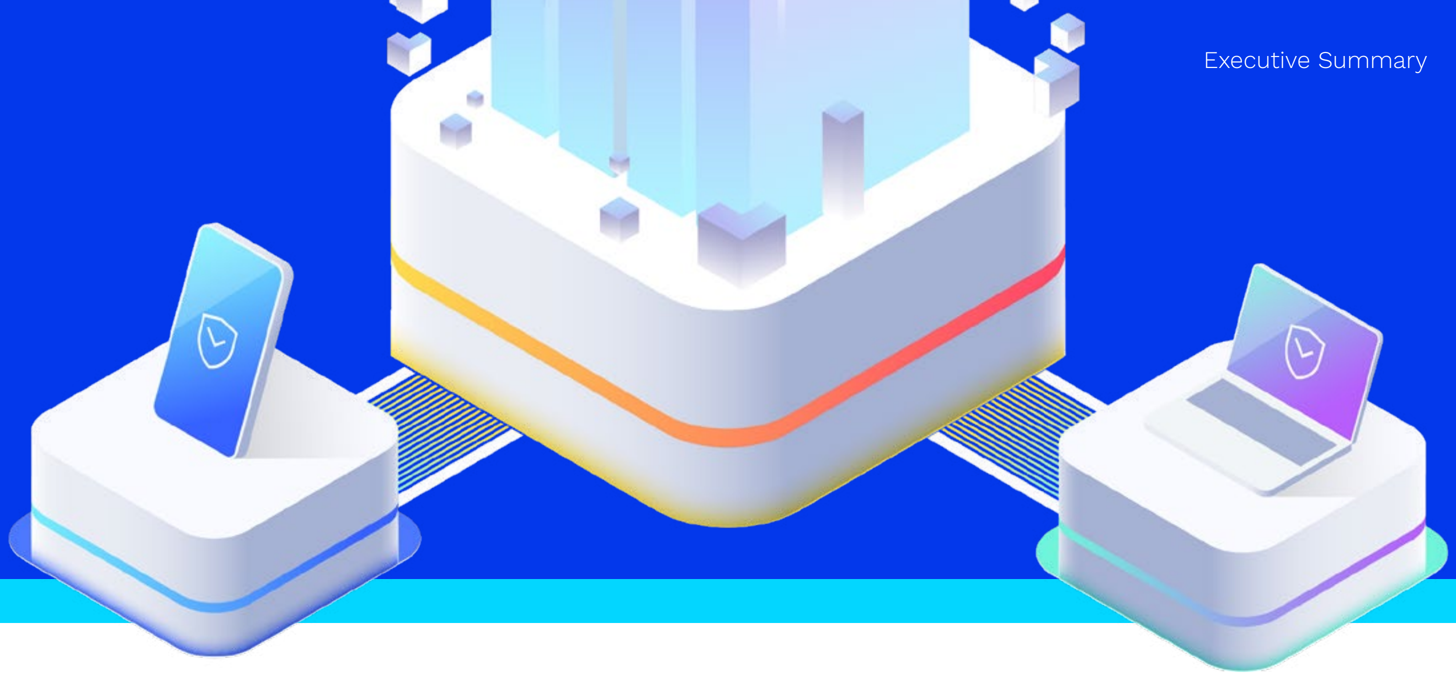
THE NEW B2B AUTHENTICATION STANDARD

THE SHIFT TOWARD AUTOMATED DIGITAL IDENTITY VERIFICATION

PYMNTS.com | trevipay

The New B2B Authentication Standard: The Shift Toward Automated Digital Identity Verification 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

Proving and authenticating an organization's digital identity is one of the biggest struggles for companies mitigating business-to-business (B2B) payments fraud. PYMNTS' data shows that 98% of B2B retailers, manufacturers and marketplaces have been victims of fraud or have missed opportunities to do business with firms that were later revealed to be legitimate. As a result, these businesses have lost 3.5% of their annual sales revenues on average.

PYMNTS' research finds that 54% of retailers and 44% of both manufacturers and marketplaces failed to accept new customers due to concerns about fraud. Another concern: Onboarding processes for new customers have caused some legitimate businesses to be falsely flagged as fraudulent, unjustly halting some business opportunities. Consequently, 49% of surveyed firms recognize that verifying new business customers' identities is an important challenge to address, with 16% of them considering this to be the most important challenge they face.

Our data also shows organizations that implemented proactive and automated anti-fraud solutions lost less revenue than average — only 2% — to fraud-related occurrences. This means that automated, proactive digital identity verification solutions offer meaningful benefits for organizations seeking to improve their customer onboarding processes and mitigate B2B payments fraud. By adopting an effective technology solution to enhance digital identity verification, organizations can dramatically stem fraudulent activity and improve their business prospects.

The New B2B Authentication Standard: The Shift Toward Automated Digital Identity Verification, a PYMNTS and TreviPay collaboration, examines how U.S. businesses can modernize their B2B identity verification strategies and securely expand their businesses. The report is based on a survey of 150 executives at companies generating $10 million to $1 billion in annual revenues that was conducted between Nov. 3, 2021, and Nov. 26, 2021.

This is what we found.

54%

OF RETAILERS **FAILED TO ACCEPT NEW CUSTOMERS** DUE TO CONCERNS ABOUT FRAUD.

First steps in modernizing B2B verification strategies

Failure to verify a business's legitimacy is a leading source of revenue loss, according to our data, with small businesses suffering greater losses in sales income. Much of this can be attributed to false positives — inaccurate fraud warnings that can negatively impact legitimate business opportunities.

Organizations lose an average of 3.5% of their annual sales to fraud-related concerns, with 1.6% of that caused by failure to sell to legitimate businesses. Small businesses tend to lose greater shares of their annual sales due to fraud-related concerns: This share is 5.1%, with 2.9% of that being sales lost to legitimate businesses.

Companies that rely on reactive and manual solutions to verify digital identities and stem fraud lose above average shares of annual sales at 4.5%, with 2% caused by failed sales to legitimate businesses. Firms using proactive and automated solutions, however, reduce their share of lost sales to 2.3%, with 1.1% due to halted legitimate sales.

ORGANIZATIONS LOSE AN AVERAGE OF **3.5%** OF THEIR ANNUAL SALES TO **FRAUD-RELATED CONCERNS.**

TABLE 1:

RATE OF SALES LOST DUE TO FRAUD OR LACK OF PAYMENT

Share of businesses' average annual sales lost, by type of business

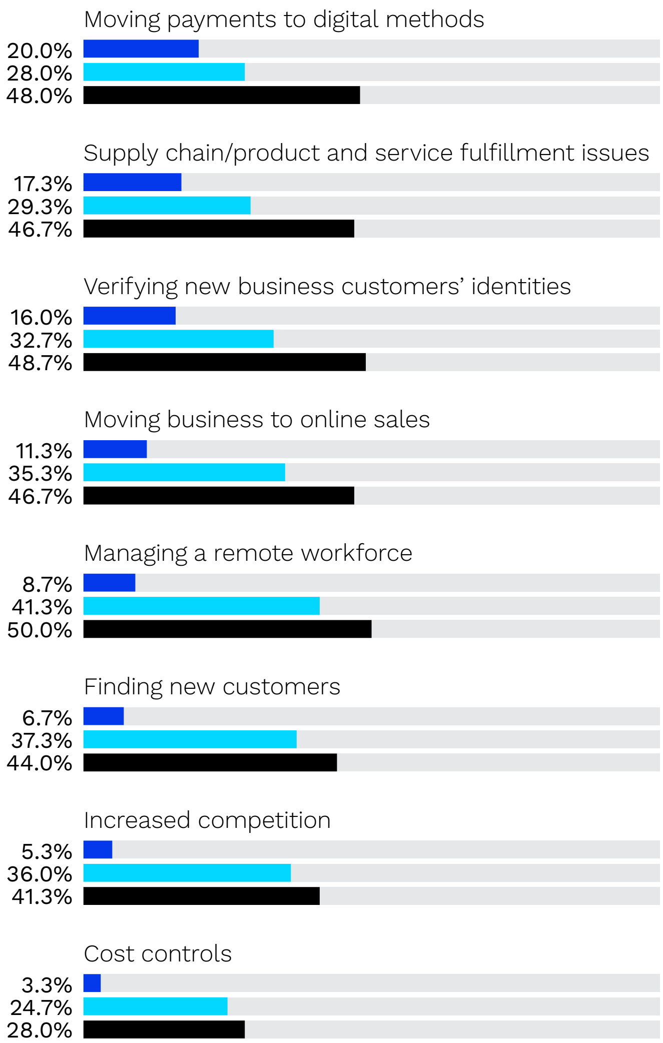
	Failed to sell to legitimate businesses	Businesses did not pay their bills	TOTAL
AVERAGE	1.6%	1.9%	**3.5%**
SIZE			
• Mid-market businesses	1.4%	1.7%	**3.1%**
• Small businesses	2.2%	2.9%	**5.1%**
INDUSTRY			
• Manufacturing	1.8%	2.1%	**3.9%**
• Retailers	1.6%	1.9%	**3.5%**
• Marketplace	1.3%	1.9%	**3.1%**
DIGITAL IDENTITY AND FRAUD PREVENTION 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.com | TreviPay
The New B2B Authentication Standard

FIGURE 1A:

BUSINESSES' MOST CITED OPERATIONAL CHALLENGES

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



N = 150: Complete responses
Source: PYMNTS.com | TreviPay
The New B2B Authentication Standard

■ Most important challenge
■ Important, but not the most important challenge
■ Total

49%

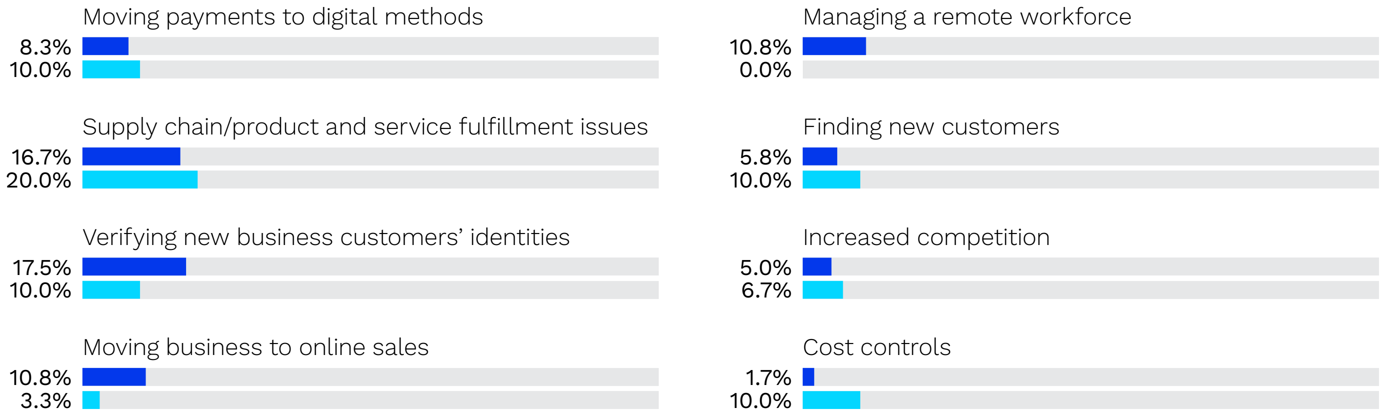
OF MERCHANTS FACE IMPORTANT CHALLENGES WHEN **VERIFYING THE IDENTITIES OF NEW CUSTOMERS.**

It is no surprise, then, that identity verification is one of the top three challenges facing surveyed retailers, manufacturers and marketplaces. Forty-nine percent of executives surveyed recognize verifying new business customers' identities as a challenge that organizations must address, and 16% believe this is their most important challenge. This importance is especially felt by mid-market organizations — of which 18% consider identity verification to be most important — and those relying on reactive and manual solutions for digital identity and fraud prevention, at 17%.

FIGURE 1B:

BUSINESSES' MOST CITED OPERATIONAL CHALLENGES

Share of businesses citing select challenges to their operations as most important, by size



N = 150: Complete responses
Source: PYMNTS.com | TreviPay
The New B2B Authentication Standard

■ Mid-market businesses
■ Small businesses

FIGURE 1C:

BUSINESSES' MOST CITED OPERATIONAL CHALLENGES

Share of businesses citing select challenges to their operations as most important, by type of solution

	TYPE OF SOLUTION			
	Proactive and automated	Proactive and manual	Reactive and automated	Reactive and manual
• Moving payments to digital methods	12.8%	4.2%	7.1%	8.5%
• Supply chain/product and service fulfillment issues	15.4%	16.7%	21.4%	16.9%
• Verifying new business customers' identities	15.4%	16.7%	14.3%	16.9%
• Moving business to online sales	2.6%	20.8%	17.9%	10.2%
• Managing a remote workforce	10.3%	8.3%	10.7%	6.8%
• Finding new customers	12.8%	4.2%	7.1%	3.4%
• Increased competition	5.1%	8.3%	0.0%	6.8%
• Cost controls	5.1%	4.2%	0.0%	3.4%

N = 150: Complete responses
Source: PYMNTS.com | TreviPay
The New B2B Authentication Standard

The digital identity self-audit

Many businesses need to assess the effectiveness of their current identity verification methods to develop a road map for modernization. Fraud attacks may happen via an array of new platforms and devices, yet ineffective methods of verifying new business customers may force firms to decline sales from legitimate businesses. As a result, manufacturers, retailers and marketplaces need to modernize their approaches to identity verification to avoid missing out on new revenue opportunities.

The following five questions comprise a self-audit of identity authentication processes for organizations.

01

HOW MANY LEGITIMATE CUSTOMERS ARE DECLINED DUE TO FALSE POSITIVES?

Some fraud solutions err too far on the no-risk end of the spectrum. In fact, 54% of companies with manual processes are sure they have declined legitimate customers.

02

DOES YOUR ORGANIZATION USE PAYMENT CARD VERIFICATION TO AUTHENTICATE PROSPECTIVE BUYERS?

Payment card verification is common practice — 73% of the B2B companies we surveyed use it — because corporate credit cards are a popular payment option. But what if your customer needs to place a large order? Customers placing larger orders prefer to purchase using trade credit. Failure to offer a payment option such as invoicing or term payments could result in losses in sales and of future clients.

03

DOES YOUR ORGANIZATION USE ADDRESS VERIFICATION SERVICES TO VERIFY NEW CUSTOMERS?

Integrating USPS address matching and verification is easy, and 47% of B2B companies use this method to verify new business customers. The solution is not foolproof, though, and might require individual follow-up.

04

DOES YOUR ORGANIZATION USE AUTOMATED ALERTS TO VERIFY TRANSACTION ANOMALIES?

Fifty-five percent of respondents report they use automated alerts to double-check transaction anomalies. These proactive systems can identify legitimate purchases quickly and weed out suspicious ones.

05

DOES YOUR ORGANIZATION USE AUTOMATED WEB MONITORING TO MINIMIZE FRAUD?

Forty-seven percent of respondents use this type of service, which helps identify suspicious domains and eliminate them proactively, protecting your company from negative consequences.

Developing a modern digital identity verification strategy

Companies may offer customers various B2B payment options, such as invoicing and term payments, yet many also rely on card verification to validate customer transactions. As a result, B2B revenue losses due to fraud often involve identity-related crimes or an inability to adequately monitor identity. Only one in five businesses gives equal importance to multiple identity verification methods when onboarding new business partners, however. PYMNTS' research finds that card verification is the leading method of digital identity verification when engaging with new business customers online, yet companies using proactive and automated anti-fraud solutions rely on more methods than other organizations.

While 73% of firms apply card verification to verify digital identity and prevent fraud when doing business online, 53% consider this the method on which they rely the most for digital identity and fraud prevention. Mid-market businesses are slightly more likely to rely on card verification than small firms, at 53% and 50%, respectively. We also find that 47% of all firms rely on address verification services and automated web monitoring.

TABLE 2A:

DIGITAL IDENTITY VERIFICATION AND FRAUD PREVENTION METHODS

Share of businesses using select methods for digital identity verification, by level of importance and organization size

	LEVEL OF IMPORTANCE			ORGANIZATION SIZE	
	Most used method	Used, but not most used	TOTAL	Mid-market businesses	Small businesses
• Card verification value services	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.com | TreviPay
The New B2B Authentication Standard

Only 31% of organizations using proactive and automated anti-fraud solutions mostly rely on card verification, whereas 67% of proactive and manual organizations and around 60% of organizations using reactive anti-fraud solutions primarily rely on card verification. Among proactive and automated organizations, 21% rely on automated alerts for transaction anomalies, 15% rely on automated web monitoring and 13% rely on payments innovations as their most used fraud prevention method.

Effectively verifying a new business customer's legitimacy remains a key challenge. As a result, organizations may use multiple methods to verify new business clients' identities. This is especially true among organizations that use proactive and automated anti-fraud solutions.

While only 19% of all firms surveyed give equal importance to all identity verification methods considered, 36% of organizations that use proactive and automated solutions consider all such methods equally important. This means that these leading entities understand that several methods in concert is stronger than any one by itself. Just 17% of firms using proactive and manual anti-fraud solutions and 12% of those relying on reactive and manual solutions recognize the importance of all identity verification methods.

TABLE 2B:

DIGITAL IDENTITY VERIFICATION AND FRAUD PREVENTION METHODS

Share of businesses' most relied on methods for digital identity verification, by type of solution

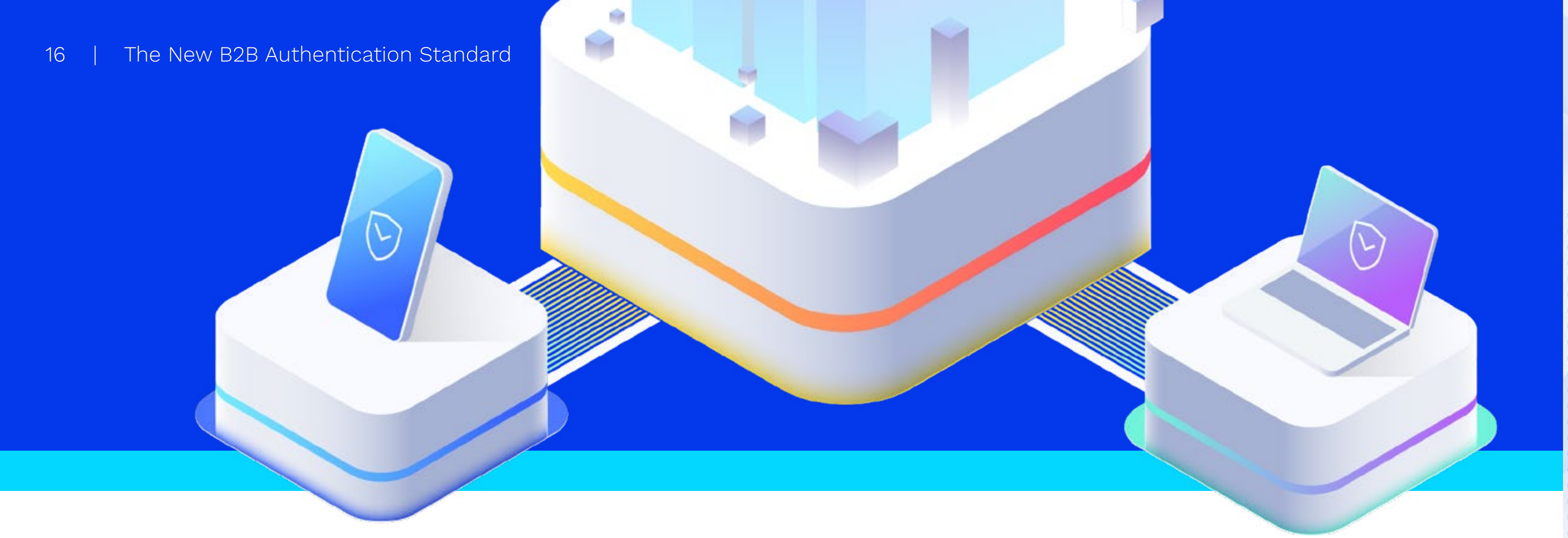
	TYPE OF SOLUTION			
	Proactive and automated	**Proactive and manual**	**Reactive and automated**	**Reactive and manual**
• Card verification value services	30.8%	66.7%	60.7%	57.6%
• Automated alert for transaction anomalies	20.5%	4.2%	17.9%	16.9%
• Automated web monitoring	15.4%	16.7%	0.0%	5.1%
• Address 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.com | TreviPay
The New B2B Authentication Standard

Using search engines to verify a new business's address and checking the employer ID were the most-cited key methods to verify a new business customer's validity, at 15% each. Using due diligence firms to perform automated know your business (KYB) checks is the most important method used to verify a business's validity for 14% of firms. At 40% and 38%, respectively, using search engines to verify that new business's address and due diligence firms that perform automated KYB checks are the most likely two methods to be seen as important — if not the most important — methods of verification.

15%

OF ORGANIZATIONS THAT **USE SEARCH ENGINES TO VERIFY A NEW BUSINESS'S ADDRESS** SAY THIS IS THE MOST IMPORTANT VERIFICATION METHOD.



19%

OF MERCHANTS RELY ON **MULTIPLE VERIFICATION METHODS FOR NEW CUSTOMERS.**

TABLE 3:

LEGITIMACY OF VERIFICATION METHODS

Share of businesses using select methods to verify that new businesses are legitimate, by level of importance and type of solution

VERIFICATION METHODS	IMPORTANCE			TYPE OF SOLUTION			
	Most important	Important, but not the most important	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 know your customer/anti-money laundering 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.com | TreviPay
The New B2B Authentication Standard

Choosing a third-party digital identity authentication platform

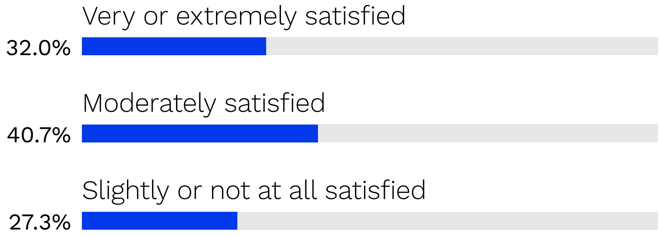
PYMNTS' research finds that two-thirds of organizations are moderately or not at all satisfied with their current digital solutions for identity verification and fraud prevention. Those with automated solutions experience the greatest satisfaction.

While only 32% of organizations are very or extremely satisfied with the identity verification and fraud prevention solutions they currently implement, approximately 50% of organizations that implement automated solutions for digital identity verification and fraud prevention are satisfied with their current solutions. Only 18% of organizations with manual solutions are very or extremely satisfied with their current solutions.

More eCommerce organizations are satisfied than those of any other industry, with 48% very or extremely satisfied with their current solutions for identity verification and fraud prevention, compared to 24% of manufacturing or retail trade organizations. At 33%, middle-market businesses are more likely to be very or extremely satisfied with their current solutions than small firms, only 27% of which report that level of satisfaction.

FIGURE 2:

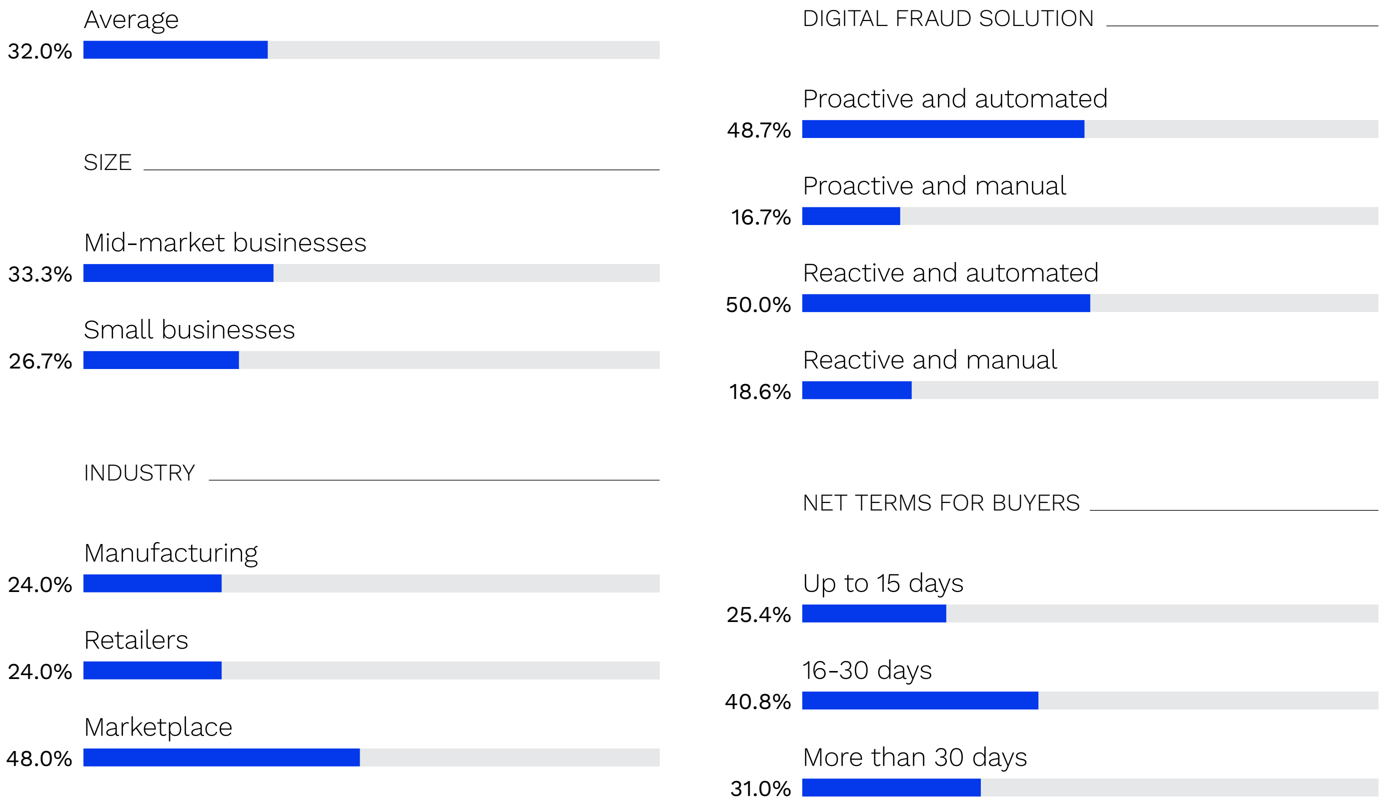
BUSINESSES' SATISFACTION WITH THEIR CURRENT DIGITAL IDENTITY VERIFICATION AND FRAUD PREVENTION SOLUTIONS
Share of businesses that report select levels of satisfaction with their current digital identity verification and fraud prevention solutions



N = 150; Complete responses
Source: PYMNTS.com | TreviPay
The New B2B Authentication Standard

50% OF ORGANIZATIONS THAT IMPLEMENT **AUTOMATED SOLUTIONS FOR DIGITAL IDENTITY VERIFICATION** ARE SATISFIED WITH THEIR CURRENT SOLUTIONS.

Share of businesses very or extremely satisfied with their current digital identity verification and fraud prevention solutions

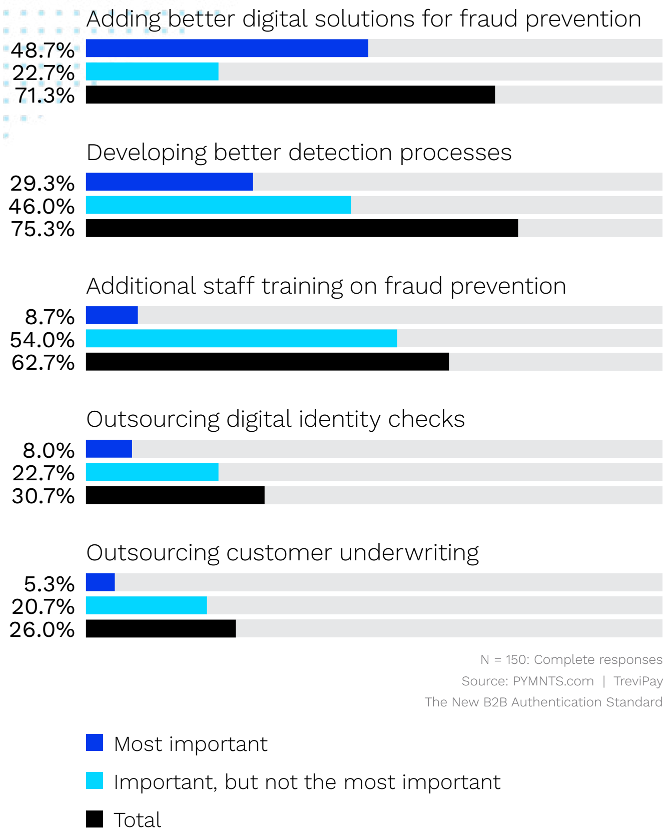


N = 47; Executives who are very or extremely satisfied with their organizations' current digital identity verification and fraud prevention solutions
Source: PYMNTS.com | TreviPay
The New B2B Authentication Standard

FIGURE 3:

BUSINESSES' PLANS TO ADDRESS DIGITAL IDENTITY VERIFICATION AND FRAUD-RELATED CONCERNS

Share of businesses that consider plans addressing fraud-related concerns to be important



N = 150: Complete responses
Source: PYMNTS.com | TreviPay
The New B2B Authentication Standard

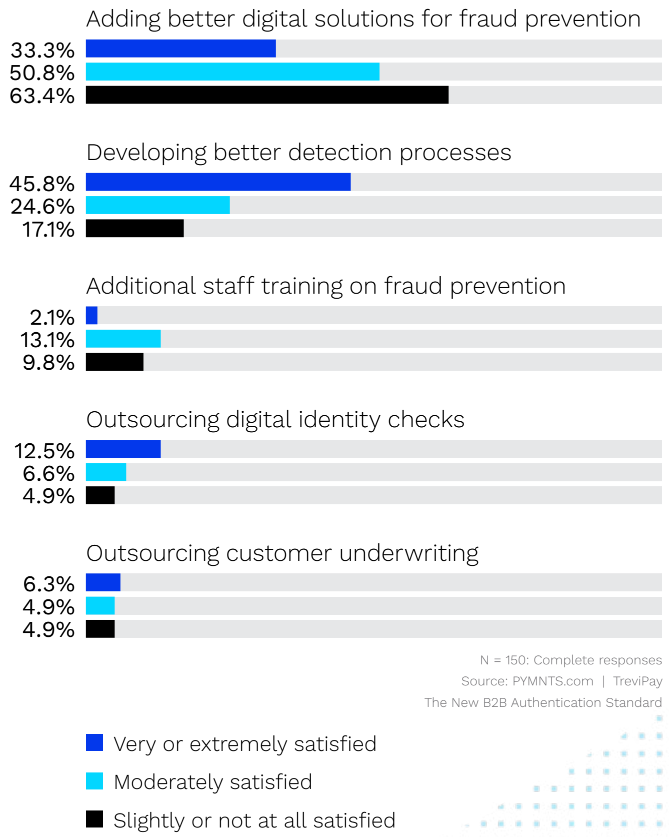
Implementing better digital solutions is one of the top strategies organizations consider for addressing digital identity verification and fraud-related concerns. This is the case particularly for organizations that are dissatisfied with their current fraud prevention solutions. Our data finds that 71% of organizations plan to implement better digital solutions for fraud prevention, with 49% considering it the most important plan to implement to prevent fraud-related issues. Sixty-three percent of executives who are slightly or not at all satisfied with their organizations' current solutions consider implementing better digital solutions to be the most important plan for preventing fraud.

While 75% of organizations plan to improve internal processes for detecting and preventing fraudulent transactions, 29% consider it their most important plan. Notably, 46% of businesses that are very or extremely satisfied with their current solutions consider it to be the most important plan for preventing fraud.

FIGURE 4:

BUSINESSES' PLANS TO ADDRESS DIGITAL IDENTITY VERIFICATION AND FRAUD-RELATED CONCERNS

Share of businesses' most important solutions for addressing digital identity verification and fraud-related concerns, by satisfaction with current fraud prevention solutions



N = 150: Complete responses
Source: PYMNTS.com | TreviPay
The New B2B Authentication Standard

Outsourcing digital identity checks is in the plans of 31% of businesses, with 8% saying it is the most important part of their plans. Among businesses very or extremely satisfied with their current solutions, just 13% consider this the most important plan for preventing fraud.

63%

OF EXECUTIVES WHO ARE SLIGHTLY OR NOT AT ALL SATISFIED WITH THEIR ORGANIZATIONS' CURRENT SOLUTIONS CONSIDER **IMPLEMENTING BETTER DIGITAL SOLUTIONS** TO BE THE MOST IMPORTANT PLAN FOR PREVENTING FRAUD.

What B2B businesses should look for in a technology solutions provider and why features matter

Barriers to innovation for B2B businesses include overreliance on legacy tools, limited human and technological resources and professional knowledge gaps around modern anti-fraud tools and risks. Businesses facing identity authentication challenges can benefit by utilizing advanced automation technologies that integrate multiple methods of verifying businesses' identities. Many businesses turn to third-party anti-fraud and identity verification solutions to launch modern strategies quickly. Here are several features to look for:

ONBOARDING THAT PROMOTES STREAMLINED IDENTITY VERIFICATION PROCESSES WITHOUT COMPROMISING SECURITY

ANTI-FRAUD MONITORING TO COVER TRANSACTIONS USING MULTIPLE PAYMENT METHODS

THE ABILITY TO MANAGE OMNICHANNEL SALES AS BUSINESS OPERATIONS SCALE

SECURE, FRICTIONLESS INVOICING AND ACCOUNTS PAYABLE/ACCOUNTS RECEIVABLE MANAGEMENT FEATURES

ANTI-FRAUD TRANSACTION MONITORING EFFORTS SHOULD BE **AUTOMATED AND SEAMLESS** IN OPERATION.

CONCLUSION

Fraud's impact on consumer experiences and business growth is significant and will only scale as new technologies and payment methods create additional points of vulnerability. Poor identity verification processes during customer onboarding can not only damage customer experiences and lead to fraud but also limit business opportunities due to false positives that halt sales from legitimate businesses. Organizations hoping to fight fraud successfully while growing their businesses ought to implement proactive and automated identity authentication and anti-fraud monitoring strategies to protect both their revenues and their customer bases.

METHODOLOGY

The New B2B Authentication Standard: The Shift Toward Automated Digital Identity Verification is based on survey responses from 150 executives from small businesses — those generating annual revenues between $10 million and $50 million — and mid-market businesses — those generating 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, 2021, to Nov. 26, 2021.

THE NEW B2
AUTHENTIC
STANDARD
THE SHIFT TOWARD AUTOMATED
DIGITAL IDENTITY VERIFICATION

ABOUT

PYMNTS.com

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.

trevi pay

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 ■

The New B2B Authentication Standard: The Shift Toward Automated Digital Identity Verification may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS.COM: 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.COM 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.COM 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.COM 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.COM 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.COM 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.