PYMNTS.com | trevi pay

REFRAMING ANTI-FRAUD STRATEGY

DEVELOPING A PROACTIVE APPROACH TO FRAUD RISK MANAGEMENT

Reframing Anti-Fraud Strategy: Developing A Proactive Approach To Fraud Risk Management, 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.

■ JUNE 2022

REFRAMING
ANTI-FRAUD STRATEGY

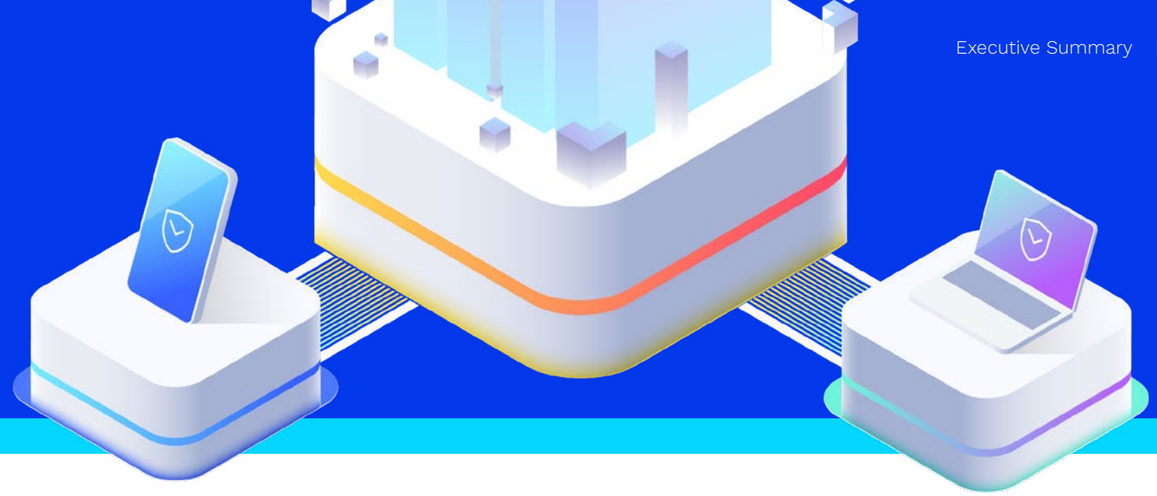
DEVELOPING A PROACTIVE APPROACH TO FRAUD RISK MANAGEMENT

PYMNTS.com | trevipay

Reframing Anti-Fraud Strategy: Developing A Proactive Approach To Fraud Risk Management 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



To accommodate consumers' most recent preferences, retailers, marketplaces and brands have revamped their eCommerce strategies, transforming smartphones into command centers for personalized shopping experiences and changing the way consumers and business-to-business (B2B) enterprises view online activity.

Along with this increase in digitization and connectivity has come new risks — and an increase in fraudulent activity. Just as new smartphone capabilities spur commercial growth, fraud causes the ecosystem to contract. According to PYMNTS research, 47% of B2B businesses chose not to onboard new clients due to a fear of fraud attacks. It was not that these businesses had no strategy in place — worse, they were certain that their existing anti-fraud measures would be insufficient.

They had good reason to hesitate. B2B businesses are often complex, involving multiple stakeholders and tend to have higher per-transaction costs — representing greater risks than business-to-consumer (B2C) transactions. A staggering 98% of B2B businesses reported fraud attacks in 2021, losing 3.5% of their annual sales revenues on average. Small businesses lost even greater shares — as much as 5% — due to fraud-related issues and concerns.

Recent PYMNTS research finds that effective answers exist. Organizations that implemented proactive and automated anti-fraud solutions lost less revenue (just 2%) to fraud-related occurrences. Businesses of all sizes that simply reacted to instances of fraud with manual solutions after they happened lost 4.5% of their annual revenues.

That data reveals an actionable insight for small and large businesses: Automated, proactive anti-fraud solutions offer meaningful benefits for organizations aiming to improve anti-fraud outcomes.

Reframing Anti-Fraud Strategy: Developing A Proactive Approach to Fraud Risk Management, a TreviPay and PYMNTS collaboration, examines how businesses can leverage new technology to modernize their anti-fraud strategies.

This is what we found.

47%

OF B2B BUSINESSES CHOSE NOT TO ONBOARD NEW CLIENTS **DUE TO A FEAR OF FRAUD ATTACKS.**

The Anti-Fraud Self-Audit

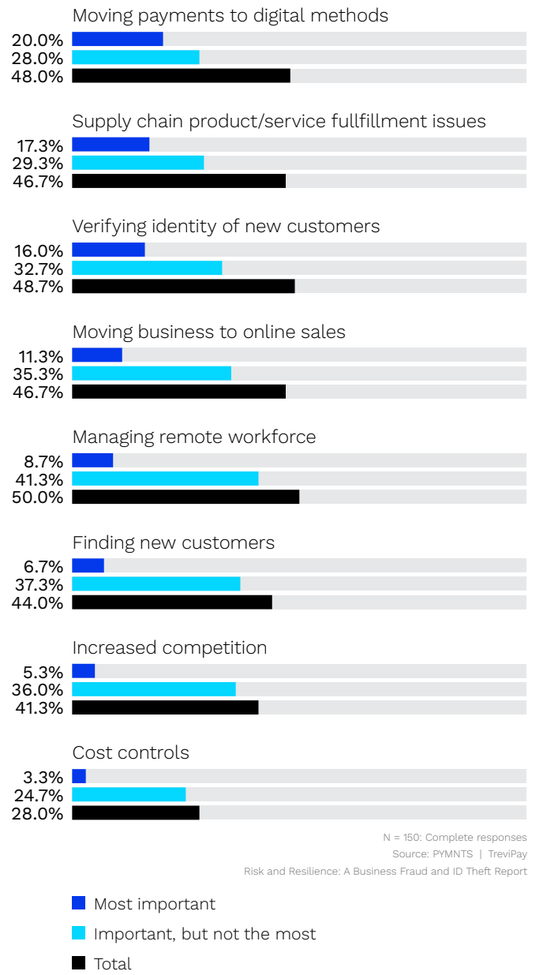
The first steps in modernizing anti-fraud strategy

While a new homeowner would be unlikely to wait until their home is burglarized before installing a lock on the front door, many businesses take a "wait-and-see" approach when it comes to fighting fraud, instituting basic anti-fraud methods at first, such as payment card verification at the time of purchase, and then enacting more robust measures, such as multichannel identity verification, depending on the severity of attacks.

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

Our research shows that a manual or reactive approach to preventing fraud has a serious impact on business growth. While most businesses use payment card verification as a key strategy, fraud is complex and requires a multichannel approach inclusive of identity verification. Nearly half of executives say that properly verifying the identities of new business customers is a challenge that their organizations have had to address.

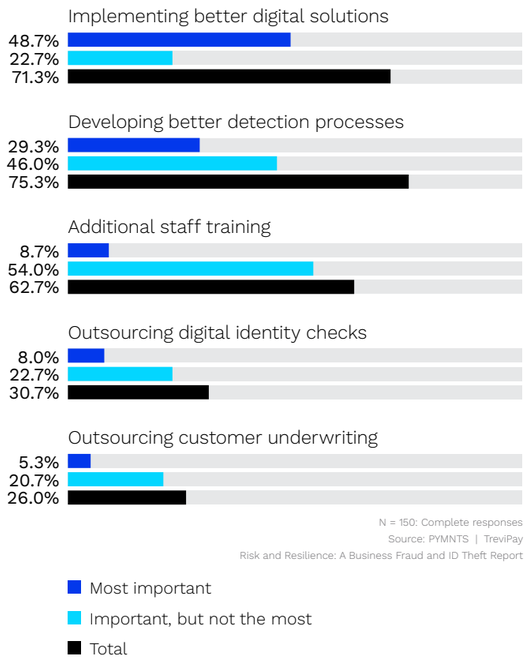
The problem for many businesses is that organizations need to assess technical debt as well as the effectiveness of their current anti-fraud methods to develop a road map for modernization. Old methods of verifying identities may not be well-suited for the age of embedded commerce, as fraud attacks may happen on and through an array of new platforms and devices. To avoid scaling financial losses, retailers, marketplaces and brands must take a modern approach to fighting B2B payments fraud.

PYMNTS.com | trevipay

REFRAMING
ANTI-FRAUD STRATEGY
DEVELOPING A PROACTIVE APPROACH TO FRAUD RISK MANAGEMENT

FIGURE 2:

BUSINESSES' ANTI-FRAUD STRATEGY EFFORTS
Share of businesses that consider plans addressing fraud-related concerns to be important



71%

SHARE OF ORGANIZATIONS THAT **PLAN TO IMPLEMENT BETTER DIGITAL SOLUTIONS** FOR FRAUD PREVENTION

Our research shows that 71% of organizations plan to implement better digital solutions for fraud prevention, and almost 50% consider it the most important plan to implement to prevent fraud-related issues.

For many businesses, anti-fraud modernization efforts may include working with a technology solutions provider to conserve technical resources and human talent, but the first step should be determining the efficacy of existing anti-fraud tools and identifying points of vulnerability.

The following five questions comprise a self-audit of risk management strategy for organizations seeking to modernize their anti-fraud efforts.

01 DO WE HAVE A COMPREHENSIVE, MODERN ANTI-FRAUD STRATEGY MODEL?

A strategy model represents an organization's approach to fraud monitoring and risk management. Manual, reactive strategy models tend to cost businesses more over time. Risk management approaches with the speed of innovation — with strategies and risk management policies adjusted according to fraud threats' evolution — are key to developing efficient anti-fraud practices.

02 IS OUR ANTI-FRAUD STRATEGY DEVICE-AGNOSTIC, SCALABLE AND PROACTIVE?

Most of the businesses in our survey have experienced a successful fraud attack. The ability to identify vulnerabilities to fraud and block them on any device as transaction volumes scale is essential for businesses seeking to limit risk effectively over time.

03 DO WE RELY ON THE ACCURACY OF MANUAL ANTI-FRAUD EFFORTS TO BLOCK ATTACKS, OR DOES OUR STRATEGY MATCH MODERN FRAUD TACTICS?

Organizations that use manual solutions or wait until evidence of fraud emerges may naturally experience greater revenue loss due to human error or inefficient identity verification or vetting procedures. For example, 46% of organizations using manual anti-fraud solutions said fraud concerns made it difficult for customers to work with them, whereas just 26% of organizations using automated anti-fraud solutions proactively said the same.

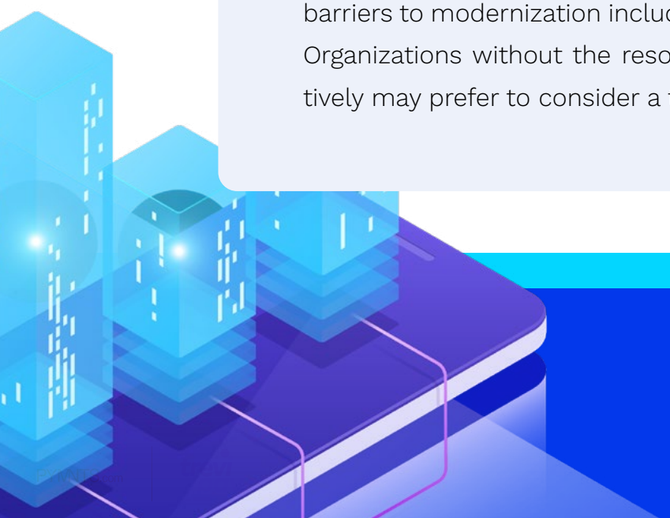
04 DOES OUR FORWARD-LOOKING FRAUD STRATEGY ENCOMPASS NEW DIGITAL SOLUTIONS? IF SO, HAVE WE ACCURATELY ASSESSED TECHNICAL DEBT AND THE RESOURCES NECESSARY TO LAUNCH A SUCCESSFUL AND FUTUREPROOF ANTI-FRAUD STRATEGY?

Our research shows that 71% 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. Key barriers to modernization include technical debt and limited resources. Organizations without the resources to manage modernization effectively may prefer to consider a third-party technical solution.

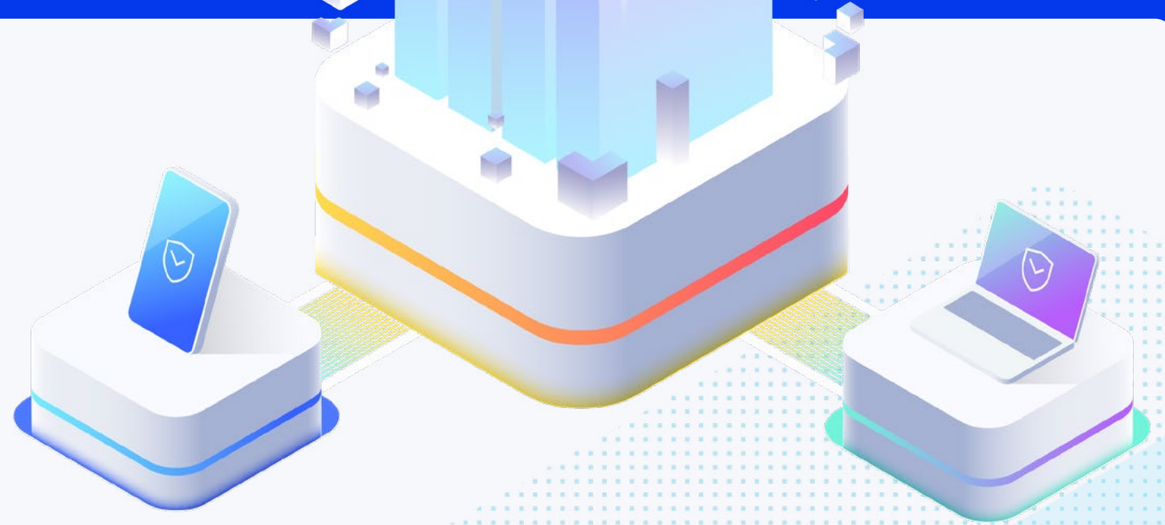
05 IS OUR ANTI-FRAUD STRATEGY HINDERED BY A LACK OF RESOURCES OR TECHNICAL EXPERTISE?

An agile, data-rich anti-fraud analytics system offers benefits for consumers and businesses seeking to reduce revenue loss. Digital transformation processes can be slow and costly as well as highly challenging to design and manage if an entity lacks the requisite expertise in anti-fraud methodologies and analytics automation. Partnership with a technical solutions provider can speed an organization's digital transformation efforts and ensure that its anti-fraud strategy can launch in a timely fashion as the business grows, even when resources are limited.

If an organization finds itself either saddled with technical debt or constrained by a lack of human resources or technical expertise, the following quick-start guidance may help businesses modernize their anti-fraud efforts quickly.



Developing and launching an anti-fraud strategy model



The first step in developing and launching a modern anti-fraud model is to understand its key components. Some important requirements for an anti-fraud strategy are as follows:

AUTOMATION

People skills are essential when dealing with clients online or face-to-face, but fraud is different. Relying on manual anti-fraud tactics often results in poor fraud monitoring outcomes, due to variable processing speeds and human error.

INTEGRATED PAYMENT CARD AND IDENTITY VERIFICATION

Payment card and identity verification work hand in hand as essential tools to block fraud attacks even at their most complex iterations, which can include synthetic identity creation (when legitimate consumer information is compiled to commit fraud) and fraudulent card-not-present transactions.

STRONG COMPLIANCE MANAGEMENT AND REPORTING FEATURES

Compliance is inextricable from anti-fraud efforts, as a business's success in each is interdependent. Organizations need true visibility across transactions as well as effective tools to speed or automate anti-fraud and compliance monitoring efforts. A single system that provides multichannel visibility and transaction management can help businesses streamline compliance and anti-fraud efforts.

SCALABILITY

Efforts to improve anti-fraud outcomes often entail improving invoicing, transaction management and overall accounts payable (AP) and accounts receivable (AR) process monitoring. A cloud-based solution can allow businesses to scale anti-fraud and identity verification processes as needed when transaction volume increases. This protects user experiences from interruption and allows businesses to maintain strong anti-fraud protocols as they grow.

While a third-party AP/AR solution with integrated anti-fraud tools can help organizations access modern anti-fraud tools quickly, this option is not the only method of reframing anti-fraud efforts. Here are three questions to ask when deciding if a third-party solution is the right choice:

01 CAN OUR CURRENT STRATEGY SCALE EFFECTIVELY?

Anti-fraud transaction monitoring efforts should be automated and seamless in operation and able to manage surges in transaction volume easily without compromising data tracking.

02 ARE AP/AR PROCESSES USER-FRIENDLY AND SECURE ACROSS ANY PLATFORM AND ON ANY DEVICE?

B2B transactions take place on a range of devices and platforms, and anti-fraud strategies should easily adapt to new payments models. User experiences should be frictionless and secure, providing intuitive user experience features, such as pay-by-invoice at checkout, that address fraud and poor user experiences simultaneously.

03 DOES OUR ANTI-FRAUD STRATEGY MATCH OUR CLIENTS' CHANGING PAYMENT NEEDS?

New business models often spur changes in the way B2B clients transact. When flexible payment terms are offered to new clients, anti-fraud controls should not be relaxed just because a new platform or payment service is being used.

If an organization struggles to meet the above standards independently, a third-party solution may be a wise choice.

Choosing a third-party anti-fraud solution

Barriers to innovation strategy include overreliance on legacy tools, limited human and technological resources and professional knowledge gaps around modern anti-fraud tools and risks. Many businesses turn to third-party anti-fraud solutions to launch a modern strategy quickly. Business growth is often directly related to an organization's confidence in its anti-fraud strategy, and the right mix of features and fraud protections are essential for businesses to scale effectively. Here are four key features to look for:

01

THE ABILITY TO MANAGE OMNICHANNEL SALES AS BUSINESS OPERATIONS SCALE

02

SECURE, FRICTIONLESS INVOICING AND AP/AR MANAGEMENT FEATURES

03

ANTI-FRAUD MONITORING TO COVER TRANSACTIONS USING MULTIPLE PAYMENT METHODS

04

ONBOARDING THAT PROMOTES STREAMLINED IDENTITY VERIFICATION PROCESSES WITHOUT COMPROMISING SECURITY

Our research finds that at least one-quarter of organizations reported that fraud-related concerns made a "very" or "extremely" large impact on their ability to expand operations.

FIGURE 3:

FRAUD'S IMPACT ON BUSINESS GROWTH
Share of businesses that identified fraud-related concerns as having a "very" or "extremely" large impact on their ability to expand operations since the beginning of 2020

Source: PYMNTS | TreviPay
Risk and Resilience: A Business Fraud and ID Theft Report

Organizations that use proactive, automated solutions, however, were the least likely to be impacted by fraud-related concerns. The wrong anti-fraud toolset also impacts user experience: Survey respondents reported that fraud-related concerns caused customers to report that it was difficult to maintain business relationships with them — an additional concern for companies banking on user experience to drive growth.

CONCLUSION

B2B businesses face a range of challenges in managing risk: growth often requires innovation to remain competitive and that means greater exposure to fraud attacks as business reach grows. Anti-fraud strategy modernization requires significant expertise in managing the unique challenges of innovation and evolving fraud threats simultaneously. For many businesses, a third-party anti-fraud solution can provide a simple option for quick-starting a scalable anti-fraud strategy. Businesses hoping to fight fraud successfully while growing their operations must implement proactive strategies — preferably leveraging the efficiencies of automated anti-fraud technologies — to protect revenues and customers over time.

METHODOLOGY

Reframing Anti-Fraud Strategy: Developing A Proactive Approach To Fraud Risk Management 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 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.

REFRAMING
ANTI-FRAUD
STRATEGY

DEVELOPING A PROACTIVE APPROACH TO FRAUD RISK MANAGEMENT

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