FIS | worldpay from FIS

GLOBAL PAYMENT RISK MITIGATION

Results and analysis from Worldpay's 2021 Payment Risk Mitigation survey

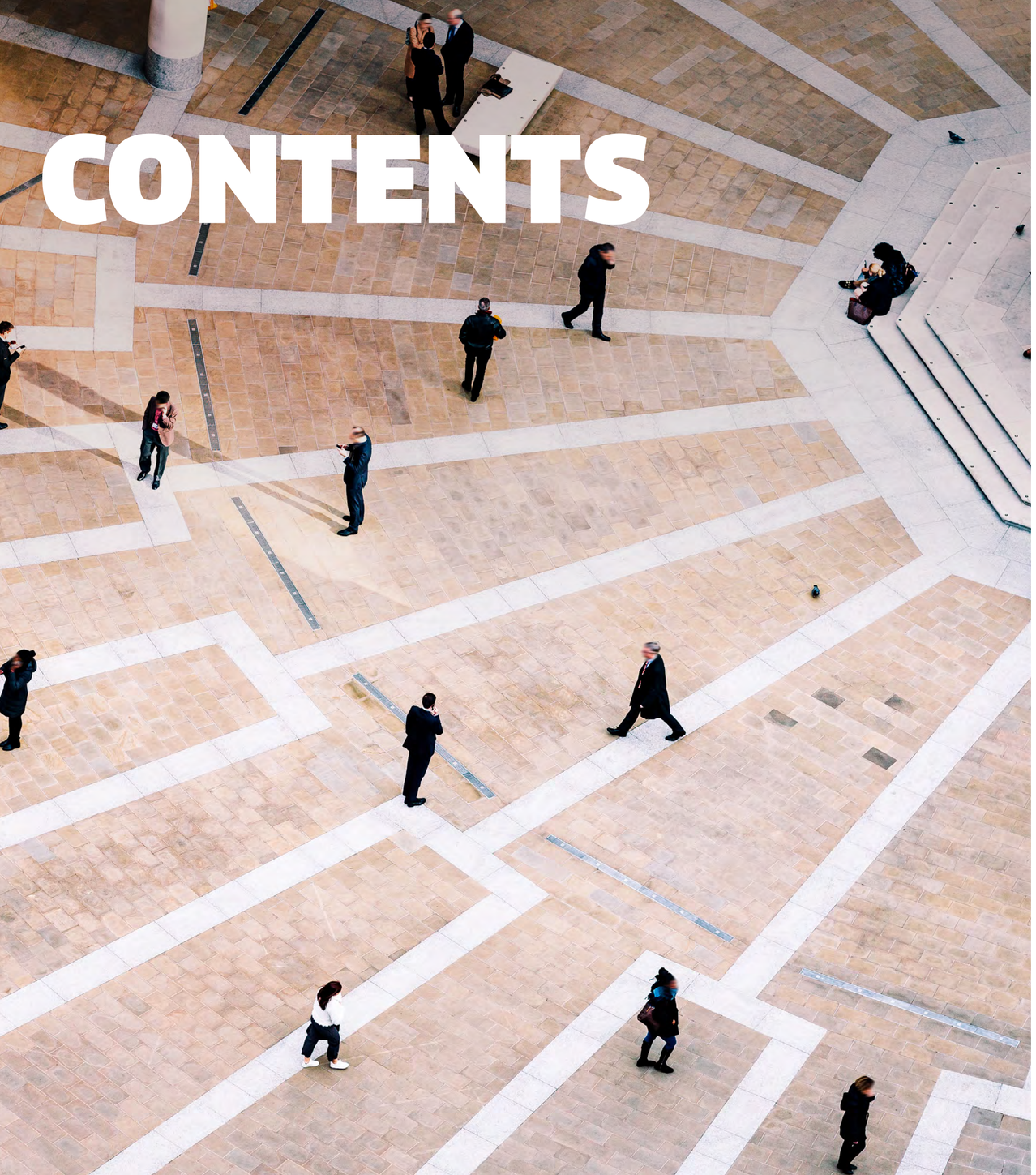
LET'S REINVENT SMARTER at fisglobal.com

NEARLY 38%

of merchants lost at least 6% of their revenue to payment fraud in 2020

TWO-FACTOR AUTHENTICATION

was cited as “very important” by nearly half of merchants surveyed



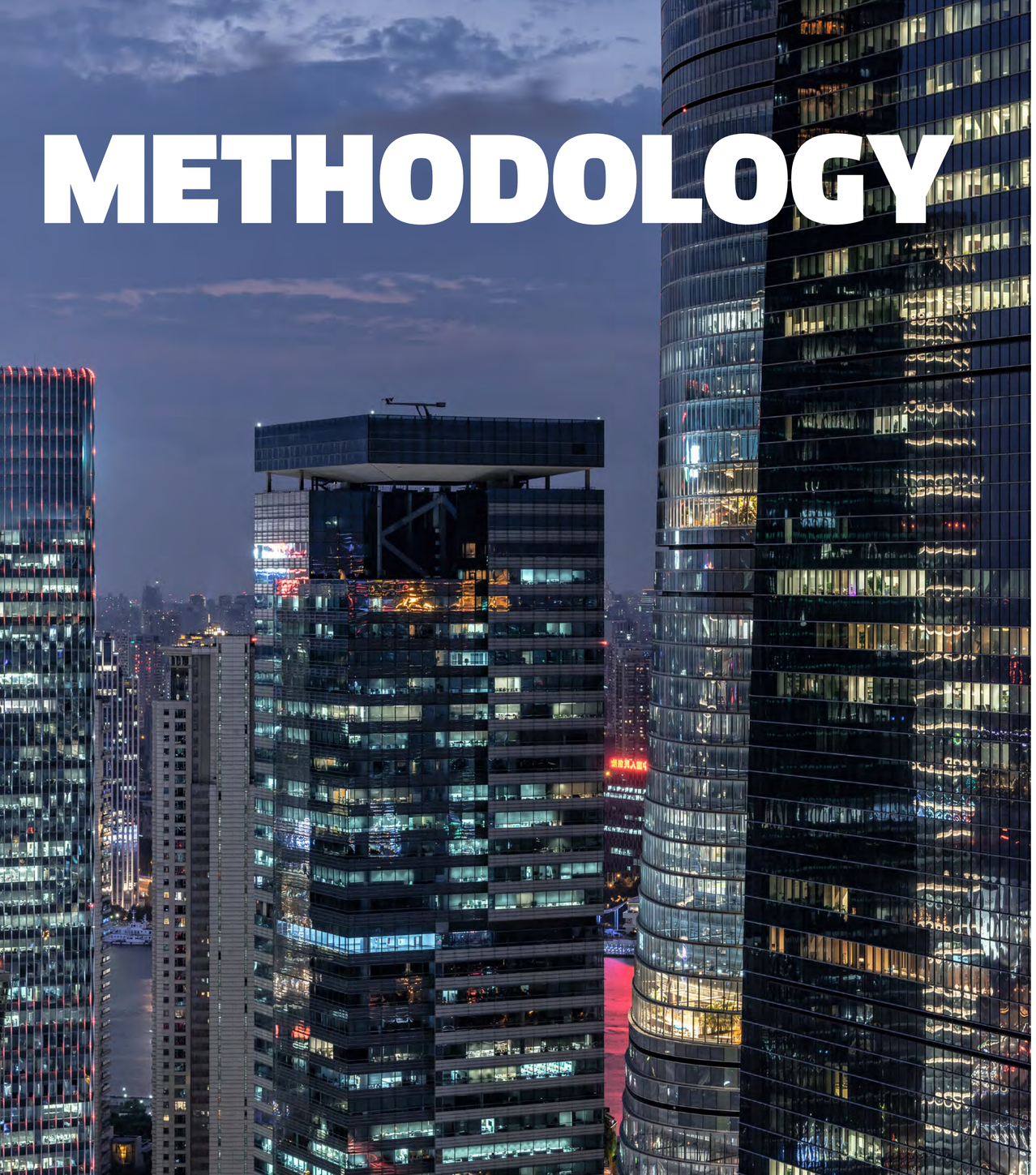
CONTENTS

INTRODUCTION

Merchants are overcoming payment challenges with cutting-edge tools, best practices and partnerships that work together as one

The Worldpay from FIS® 2021 Global Payment Risk Mitigation report offers an overview of the global payment fraud landscape, including the top payment trends and challenges merchants faced in 2020, and their plans to rebuild smarter in 2021. **We went directly to global merchants themselves for answers**.

We asked about payment and fraud mitigation initiatives, the investments merchants are prioritizing, the return they're seeking to realize from those investments, and how they're evaluating fraud detection and ID verification solutions. We conclude with key takeaways for merchants from our team of payment risk mitigation experts.



METHODOLOGY

In December 2020, Worldpay from FIS commissioned Forrester Consulting to conduct a study of global online and enterprise merchants to better understand how they perceive payments risk. We explored merchants' views related to payment card fraud, authentication, chargebacks, consumer experience, risk management, losses, recovery rates and tools deployed.

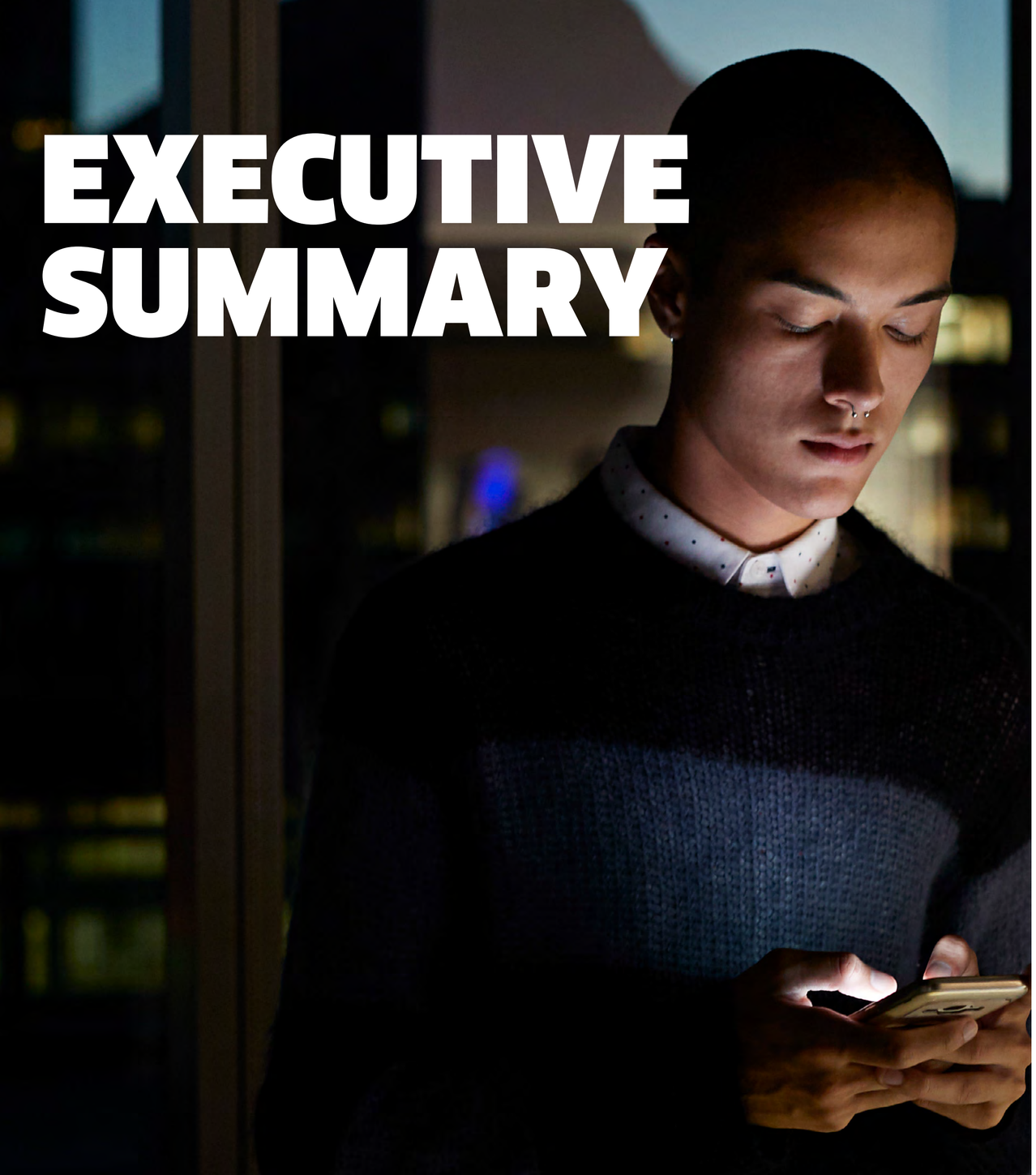
We surveyed 671 C-level executives, vice presidents, directors, managers and other decision-makers. Participants were selected across functional areas including compliance/risk management, e-commerce and digital businesses, finance, accounting, payments, IT/technology and operations. The overwhelming majority of survey respondents were the final decision-maker or part of a team of decision-makers for their organization's customer-facing security, fraud detection and/or ID verification efforts.

Survey participants included merchants from Argentina, Australia, Brazil, Canada, France, Germany, Japan, Mexico, Singapore, the U.K. and the U.S. Survey participants represented airlines, dating apps, financial services, hospitality, insurance, internet gambling, logistics, omnichannel retail, online education, online gaming, retail, transportation, travel and video game industries.

All statistics and trends mentioned in this report represent the result of Worldpay from FIS' 2021 Payment Risk Mitigation survey, unless specified otherwise.

11 Countries

600+ C-level executives, vice presidents, directors, managers & other decision makers were surveyed



EXECUTIVE SUMMARY

Merchants enter 2021 facing daunting payment challenges

Payment challenges span the payments life cycle, from pre-transaction authentication, fraud detection and mitigation to post-transaction chargeback deflection and recovery. These challenges intensified in 2020 with COVID-19, elevating the priority of merchants' mitigation efforts in 2021.

Merchants want solutions that simplify fighting fraud and chargebacks

Merchants surveyed are focused on measures that protect their hard-earned revenue. That's especially true for global enterprise and e-commerce merchants whose scale magnifies the bottom-line importance of properly managing payment risk.

The costs of fraud can determine success

38% of merchants report losing 6% or more of their revenue to payment fraud. Challenges cited include the costs of payment acceptance, security and payment fraud. IT implementations, customer data security and cross-channel payment solutions urgently demand merchants' attention.

Merchants report widespread increases in e-commerce fraud, synthetic ID and new account fraud

The impacts of payment fraud cut across cultures, economies and geographies, from revenue and productivity losses to increased operational expenses and customer churn.

The impact of payment fraud and chargebacks isn't felt by merchants equally

More than two-thirds of merchants surveyed are satisfied or very satisfied with their current fraud management solution. Nearly half (46%) use a best-practice hybrid approach that mixes rule-based decision-making with adaptive machine learning technologies.

Managing risk and protecting revenues requires dynamic protection against fraud

Merchants are overcoming payment challenges with a mix of cutting-edge tools, best practices and partnerships that work as one to reduce risk, promote customer experiences and safeguard the future.

OVERVIEW OF PAYMENT AND FRAUD LANDSCAPE

TOP PAYMENT CHALLENGES

Safeguarding merchant revenue requires smart, dynamic protection against fraud throughout the payments life cycle

Understanding the challenges that inevitably arise throughout that life cycle is a critical first step in reducing payment risks.

When asked about leading payment-related challenges in 2020, merchants' top concerns related to costs. **IT upgrade costs were cited by 30% of our respondents,** while 25% cited the costs of payment acceptance (interchange, processor, and network fees) as a leading challenge.

Fraud and security issues proved challenging to merchants in 2020. Implementation of security efforts such as tokenization and 3DS2 was cited as a top challenge by 25% of respondents, while **21% faced higher volumes of sophisticated payment fraud, such as card testing.**

21%

of merchants faced higher volumes of sophisticated payment fraud, such as card testing

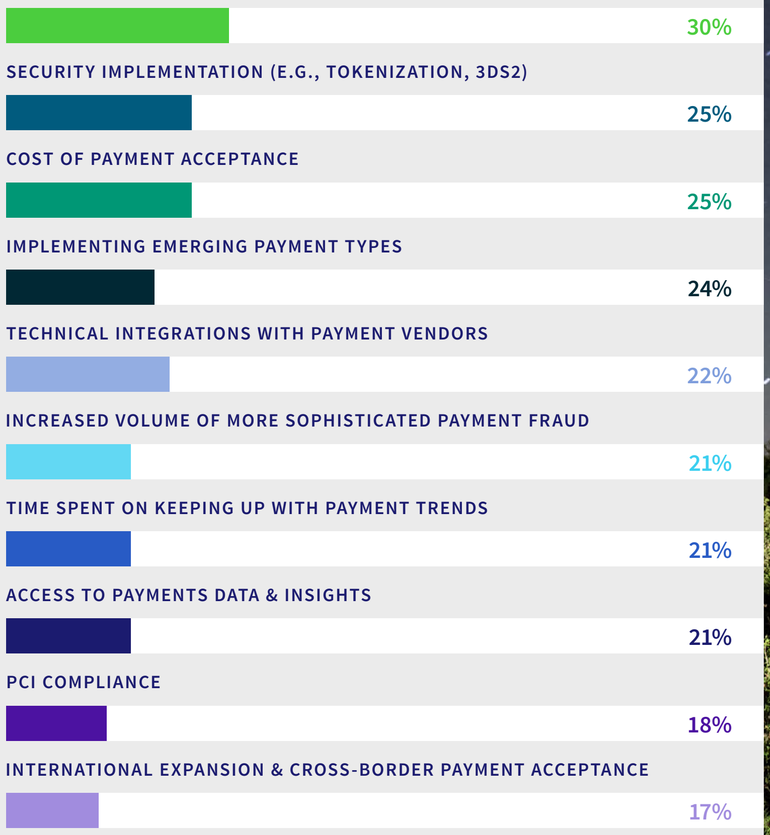
FAST FACTS

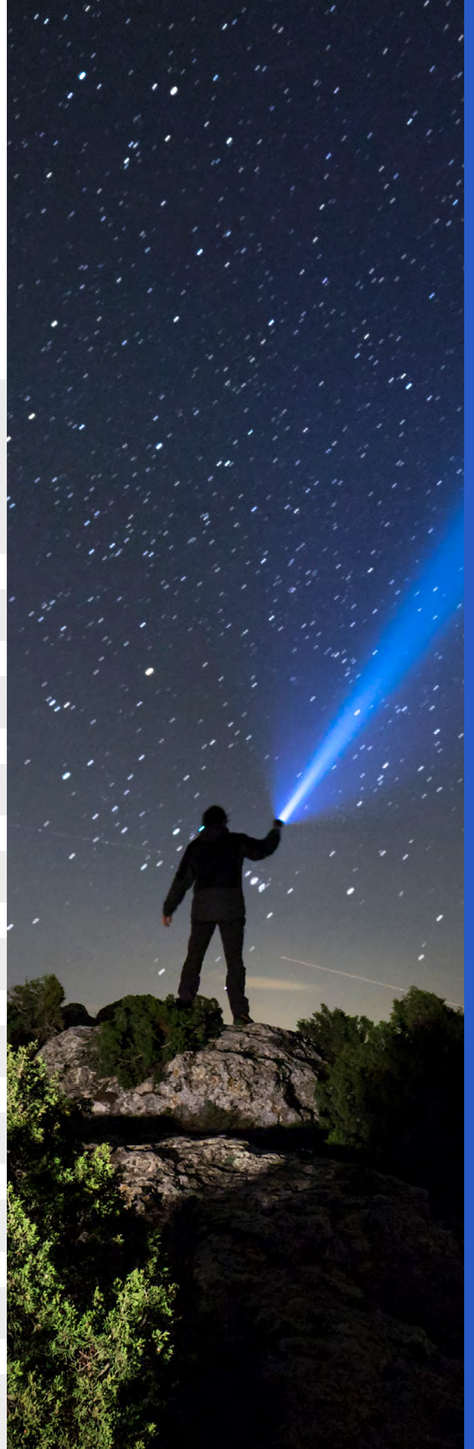
IT upgrades and **the costs of payment acceptance** are top merchant challenges

1 in 4 merchants are challenged by efforts required to implement payment security solutions

Access to payment **data and regulatory compliance** are merchant pain points

WE ASKED: WHAT ARE THE TOP PAYMENT CHALLENGES THAT YOUR TEAM FACED IN THE LAST 12 MONTHS?





FURTHER INSIGHTS

Top challenges for APAC merchants included IT upgrade costs (29%), **security implementation like tokenization and 3DS2 (28%)** and technical integrations with payment vendors (27%).

IT upgrade costs (31%), access to payments data and insights (29%) and the **cost of payment acceptance (28%) were cited most often as challenges** by respondents in Europe.

North American respondents reported **challenges with the implementation of new emerging payment types** (31%), IT upgrade costs (31%) and security implementations (27%).

Implementation of new emerging payment types (32%), **security implementations (30%)** and IT upgrade costs (29%) posed the most widespread challenge for South American merchants.

The implementation of new and emerging payment types and managing chargebacks are proving especially **challenging in online gambling**, each cited as a top challenge by 31% of respondents in the internet gambling industry.

PRIORITIZING PAYMENT CHALLENGES TODAY

If your business faces payment fraud challenges, you're not alone. Addressing the core issue of managing payment fraud is widespread, being "very challenging" or a "critical challenge" for more than half of businesses in our survey. **Securing customer data is another top priority among merchants and a "critical" challenge for one-in-five merchants surveyed.**

A recurring theme in the results of our survey were the difficulties businesses experienced managing payments in-house. The complexity of managing multiple payment solutions, keeping pace with new payment methods and rising consumer expectations, managing multiple payment partners and the lack of internal payment expertise are challenges that weigh heavily on today's merchants.

WE ASKED: HOW CHALLENGING ARE THE FOLLOWING TO YOUR BUSINESS TODAY?

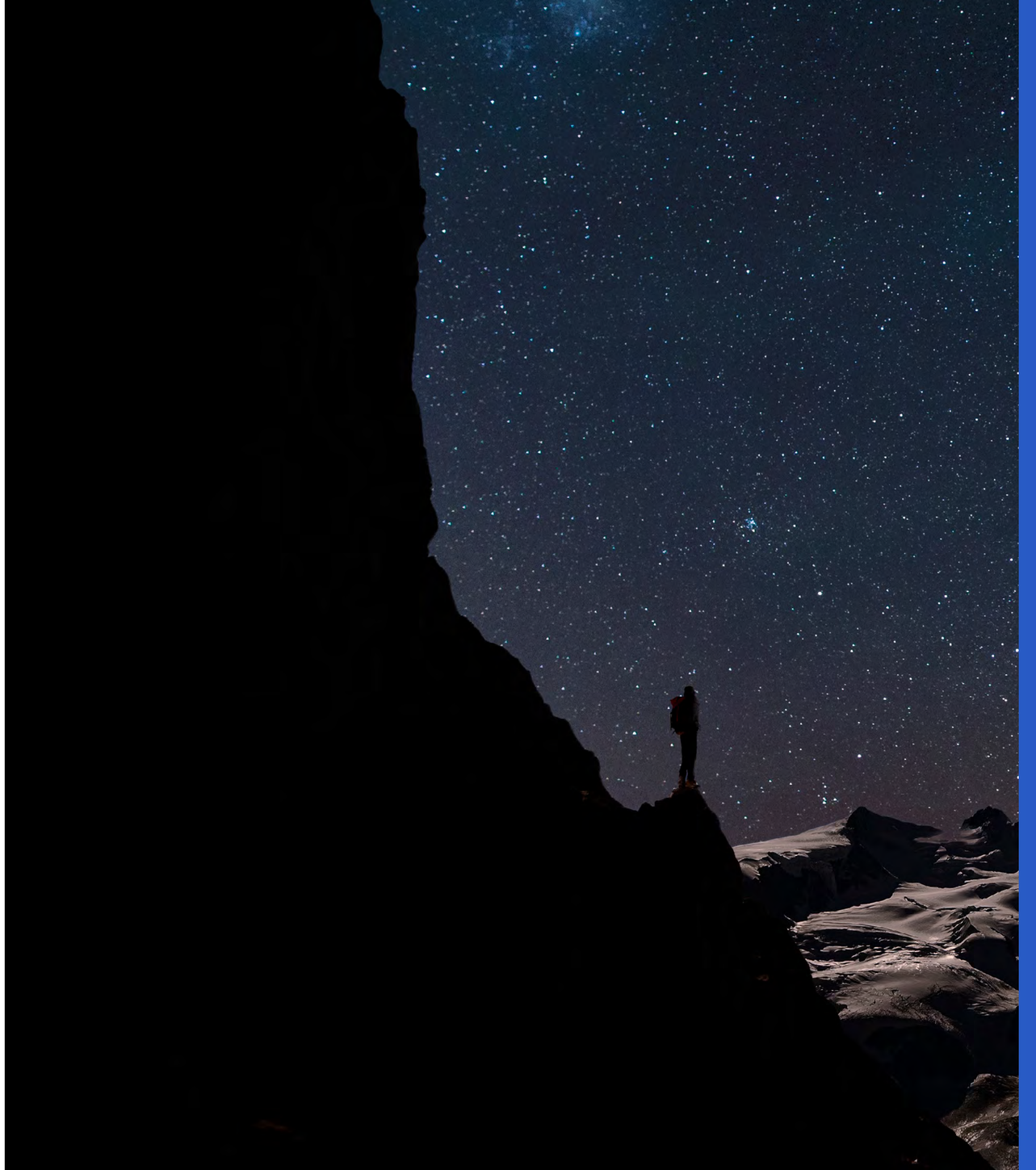
	CRITICAL CHALLENGE	VERY CHALLENGING	NOT CHALLENGING
PAYMENT FRAUD	22%	33%	4%
CUSTOMER DATA SECURITY	20%	31%	5%
COMPLEXITY OF MULTIPLE PAYMENT SOLUTIONS/PARTNERS	18%	33%	7%
INTEGRATING PAYMENT SOLUTIONS ACROSS CHANNELS	17%	31%	7%
TRACKING ROI OF PAYMENT SOLUTIONS	16%	31%	5%
COST OF EXPANDING CROSS-BORDER	18%	28%	5%
NUMBER OF PAYMENT TYPES WE NEED TO SUPPORT	16%	30%	7%
RISING CUSTOMER EXPECTATIONS AROUND PAYMENT CHOICE	16%	30%	5%
LOCAL PAYMENT-RELATED REGULATIONS	16%	30%	7%
LACK OF LOCAL MARKET SUPPORT	18%	27%	8%
LACK OF INTERNAL PAYMENT EXPERTISE	15%	29%	8%

FAST FACTS

A majority (55%) of merchants find **payment fraud significantly challenging**

Merchants struggle managing **payment complexity**

Customer data security is a critical challenge for **1 in 5 merchants**



FURTHER INSIGHTS

Top challenges for APAC merchants included integrating payment solutions across channels, **navigating the complexities of multiple payment solutions** and managing rising customer expectations around payment choice.

Payment fraud proved most challenging for European merchants. Beyond fraud, respondents cited managerial challenges as their highest concern, including a **lack of local market support** and the complexity of administering multiple payment solutions.

Managing payment fraud and data security issues were top challenges in North America. A majority of North American merchants cited the rising number of payment types requiring support and a **lack of internal payment expertise** as “very challenging” or a “critical challenge.”

Managing payment fraud and customer data security proved most challenging for South American merchants. More than half (55%) of merchants in South America cited **managing the complexity of local payment regulations** as “very challenging” or a “critical challenge.”

2020 FRAUD TRENDS

Synthetic identity fraud, account takeover fraud, identity theft and new account fraud rose in 2020 for more than half of global merchants surveyed

The Coronavirus pandemic caused massive disruption throughout the global economy in 2020. Among the most important consequences for merchants was an uptick in payment fraud. One potential reason for this could be because fraudsters saw disruptions to established consumer patterns as an opportunity, adding additional challenges to merchants already operating under adverse conditions.

The scope of the fraud increases in 2020 was broad: more than half of survey respondents indicated they experienced more of every type of payment fraud. **Over 80% of respondents globally reported the same or higher volumes of all payment fraud types** in 2020 versus 2019.

Increases in card-not-present fraud were reported by 59% of merchants, including 21% citing significantly more fraud volume in 2020 versus 2019. A majority of businesses surveyed cited increasing levels of chargeback and “friendly” fraud in 2020, with one in five merchants citing significantly higher volume of consumers disputing valid charges year over year.

Synthetic identity fraud, account takeover fraud, **identity theft and new account fraud rose in 2020 for more than half of global merchants** surveyed, highlighting the importance of customer authentication efforts.

59%

of merchants reported increases in card-not-present fraud

FAST FACTS

Synthetic identity fraud and **new account fraud** are growing trends

Nearly **6 in 10 merchants reported higher rates** of e-commerce fraud in 2020

Fraud is broad: **more than half** of merchants experienced more of all fraud types

WE ASKED: HAS YOUR COMPANY DETECTED LESS, MORE OR AN EQUAL AMOUNT OF THE FOLLOWING TYPES OF PAYMENT FRAUD IN 2020 VERSUS 2019?

	SIGNIFICANTLY MORE	SLIGHTLY MORE	SAME	SLIGHTLY LESS	SIGNIFICANTLY LESS
CARD-NOT-PRESENT FRAUD (E-COMMERCE, ETC.)	21%	38%	25%	12%	3%
SYNTHETIC IDENTITY FRAUD	21%	34%	28%	11%	5%
CHARGEBACK FRAUD (DISPUTING VALID CHARGES)	20%	35%	30%	11%	3%
CARD TESTING	20%	33%	32%	12%	3%
IDENTITY THEFT/NEW ACCOUNT FRAUD	20%	32%	30%	13%	5%
FRIENDLY FRAUD	22%	29%	31%	13%	5%
ACCOUNT TAKEOVER FRAUD	20%	30%	31%	13%	5%

FURTHER INSIGHTS

Increases in synthetic identity fraud were reported most by survey respondents in APAC. 61% of APAC merchants reported **higher rates of synthetic identity fraud**.

A rise in **card-not-present fraud** was reported most widely in Europe, cited by 59% of respondents in both Germany and the U.K.

As e-commerce surged during the pandemic, **two in three** North American merchants reported more card-not-present fraud in 2020; 61% reported more chargeback fraud than in 2019.

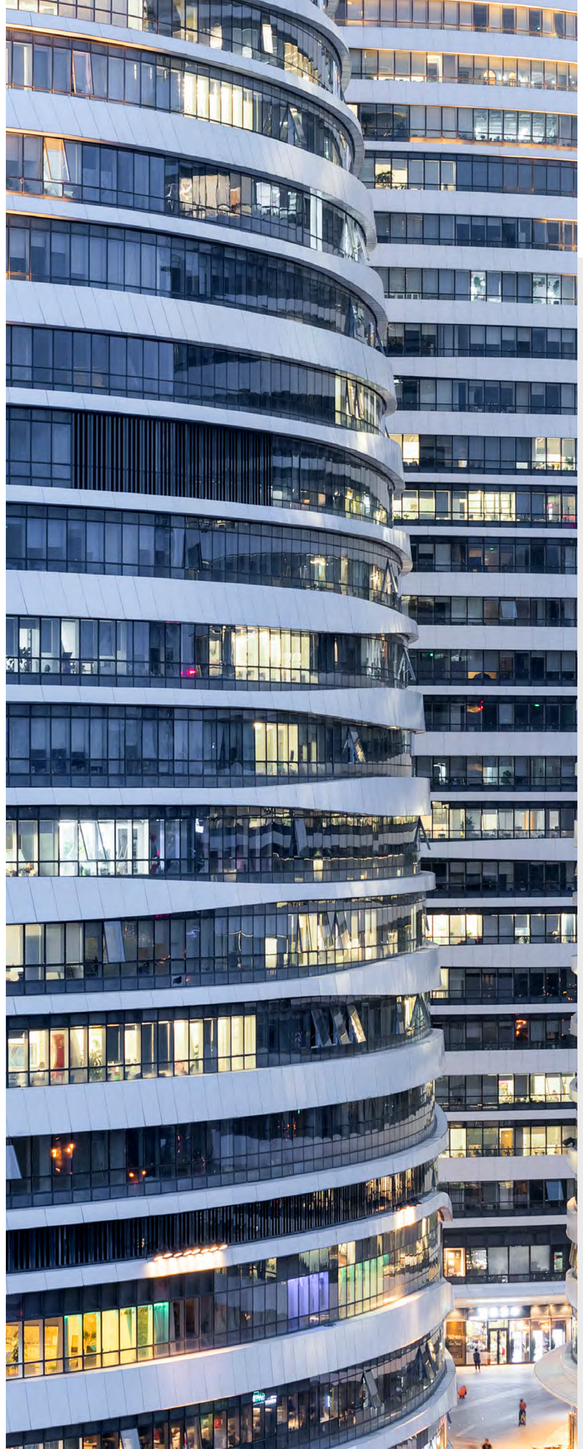
Merchants in South America detected card-not-present fraud, chargeback fraud and card testing most among fraud types in 2020. **Significantly higher volumes** of card-not-present fraud and identity theft/new account fraud were reported by one in four merchants.

THE IMPACT OF PAYMENT FRAUD

Payment challenges have widely varied impacts on merchants. We wanted to better understand the intensity of those challenges – globally, across regions and across merchant sectors.

Unsurprisingly, merchants report that the direct costs of payment fraud are substantially impacting financial performance. Direct revenue losses due to higher chargeback volume, back-office operational expenses and legal fees cause significant impact to merchants' bottom lines.

Beyond the bottom line, the indirect costs of payment fraud also weigh heavily on merchants. Opportunity costs of fraud are significant, with **60% of merchants citing that lost productivity due to payment fraud had a substantial or significant impact on their businesses**. Customer churn, negative publicity and reputational damage stemming from payment fraud are also top merchant concerns.



WE ASKED: WHAT IMPACT DOES PAYMENT FRAUD HAVE ON THESE AREAS OF YOUR BUSINESS?

	SUBSTANTIAL/ SIGNIFICANT	SOME/ MINIMAL	NO IMPACT
REVENUE LOSS	60%	38%	2%
LOST PRODUCTIVITY	60%	37%	3%
DIGITAL PAYMENT FRAUD (E.G. DIGITAL WALLETS, MOBILE TRANSACTIONS)	59%	38%	3%
CUSTOMER CHURN	58%	38%	4%
INCREASED BACK OFFICE OPERATIONAL EXPENSES	58%	40%	2%
CHARGEBACKS	58%	40%	2%
INCREASE IN COSTS FOR LEGAL DEFENCE AND/OR PUBLIC RELATIONS SERVICES	57%	40%	3%
BAD PUBLICITY/BRAND OR REPUTATIONAL DAMAGE	56%	40%	4%
FRAUD LOSS WRITE-OFFS	56%	42%	2%
FINES/LAWSUITS FOR NONE-COMPLIANCE WITH REGULATIONS	54%	41%	5%
INCREASE IN COSTS FOR VICTIM REMEDIATION	53%	45%	2%

FAST FACTS

Revenue loss from payment fraud had a significant impact on **6 in 10** businesses

Merchants are understandably concerned about **reputational damage from fraud**

Payment fraud affects more than just revenue loss as merchants' impact to bottom lines also include **back office expenses, productivity loss and customer churn**

FURTHER INSIGHTS

Increased costs for **remediation of payment fraud victims** in 2020 negatively impacted merchants in APAC, with 57% reporting substantial or significant impacts.

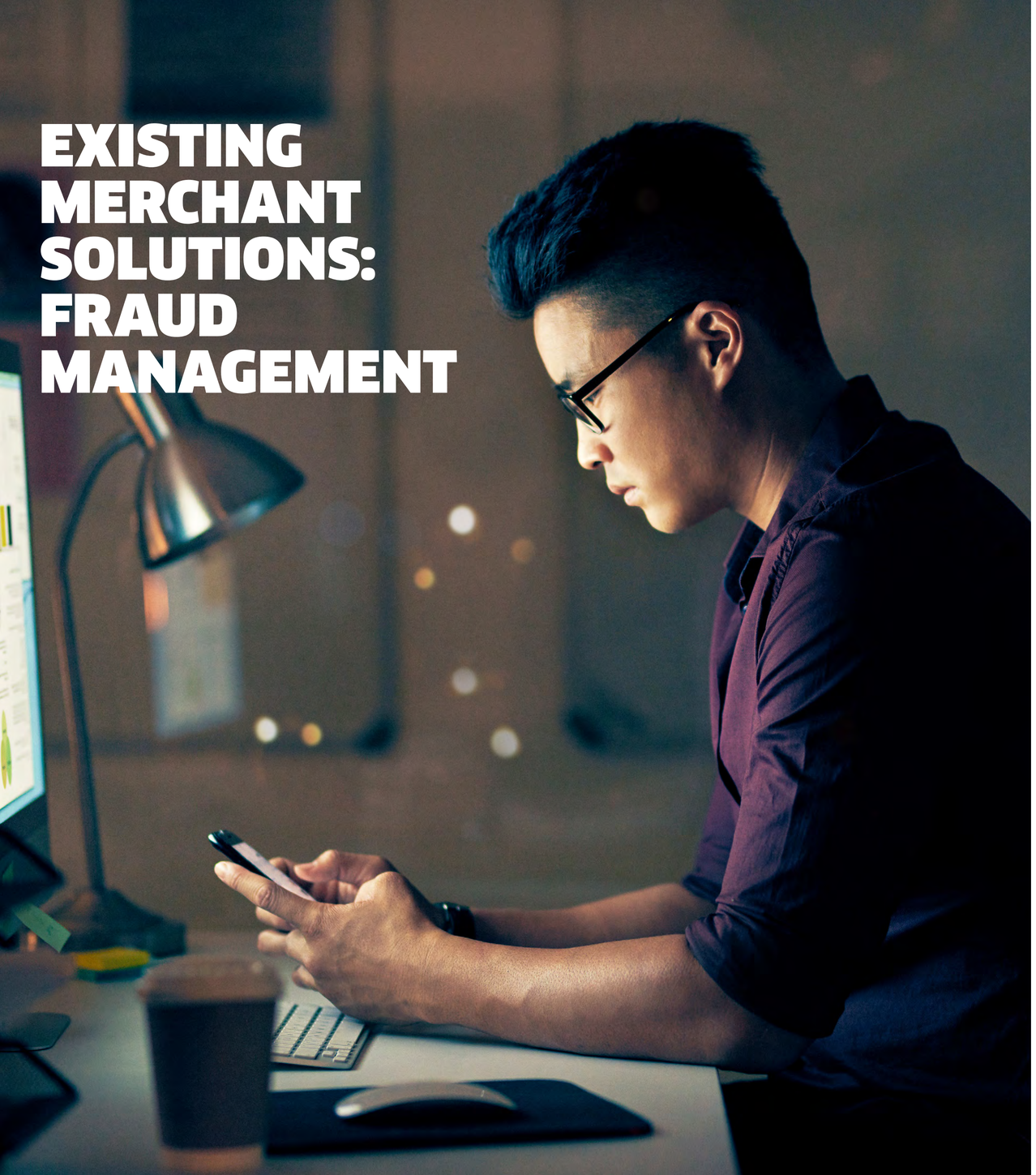
More than half (51%) of European merchants reported chargebacks having substantial or **significant impacts on their businesses**.

Fraud loss write-offs are of notable concern in North America, with **6 in 10 merchants citing write-offs** as having a significant or substantial business impact, including 66% of U.S. merchants.

Fraud-related productivity losses proved vexing to South American merchants, cited as causing significant or **substantial impact by 69% of merchants**.

The impact of payment fraud on customer churn is impacting video game businesses, noted as having significant or **substantial impact by 62% of gaming industry respondents**.

Fraud's impact on back-office operational expenses was cited as a concern by **71% of global retailers**.



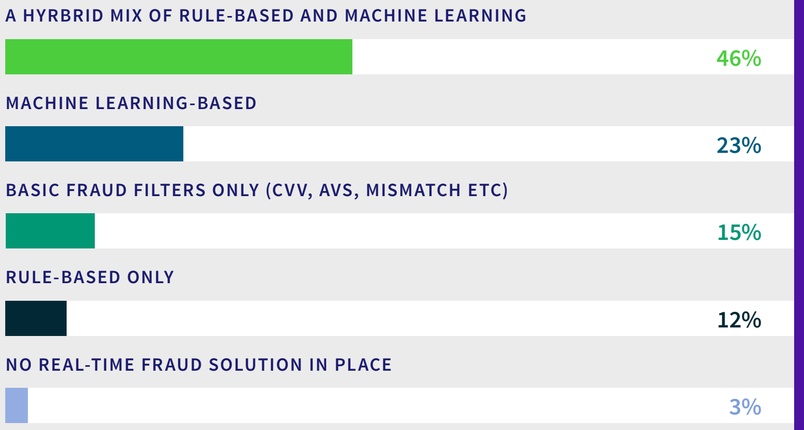
EXISTING MERCHANT SOLUTIONS: FRAUD MANAGEMENT

Real-time fraud management solutions in the marketplace today vary considerably and are evolving at an accelerating pace. Legacy methodologies and systems continue to be leveraged, competing with a new generation of solutions that combine the latest technologies like machine learning with best practices informed by data from billions of transactions.

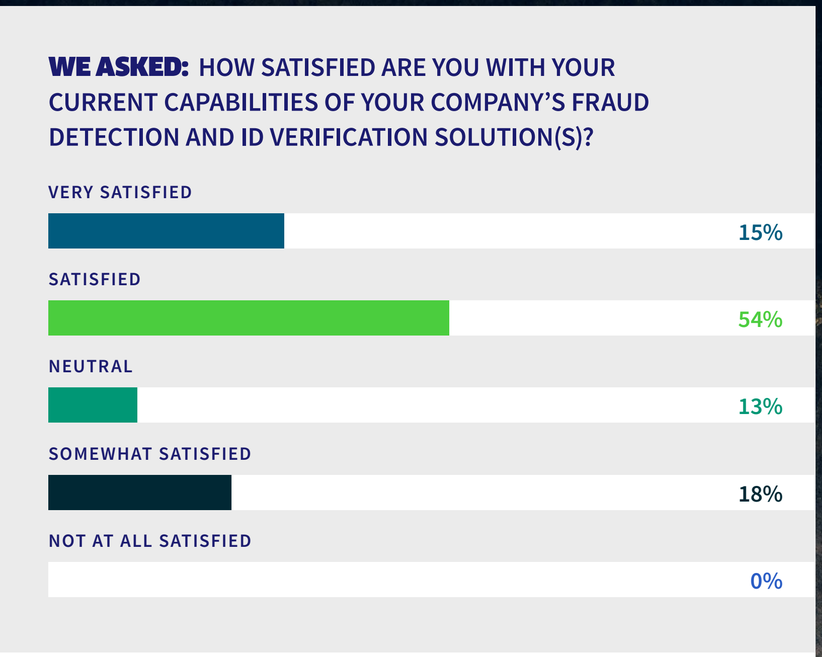
A hybrid approach that mixes rule-based decision-making with adaptive machine learning technologies is favored by 46% of merchants.

Approaches that rely exclusively on machine learning were reported as being used by 23% of merchants surveyed. Legacy approaches that utilize basic fraud filters are used by 15% of merchants, while 12% rely only on rule-based decision-making. A small number of merchants (3%) forge ahead with no real-time fraud solution.

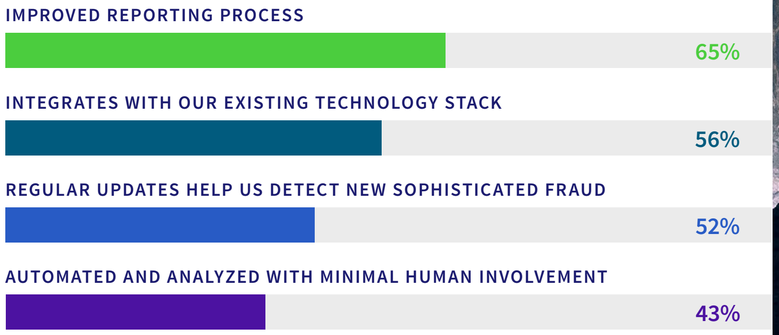
WE ASKED: HOW WOULD YOU BEST DESCRIBE YOUR CURRENT FRAUD MANAGEMENT SOLUTIONS?

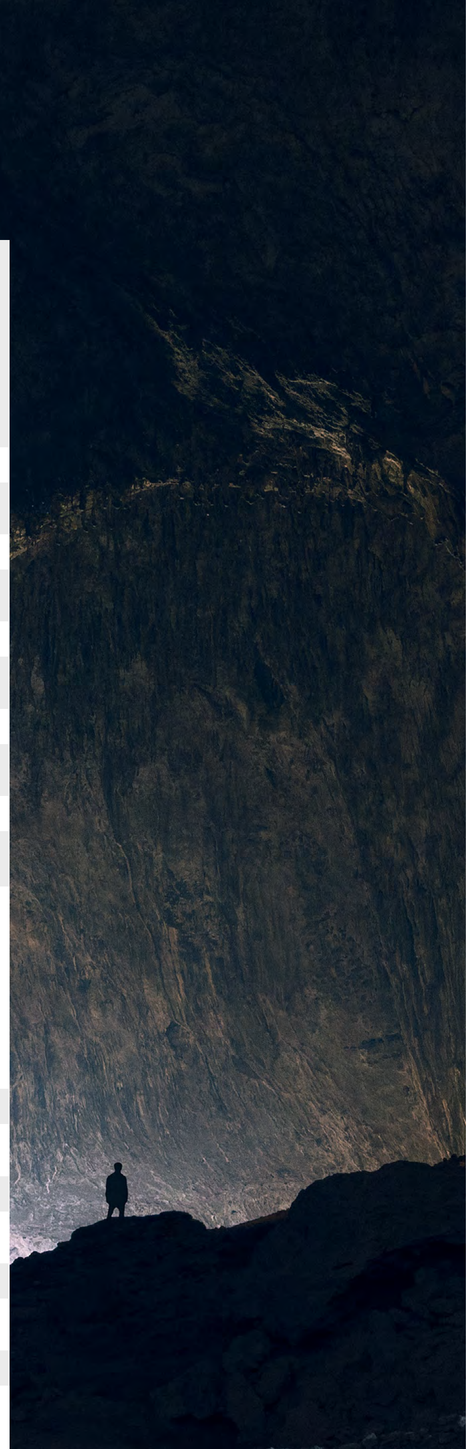


WE ASKED: HOW SATISFIED ARE YOU WITH YOUR CURRENT CAPABILITIES OF YOUR COMPANY'S FRAUD DETECTION AND ID VERIFICATION SOLUTION(S)?



AMONG MERCHANTS REPORTING BEING SATISFIED OR VERY SATISFIED WITH THEIR CURRENT SOLUTION, **WE ASKED** WHY THEY WERE SATISFIED?





Among merchants unsatisfied with their current fraud management solution, increased customer churn and an inability to detect new sophisticated fraud were each cited by half of merchants as a primary reason for their dissatisfaction. **Loss of revenue was the cause for 49% of merchant's dissatisfaction**, while 46% of those dissatisfied stated that their solution was not making a difference in mitigating fraud.

Among the 69% of survey respondents who were satisfied or very satisfied with their current fraud management solution, improved reporting processes were cited most often (65%) as a reason for satisfaction. Merchants valued ease of integration with existing technology stacks, cited by 56% of satisfied merchants. More than half (52%) cited systems that offer regular updates to detect new sophisticated fraud as a reason for their satisfaction levels, while **43% cited automated systems that minimized human involvement**.

FURTHER INSIGHTS

Hybrid fraud management solutions are favored by 68% of merchants surveyed in Mexico.

Merchants in Australia reported considerable satisfaction, with 90% reporting that they were satisfied (70%) or very satisfied (20%) with their existing fraud solutions.

The quality of **real-time reporting on fraud mitigation is a critical component** of merchant satisfaction in North America, cited by nearly three-quarters (74%) of merchants in the U.S.

Among merchants reporting a **lack of satisfaction with their current fraud solution**, 67% of video game merchants and 71% of travel and hospitality merchants cited not seeing a difference in the mitigation of fraud.

PRO TIPS

- Balancing efforts to stop fraud with **reducing impacts on customer experience** (e.g. false positives) is key to successful fraud mitigation solutions.

- Legacy fraud solutions are effective in mitigating basic fraud events. However, investing in **more robust fraud detection** and prevention solutions – such as those that use machine learning – will help mitigate advanced fraud events with greater accuracy.

- Fighting fraud effectively is difficult work that's constantly evolving. Merchants should therefore **turn to industry experts** for guidance and the latest best practices.

SUNNY THAKKAR
SENIOR PAYMENTS FRAUD MANAGER
WORLDPAY FROM FIS

THE BOTTOM LINE: THE TOTAL COST OF FRAUD

38%

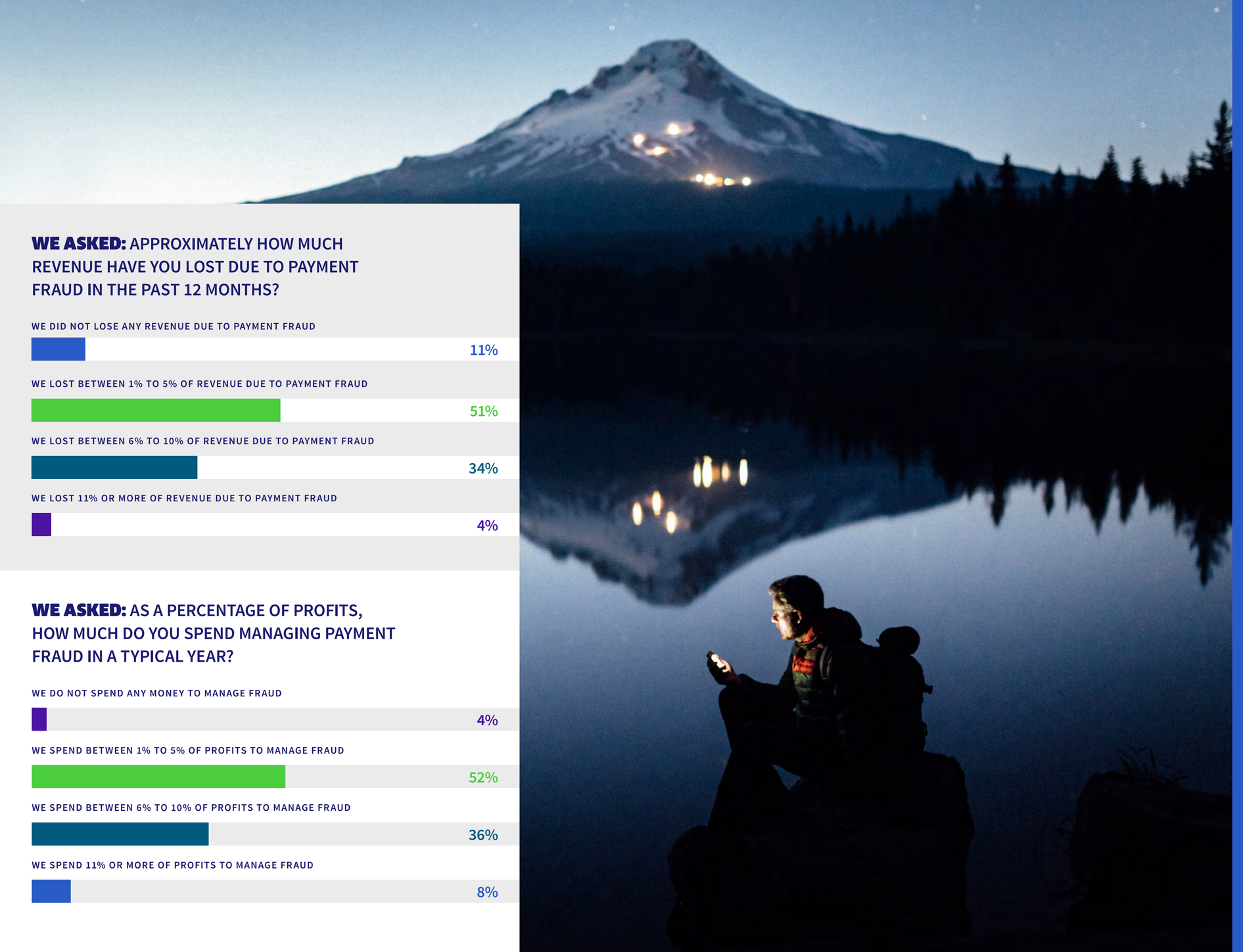
of merchants lost 6% or more of their revenue due to payment fraud in 2020.

The goal of efforts to better understand payment risk and manage fraud is to identify and implement solutions that protect your hard-earned revenue

Direct merchant revenue losses as a result of payment fraud vary, though are widespread globally: **89% of merchants reported losing at least 1% of revenue in 2020**. Nearly 38% lost 6% or more of their revenue due to payment fraud in 2020.

When assessing the bottom-line impact of fraud, direct losses are only part of the equation. While taking the appropriate steps to minimize fraud-related losses is critical, managing the costs of those efforts is a key consideration for merchants.

A majority (52%) of merchants surveyed reported **spending between 1% and 5% of profits in their efforts to fight and manage payment fraud** in a typical year. Almost half (44%) of merchants globally report dedicating more than 6% of profits to mitigate fraud losses.



WE ASKED: APPROXIMATELY HOW MUCH REVENUE HAVE YOU LOST DUE TO PAYMENT FRAUD IN THE PAST 12 MONTHS?

WE ASKED: AS A PERCENTAGE OF PROFITS, HOW MUCH DO YOU SPEND MANAGING PAYMENT FRAUD IN A TYPICAL YEAR?

FURTHER INSIGHTS

A growing number of APAC merchants appear to be managing fraud with remarkable effectiveness: **16% of merchants reported no losses** due to payment fraud in the past year.

High costs of **managing payment fraud are eroding profits** among European merchants. 16% of French merchants and 14% of German merchants report that the costs of fraud mitigation exceed 10% of annual profits.

One in ten North American merchants report that the costs of **managing fraud exceed 10% of profits** for a typical year.

South American merchants reported **higher costs of managing fraud**, with half of merchants surveyed indicating that fraud absorbs between 6% and 10% of profits annually.

PRO TIPS

- Understanding the **full impact of fraud can be difficult to calculate** as it involves more than just revenue loss. Fraud losses can also include chargeback processing costs, marketing costs, shipping/handling costs and even reputational cost to merchants.

- Excessive fraud events can result in significant network compliance fee. Merchants should **take the time to understand fraud rates** and regularly adjust fraud prevention measures to mitigate excessive fraud events.

- Monitoring a fraud solution's performance should include more than just fraud reduction. The impact to **authorization rates should also be examined** to ensure fraud measures are not overly stringent and potentially impacting too many good transactions.

SUNNY THAKKAR
SENIOR PAYMENTS FRAUD MANAGER
WORLDPAY FROM FIS

OVERVIEW OF EXISTING PAYMENT RISK SOLUTIONS

CURRENT PAYMENT FRAUD MANAGEMENT STRATEGIES

We wanted to better understand the types of strategies currently used among global merchants to prevent fraud, protect their revenue and provide exceptional customer experience.

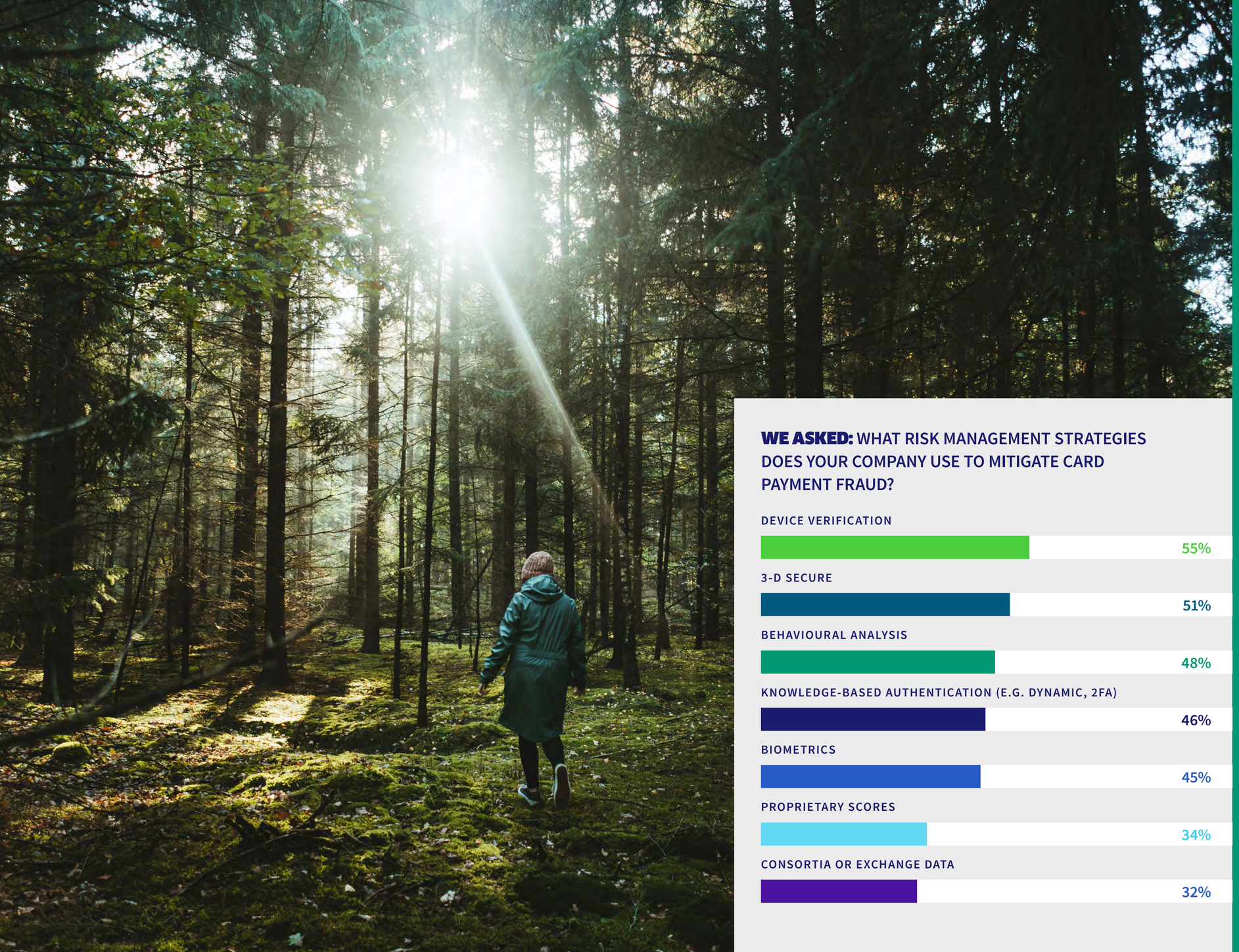
Among merchants globally, device verification (a.k.a. device authentication) was reported as the most widely used **fraud prevention strategy, employed by 55% of merchants surveyed**. A majority of respondents (51%) report using 3-D Secure, a payment authentication method that connects and shares transaction data among financial institutions, merchants and payment networks.

Behavioral analysis of prior customer transactions to determine the legitimacy of current transactions is in use by 48% of merchants surveyed. Knowledge-based authentication methods that utilize two-factor authentication and other dynamic security methods were reported by 46% of merchants, while 45% use some form of biometric security to confirm the legitimacy of a payment transaction.

Though employed by a majority of global merchants, **3-D Secure was cited most by survey respondents as a method that was a matter of concern** when implementing digital wallets. Merchants also expressed concerns about data privacy, two-factor authentication and identity verification methods.

55%

of merchants use device verification as a fraud prevention strategy



WE ASKED: WHAT RISK MANAGEMENT STRATEGIES DOES YOUR COMPANY USE TO MITIGATE CARD PAYMENT FRAUD?

FURTHER INSIGHTS

Omnichannel retailers were most likely **to report using 3-D Secure**, with nearly two-thirds (63%) currently deploying the solution, followed by dating apps and online gambling (58%).

Online education (42%) and dating apps (45%) were the most likely businesses to **utilize proprietary data scores** to combat fraud.

Keeping up with the **fast pace of change in payment trends** was the challenge cited most often (33%) by video game / online gaming merchants.

PRO TIPS

- Enabling device and behavioral data collection allows merchants to obtain **critical unique data elements** that can significantly increase the ability to mitigate fraud.

- Employing behavioral data collectors for fraud mitigation is gaining in popularity due to the **increase in sophisticated bot attacks** experienced by merchants.

- Two-factor authentication, **via 3DS or other internal means**, is an increasingly common way for merchants to reduce both payment fraud and account takeover fraud.

SUNNY THAKKAR
SENIOR PAYMENTS FRAUD MANAGER
WORLDPAY FROM FIS

EVALUATING FRAUD DETECTION & ID VERIFICATION SOLUTIONS

Evaluating fraud detection and ID verification solutions requires review of a broad set of vendor capabilities

Multifactor authentication, predictive analytics and multichannel applicability were the most important capabilities in fraud solutions, each cited by 74% of our survey respondents worldwide. **Two-factor authentication was cited as “very important” by nearly half (45%) of all respondents**.

The use of artificial intelligence and machine learning technologies ranked highly, as did having a fraud detection and ID verification solution that provides actionable real-time insights; each were cited as “important” or “very important” by 72% among our survey respondents.

45%

of respondents cited AI & machine learning as "important" or "very important"

WE ASKED: HOW IMPORTANT ARE THE FOLLOWING CAPABILITIES WHEN EVALUATING A FRAUD DETECTION AND ID VERIFICATION SOLUTION?

	IMPORTANT	VERY IMPORTANT	TOTAL
TWO-FACTOR AUTHENTICATION	29%	45%	74%
MULTICHANNEL (WEB, MOBILE APP, CALL CENTRE, IN PERSON)	34%	40%	74%
PREDICTIVE ANALYTICS	35%	39%	74%
ARTIFICIAL INTELLIGENCE (AI)/MACHINE LEARNING	32%	40%	72%
REAL-TIME/ACTIONABLE INSIGHTS	34%	38%	72%
EASY TO INTEGRATE WITH EXISTING TECHNOLOGY STACK	33%	38%	71%
SELF-SERVICE CONFIGURABILITY/POLICY MANAGEMENT	37%	34%	71%
RELAIANCE ON NON-SELF-ASSSERTED DATE (PUBLIC RECORDS, ETC)	34%	36%	70%
3-D SECURE	33%	36%	69%
CONSORTIUM-BASED DATA SHARING	35%	34%	69%

FURTHER INSIGHTS

A solution being easy to integrate with an existing technology stack, the availability of real-time actionable insights and two-factor authentication were the capabilities most important in APAC, each cited by **74%** of respondents.

European merchants cited multichannel applicability (**73%**), two-factor authentication (**71%**) and 3-D Secure (**70%**) as the most important factors when evaluating fraud detection solutions.

Multichannel applicability (**76%**), two-factor authentication (**73%**) and the availability of real-time actionable insights (**73%**) are the most important capabilities to North American merchants.

Respondents in South America cited predictive analytics (**84%**), artificial intelligence and machine learning (**84%**) and two-factor authentication (**80%**) as the most important capabilities.

Social media analytics were cited as “important” capabilities by **80%** of merchants in online dating, with **63%** of industry leaders citing social media analytics as “very important.”

PRO TIPS

- **Technical implementation** of fraud detection and prevention solutions **can be burdensome** and costly for merchants.

- Merchants should **look for solutions that are easy to implement**, as well as solutions that offer multiple fraud mitigation strategies via a single or limited integration points.

SUNNY THAKKAR
SENIOR PAYMENTS FRAUD MANAGER
WORLDPAY FROM FIS

3-D SECURE: LEADING SECURE CUSTOMER AUTHENTICATION

37% of merchants cited too much friction at checkout as the reason for not using the technology

3-D Secure (3DS) is a primary mechanism for authenticating card payment transactions globally. The use of 3DS satisfies the Secure Customer Authentication (SCA) requirements of the EU's revised Payment Services Directive (PSD2).

Though effective, the original 3DS protocol added friction to the shopper checkout experience – usually in the form of a static password – and thus increased cart abandonment rates. Though exemptions were allowed for low-value transactions, a more user-friendly solution was required. **The next generation of 3-D Secure, 3DS2, enables a more frictionless experience** where an authentication challenge is required, using one-time passwords and/or biometric authentication to satisfy SCA requirements.

Among merchants surveyed, 82% report using 3DS today: 48% report using the original version of the 3DS protocol, while 34% report using the newer 3DS2.

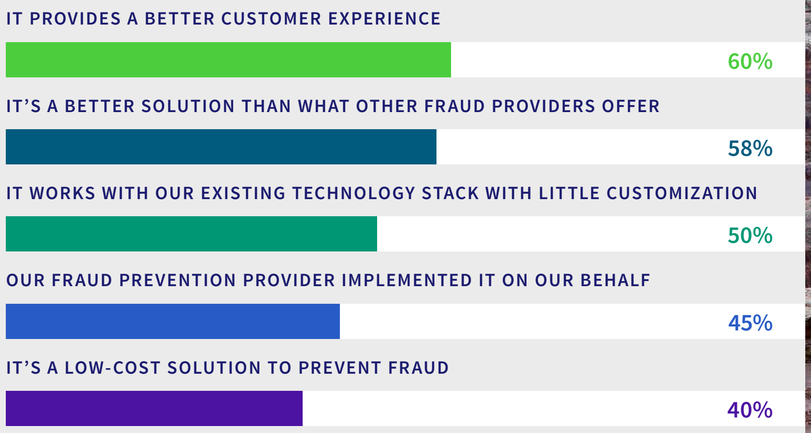
Among those merchants that currently use 3DS, 60% cited the better user experience as a key factor influencing the technology's adoption. Half of merchants using 3DS cited the ease of integration and the ability to work with existing technology stacks with little customization. **Four in ten merchants cited the relatively low cost of 3DS as a fraud prevention solution**.

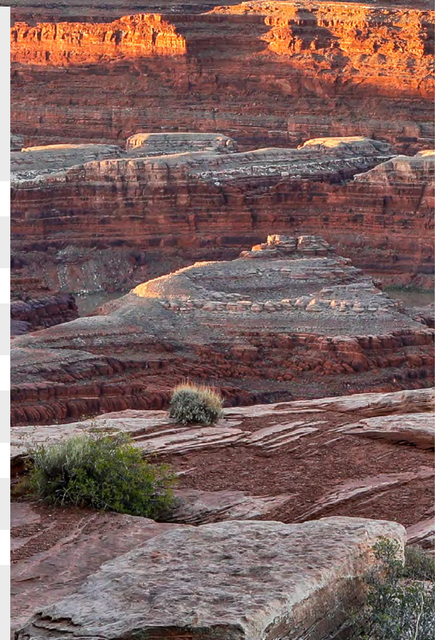
Among the 18% of global merchants surveyed that were not utilizing 3DS, 41% cited use of an alternative solution, while 28% indicated that the technology wasn't relevant to their services. Despite the rise of the more user-friendly 3DS2, 37% of merchants cited too much friction at checkout as the reason for not using the technology.

18%

of global merchants surveyed were not utilizing 3DS

WE ASKED: WHAT ARE THE KEY FACTORS INFLUENCING YOUR DECISION TO IMPLEMENT 3-D SECURE?





Communication with customers is important. That's especially true when it comes to issues related to payments and security. An overwhelming majority of merchants understand this importance: **85% of global merchants report having communicated to their customers that they're using SCA**.

Among the majority of merchants answering in the affirmative, more than half (51%) responded that clear, effective communication is vital for great customer experience. Nearly a third (32%) did so in order to ensure a greater sense of security.

FURTHER INSIGHTS

Canadian merchants reported the lowest rates of 3DS adoption (68%) while merchants in France reported the highest (90%, including 38% adoption of the more advanced 3DS2 protocol).

Nearly two-thirds (66%) of North American merchants cited the **better customer experience of 3DS2** as a key factor in its use, suggesting that the early usability challenges in 3DS have been overcome in 3DS2.

Customer experience is a vital consideration for all businesses, especially online dating; **81% of online dating app merchants cited the better customer experience** of 3DS2 as a key factor in its use.

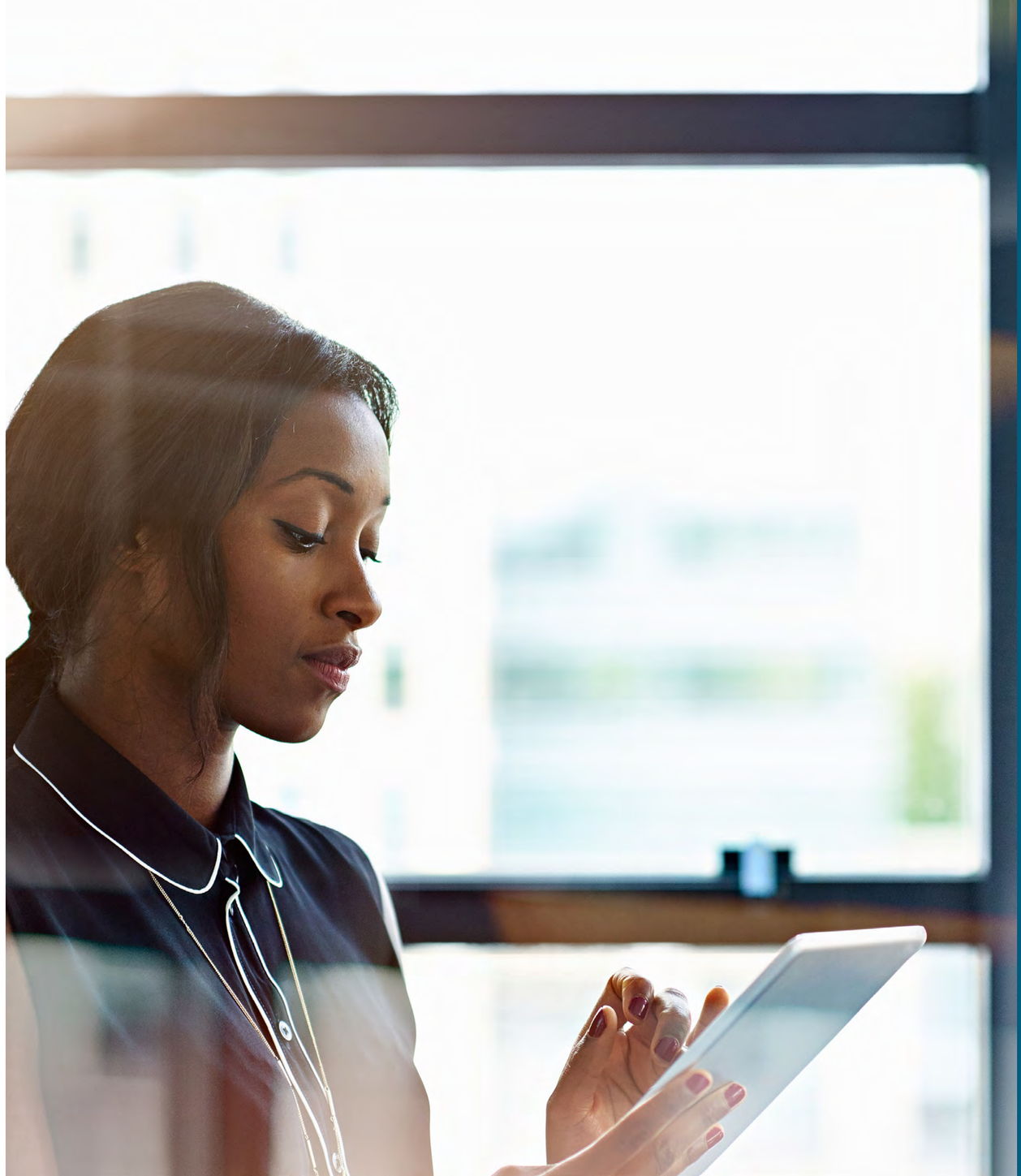
PRO TIPS

- EMV 3DS2 offers a significantly **improved user experience compared to its predecessor**, an important consideration as merchants look to ensure a secure environment as well as an optimized customer checkout experience.

- EMV 3DS and the MPIs which support it **streamline the implementation** and integration process, making it easy to deploy.

- Beyond fraud mitigation, 3DS authentication offers a **fraud liability shift** on fully authenticated transactions. Merchants using 3DS are realizing cost-reduction benefits from no longer being financially liable for fraud chargebacks where the underlying transaction was authenticated.

JEREMY BELLINO
SENIOR FRAUD AND AUTHENTICATION MANAGER
WORLDPAY FROM FIS



EXISTING MERCHANT SOLUTIONS: CHARGEBACKS

18% report using a hybrid model that combines internal teams and third-party vendors

Managing chargebacks and disputes is a classic “necessary evil.” Effective chargeback management that utilizes best practices and the latest technologies is essential to recoup what would otherwise be lost revenue. For global e-commerce and enterprise-scale merchants, an effective chargeback management solution can make a big difference to the bottom line.

We wanted to understand basic characteristics of merchants’ existing chargeback management practices. In-house teams manage chargebacks for half of the merchants surveyed. External teams manage chargebacks for 31% of global merchants surveyed, while **18% report using a hybrid model that combines internal teams and third-party vendors**.

Managing the chargeback representment process starts with gathering evidence related to the charge under dispute. Among the types of supporting evidence typically gathered, **66% of merchants surveyed cited using the customer’s IP address**.

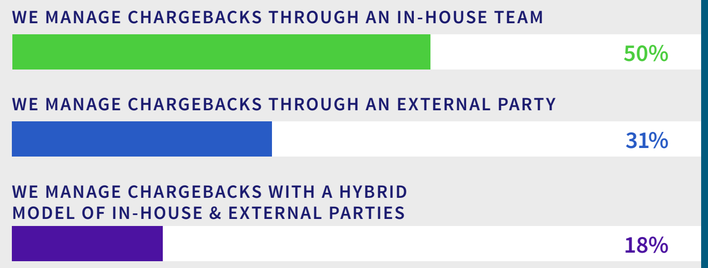
58%

of merchants use signed delivery confirmations

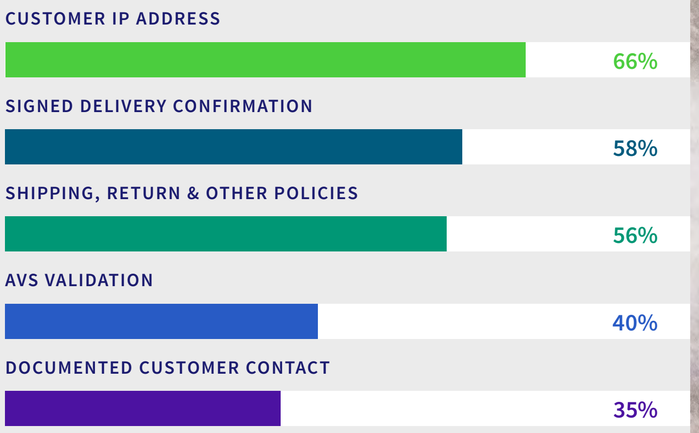
Signed delivery confirmations were used by 58% of merchants, while 56% cited the use of reference shipping, return and other policies in the representment process.

The methods used to receive and submit representments varies widely. Though often indicative of a cumbersome manual process, email is the most widely used method for chargeback communication, cited by 66% of merchants. Application Programming Interfaces (APIs) are used by 47% of businesses surveyed, while portals (45%) and customer dashboards (42%) help various merchants manage disputes.

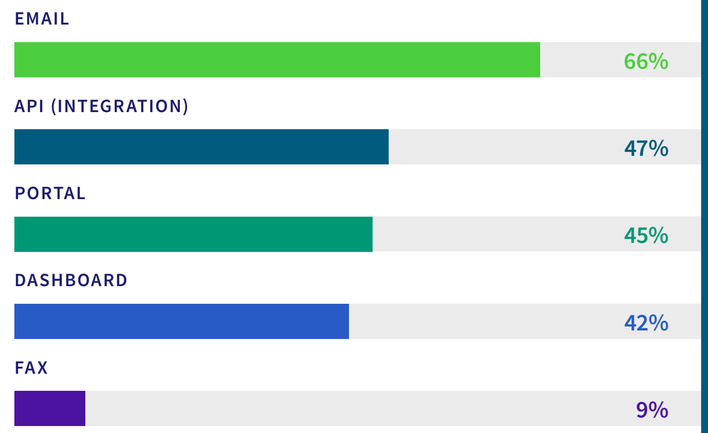
WE ASKED: DO YOU MANAGE YOUR CHARGEBACKS THROUGH AN IN-HOUSE TEAM OR AN EXTERNAL PARTY?



WE ASKED: WHAT TYPES OF SUPPORTING EVIDENCE ARE YOU USING WHEN DEFENDING CHARGEBACKS?



WE ASKED: HOW DO YOU RECEIVE YOUR CHARGEBACKS AND SUBMIT REPRESENTMENTS TODAY?



PRO TIPS

- While some merchants view chargebacks as an operational cost overhead, **chargebacks represent revenues that can be recovered** and losses that can be avoided.

- Today's chargeback systems and solutions can **automate chargeback defense**, reducing costs and sources of error while streamlining the process and increasing win rates.

- APIs allow merchants to directly integrate chargeback disputes into existing IT systems, **offering a more tailored experience** for their analysts while leveraging existing enterprise data.

SIMON POTTS
SENIOR DISPUTES MANAGER
WORLDPAY FROM FIS

LOOKING AHEAD

PRIORITIZING 2021 PAYMENT INITIATIVES

Following a year unlike any other, merchant priorities for 2021 reflect the critical issues of our time

Given the rise of card-not-present e-commerce fraud during the pandemic, it comes as no surprise that **improved fraud detection and mitigation efforts were cited most (44%) by merchants** as one of their priorities for 2021.

Merchant priorities follow consumer preferences, leading to a near-term emphasis on **improving the payment experience on mobile devices (40%)**. Those efforts are understandably geared to increase revenue and profit from mobile channels, a 2021 priority cited by 38% of merchants surveyed.

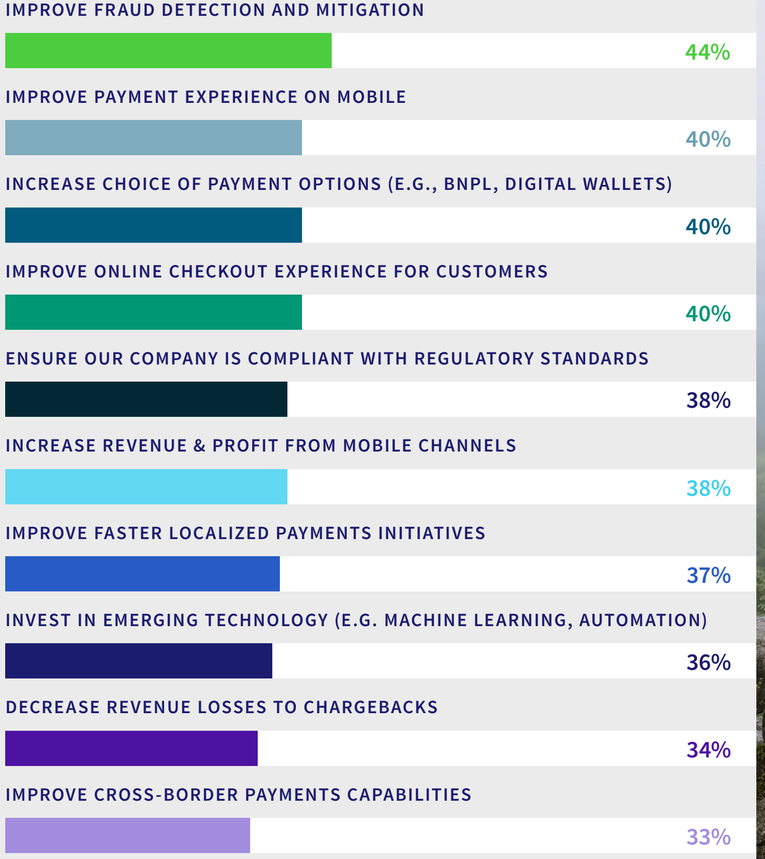
40%

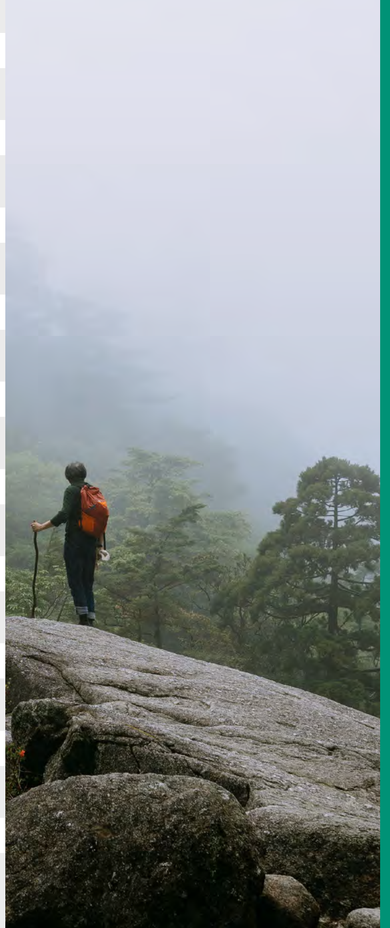
of merchants' priorities are improving the payment experience on mobiles

Merchants are striving to improve their customers' online checkout experience, in large part by increasing payment option choices, such as buy now, pay later (BNPL) and through offering a variety of the most popular digital wallets, each cited by 40% of merchants.

Other leading merchant **priorities for 2021 include staying compliant with evolving regulatory standards, reducing revenue losses** due to chargebacks, and investing in emerging technologies like machine learning and process automation.

WE ASKED: WHICH OF THE FOLLOWING PAYMENT INITIATIVES ARE YOU PRIORITIZING OVER THE NEXT 12 MONTHS?





FURTHER INSIGHTS

Top 2021 priorities for APAC merchants include improving fraud detection and mitigation (44%), **improving payment experience on mobile** (40%) and ensuring compliance with regulatory standards (38%).

For European merchants in 2021, top priorities include **improving online checkout experience for customers** (44%), improving fraud detection and mitigation (41%), and increasing revenue and profit from mobile channels (39%).

In 2021, leading North American merchant priorities include improving fraud detection and mitigation (44%), **increase choice of payment options** like digital wallets (44%) and improving payment experience on mobile (40%).

Top priorities for merchants in South America in 2021 include improving fraud detection and mitigation (49%), improving payment experience on mobile (47%) and **improving online checkout experience for customers** (45%).

PRO TIPS

- As EMV 3DS continues to be improved and optimized globally, it will become more prevalent in the e-commerce ecosystem as a means to **ensure a positive consumer experience** while delivering both fraud reducing and financial liability shift benefits.
- Buy Now Pay Later (BNPL) payment methods continue to **grow in popularity** among younger generations of shoppers, driving purchase decisions for those shoppers however they shop.

JEREMY BELLINO
SENIOR FRAUD AND AUTHENTICATION MANAGER
WORLDPAY FROM FIS

REALIZING ROI FROM END-TO-END PAYMENT PROTECTION

Merchants understandably seek concrete returns on investments in their payment security infrastructure

A nod to the importance of holistic, end-to-end payment and fraud management, merchants are seeking to achieve measurable improvements throughout the payment life cycle, from pre-transaction through post-transaction.

Global merchants deploy a patchwork of risk management solutions, ranging from best practices to no practices. An overwhelming majority (96%) of merchants use fraud management tools. However, **only 25% of merchants are protecting their entire payments life cycle** by using fraud management tools in conjunction with authentication, tokenization and chargeback solutions.

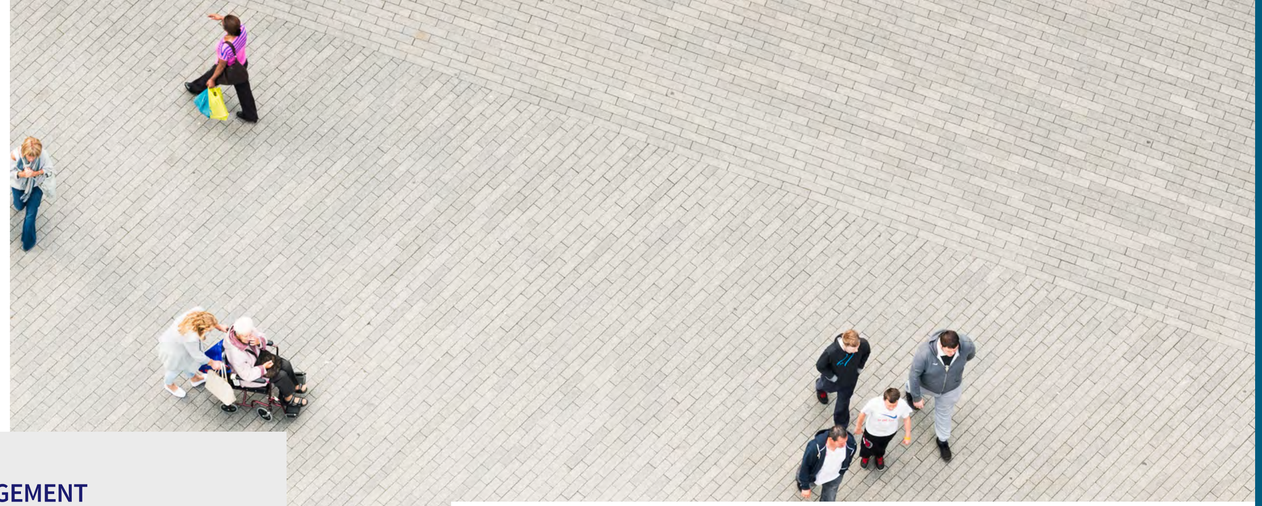
25%

of merchants are protecting their entire payments life cycle

A majority of merchants surveyed use fraud management tools either alone or with individual authentication, tokenization and/or chargeback services – without all the services working together. Creating safe, easy and convenient payment experiences for consumers has the potential to translate into more satisfied customers, who in turn make more purchases.

A safer payments ecosystem could mean more sales. Understandably, the leading benefit **merchants hope to achieve through payment security investments is an increase in total transactions**, cited by more than half (51%) of merchants surveyed.

Merchants are hoping investments in payment security pay off with consumers, both in improved reputation (49%) and higher customer satisfaction (47%). Merchants seek direct, measurable return on investment: **48% want to reduce direct losses for each fraud incident**. Merchants want to lower false positive rates and improve authorization rates to ensure legitimate customers can make purchases without friction.



WE ASKED: ARE YOU CURRENTLY USING FRAUD MANAGEMENT TOOLS? IF SO, HOW ARE YOU INTEGRATING AUTHENTICATION, TOKENIZATION AND CHARGEBACKS TOOLS?

I USE FRAUD MANAGEMENT TOOLS WITH AUTHENTICATION, TOKENIZATION AND CHARGEBACKS — 25%

I USE FRAUD MANAGEMENT TOOLS WITH AUTHENTICATION — 20%

I USE FRAUD MANAGEMENT TOOLS WITH TOKENIZATION — 13%

I ONLY USE FRAUD MANAGEMENT TOOLS — 11%

I USE FRAUD MANAGEMENT TOOLS WITH CHARGEBACKS — 10%

I USE FRAUD MANAGEMENT TOOLS WITH AUTHENTICATION AND TOKENIZATION — 8%

I USE FRAUD MANAGEMENT TOOLS WITH AUTHENTICATION AND CHARGEBACKS — 6%

NO, I DON'T USE FRAUD MANAGEMENT TOOLS — 4%

I USE FRAUD MANAGEMENT TOOLS WITH CHARGEBACKS TOOLS AND TOKENIZATION — 3%

WE ASKED: WHAT ARE THE TOP BENEFITS/ADVANTAGES YOUR COMPANY HOPES TO ACHIEVE THROUGH IMPROVING YOUR PAYMENT SECURITY SOLUTION AND CAPABILITIES?

INCREASED NUMBER OF TRANSACTIONS — 51%

IMPROVED REPUTATION — 49%

REDUCTION IN DIRECT MONETARY LOSSES PER FRAUD INCIDENT — 48%

HIGHER CUSTOMER SATISFACTION — 47%

LOWER FALSE POSITIVE RATES — 47%

IMPROVED AUTHORIZATION RATES — 43%

REDUCTION IN DIRECT MONETARY LOSSES OF CHARGEBACKS — 41%

IMPROVED INTERNAL FRAUD MANAGEMENT SYSTEMS TO REDUCE COSTS — 31%

PRO TIPS

- Deploying a full-scale payments security infrastructure offers **challenges with development, interconnectivity, and consumer experience**. Successfully implementing these solutions requires the right partners to ensure payments are protected while optimizing the customer experience.
- Maintaining and improving authorization and order approval rates is **essential for merchants** in an already competitive environment. Fraud mitigating solutions must strike the right balance between risk and consumer experience.

JEREMY BELLINO
SENIOR FRAUD AND AUTHENTICATION MANAGER
WORLDPAY FROM FIS

KEY TAKEAWAYS

KEY TAKEAWAY 01

Protecting the payment parts – as a whole

It is clear from listening to merchants that payment and fraud mitigation teams should consider working in tandem. An integrated approach can offer additional synergies and efficiencies.

Each component of the payment life cycle is significant, starting with a hybrid fraud detection model that leverages machine learning.

Secure Customer Authentication (SCA) is an essential component to reduce risk, increase security and improve customer experiences. A disputes management solution with API and portal functions can help merchants save time and money.

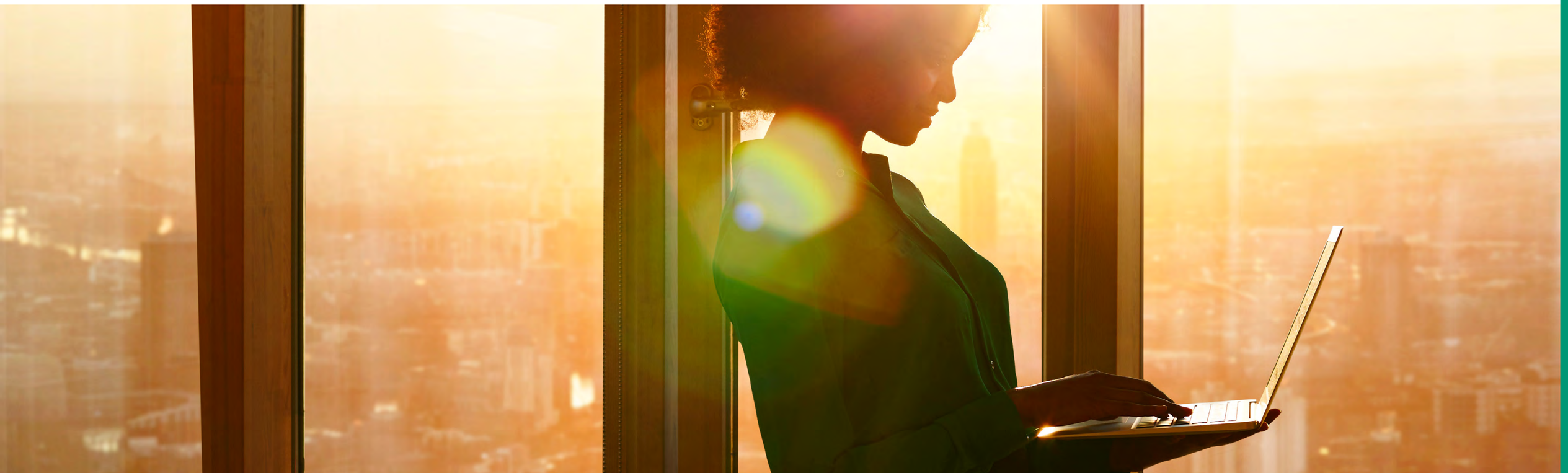
KEY TAKEAWAY 02

The importance of managing risk and optimizing CX

In an ideal world, efforts to manage payment risk and those devoted to delivering exceptional customer experience would never come in conflict. Fraud defences would stop 100% of illegitimate transactions while never causing a second of friction with the consumer. Customer logins would always be seamless, and every legitimate payment would go through instantly.

While we don't live in an ideal world, merchants today do strive to manage payment risk holistically. Successful merchants are prioritizing dual integrated goals of managing risk while optimizing customer experience.

Ensuring smooth, safe, fast customer experience is every bit as important as deploying dynamic defences to deny fraudulent transactions. Striking that balance requires a dynamic synthesis of best practices, starting with integrated payment risk management.



KEY TAKEAWAY 03

Quality payment partnerships are essential

Specifically, merchants require a partner that can help them tie all the pieces together in a coherent way. Merchants finding success in overcoming today's challenges typically have payment and security partners who can address each situation in the consumer payment life cycle.

Merchants of global scale require partners with the breadth and scale to treat the entire payment life cycle holistically while acting with the agility the changing times demand. As the world's leading payment processor, Worldpay from FIS has dynamic protection solutions to help merchants manage the total payment life cycle. Contact us to learn more.

About FIS

FIS is a leading provider of technology solutions for merchants, banks and capital markets firms globally. Our more than 55,000 people are dedicated to advancing the way the world pays, banks and invests by applying our scale, deep expertise and data-driven insights. We help our clients use technology in innovative ways to solve business-critical challenges and deliver superior experiences for their customers. Headquartered in Jacksonville, Florida, FIS is a Fortune 500® company and is a member of Standard & Poor's 500® Index.

About Worldpay from FIS
Worldpay from FIS (NYSE: FIS) is a leading payments technology company that powers global commerce for merchants, banks and capital markets. Processing 75 billion transactions topping $9T for 20,000+ clients annually, Worldpay lifts economies and communities by advancing the way the world pays, banks and invests.

For further inquiries, please contact:
MerchantSolutionsMarketResearch@fisglobal.com

LET'S REINVENT SMARTER at fisglobal.com