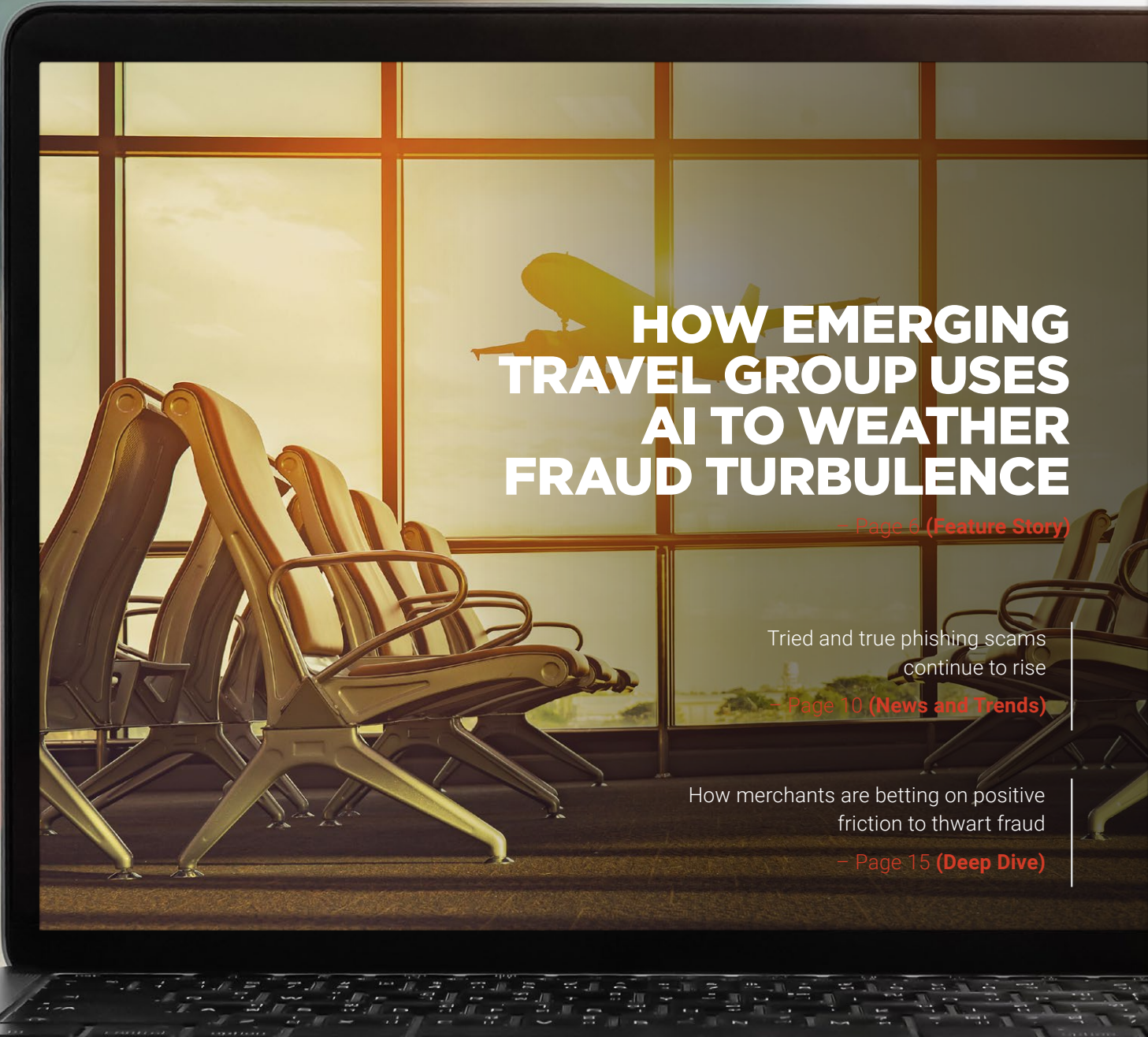


MERCHANT

FRAUD DECISIONING

PLAYBOOK



HOW EMERGING TRAVEL GROUP USES AI TO WEATHER FRAUD TURBULENCE

— Page 6 (Feature Story)

Tried and true phishing scams
continue to rise

— Page 10 (News and Trends)

How merchants are betting on positive
friction to thwart fraud

— Page 15 (Deep Dive)

TABLE OF CONTENTS

03

WHAT'S INSIDE

A look at how businesses' demands for agile, evolving anti-fraud solutions are leading to the speedy adoption of AI and ML across various industry segments

06

FEATURE STORY

An interview with Felix Shpilman, CEO of Emerging Travel Group, on how the online travel agency worked toward eliminating chargebacks and giving customers frictionless payment experiences

10

NEWS & TRENDS

The latest developments in the space, including why merchants are betting big on AI and ML to fight fraud and how victims struggle to recoup losses from wire transfers and other scams

15

DEEP DIVE

An in-depth look at why the search for sophisticated fraud schemes' silver bullet is leading many merchants to employ positive friction to thwart fraud and enhance customer trust

18

ABOUT

Information on [PYMNTS.com](https://pymnts.com) and Simility

ACKNOWLEDGMENT

The Merchant Fraud Decisioning Playbook is produced by PYMNTS and sponsored by Simility. PYMNTS is grateful for the company's support. [PYMNTS.com](https://pymnts.com) retains full editorial control over the following findings, methodology and data analysis.

WHAT'S INSIDE



A sad reality remains despite online merchants' continuing fights against fraud: Attacks' frequency and complexity will continue to rise. Fraudsters are concocting more sophisticated schemes to strike online merchants, taking advantage of easily available personally identifiable information (PII) to orchestrate a variety of schemes that range from clean fraud to phishing. Online merchants dealing with these issues are often at a loss, especially when they rely on legacy systems that utilize rules-based engines and predictive models.

Merchants looking to stay ahead of fraudsters are turning to advanced learning tools such as artificial intelligence (AI) and machine learning (ML). Fraudsters are utilizing the same set of tools, however, to sidestep authentication processes, impersonate legitimate customers and perpetrate fraud. It has thus become imperative for online merchants to take more nuanced approaches to identifying and fighting fraud.

Merchants must gather information from various data sources and utilize advanced learning tools such as AI and ML to organize and transform those details into actionable insights. Legacy systems or manual reviews can leave them vulnerable and unable to keep up with fraud's dynamic nature. Online retailers must also safeguard their customers and platforms without alienating legitimate users with stringent authentication procedures.

Such moves will become critical as the overall eCommerce space **grows** to \$700 billion over the coming years, as will establishing fraud decisioning processes that evolve and scale to that growth. This edition of the Merchant Fraud Decisioning Playbook seeks to identify emerging threats and explain how online merchants can identify fraud and improve their decisioning capabilities to eliminate or reduce these risks.

ACROSS THE FRAUD DECISIONING SPACE

Fraudulent transactions' costs are rising sharply as card-not-present (CNP) fraud grows, but few **merchants** have the resources or the knowledge to properly manage related chargebacks. Thirty-one percent of online merchants reported that being unable to identify friendly chargeback fraud was a major challenge, while others struggled when disputing such charges — a factor that will only encourage more chargebacks.

Phishing attempts are also on the rise, surging 640 percent last year alone, with hackers placing malicious URLs on domains such as Apple, Dropbox, Facebook, Google, Microsoft and PayPal, according to a recent **report**. Typical schemes conned users into clicking malicious links that would infect their computers with viruses. Such activities, including business email compromise (BEC), have **cost** businesses \$12 billion over the past five years, according to the FBI.

Human-driven attacks are surging as well, thanks to a surprising new tactic. Fraudsters are **utilizing** low-cost labor and sweatshop-style workforces to boost the number of crimes they can commit. These workers, who are based in countries such as the Philippines, Russia and Ukraine, caused a 90 percent increase in fraud attacks from October 2019 to December 2019. An analysis of 1.3 million transactions found that their focus has been on new account registrations

and logins across eCommerce, gaming and social media platforms.

For more on these stories and other recent fraud decisioning headlines, read the Playbook's News & Trends (p. 10) section.

USING AI, ML FOR IMPROVED FRAUD DECISIONING

Fraud is expected to cost the travel industry more than \$25 billion this year, meaning online travel merchants must focus on balancing seamless buying experiences with fraud-free platforms. For this month's Feature Story (p. 6), Felix Shpilman, CEO of **Emerging Travel Group**, discussed how the company has fought chargebacks and other scams with AI and ML capabilities while giving ticket buyers more seamless and satisfying experiences.

DEEP DIVE: THE CASE FOR INTRODUCING POSITIVE FRICTIONS AND MULTILAYERED FRAUD PREVENTION STRATEGIES

Merchants are digging deep into their fraud-prevention toolboxes to find the optimal solutions to combat marauding cybercriminals. Many online firms are thus embracing the addition of well-placed frictions in the authentication process to avert fraud attempts. This month's Deep Dive (p. 15) explores how ML tools can work with other techniques, such as device fingerprinting, to facilitate strategic positive frictions without hampering customers' experiences.

FIVE FAST FACTS

5

\$11B

Amount online travel agencies are projected to lose annually to fraud this year



20%

Share of retailers that are prioritizing fraud prevention over smooth checkout processes



\$118B

Approximate annual cost of false positives for U.S. merchants



\$5.2B

Estimated cost of U.S. eCommerce fraud losses this year



9,705

Total number of data breaches recorded between January 2005 and October 2019 — an average of 1.8 a day

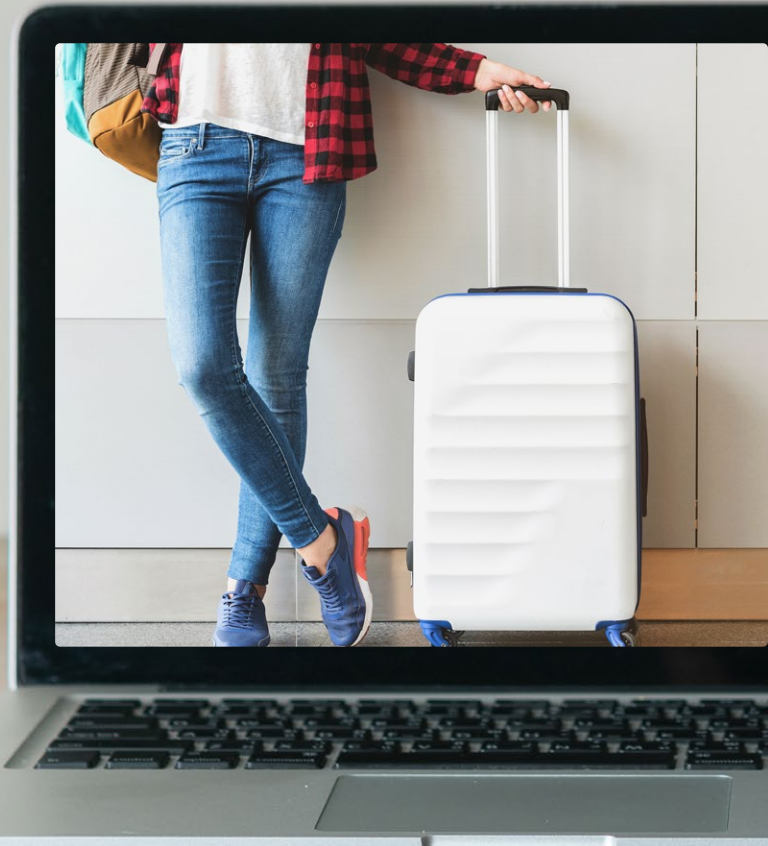


HOW EMERGING TRAVEL GROUP USES **AI TO WEATHER FRAUD TURBULENCE**



FEATURE STORY

The global travel industry has seen its fair share of turbulence over the past decade. The industry is **projected** to reach approximately \$11.4 trillion in value by 2025, but fraud losses in the space are estimated to exceed \$25 billion this year alone as cybercriminals employ sophisticated tools and technologies to steal funds and valuable customer details.



Fighting travel fraud is particularly challenging, however, especially for online travel agencies (OTAs) and hotels, according to Felix Shpilman, CEO of global online hotel accommodations and travel services provider **Emerging Travel Group**. These businesses are often hit hard when attacked, prompting many to employ AI and ML when building their defenses, he explained. Such technologies safeguard the onboarding and payment processes without adding unwanted frictions.

BATTLING FAST-GROWING OTA FRAUD

OTAs often have diverse sets of travel products that can be sold across various channels, making fraud more difficult to detect unless automated processes are involved. Such tools can easily sift through transactional and user data, but many online travel merchants instead rely on systems that focus on purchase order (PO) data to find possible threats — a process that often results in

false positives. OTAs are also seeing a rise in fraudulent chargebacks, which are **estimated** to increase 20 percent per year, taking a huge bite out of merchants' profits.

"All of the large online travel companies spend a significant amount of resources fighting fraud," Shpilman explained. "Fraud has evolved over the years, and chargeback fraud, which used to be the primary type of fraud that people fought with, is just one of the many things we have to fight with [now]."

Chargebacks and false positives can also take heavy tolls on online travel merchants' bottom lines.

"Travel, in principle, is a fairly low-margin business [in which] the majority of the companies make anywhere between 2 [percent] and 15 [percent] — maybe 20 percent — of the turnover [on] their net revenue," he said.

Online travel platforms looking to stay competitive must thus continually balance robust safety protections with seamless experiences for customers.

"Fighting fraud is an important priority for most of the modern travel companies," Shpilman said. "That said, the balance between fighting fraud and having a consumer-friendly user experience is also very important."

The company reexamined its in-house operations and the merits of working with

third-party solution providers to achieve this balance. It also revamped its authentication procedures, ensuring that only verified customers can transact on its platform.

DEPLOYING AN AI-BASED FRAUD SOLUTION

Emerging Travel Group had originally built a flexible, in-house, anti-fraud system, Shpilman said, but the rules-based product was difficult to scale in unknown markets. The company wanted a solution that could unlock greater access to data from multiple databases, companies and industries so it could provide deeper protection and accuracy. It thus sought outside help to acquire the right anti-fraud offering.

The company implemented a third party's AI- and ML-powered system in 2018 that works in tandem with its internal system to better detect fraudulent behaviors. The product has largely made customer experiences frictionless by keeping authentication on the back end, where customers cannot experience it, according to Shpilman.

"The customers have no idea they are being evaluated by the third-party solution," Shpilman explained. "The idea is to ensure that the customers' experiences are not diminished by the fact that we have this solution [while still providing added security to protect their transactions]."

Emerging Travel Group only authorizes credit card payments, he noted, and presently does not employ additional protocols like 3D Secure or two-factor authentication (2FA) to thwart CNP fraud at checkout. It does rely on automation to improve verification outcomes, however.

“All of the risks are covered by the analysis made by the anti-fraud system that uses AI and ML to analyze the customer and make a decision on the order,” Shpilman said. “There is no human involvement in the process. All of the relevant data is sent to our third-party tool via an [application programming interface, which returns its] decision [on] whether we should or should not approve the order.”

The AI-based system has largely eliminated Emerging Travel Group’s fraudulent chargebacks. If the chargebacks do happen, however, the system also helps to contest them. Affected banks are also contacted and given as much information as possible, including evidence from the fraud prevention system, partners and hotels.

CHALLENGES WITH PLATFORM INTEGRATION

Shpilman acknowledged that integrating third-party systems often requires extensive work and support from development teams, especially when firms have their own in-house software. Application programming

interfaces (APIs) can feed the necessary data into the new AI-based systems once integration is complete, enabling the product to analyze users’ behaviors and determine fraudulent orders.

Having access to data insights and implementing the right tools is critical to accommodating the emerging payment trends that impact OTAs, such as mobile payments and virtual cards. Some organizations use the latter to provide business travelers with 16-digit credit card numbers for one-time purchases including hotel stays, rental cars and other travel-related services. Virtual cards act as anti-fraud tools on their own, preventing permanent credit card and personal information from entering OTAs’ databases.

The global travel industry has had its share of ups and downs, but AI- and ML-based anti-fraud systems can safeguard everything from onboarding to payments while easing frictions on customers. OTAs and hotel management teams looking to remain prominent in the space will need to stay on top of guests’ payment preferences and ensure the anti-fraud solutions they develop travel well — both today and for years to come.

NEWS & TRENDS



PHISHING AND WIRE TRANSFER SCAMS

PHISHING ATTACKS GROW 640 PERCENT

Fraudsters' digital fraud schemes may be getting more sophisticated, but older cyberattack methods remain both effective and popular. A recent **report** from information management solutions provider OpenText found that there was a 640 percent increase in phishing attempts last year. Hackers placed one in four malicious URLs on non-malicious domains such as Apple, Dropbox, Facebook, Google, Microsoft and PayPal, and the most common schemes led users to click links that infected their computers with viruses. The report added that malware targeting computers running Windows 7 rose 125 percent.

Phishing is one of the oldest fraud techniques, having existed since the 1990s, but it remains a very effective and damaging activity. The FBI **reported** that phishing and BEC cost businesses \$12 billion over the past five

years, with more than \$1.2 billion reported in 2018 alone. Even larger firms such as Equifax and Amazon have been hit with phishing scams, which have average recovery costs of \$3.9 billion.

EMAIL WIRE TRANSFER SCAM VICTIM FIGHTS BACK

Most merchants **recover** less than 25 percent of their fraud losses, and businessman Frank Krasovec's efforts to regain funds lost in a major email hacking scam illustrate recollection's difficulties. Krasovec, chairman of Dash Brands Ltd., which owns Domino's franchises in China, recently **sued** PlainsCapital Bank to recover the \$450,000 he lost to scammers who hacked his account. He claims that digital fraudsters fooled his assistant into wire transferring money to a Hong Kong account and he blames the bank for lacking anti-fraud protocols. The bank has refused to refund the money, asserts that Krasovec failed to install proper internal safeguards and is demanding that he repay the stolen funds with interest.

Scam victims normally get refunded fraudulent charges, but that does not apply to wire transfers, according to the American Bankers Association (ABA). Such schemes see fraudsters combine sophisticated hacking with wire transfers, which the FBI **reported** cost firms close to \$1.8 billion last year — up from approximately \$1.3 billion in 2018. These costs hit \$26 billion worldwide between June 2016 and July 2019.

MERCHANTS CANNOT COUNTER CHARGEBACKS

Recent **reports** suggest that online sales scams are on the rise, raising concerns that merchants cannot properly fight fraud. Many retailers **state** that friendly chargebacks overwhelm them, mainly because they lack the resources and knowledge to manage them, with 56 percent of more than 200 online, multichannel and mobile commerce merchants claiming that such instances rose over the past three years. The biggest obstacles to combating friendly fraud are that 31 percent of merchants struggle to identify it, while 29 percent face challenges when disputing such claims.

Experts argue that not challenging friendly fraud only encourages repeat incidents. Many retailers do not take advantage of third-party anti-fraud solutions, which have proven to be effective in many cases, while others note that major credit card issuers' measures have been ineffective in managing chargebacks.

HACKERS USING 'SWEATSHOPS' TO OUTSOURCE ATTACKS

Sweatshops are most notably tied to giant consumer companies looking to take advantage of low-cost labor, but such tactics are now becoming popular among fraudsters seeking to augment and boost their criminal schemes. Human-driven fraud attacks reportedly **surged** almost 90 percent from October 2019 to December 2019 as a result of these new sweatshops in the Philippines, Russia and Ukraine, among other countries. Those working at these institutions are responsible for launching online attacks or making fraudulent transactions. An analysis of more than 1.3 million transactions indicated that there have also been increases in attacks targeting new account registrations and logins across eCommerce, gaming and social media platforms.

HACKING CAUSES MENTAL AND FINANCIAL STRESS

IDENTIFY THEFT WORRIES PLAGUE ONLINE CONSUMERS

Much of the news surrounding data breaches tends to focus on financial impacts, but the daily drumbeat of cybercrime can also cause emotional stress. Data breaches have become a daily occurrence, with the Privacy Rights Clearinghouse recording 9,705 data breaches between January 2005 and October 2019 — an average of 1.8 a day. A recent **survey** of consumers from nine countries

found that 89 percent are at least somewhat worried that criminals will hack their bank accounts to steal money, and 87 percent are concerned that their identities will be used to commit crimes.

ID theft stresses have their geographical and gender nuances, with Brazilian users more likely to report that cybercrimes have personally affected them than those in the U.S., for example. Women also tend to be more worried about identity theft and cybercrime than men, though the latter tend to experience such attacks more frequently. Businesses are thus showing more interest in solutions that can help track down exposed information and advanced learning tools that can identify risks faster, giving consumers more time to protect themselves, enhancing their sense of control and lowering their concerns.

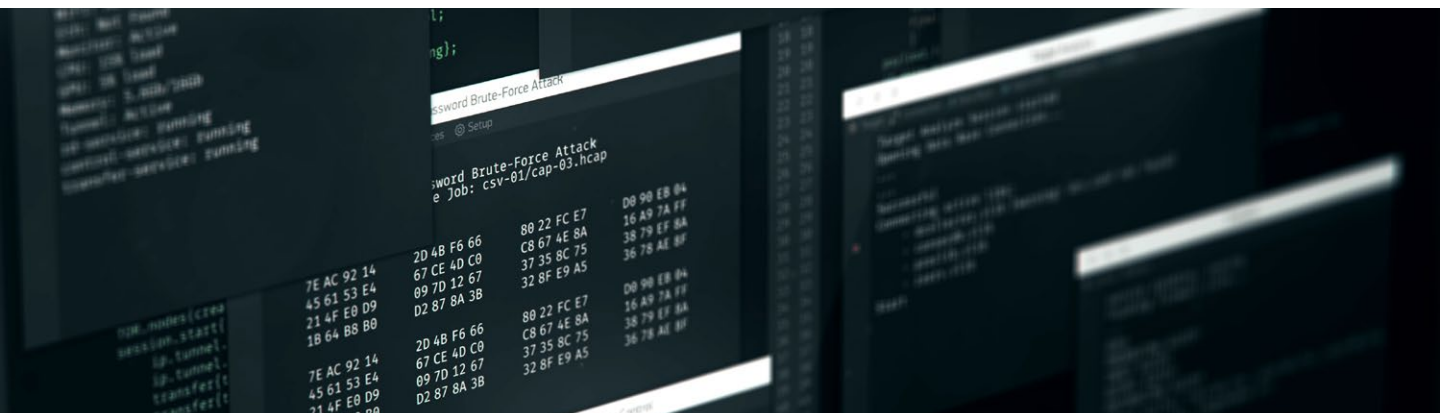
INSIDER DATA BREACHES CONFOUND IT PROFESSIONALS

Data breaches that occur within organizations have long been a concern, and research

indicates that IT departments are seemingly ill-equipped to combat the problem. A recent [survey](#) of more than 500 IT leaders and 5,000 employees across the U.K., U.S. and the Benelux region found that 97 percent fear that employees may compromise information. Their concerns are not unfounded, either: Many businesses do not have risk management practices.

This issue is particularly pervasive among senior-level employees, who often exhibit reckless approaches to data protection and lack senses of data ownership and responsibility. The survey found that 78 percent of directors intentionally shared data against company policy, compared to just 10 percent of clerical staff members. Seventy-eight percent of IT leaders also reported that employees at their places of business fell victim to phishing attempts and accidentally put company data at risk.

Few companies are using the right tools and technologies to protect themselves against



data breaches, despite the associated risks. Only half of IT leaders use anti-virus software to counter phishing attacks, and 58 percent rely on employees who report breaches, as opposed to any detection system.

SCAMMERS CASHING IN ON ONLINE LOYALTY PROGRAMS

Consumers have accumulated \$48 trillion in unspent loyalty points, and fraudsters are looking to cash in. Merchants — much like IT professionals — are ill-prepared to counter fraud on popular rewards programs. A recent [report](#) found that loyalty fraud soared 89 percent year over year — and with 45 percent of these reward accounts sitting inactive, fraudsters find them to be easy targets.

Far too many merchants lack the skills and resources to thwart such attacks, unfortunately. The survey found that 42 percent do not possess the necessary skills to prevent fraud and that approximately 50 percent lack the resources to build and support sturdy defense systems. Account takeovers (ATOs), new account fraud and policy abuse represented the most prominent attacks, according to the report.

LAW OFFICIALS BUST WALMART GIFT CARD SCAM

Law enforcement has been actively cracking down on online scams, scoring a victory for elderly victims of a Walmart gift card scam in Utah last month. The state's Attorney General's Office [indicted](#) two Chinese nationals for conning primarily senior citizens into

putting large sums of money onto Walmart gift cards. The suspects, Junliang Tang and Shuyan Wang, posed as government agents, bail bondmen and even IRS agents to con victims into putting funds onto cards. The fraudsters then instructed them to reveal the code on the back and send photos of the cards, which were used to buy “closed loop” cards — gift cards that can only be used at a single retail location — which they then sold online for a profit. The scheme spanned 46 states and cost victims and Walmart more than \$600,000, according to law officials. Such scams are on the rise, [costing](#) victims more than \$50 million in 2018.

Young consumers also fall victim to online scams and do so more than those aged 60 and older, according to [reports](#). Senior citizens [experienced](#) higher average losses, however, totaling more than \$342 million.

ALLIANCES, PARTNERSHIPS PUSH PREVENTION

PAYONEER SELECTS FRAUD PREVENTION TECHNOLOGY

Many firms are only able to [recover](#) less than 25 percent of their fraud losses, making prevention vital when selecting prevention solutions. Financial services firm Payoneer recently formed a partnership to embrace a new fraud prevention system that reportedly utilizes ML to block criminal attacks and minimize false positives against its 4 million customers. The ML models can be built



offline and integrated into third-party algorithmic systems, which match them in real time against fresh data. Real-time data processing can help boost response times and prevent fraud-related and money laundering issues.

RELX ACQUIRES U.S. FRAUD PREVENTION STARTUP

U.K.-based information and analytic firm RELX is also betting big on anti-fraud systems. The company is purchasing Arizona-based fraud prevention firm Emailage for \$480 million, according to [reports](#). Emailage uses ML, its own data and a global network of partners to predict fraud associated with email addresses and online identities, and it will play a role in

Relx's transformation from publishing to business information and data services. RELX, formerly Reed Elsevier, acquired two other companies in these categories, including San Diego-based ID Analytics for \$375 million.

RELX's risk and analytics unit, LexisNexis Risk Solutions, secured the Emailage deal, which comes amid some challenges for the former. RELX missed growth expectation for the first time in several years in 2019, and it has also been embroiled in public disagreements with universities across the U.S. regarding the firm's high profit margins. RELX [reported](#) continued growth in revenue and operating profits for 2019 earlier this month and issued a positive outlook for its business growth strategy.

BUGUROO ENHANCES ACCOUNT FRAUD PREVENTION

Madrid-based security firm buguroo has its sights set on cybercrimes as well, focusing specifically on account opening fraud. The firm noted in a [press release](#) that its new solution, bugFraud, helps prevent fraudsters from opening accounts. The system's deep learning techniques can detect fraud by measuring how application processes compare to known legitimate transactions and determine if the devices being used or their locations are abnormal. BugFraud also detects malware and other software anomalies and can be used with other procedures such as ID documentation and physical biometrics.

DEEP DIVE



USING POSITIVE FRICTION AND A MULTI-PRONGED APPROACH TO FRAUD DECISIONING

Merchants can find themselves fighting with one hand tied behind their backs in their battle against fraud. They must not only implement innovative technologies to ward off evolving and aggressive cyberattacks but also make sure not to turn off legitimate customers and lose revenue with restrictive fraud prevention solutions.

Merchants seem to fear adding payment or onboarding process pain points more than they worry about fraudsters, but forward-thinking sellers know that friction does not have to be negative. Many argue that it might reinforce their relationships with customers and suppliers if it is sensibly placed in the payment or fraud prevention processes. Strategic positive friction can help companies achieve the delicate and critical balance between providing robust security and seamless customer experiences.

BALANCING SECURITY AND CUSTOMER EXPERIENCE PAYS DIVIDENDS

Recent research illustrates the conundrum retailers encounter when fighting fraud. One [survey](#) found that 20 percent prioritize fraud prevention over smooth checkout experiences, for example — and for good reason. The most seamless checkout processes on the web will not keep customers loyal if the tradeoff is risking their hard-earned funds.

Fraud prevention costs can significantly eat into merchants' bottom lines, however. The average retailer will spend an [estimated](#) 8 percent of its annual revenues combating online fraud, and some projections suggest that eCommerce fraud losses could [increase](#) to approximately \$5.2 billion this year. Recovering fraud losses — both stolen funds

and customers' and suppliers' broken trust — is thus daunting.

Many retailers are trying to balance enhanced safety measures with smooth customer experiences, with 26 percent of those **considering** fraud protections as a top priority also putting the need to provide friction-free checkouts at the top of their lists. Merchants in this category seem to be putting positive friction to use.

Negative friction creates bottlenecks in payment or authentication processes without adding customer benefits, often resulting in churn and lost revenues. False positives can also occur, which is a pricey mistake for both customers and merchants: Incorrectly rejecting legitimate consumers' transactions **costs** U.S. merchants \$118 billion per year. Even the fear of fraud causes the average online seller to **reject** a fair amount of incoming orders that might turn out to be legitimate. The result is that false positives are a real and growing possibility.

THE BENEFITS OF POSITIVE FRICTION

Industry analysts argue that positive frictions can help mitigate fraud and prevent false positives while also minimally disrupting legitimate customers. Many shoppers regard requests to authenticate their accounts on several devices or to give their card verification value (CVV) codes at checkout as reasonable, for example — such steps show added security layers for their payment and personal details.

A recent **survey** found that most consumers do not mind measures like 2FA being added to checkout or other processes if they help fight fraud. Customers take comfort in businesses' focuses on security, and being known as a safe and secure seller will burnish merchants' reputations with suppliers.

Matching the right amount of positive friction to the type of business and customers' tolerance levels is also important. That being said, positive friction should not be **applied** unilaterally. Merchants could use data or other analytical tools to track users' behaviors and apply positive friction to those deemed suspicious, for example. This does not inconvenience legitimate customers and will keep them coming back for future business while preventing bad actors from perpetrating their schemes.

EVOLVING TECHNOLOGY CREATES DYNAMIC FRAUD-BUSTING STRATEGIES

Online retailers and other firms are augmenting positive friction's strategic use and continuing to spend heavily on the newest fraud-busting technologies, such as multilayered solutions that minimize frictions. AI- and ML-powered systems with predictive capabilities are being employed to counter fraudsters who are also using ML but are doing so to elude fraud-detection systems.

Overall business spending on both technologies is expected to triple by 2021, and the

share of organizations using AI and ML will grow sharply over the next year or two. Many of those firms will likely be online merchants, which are facing **skyrocketing** costs — especially from chargeback fraud. Implementation costs might give some pause, but smart retailers see the benefits of technologies that accurately detect evolving fraud attacks in real time.

Multilayered approaches that involve deploying several tools and technologies can enable merchants to keep pace with the ever-changing face of fraud, and such strategies move beyond the static, rules-based legacy systems that cannot detect new fraud patterns in real time. This is exemplified by how supervised and unsupervised ML models are used to power fraud analytics. The former requires continual human monitoring and input to learn new rules, while the latter can automatically adjust and adapt its responses based on the patterns it learns.

Device fingerprinting is another tool that allows merchants to analyze shoppers' computer operating systems, browsers and even installed language options when they place their orders, adding more data points for deeper customer analysis. Combining risky IP addresses with bank identification numbers (BINs) might provide dynamic and accurate prediction when layered into an anti-fraud system. Any sudden uptick in activity that contains both factors would signal fraud, raising the combination's risk level across all



systems that utilize anti-fraud models with this feature and giving merchants the ability to continually manage emerging fraud schemes' risks.

Fraud attempts and threat levels are **increasing** despite these investments, though, and even the most sophisticated digital barriers cannot entirely block them. Savvy merchants know adding positive frictions to their toolboxes gives them another weapon in a layered anti-fraud strategy — one that just might give them a leg up in their ongoing fight against digital crooks.

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 companies in payments share relevant information about the initiatives that make news and shape the future of this dynamic sector. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovations at the cutting edge of this new world.



Simility's portfolio includes real-time risk and fraud-decisioning solutions that take data-first approaches to detecting fraud vulnerabilities. The solutions combine AI and Big Data analytics to help businesses address fraud challenges as well as reduce friction and build trust in their brands. To learn more, visit www.simility.com.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe to this report, please email us at frauddecisioning@pymnts.com.

DISCLAIMER

The Merchant Fraud Decisioning Playbook 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.

Components of the content original to and the compilation produced by PYMNTS.COM is the property of PYMNTS.COM and cannot be reproduced without its prior written permission.