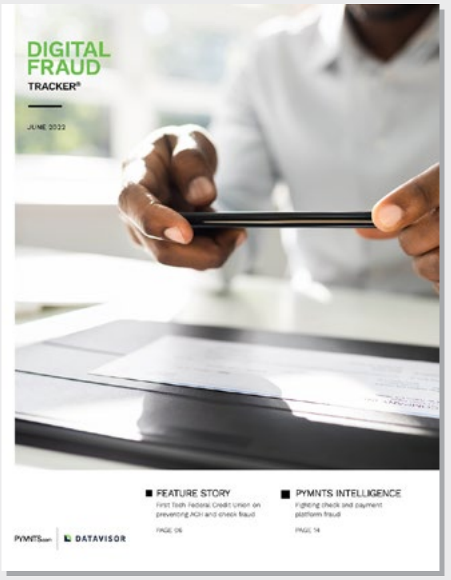
DIGITAL FRAUD

TRACKER®

JULY 2022

PYMNTS.com | DATAVISOR

Read the previous edition



DIGITAL FRAUD
TRACKER®

JUNE 2022

■ FEATURE STORY
First Tech Federal Credit Union on preventing ACH and check fraud
PAGE 06

■ PYMNTS INTELLIGENCE
Fighting check and payment platform fraud
PAGE 14

PYMNTS.com | DATAVISOR

■ JUNE 2022

Digital Fraud Tracker®

DIGITAL FRAUD TRACKER®

PYMNTS.com | DATAVISOR

ACKNOWLEDGMENT

The Digital Fraud Tracker® was produced in collaboration with DataVisor, 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

EDITOR'S LETTER

Digital fraudsters are often depicted as professional hackers lurking on the dark web, leveraging sophisticated technologies to defraud their victims of funds, data or login credentials. This scenario is not unrealistic, but what is less well-known is that a large contingent of fraudsters consists of ordinary consumers. These individuals abuse chargebacks, promotions, returns or merchant and financial services firms' policies to abscond with free merchandise or payouts, often in plain sight. This so-called first-party fraud — thus named because fraudsters often use their own identities rather than concealing them as third parties — costs merchants upward of $89 billion per year, according to a recent PYMNTS study.

First-party fraud is both pervasive and insidious, with many customers committing it without even realizing its seriousness. A recent study found that 52% of shoppers have tried to use an expired coupon, 49% have attempted to use a coupon for ineligible products and 63% have tried to apply multiple promotions that could not be combined. Coupon abuse costs the retail industry more than $100 million each year, with 73% of eCommerce companies experiencing it in the past 12 months and 90% of brands highly concerned about its impact on their long-term revenue.

Policy abuse, another common tactic, can cost even more per incident, with perpetrators exploiting return or chargeback policies by claiming they never received items and demanding refunds. More than three-quarters of eCommerce merchants saw item-not-received abuse increase in the past year, while 66% reported an increase in return abuse during that time frame. In some cases, vulnerabilities in merchants' or financial services firms' policies can be exploited by organized criminals, leading to an exponential increase in losses.

Fighting first-party fraud without sacrificing legitimate customers' experiences is a tough assignment, but new technologies offer the potential to balance these competing objectives. Entirely digitizing promotions allows merchants to generate unique coupon codes that are time-stamped and deleted when redeemed, eliminating duplication or use of expired coupons. This strategy also has the benefit of providing merchants with a cache of valuable data for personalizing legitimate customers' experiences.

This edition of the Digital Fraud Tracker®, a PYMNTS and DataVisor collaboration, examines the various means of first-party fraud and the most effective methods for preventing it without alienating legitimate customers. Promotions and friendly customer policies are essential strategies for generating revenue, and digitization could be the key to maximizing their benefits for both consumers and merchants or financial institutions (FIs).

THOUGHT LEADERSHIP TEAM

PYMNTS.com

🟩 Feature Story

Ujji On Fighting First-Party Fraud And Coupon Abuse

FRAUDULENT ABUSE OF COUPONS AND PROMOTIONS HAS BECOME SO COMMONPLACE IN THE RETAIL INDUSTRY THAT SOME MERCHANTS MAKE ROOM IN THEIR BUDGETS TO ALLOW FOR PROJECTED LOSSES.

Larger retailers have many different items on their shelves or warehouses, so these retailers can make up this lost revenue in other areas, but for smaller retailers and specialty online merchants with limited wares, first-party fraud can take a serious chunk out of the bottom line. It can siphon off critical capital if it happens too often, and the worst part is that it can be impossible to catch those responsible, so many companies invest a lot of time and money to keep it from happening.

"It just came down to being an attentive founder who is looking at orders each day, and I saw something come in and was able to cancel the order before it was fulfilled," said Jake Doering, founder and creative director of ujji, a provider of plant-based wellness drinks.

Doering's run-in with first-party fraud came in the form of an unknown fraudster who found an expired promotion that the company ran when it was a fledgling merchant on Shopify.

"That was not on our website and not sold explicitly, but somehow the customer was actually able to locate that," Doering told PYMNTS in a recent interview. "So the question is, how did they find our unlisted products that we can only see on the back end?"

PRODUCT AND PRICE INTEGRITY: THE FIRST LINE OF DEFENSE

Doering said that promotions fraud and chargebacks are exceedingly common problems for many brands. He believes that combating these issues comes down to finding the right tools, such as coupons specifically designed with complicated coding strings that expire after one use and software that detects chargeback abuse. He said his company is fortunate to suffer less of this experience than larger brands and can concentrate more on creating the best customer experience — a circumstance he ascribes to offering premium quality at a fair price.

Doering said his company focuses on making one product so effective that he offers a 30-day refund guarantee, even if the customer uses a portion of the product. This poses a risk: Unlike clothing retailers that can return a garment to the shelf for sale, a refunded product means lost revenue. Nevertheless, he said, the refund rate on his products is less than 1%.

“There’s no vetting process or verification, as they just email us and we immediately refund everything, so for us, it’s about trusting that the product is amazing,” he said. “The best way to encourage someone to buy a product is to literally guarantee that they’ll like it and, if they don’t, to just give the money back. But in order to do that, you have to first build a best-in-class product.”

To ensure his company is not a target of first-party fraud, Doering said he rarely offers promotions and tries to maintain the fairest price he can to make ujji enticing to customers without offering discounts.

“I think maintaining price integrity is kind of the first line of defense,” he said. “If you don’t run a ton of promotions and you stay true to your fair price and offer it to the best customers, then you have a lot less to worry about.”

FIGHTING FIRST-PARTY FRAUD THROUGH TAILORED COMMUNICATIONS

With the increase in eCommerce retailers on mobile platforms, Doering said that brands must be more vigilant to ensure fraudsters do not take advantage of fewer in-person touch points to commit first-party fraud.

He said that strategies such as using dynamic discount codes with personalized usage limits, for example, are safer than “one-size-fits-all” coupons that anyone with internet access can find on coupon sites. These coupons can sometimes work despite a stated expiration date and can force a company to offer the discount to keep the customer happy.

In addition, he said that tailored communications with customers can help cut down on fraud. Many brands, he said, will send email “blasts” to a multitude of customers at one time with generic codes. Inevitably, at least one recipient will try to take advantage of a coupon by using it more than once or “stacking” it with other coupons to get multiple discounts.

The success of any eCommerce business in the future, especially those without a brick-and-mortar presence, will depend on merchants’ ability to know and understand their customers and match their needs. Coupon and promotions abuse will always be an existential threat to a retailer, but employing the right policies and technology can mitigate the dangers that businesses face.

Q&A

YINGLIAN XIE
CEO

DATAVISOR

Digital businesses depend on promotions and favorable policies to speed growth and retain customers, but such customer-centricity has a downside: first-party fraud. How does this differ from third-party fraud, and how does it change the game for fraud teams?

While not identical in meaning, policy abuse, promo abuse, first-party fraud, friendly fraud and similar issues share an identity in the fact that they are illicit acts perpetrated by individuals who don't necessarily hide or misrepresent their identities. In these forms of fraud, which we can refer to as policy abuse for simplicity, customers who are who they say they are behave in illicit ways to exploit companies' policies to their advantage.

The implications of this definition are noteworthy for two reasons:

First, traditional fraud-prevention measures and tools are not great at detecting policy abuse because they are designed to look for instances where identities, credentials and payment methods are compromised, as is not the case with these issues. We go into more detail on this below.

Second, organizations are responsible for designing the policies they offer their customers and must do so [while] taking into account the possibility of abuse.

While many people associate promotion abuse with retailers and merchants exclusively, the truth is that financial services firms, most often in the FinTech space, can also fall prey to these attacks. For example, neobanks and cryptocurrency exchanges that implement referral bonuses or customer acquisition incentives must be vigilant to ensure that these strategies reach the right hands.

It is also worth keeping in mind that policy abuse vulnerabilities can be exploited by organized criminals. In this sense, the line between policy abuse and third-party fraud can be quite thin. Fraudsters could exploit sign-up bonuses and other promos using bots and batches of false identities, leading to exponential losses for well-intentioned FIs and retailers.

Why are traditional fraud detection strategies ineffective against policy abuse?

If you are using a legacy fraud detection platform to try to mitigate first-party fraud, you may be experiencing the frustration of seeing costs soar for your company. The main reason for this is that abuse can come from real customers who have successfully completed onboarding identification steps and, in all likelihood, have a transaction history with your company.

Traditional fraud prevention efforts, including two-factor authentication, identity validation measures and biometrics recognition solutions, are designed to prevent unauthorized individuals from passing as legitimate users to commit fraud. However, these measures are rendered null by legitimate users committing policy abuse in their own names and accounts.

As I mentioned above, sometimes policies can be abused by criminal groups in more complicated fraud attack schemes. The use of bots to perform these large-scale attacks also poses additional challenges for teams without cutting-edge fraud detection tools that do not have the capabilities required to identify complex bot-scripted attacks.

Advanced fraud solutions such as DataVisor's proactive detection platform offer additional layers of protection by continuously monitoring user activity at various levels and allowing fraud teams to act before it is too late. This allows companies to retain their most loyal clients and attract new ones without wasting marketing dollars on multi-accounting, fraudulent registrations and user collusion. The secret is a resilient fraud architecture through detailed data analysis, a time-tested rules platform, supervised and unsupervised machine learning models and intuitive visualization and decision tools.

What are some of the best ways for merchants or financial services firms to ensure that fraudsters don't abuse their promotions and other policies?

The first step toward solving the problem of first-party fraud is identifying it as such. Many companies still treat certain forms of policy abuse as a cost of doing business, a customer support issue or another type of matter. The lack of clarity regarding the ownership of policy abuse within organizations increases the difficulty of creating cohesive, company-wide strategies designed to ensure that policies are effective in their goals and do not lend themselves to abuse by deceitful agents.

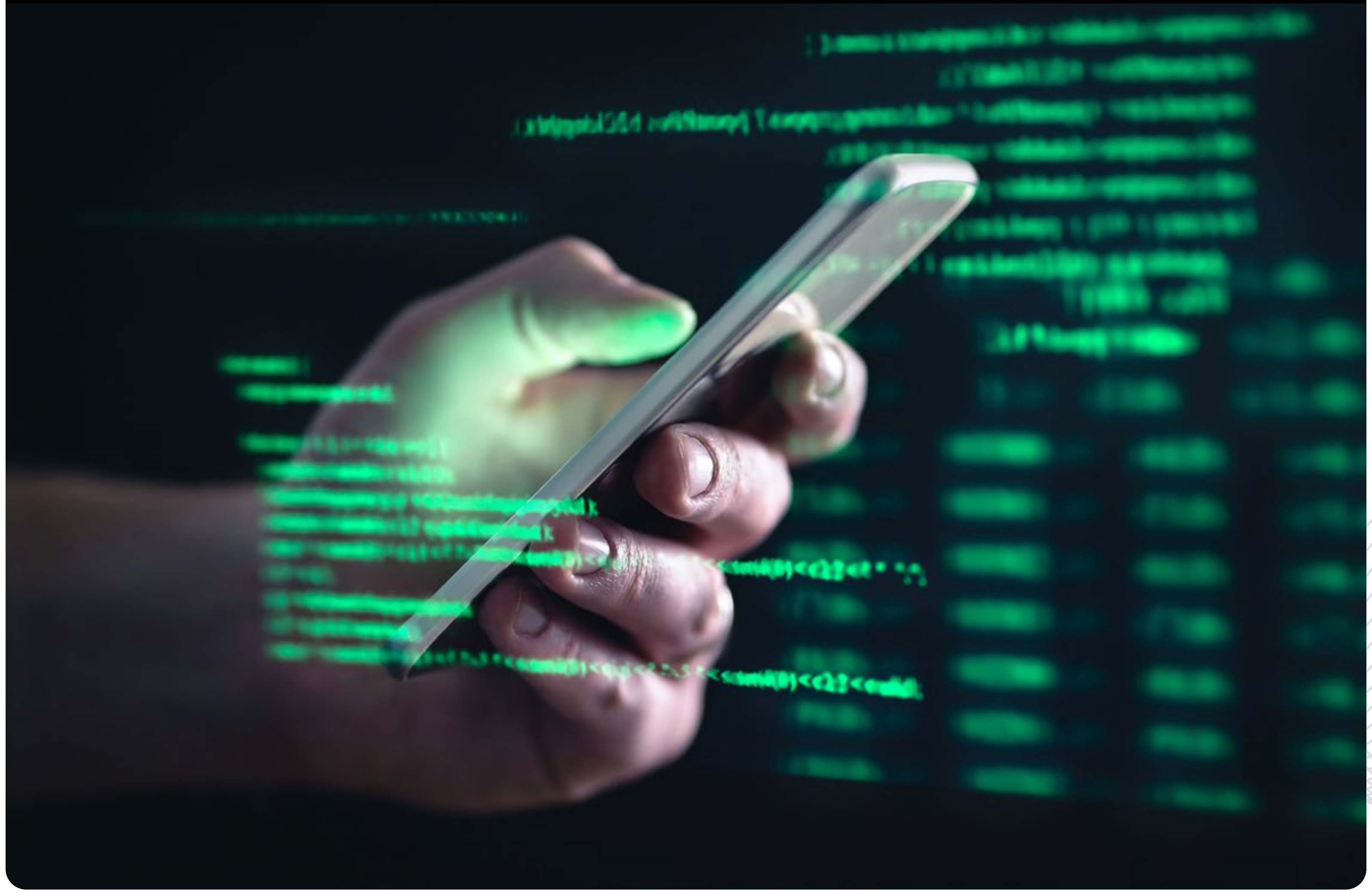
Another suggestion is to migrate from transaction level-only fraud detection, which by itself is incapable of detecting most forms of policy abuse. This is especially the case with repeated first-party fraud behavior, where policies are abused by the same customers over and over.

For example, transaction level analysis would be ineffective at mitigating the damage caused by the customer of a financial company abusing sign-up bonuses by opening hundreds of accounts using different email addresses. When seen in isolation, each of these account openings could seem valid, but when analyzed in bulk, a different reality would appear.

When deciding to keep, modify or cancel certain policies that might open the door for fraud, firms must use company-wide data analysis. Once a fraud team is empowered with the tools to identify policy abuse, it can share insights with other functional areas to keep track of the incidence of each type of abuse and its consequences on the firm's bottom line. Ultimately, this collaborative approach will allow more informed decision-making.

PYMNTS Intelligence

Protecting Against Promotion Abuse And Other Forms Of First-Party Fraud



DIGITAL FRAUDSTERS' POPULAR IMAGE IS THAT OF A SHADOWY CABAL OF HACKERS, EITHER LEVERAGING SOPHISTICATED ALGORITHMS TO BREAK INTO CORPORATE SYSTEMS OR TRICKING INDIVIDUAL CONSUMERS INTO GIVING UP THEIR FUNDS, DATA OR LOGIN CREDENTIALS.

This image is undoubtedly credible, but a considerable portion of digital fraud comes from consumers themselves abusing chargebacks, promotions, returns or merchant policies and attempting to score free merchandise or payouts. This latter scenario is known as first-party fraud, which costs merchants upward of $89 billion per year, according to a recent PYMNTS study.

Consumers leverage an astonishing variety of tactics to wage first-party fraud, leaving merchants with a critical dilemma: Do they tighten up their generous policies and attempt to curb this fraud at the expense of legitimate-customer loyalty, or do they maintain current policies and accept first-party fraud as one of the costs of doing business? Both choices have significant drawbacks, but new technologies can spare merchants either sacrifice. This month, PYMNTS Intelligence explores the various means of first-party fraud and the most effective methods for preventing these fraud losses without alienating legitimate customers.

FIRST-PARTY FRAUD TECHNIQUES

First-party fraud is incredibly pervasive, with many customers committing it without even realizing its gravity. One of the most common forms of this fraud is the misuse of coupons or other promotions. A recent study found that 52% of shoppers have tried to use an expired coupon, 49% have attempted to use a coupon for ineligible products and 63% have tried to apply multiple promotions that were not stackable. Coupon abuse often goes unnoticed at the point of purchase due to inattentive, overworked or conflict-averse cashiers. The study found that 57% of cashiers manually overrode coupons that their systems said were incompatible. This type of abuse costs the retail industry more than $100 million each year, and 90% of brands surveyed said they were deeply concerned about the impact coupon fraud could have on their long-term revenue.

Policy abuse is another prominent form of first-party fraud, costing retailers as much as 2.4% of their annual revenues. While promotion and coupon abuse was the most common type of fraud by incidents reported — with 73% of eCommerce companies experiencing it in the past 12 months — policy abuse can cost much more per incident, with consumers exploiting return or chargeback policies by claiming they never received items and demanding refunds. Seventy-six percent of eCommerce merchants said that item-not-received abuse had increased during the past 12 months, while 66% of eTailers reported an increase in return abuse over the same period.

Fighting first-party fraud without affecting legitimate customers' shopping experiences is a tall order, but new technologies offer the potential to strike a balance between these competing objectives.

PREVENTING PROMOTION ABUSE

One of the most important ways to limit promotion abuse is to make the promotions entirely digital and remove the element of human error from the equation altogether. These digital promotions allow merchants to generate original coupon codes that are date- and time-stamped and then deleted once used at the point of sale or after the expiration date. This strategy eliminates several methods of coupon fraud by making it impossible to copy a coupon code as well as making it impossible to present retail staff with an expired coupon. Walgreens enacted one such example in 2020, and the chain quickly realized several advantages besides fraud prevention. Customers could access digital coupons remotely instead of cutting them out of newspapers or receipts, providing the stores with a trove of valuable data for improving customers' experiences through personalized offers.

Digital coupons are not perfect, however. Hackers occasionally steal consumers' coupons and attach them to their own accounts by intercepting requests from victims' devices and the servers of the coupon providers. Shoppers may also return items purchased via a digital coupon for the full price. These fraud techniques are much rarer than fraud perpetrated via paper coupons, however, making digital coupons a much safer method overall.

First-party fraud prevention is a top priority for merchants, regardless of the method used. PYMNTS research has shown that more than three-quarters of merchants either already invest in chargeback prevention strategies or plan to in the next year.

Promotions and coupons are a key strategy for generating revenue, and any means of preventing their abuse must also avoid alienating legitimate customers. Digitization can go a long way toward achieving the perfect balance.

NEWS & TRENDS

GLOBAL FRAUD TRENDS

CANADIAN RETAIL FRAUD INCREASED DURING THE PANDEMIC, REPORT FINDS

Retail fraud in Canada increased 15% since the beginning of the pandemic, accounting for hundreds of millions in losses to retailers, according to a recent report. Several possible causes have been proposed, including a rise in the number of businesses that switched to online or curbside pickup orders.

Despite the changes to in-store traffic, the report noted that increases include professional return fraud, which involves thieves stealing items from stores with the intent of returning them later without receipts to obtain gift cards. The fraudsters then use the gift cards to buy items at different stores and return them for cash. Delivery theft, a method in which bad actors leverage stolen credit cards to purchase products and have them delivered to a different address or steal them as they arrive, is also increasing. The report found that many retailers have also fallen victim to chargeback fraud, in which consumers dispute transactions and claim they never received packages, resulting in tens of millions of dollars in losses.

LOSSES FROM CRYPTO SCAMS TOP $1 BILLION SINCE 2021, REPORT FINDS

Some have touted cryptocurrency as the next big investment opportunity, but the digital currency is far from risk-free. A new report from the Federal Trade Commission (FTC) warned that more than 46,000 people have lost upward of $1 billion in cryptocurrency scams since the start of 2021, with the median reported loss at $2,600. The FTC received reports of $680 million in losses due to crypto fraud in 2021, and approximately $329 million had been lost as of Q1 2022. The 2021 losses were nearly 60 times more than those reported three years prior, the report added.

The report attributed the rise in fraud to crypto transactions' irreversibility and the lack of government protections for these transactions, noting that crypto fraud is currently responsible for more financial loss than any other payment method. Nearly half of these losses result from scams on social media, the report said, with investment-related fraud, romance scams and impersonation of business or government officials being the most common fraud types.

ENTERPRISE FRAUD

PAYMENTS FRAUD INCIDENCE AT LOWEST RATE IN SEVEN YEARS, STUDY FINDS

A recent survey of 550 financial professionals found that although 71% of respondents said their firms had been the target of payments fraud in 2021, it was the lowest incidence recorded since 2014. Interestingly, 47% of organizations that saw an increase in fraud did not believe increases in remote work were to blame.

Of those targeted, 66% said check payments were the most targeted payment method, and ACH debits represented just more than one-third of the targets. Instances of business email compromise (BEC) fraud were down, with 68% of organizations saying they were targeted, a decrease from 76% in 2020. Approximately 58% of those surveyed said accounts payable departments were the target of BEC scams.

STUDY FINDS TWO-THIRDS OF U.K BUSINESSES EXPERIENCED INCREASED CYBERCRIME, FRAUD

Meanwhile, a new report finds that 64% of U.K. businesses have been the target of economic fraud in the two years since the pandemic began, significantly higher than the global average of 46%. This rate also represents an increase from 2020, when 56% of U.K. companies reported being victims of economic crime. Cybercrimes were the most prevalent type of fraud, with nearly one-third of respondents having been the target of a cyberbreach.

The report suggested that companies' emphasis on speed over security when rolling out digital platforms for remote work during the pandemic was a factor in the fraud increase. One-fifth of U.K. firms reported experiencing supply chain fraud, with the report noting that remote work made it difficult to monitor supply chains properly.

CORPORATE BOT ATTACKS GO UNNOTICED FOR FOUR MONTHS, STUDY FINDS

Businesses around the world are constantly on the lookout for online threats, but a recent report found that companies in the U.S. and the U.K. fail to uncover bot attacks for an average of 16 weeks — an increase of roughly two to four weeks from the same study a year ago. The attacks no longer target just websites, with 60% of firms surveyed saying they have detected bot attacks on application programming interfaces (APIs) and 39% having detected attacks against their mobile apps — both notable increases from a year ago.

Even though most businesses are using mitigation measures to help detect and cut down on attacks, the increased average time to detection suggests that bot attacks are getting more intelligent. The report found that companies dedicate too little to bot management at just under 8% of security budgets, increasing from 5% in 2021.

PASSWORD PROTECTION REMAINS FOCUS OF FRAUD CONTROL STRATEGY FOR U.S. COMPANIES

For many consumers and businesses, the humble password is the gatekeeper that controls outside access to crucial data. According to a recent report, 88% of U.S. businesses and 80% of global businesses said they were satisfied that current security policies are protection enough. Still, more than half of firms around the world and nearly two-thirds of firms in the U.S. indicated that an increase in remote work has compelled the adoption of password management tools to help control unauthorized access that could lead to fraud and online theft.

Of the measures businesses are taking, 67% of U.S. businesses said a minimum password length was the most common management tool mandated for employees, as just more than half said that weak passwords were a common bad habit in their organizations. Just more than half of U.S. respondents also indicated that outside contractors and consultants presented high security risks. Despite these threats, just 41% of U.S. businesses use password managers for third parties. Slightly more than one-third of U.S. firms surveyed indicated that poor password management led to a security breach, and 62% said breaches at other companies were the impetus for shoring up their password management policies.

DIGITAL FRAUD

TRACKER®

ABOUT

PYMNTS.com

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

DATAVISOR

DataVisor's mission is to build and restore trust online. It partners with the largest financial and internet properties in the world to protect them from a wide array of attacks, including fraud, abuse and money laundering. The company's unsupervised ML-based detection solution detects attackers without needing training data and often before they can do damage.

DataVisor is made up of a team of world-class experts in Big Data infrastructure and ML. It builds advanced algorithms to fight the world's most sophisticated online attackers.

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

DISCLAIMER

The Digital Fraud Tracker® 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.

Digital Fraud Tracker® is a registered trademark of What's Next Media & Analytics, LLC ("PYMNTS.com")