DIGITAL FRAUD

TRACKER®

FEBRUARY 2022

FEATURE STORY

TSYS On Fraud-Fighting FinTech Trends In 2022 And Beyond

PAGE 06

PYMNTS INTELLIGENCE

How first-and third-party fraud threaten the digital ecosystem

PAGE 14

PYMNTS.com | DATAVISOR

DIGITAL FRAUD

TRACKER®

PYMNTS.com | DATAVISOR

ACKNOWLEDGMENT

The Digital Fraud Tracker 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

04 EDITOR'S LETTER
A look at digital fraud trends that are already making their mark in the new year from the PYMNTS Thought Leadership Team

06 FEATURE STORY
An interview with Dondi Black, senior vice president and head of product at global payments company TSYS, on the newest tools and technologies keeping fraudsters at bay in 2022 and beyond

10 Q&A
Yinglian Xie, CEO and co-founder at DataVisor, on growing digital fraud threats and how eCommerce and financial services fraud teams can combat them

14 PYMNTS INTELLIGENCE
An in-depth look at the problems of first- and third-party fraud and how they threaten the digital ecosystem

18 NEWS AND TRENDS
The latest headlines from the digital fraud space, including how 67% of U.S. executives said their companies were victims of external fraud over the last 12 months and why only 35% of their businesses have implemented cybercrime prevention and response programs

24 ABOUT
Information on PYMNTS.com and DataVisor

EDITOR'S LETTER

The pandemic-driven shift to digital channels gave rise to a sizable increase in fraud beginning in 2020, and this trend shows no signs of slowing. The World Economic Forum's 2022 report on global risks noted that internet banking fraud in the United Kingdom rose 117% in volume and 43% in value year over year in 2021 as consumers spent more time shopping online. A new KPMG study reported that United States firms will face a rising triple threat of fraud, cyberattacks and compliance violations in the next 12 months, and two-thirds of senior risk executives predict that the risk of external fraud will worsen in 2022.

The term "fraud" itself is a deceptively simple umbrella covering a growing variety of sophisticated cybercrimes, including identity fraud, account takeovers (ATOs) and friendly fraud, so named to describe the case in which consumers themselves become the bad actors, claiming refunds or missed deliveries on goods they have received and used. eCommerce and retail fraud continue to rise, with a new report finding that U.S. eTailers paid $3.60 for every $1 lost to fraud in 2021, up 7.1% in only a year.

In banking, ATOs, authorized push payment schemes and new account fraud constitute the major fraud trends. Nearly 40% of Americans have fallen victim to identity theft used to commit application fraud in the banking industry, and a slightly larger share have faced ATOs. Fraud costs for financial services and lending institutions also remain significantly higher than pre-pandemic levels: U.S. financial services firms now pay $4 for every $1 of fraud loss, up nearly 10% from 2020.

This edition of the Digital Fraud Tracker®, a PYMNTS and DataVisor collaboration, examines current digital fraud trends and the outlook for the rest of 2022 and beyond. All signs suggest that it will take a concerted effort from consumers and businesses to effectively combat increasing fraud levels. Third-party vendors have big-picture insights into the fraud landscape and may be key resources in helping organizations find solutions to complex threats.

Thought Leadership Team

PYMNTS.com

Feature Story

TSYS On **Fraud-Fighting FinTech** Trends In 2022 And Beyond

FRAUD HAD A RECORD-BREAKING YEAR IN 2021, SO PRUDENT COMPANIES ARE TAKING SPECIAL CARE TO STAY INFORMED, AWARE AND CAUTIOUS IN THE YEAR AHEAD.

Whether fraudsters up their games in 2022 or not, many in the banking and payments industries are looking to strike back. Dondi Black, senior vice president and head of product at TSYS, a global payments company headquartered in Georgia, believes that this challenge comes with the territory, as banking itself is what she calls the business of risk.

"Our payment clients are perpetually navigating [a] fine line, trying to keep [the] balance between protecting all of us as consumers and businesses [and] delivering really great experiences that make our lives easier," she told PYMNTS in a recent interview. "Fast, simple and secure — that's the North Star."

Black contends that the role of payment providers includes protecting the life cycle of each transaction from the point of origination to settlement. Guarding against rising threats, she said, will require companies to leverage cutting-edge technologies to analyze and authenticate every transaction as it happens in real time.

> "Our payment clients are perpetually navigating [a] fine line, trying to keep [the] balance between **protecting all of us** as consumers and businesses [and] **delivering really great experiences."**

BUILDING THE FRAUD PREVENTION OF THE FUTURE

Black said that to address today's growing fraud problem, it is vital to acknowledge that we have entered a new era, one in which the major parts of our lives — professional, financial and personal — have gone online, making for new risks.

"I think we all recognize the digital transformation was well on its way before the entire world paused and pivoted to meet the challenges of the pandemic," she said. "[We have] new ways for making payments [and] for accepting payments, and that [has] translated to more surface area to protect [and] more points of potential compromise for fraudsters to exploit."

Synthetic identities, card-not-present (CNP) fraud and account takeovers (ATOs) are the fraud trends Black said TSYS has seen rising throughout 2021. Although she was quick to say that no one has a crystal ball, she does not think these security risks are going away anytime soon. She instead predicts they will continue to drive risk management for banks, credit unions and FinTechs for years to come.

"Modern fraud schemes are generally going to be multifaceted," she said.

Black anticipates that anti-fraud technologies, therefore, are also going to be an integral part of the payments space in 2022. She believes that new technologies such as artificial intelligence and machine learning will become a standard part of security practice to protect payment gateways by ensuring that every payment is valid and secure when going from point A to point B.

"That means validating and interrogating data points that can be directly verified [via] things like a name matched to a Social Security number ... and other data points that might [be used] for detection and prevention, such as device ID or applying 3D Secure technologies," she said.

These technologies are able to use context — such as location — to eliminate false positives and create nearly frictionless experiences for consumers.

"I think we all recognize that fraud prevention with a broad brush leads to bad customer experiences in many cases and high false-positive declines," Black said, "and that's not good for anyone."

Both the payments world and the technologies within it are constantly changing, she said, and fraudsters are sharp, so payments providers must be ready.

"We all have to focus on moving forward together, and I think that's really the future of fraud prevention for the industry," she concluded.

Q&A

YINGLIAN XIE
CEO and co-founder
DATAVISOR

Research indicates that U.S. firms face a growing threat of digital fraud perpetrated by criminals who are increasingly sophisticated. How can eCommerce and financial services fraud teams keep up with such criminals?

"Unfortunately, this is very common. Fraud teams everywhere feel overwhelmed by playing catch-up with foes who innovate skillfully. By the time [teams] dissect an attack and implement defenses, the attackers have a new modus operandi and are cashing in again. The cycle then repeats itself.

Instead of finding better ways of keeping up, we need to focus on staying ahead of fraud. Only with a truly proactive strategy that gives companies the benefit of foresight can the fraud cycle be stopped once and for all.

Sounds great, right? And the best part is that the technology to accomplish this is available. At DataVisor, we have helped hundreds of teams reimagine their fraud strategies with tools like our Unsupervised Machine Learning Engine, which processes events and account activities to analyze patterns across hundreds of millions of accounts, users and transactions. This enables detection of suspicious connections between events, even when attackers are incubating accounts, mimicking legitimate user activities or changing techniques."

The term "fraud" can be deceptively simple, encompassing a growing variety of sophisticated cybercrimes. What are the most relevant fraud trends that business and fraud leaders need to be aware of in 2022, and what are the most effective solutions?

"We have the pleasure of working with fraud teams across industries and have been hearing a lot about two main trends lately.

First, we have noticed that more and more companies are talking about policy and promotion abuse as a form of fraud. A lot of companies that used to treat issues of policy abuse (e.g., return fraud and promotion abuse) as a cost of business, a customer support issue or another type of matter other than fraud are now shifting strategies.

This is good news because it allows them to create more cohesive strategies led by their fraud teams in order to mitigate the costs associated with policy abuse and first-party fraud in general. One recommendation for curbing promo and policy abuse is to zoom out of transaction-level fraud detection and consider user accounts and even user groups as a whole to detect fraudulent activity before it is too late.

Second, we have noticed increased interest in the need to fight bot-scripted attacks in financial services and eCommerce. It seems like the industry now knows for sure that a substantial portion of fraud attacks are perpetrated at scale and with a higher degree of technological sophistication.

Fraudsters nowadays have access to advanced gadgets and techniques that include emulators, credential stuffing, cloud phones, app cloners, proxies, hooks and jailbreaks. Companies should make sure that their fraud teams are equipped with technology that allows them to see through these attack techniques, especially device intelligence that goes beyond simple device IDs."

On the topic of first-party fraud, what are the factors that have contributed to bringing this subject to the forefront of the conversation?

"It seems like this can be answered from two perspectives. In a general sense, almost all industries have discovered the importance of customer-centricity to attract new users and retain them. For example, FinTech has transformed the financial services industry by placing the user in the center and investing heavily in policies and interaction points that focus on the customer experience. In retail and perhaps driven by giants like Amazon, companies now offer very friendly policies like return allowances to be able to compete for customers with higher and higher expectations. As companies create more friendly policies and interaction points, fraudsters inevitably take notice and seek ways to exploit them to their advantage, lawfully or not.

In a more particular sense, companies are talking about first-party fraud more often than before because they have realized that traditional fraud prevention strategies are not very efficient at detecting and stopping fraud perpetrated by people who do not hide or misrepresent their identities, as is the case with most instances of policy abuse.

Specifically, identity verification measures, such as biometric checkpoints, and identity validation checks, such as credit bureau inquiries, fail to offer protection against first-party fraud because individuals are who they say they are but are acting in ways that are abusive and unlawful. In order to detect these actors, companies need more advanced tools, such as behavioral analytics, that can spot abuse before it [appears] in their bottom line."

The Problems Of First- And **Third-Party Fraud In The Digital Ecosystem**

Digital fraud is a constant threat to banks, businesses, government entities and individuals, and its volume and costs continue to expand despite the best efforts of oversight agencies and security and risk management teams. The rate of suspected digital fraud attempts swelled 17% worldwide year over year in Q2 2021, and certain industries were targeted far more than others. The gaming industry experienced a fraud increase of 393%, for example, and fraud affecting travel and leisure companies grew by 156%.

Fraud can largely be divided into two general types: third-party fraud, in which bad actors mask their identities to stage cyberattacks, and first-party fraud, in which disingenuous actors use their own identities in malicious ways. Both are pernicious threats to consumers and organizations of all types. This month, PYMNTS explores the various methods that third-and first-party fraudsters leverage in their schemes.

THIRD-PARTY FRAUD

One of the most dangerous methods of third-party fraud is new account fraud, in which bad actors deploy fake identities to open new accounts at banks or businesses for use as staging grounds for fraudulent activity. Identity theft is the most well-known source of these false identities, but some fraudsters develop synthetic identities instead. New account fraud is a relatively new phenomenon, as banks considered it a low priority in the early 2000s, but it has grown into a full-blown scourge, with 85% of financial institutions (FIs) reporting fraud in the account opening process. Banks were expected to lose $3.5 billion to new account fraud in 2021.

Some bad actors instead seize control of existing accounts, a method known as ATO fraud. A 2021 report found that 22% of U.S. households have been victimized by an ATO at some point, costing victims an average of $12,000 per incident. The source of these attacks can vary greatly. Sixty percent of ATO victims report using the same passwords across multiple accounts, a practice that puts them at high risk of identity theft if their passwords are compromised. Bad actors have a variety of means of accessing potential victims' personal information, with some obtaining it themselves through phishing emails or malware, while others purchase logins in bulk from dark web marketplaces.

Third-party fraud can be devastating and represents the most common perception of fraud, but it is by no means the only type. First-party fraudsters, for example, are even bold enough to use their own identities.

FIRST-PARTY FRAUD

Most first-party fraud, also called friendly fraud, revolves around exploiting or abusing existing company policies, such as returns, chargebacks or promotions. The most common form of friendly fraud occurs when customers request undue chargebacks from their banks, falsely claiming that their transactions were fraudulent or that their orders never arrived. The banks overturn the sales, refund the customers and then go back to the merchants to recoup the payment. Chargebacks accounted for 29% of eTailers' fraud losses last year.

Other first-party fraudsters interact with victims directly rather than using a go-between such as a bank or credit card provider. Promotion abuse, for example, consists of fraudsters reusing discount codes, making multiple new accounts or signing up for multiple free trial periods to take advantage of limited-time or one-per-customer promotions. Other bad actors leverage return fraud, exploiting generous return policies to claim items were defective when in fact they were not. These fraudsters demand refunds while keeping the items they purchase, essentially scoring them for free. Some fraudsters do this solely for the sake of obtaining items for themselves, while others make a career of selling the stolen goods for below-retail prices.

In short, bad actors utilize a staggering variety of fraud methods, and businesses of all types are struggling to defend against them. It is unlikely that a one-size-fits-all solution exists, so businesses must take a multilayered approach to data security.

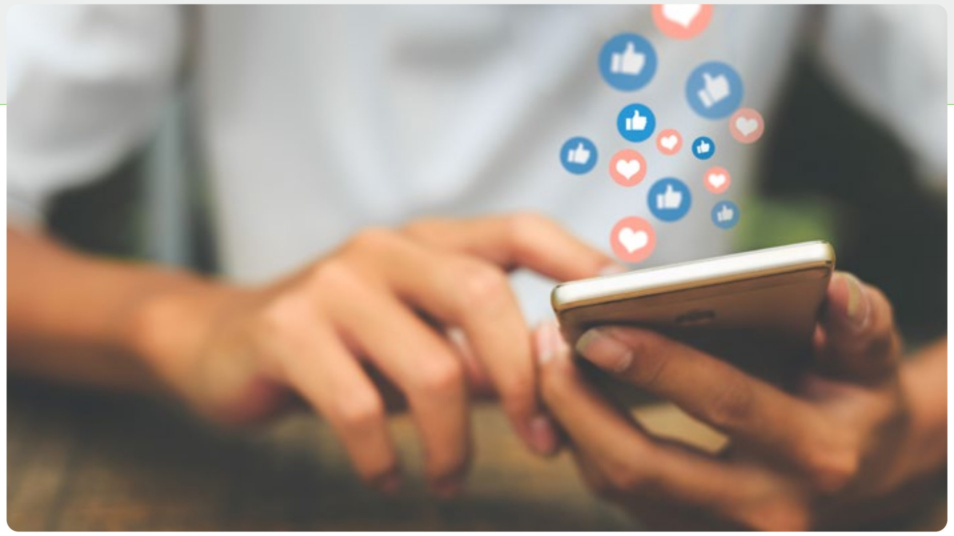
NEWS & TRENDS

FRAUD COSTS AND RISKS

FINANCIAL FRAUD COSTS REMAIN HIGH

The drive toward digital channels throughout the pandemic led to a large spike in fraud attacks, and the trend shows no signs of slowing. A recent report found that fraud costs and volume remain notably higher than pre-pandemic levels for financial services and lending institutions, with U.S. financial services firms now paying $4 for every $1 of fraud loss, compared with $3.64 in 2020.

Mortgage lenders have been hit particularly hard, with mortgage lending fraud costs now 24% higher than just before the pandemic's onset in early 2020. Though marginally lower than its initial pandemic jump, every $1 of mortgage lending fraud loss still costs $4.40. Further, more than half of U.S. credit lenders and banks polled said they have experienced at least a 10% increase in mobile channel fraud in 2021.



US CONSUMERS LOST $770 MILLION TO SOCIAL MEDIA FRAUD SCAMS IN 2021

Social media is proving to be a treasure trove for fraudsters. A new Federal Trade Commission report announced that consumers lost $770 million to social media scams in 2021, more than one-quarter of all fraud losses last year. The figure, up a staggering 18 times from 2017, made social media the single most profitable contact method for fraudsters in 2021.

Younger consumers are also becoming a key target, with adults ages 18 to 39 reporting fraud losses at 2.4 times the rate of adults ages 40 and over. Social media fraud affected more than 95,000 victims — twice 2020's number — accounting for 26% of dollars lost to fraud, followed by websites and apps at 19% and phone calls at 18%. Investment scams, often involving bogus cryptocurrency purchases, and romance scams, in which fraudsters pose as romantic interests who then ask for money, were the top two most lucrative fraud types for social media scam artists last year.

US BUSINESSES CAN EXPECT INCREASING FRAUD LOSSES, ACCORDING TO RISK EXECUTIVES

U.S. firms face a growing threat of fraud losses in the next 12 months, according to a recent study. Two-thirds of U.S. upper-level risk executives surveyed predicted external fraud to spike in 2022, 84% expect cybersecurity risks to increase and 73% see compliance risks becoming a greater issue this year. Only 35% of these executives' businesses have implemented cybercrime prevention and response programs, however, highlighting the severity of organizations' digital insecurity.

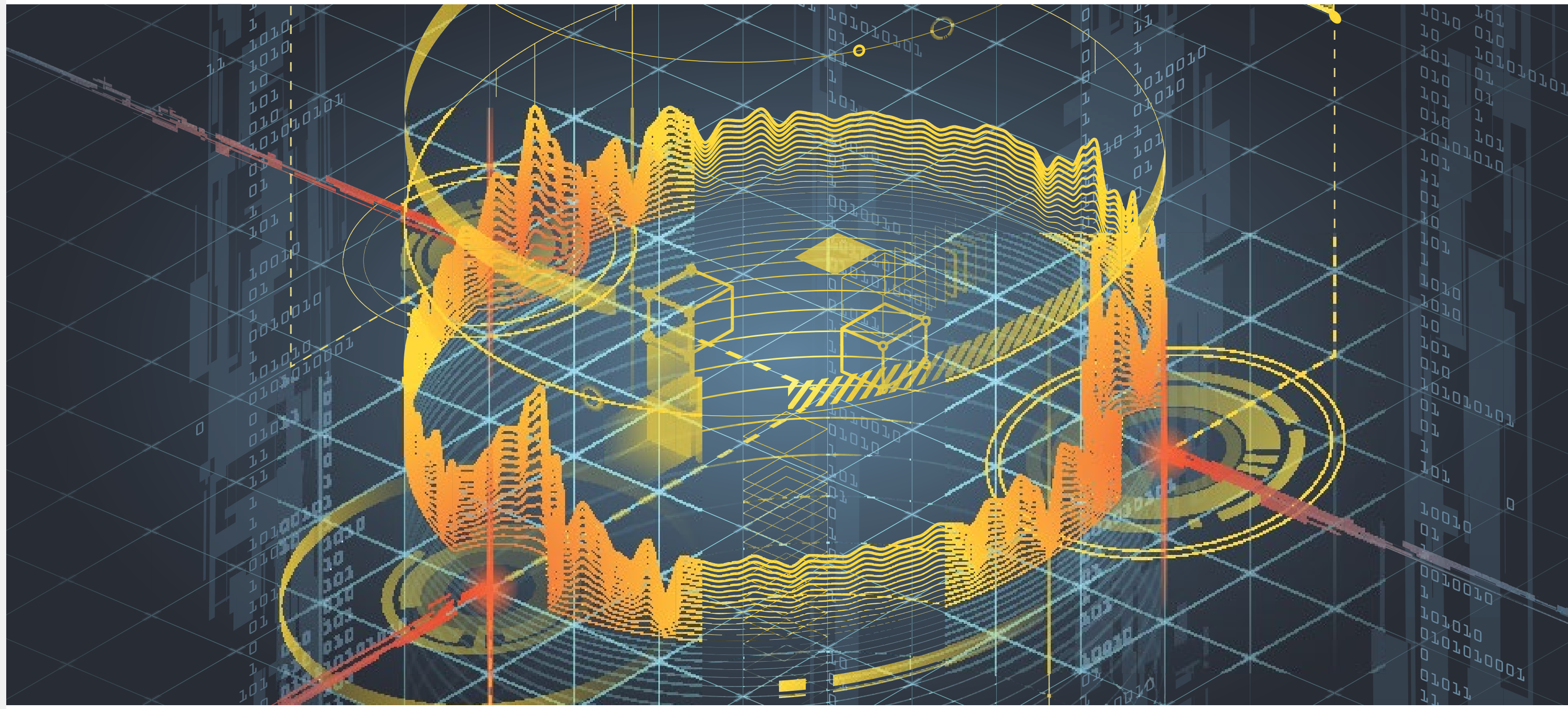
Study researchers noted that these three issues combine to create a "threat loop" of economic, regulatory and reputational losses for which companies are ill-prepared. The research further indicated that 67% of respondents said their companies were victims of external fraud, including credit card fraud, identity theft and other forms of fraud perpetrated by individuals outside the company, over the last 12 months. Researchers concluded that U.S. companies should prioritize external fraud but cannot afford to ignore cybersecurity and noncompliance issues as their urgency grows as well.

FRAUD PREVENTION AND SOLUTIONS

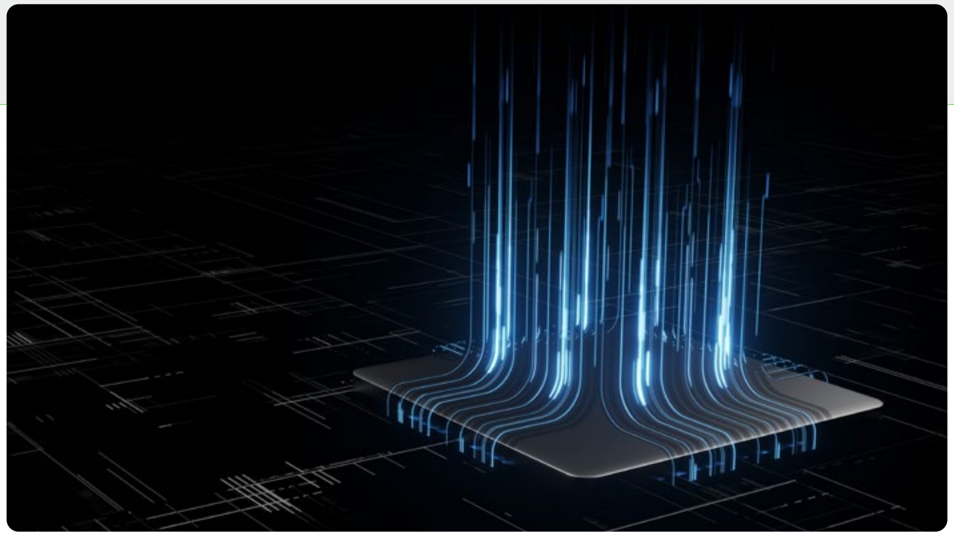
FIs ILL-PREPARED TO COMBAT INCREASING FRAUD RISKS

Many FIs are still struggling to deploy fraud prevention tools and software despite the growing risk of fraud. One-third of respondents in a survey of 128 financial fraud prevention experts admitted they were "only somewhat" or "not at all" effective in the routine maintenance, operation and control of their fraud mitigation technologies. Further, 37% of FIs fear that their companies are not properly equipped to assess or react to evolving and emerging fraud patterns, and 66% cited fraud trends as their greatest challenge.

Cost and infrastructure challenges were two major contributors to firms' difficulty in implementing effective fraud prevention, with 35% of respondents saying they had inadequate investment in fraud mitigation tools and 38% admitting that outdated technology stood in the way of improving cybersecurity. Third-party vendors have greater insight into the fraud landscape and may offer possible solutions to help organizations respond to complex threats.



> “19% of technology firms say **financial fraud** is their **top AR pain point.**”



NEARLY ONE-FIFTH OF TECH FIRMS SAY FINANCIAL FRAUD IS THEIR TOP AR PAIN POINT

Fraud is a scourge to all businesses, but it takes a particularly heavy toll on technology firms. A recent PYMNTS report noted that 19% of technology firms say financial fraud is their top accounts receivable (AR) pain point. Financial fraud has been a growing concern across industries as bad actors exploit the rising amount of economic activity online. Fraud was far and away technology companies’ top reported pain point, followed by the complications of managing multiple vendor relationships at 12%.

Companies must carefully calibrate their fraud prevention strategies, however, as ineffective fraud detection can create “false positives” that improperly block legitimate payments. For technology companies with core competencies that do not include fraud protection, seeking expert advice and solutions appears to be a key strategy. Fraud detection was the area for which technology companies were most likely to turn to vendors for support, with 29% reporting that they work with third-party providers in this aspect of their businesses.

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.

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