PYMNTS.com

DIGITAL FRAUD TRACKER®

HOW TICKETMASTER REWARDS FANS AND Bars Fraudsters

FEATURE STORY
Page 6

NOVEMBER 2019

DATAVISOR

DIGITAL FRAUD TRACKER

ACKNOWLEDGMENT

The Digital Fraud Tracker® was done 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.

PYMNTS.com | DATAVISOR

WHAT'S INSIDE

Retailers see the holiday season as a prime time to entice customers to take advantage of discounts on sought-after items, but fraudsters view it as an opportunity to steal busy shoppers' payment information and make off with retailers' merchandise.

Online shopping ecosystems have attracted fraudulent activity ever since the expansion of EMV chip-enabled payment cards made it harder for bad actors to steal credit card information at the point of sale (POS). Europe has been particularly affected by this type of activity, with 71 percent of fraud-related losses connected to eCommerce transactions or card-not-present (CNP) fraud, according to data from the European Central Bank. One in five United Kingdom citizens have experienced online fraud, as well.

Advertisers are also being targeted by cybercriminals this holiday season. Automated bots combined with human-operated "click fraud farms" and other deceitful actors download mobile apps and engage with advertising without intending to become legitimate customers. These fraudulent groups make money off payments per download while advertisers lose funds by paying for unreliable impressions.

These and other tactics appear to have prompted several banks, retailers and other businesses to take more aggressive stances in their anti-fraud efforts.

THE LATEST TRENDS IN THE FRAUD FIGHT

Several companies and even some municipalities have realized that getting ahead of bad actors is better than simply responding after incidents occur. Financial services giant Mastercard is among the latest players to deploy a proactive anti-fraud strategy, launching a new service called Threat Scan to detect troublesome activity in real time and enable businesses to respond to fraud as it occurs. The service can simulate known fraudulent activity against credit card issuers' systems to locate vulnerabilities, helping businesses address weak spots before they are exploited.

Digital wallet solution provider Radpay recently debuted a feature for its payment system that offers heightened identity and transaction validation processes to provide security for digital payment methods stored on mobile devices like smartphones and wearables. Radpay said the solution can better protect against both card present and CNP fraud.

Philadelphia, Pennsylvania, meanwhile released a new solution to address property scams, as the city has seen a sharp rise in such fraud over the past two years. Bad actors perpetrating these schemes use stolen property deeds, forged sales documents and notary stamps to steal properties, often before owners realize what has happened. City officials launched a new Fraud Guard

service that allows property owners to register their homes and receive alerts if their names or addresses appear on any documents filed with the Philadelphia Department of Records.

For more on these stories and other digital fraud headlines, check out the Tracker's News and Trends section (p. 10).

TICKETMASTER'S STRATEGY TO SORT FANS FROM FRAUDSTERS

Nearly 94 million U.S. consumers bought concert tickets last year, but a significant share fell victim to ticket scams. In this Tracker's Feature Story (p. 6), Gui Karyo, chief information officer at Ticketmaster, discusses how the ticketing platform's solutions improve fans' experiences while keeping out fraudsters.

DEEP DIVE: HOW MERCHANTS AND CONSUMERS CAN AVOID RESHIPPING FRAUD

The Better Business Bureau (BBB) has a warning for the public: When an offer appears too good to be true, it probably is. One scheme that fits this description is reshipping fraud, a type of scam that often lures in unsuspecting participants by offering them money to work from home and ship products overseas. The Tracker's Deep Dive (p. 15) explores how fraudsters are able to lure participants into their scams and how consumers can stay vigilant against this type of activity.

EXECUTIVE INSIGHT

Shipping fraud has become a major concern for delivery services such as FedEx, UPS and USPS. What steps can these businesses take to keep their shipments fraud-free?

"Balancing customer experience and business risk is one of the great challenges of our digital era. As customers increasingly demand online experiences that are quick, easy and seamless, businesses have to deliver these experiences without incurring additional risk.

Shipping is an arena where this challenge is uniquely acute. Customers are used to easy-access shipping portals with low-friction login requirements. However, these portals are increasingly being exploited by fraudsters who see new opportunities for illicit profit and [use them to] engage in identity theft and fake account registration.

To prevent reshipments and other fraudulent shipping actions, businesses have to block fake and malicious accounts at the point of registration, before they can be used for malicious purposes. Determining which accounts are legitimate can be done with advanced AI and unsupervised machine learning (UML) technologies that can reveal connections and patterns across large numbers of newly registered accounts.

Advanced data analysis can produce actionable insights from large volumes of data by taking a holistic approach to reviewing and analyzing a wide variety of event types, digital fingerprints, and profile information related to accounts, shipments and deliveries.

Comprehensively detecting and preventing sophisticated shipping fraud necessitates implementing proactive strategies that can expose fake and malicious accounts early — before downstream damage can occur. By analyzing registration data holistically using UML, it is possible to expose the shared attributes across accounts that identify them as being part of a coordinated attack.

Adopting strategies like these enables shipping platforms to continue offering friction-free experiences without fear of incurring increased risk of attack."

YINGLIAN XIE
co-founder and CEO at DataVisor

5 FIVE FAST FACTS

90%

Share of data breaches carried out through phishing attempts

$100B

Global digital advertising fraud's projected cost by 2023

60%

Share of fake accounts that commit abuses within two hours of creation

11.5M

Estimated number of U.K. citizens who have been defrauded while shopping online

71%

Portion of fraud losses related to CNP eCommerce transactions

FEATURE STORY

How Ticketmaster Rewards Fans And **Bars Fraudsters**

FEATURESTORY

Almost 94 million American consumers bought concert tickets last year, but a significant share of those music fans were unfortunately in for unpleasant experiences.

Approximately 12 percent of live concert attendees — about 11 million people — fell victim to ticket scams last year, including those in which consumers purchased fake tickets or paid for ones that ultimately never materialized. Schemes like these can ruin fans' overall experiences and reflect poorly on ticket vendors that fail to prevent fraudulent sales on their platforms.

Digital events platform Ticketmaster is all too familiar with such issues and has worked to earn consumers' trust by balancing seamlessness and security. Gui Karyo, the company's chief information officer, noted that Ticketmaster has invested in solutions that both stop fraudulent ticket sales and recognize fans' behaviors to enhance their overall experiences. Karyo discussed how the platform's Verified Fan and SafeTix initiatives encourage friction-free and safe buyer experiences.

"[We] think about our system not just [as] about the delivery of an item, but as a platform of relationships and [entitlements] where what we know about the consumer augments their experience to [both] give us better fidelity and give them a better experience as a whole," Karyo said.

GETTING TO KNOW FANS WITH DATA

Ticketmaster is one of many online ticket sale platforms that have acted to protect their offerings against emerging threats such as account takeover (ATO) attacks and credit card fraud. Karyo said that getting ahead of these threats is essential for Ticketmaster to successfully connect fans with the tickets they rightfully purchased.

"Our principal lens is on the fan experience — making sure that [from the start] we are confident that real fans have [the] first and best access to tickets that go on sale," Karyo said.

He said the company's Verified Fan program delivers that vision by providing "preferential treatment" to legitimate users. The offering allows Ticketmaster users to register for early announcements about shows they may be interested in attending and then make purchases through unique access codes provided by the company to ensure that fans, not bots, are given the first chances to buy tickets.

The program's goal is twofold, Karyo said. The first mission is to help artists and event promoters better connect with fans and provide them with earlier ticket access, and the second focuses on data collection and developing a clearer understanding of users trying to access the system. This helps differentiate legitimate customers from bad actors.

"Pragmatically, [the service] is a point of friction [for bad actors] and validation [for legitimate fans] to get greater insights and understanding of who is coming into [our] ecosystem to buy tickets, so that we can give preferential treatment to fans first," Karyo said.

Fans are asked to verify their identities either through Ticketmaster directly or partner sites. Data collected from these steps is paired with the company's own review to ensure that tickets being sold or resold through the platform are legitimate and going to real buyers. The service uses machine learning (ML) technology to assign user scores that allow Ticketmaster to feel more confident that tickets are going where they should.

"Some of our most interesting machine learning work is really around driving [consumer benefits] so that as real consumers come into the site, they are given a smooth experience that is unfettered by the friction we want to put in front of bad actors," Karyo said.

KEEPING TICKETS SECURE

Ticketmaster recently started a new service to ensure tickets stay with legitimate customers until the moment they are used to enter venues or resold. The company's SafeTix technology was launched in partnership with the National Football League and provides users with unique barcodes that constantly refresh, thus preventing them from being stolen or duplicated by fraudsters. Karyo said the service addresses a common vulnerability of tickets — their static barcode images.

"The moment you take a screenshot or PDF and pass a static image around, there is little if anything we can do to protect that chain of custody," he said. "You could print

[it 100 times] and you have a situation where the first person in is the one who wins."

SafeTix provides ticket accountability and ensures that legitimate customers receive all the rights and privileges from their purchased tickets.

"[The program] ensures that it's not the barcode or the image that is the entry token," he said. "[What lets you enter is] the combination of our relationship with you, your account identity [and] an entitlement we have delivered to you."

Karyo added that solutions like SafeTix and Verified Fan will be increasingly important for eCommerce platforms as fraudsters' efforts become more creative. Digital marketplaces have become attractive to bad actors as in-person retail fraud becomes more challenging to commit in a world of EMV-equipped credit cards and point-of-sale (POS) terminals.

"Ticketing has always been an alluring industry to target because of the arbitrage value of the things we sell," Karyo said.

This puts pressure on Ticketmaster and other eCommerce merchants to strike the right balance of smooth purchasing experiences for customers and strong security measures that address suspicious users. Karyo said the company achieves this equilibrium by building strong customer relationships and constantly learning to better distinguish good actors from bad ones.

"My hope for Ticketmaster is that we continue to invest in a consumer experience that increasingly offers our fans great reasons to come and interact with us, be rewarded everywhere from the beginning [purchasing] experience to the point they enter the venue, [be] rewarded for sharing that experience through our platform and coming back and [then be] rewarded for that repeat behavior with a higher level of trust and access," he said.

Building stronger trust among fans is essential for event-based eCommerce platforms to thrive and assure customers that their tickets will be valid when their favorite artists come to town.

UNDER THE HOOD

Gui Karyo, chief information officer for Ticketmaster, discusses the challenge of balancing seamless user experiences for legitimate ticketholders with stringent security protocols to thwart potential bad actors.

"A large percentage of bad actors are in [and] of themselves some form of automation that has been largely designed to look like a person. It is often difficult to differentiate between an automation with [a negative purpose] in mind that is designed to mimic a human being from a human being itself. Our general thesis, as represented in a lot of what we're doing with Verified Fan, is we can create a consumer experience that is both [better] for consumers and also a set of features … to help us make that differentiation.

While [Verified Fan] is in general an increasingly [difficult] experience for bad actors who are trying to … mimic good actors, [the program] is also a comfortable and organic experience to end customers that offers them a great benefit in the end, particularly when that benefit is preferential access to content."

NEWS&TRENDS

FIGHTING ONLINE AD FRAUD

RESHIPPING SCAMS TARGET JOB SEEKERS

The BBB is warning the public — especially job seekers — to stay vigilant against reshipping scams, which trick victims into participating in elaborate criminal activities that cover for fraudsters. Such scams occur when stolen credit card data is used to buy expensive goods online. Fraudsters have the items shipped to the home addresses of victims who believe they are working for legitimate employers, and the recipients repackage and ship the goods to other locations, often overseas. Cybercriminals attempt to recruit participants with false job offers that promise good money and the flexibility to work from home. The BBB advises job seekers to be suspicious of employers that initiate contact and offers that do not require in-person interviews.

UNTANGLING FAKE CONSENT STRINGS

Job seekers are not the only targets of elaborate fraud schemes. Advertising technology publishers and vendors in the European Union (EU) were recently warned that real-time advertisement bidding's data collection method is vulnerable to consent string abuses. Consent strings are collections of numeric zeros and ones that indicate whether users have granted data permission to receive General Data Protection Regulation (GDPR)-compliant advertisements and identifies the status of an advertising vendor. A zero indicates no consent while a one specifies that it has been provided, and the number positioning indicates the vendors that have received consent and for which purposes.

The U.K.'s Information Commissioner's Office (ICO) — the agency charged with ensuring GDPR compliance — warned in May that some vendors are using fake consent strings to give the impression they have more consent than they do, most likely in an effort to retain current revenues. ICO issued a report on the ad tech sector's best practices and plans to investigate the matter further.

FACEBOOK REVEALS NEW ANTI-FRAUD STRATEGY

Social media giant Facebook appears ready to use a new fraud tackling approach to obstruct bad actors from scamming on its platform, outlining a new strategy in October at the @Scale engineering conference in San Jose. The concept relies on digital signatures — information based on cryptographic solutions that act as virtual stamps — instead of real users' data for authentication purposes. Facebook said its goal is to ensure that certain activities are performed by legitimate users without giving away too much data. Solutions that detect the

battery charge on a user's phone or data from the mobile device's accelerometer to determine if a login attempt is legitimate still reveal such data to app developers. The proposal comes as losses caused by global digital advertising fraud are on track to reach $100 billion by 2023.

TRANSFER TRICKERY

TSB OFFERS CONSUMERS FRAUD REFUND GUARANTEE

Fraudsters continue to get creative, even persuading consumers to authorize transfers under false pretenses. U.K. bank TSB is warning consumers about "safe account" fraud, in which criminals pretend to represent the bank or law enforcement officials and warn customers that their accounts have been compromised. These bad actors then urge consumers to transfer their funds to different accounts that the fraudsters control. TSB said it is also seeing an increase in "money mule" efforts that deceive customers into receiving money from one account before transferring it to another — which can land consumers in legal trouble for money laundering. TSB recently launched a fraud refund guarantee for its 5.2 million customers, promising to compensate victims in full.

NIKKEI REPORTS $29M IN LOSSES DUE TO FRAUDULENT TRANSFER

Bank customers are not the only parties that can be hit hard by fraud: Even large companies like Japanese

financial media firm Nikkei have been targeted by fraudulent money transfers. The company recently reported that its U.S. subsidiary lost $29 million in a scheme involving international wire transfers to Hong Kong. It said in a statement that the transfers were made in September by an employee of Nikkei America "based on fraudulent instructions by a malicious third party who purported to be a management executive of Nikkei." The statement added that the company is cooperating with investigations.

The media firm is among several that have recently fallen victim to fraudulent international transfers. *The Financial Times*, which is owned by Nikkei, reports that cybercriminals used international transfers to steal $81 million from the central bank of Bangladesh in 2016.

FINANCIAL SERVICES' ANTI-FRAUD EFFORTS

MASTERCARD GETS PROACTIVE TO FIGHT FRAUD

Nikkei's incident highlights an ongoing problem facing businesses dealing with fraud: A company's anti-fraud and security teams need to be effective 100 percent of the time, while cybercriminals need only one success to make their efforts worthwhile. Financial services giant Mastercard launched a service called Threat Scan in October to help businesses proactively counter fraudsters rather than address incidents after detection.

Johan Gerber, Mastercard executive vice president of security and decision products, recently told PYMNTS' Karen Webster that the solution reviews real-time data to identify emerging threats. Threat Scan can simulate known fraudulent attacks against credit card issuers' systems to differentiate fraud types that are being caught from those that could evade detection. Gerber said fraudsters are looking to abuse any vulnerability in card issuers' systems, so Threat Scan aims to find these weaknesses before criminals can. The U.K.'s NCSC reported it had investigated 658 credit card fraud-related cyberattacks between September 2018 and August 2019.

CYBERATTACKS ARE BUSINESS LEADERS' BIGGEST FEAR

Mastercard's latest effort to stay ahead of fraudsters comes as new data shows the risk of a cyberattack is the top concern for most business leaders. A recent World Economic Forum (WEF) survey found executives in Canada, the EU and the U.S. are most concerned about cyberattacks. Business leaders in these markets are also worried about data breaches and theft, energy price shocks, extreme weather events and terrorist attacks, among other issues, and fiscal crises were identified as the top concern among all global economies.

The WEF's Regional Risks for Doing Business 2019 report was based on approximately 13,000 responses from business leaders in 133 global economies who were asked to identify the five global risks of highest importance to their businesses over the next 10 years.

FRAUD ATTACKS HIT FINANCIAL SERVICES, LENDING FIRMS HARDEST

A recent study reported that two sectors face the greatest burdens when acts of fraud are successful. It found financial services companies lose $3.25 for every dollar lost in an act of fraud due to fees, fines, interest, legal expenses and lost transaction values as well as labor and investigative efforts. These findings reflect an increase

from 2018's rate of $2.92 for every fraud dollar lost. Fraud costs are also high for lending businesses, which lose $3.44 for every dollar lost to fraud, an increase from the $3.05 per fraud dollar lost in 2018. The report highlighted several trends that contributed to growing costs, including expanded access to mobile channels, an increase in cross-border transaction activities and a failure to address a rise in botnet activities.

RADPAY ADDS FRAUD RESISTANCE TO DIGITAL WALLET

Phoenix, Arizona-based startup Radpay, which offers blockchain-enabled anti-fraud solutions, recently announced that it added a patent-pending fraud resistance feature to its digital wallet and payment system. The offering includes heightened identity and transaction validation processes designed to make digital payment methods more secure and links debit and credit cards to smartphones or wearable devices. The solution can also access Radpay's rewards system and allow consumers to earn perks or points on purchases.

The feature will be used to mitigate both card present and CNP fraud, which cost card issuers, merchants and transaction acquirers $33 billion each year. The move follows Radpay's earlier blockchain-based solutions, CryptoClick for eCommerce retailers and SpeedPath for restaurants.

GOVERNMENTS FIGHT FRAUD

PHILADELPHIA LAUNCHES TOOL TO ADDRESS STOLEN PROPERTY DEEDS

Fraud attacks are felt by more than just financial services and lending firms, as property owners are also being targeted by cybercriminals who take homes by stealing deeds. The city of Philadelphia has recently seen an uptick in homes being stolen in property scams in which thieves steal property deeds and forge sales documents and notary stamps before selling the houses to unaware third parties. The deeds have often moved several times between parties by the time homeowners realize what has happened.

An investigation by NBC affiliate NBC10 found that 132 instances of property fraud were reported in the city in 2018, much higher than its annual average of 72 from 2013 to 2017. Approximately 110 properties have been stolen in this manner so far this year, prompting Philadelphia officials to launch a Fraud Guard website to address the situation. Property owners register on the site and receive email alerts if their names or addresses appear in documents filed at the City Recorder's Office.

BANKS IN JOHANNESBURG, SOUTH AFRICA, HIT BY CYBERATTACKS

A South African municipality — along with several of its local banks — was also recently hit by cyberattacks. Hackers targeted Johannesburg with a ransomware attack that shut down several city programs, including online services and bill payments. The strike also affected the city's emergency call center. Hackers demanded four Bitcoins — valued at $37,000 USD — as ransom. The attack was most likely carried out via phishing, an fraud type responsible for 90 percent of all data breaches.

Hackers also struck several South African FIs around the same time Johannesburg was targeted. Large banks including Absa and Standard Bank were targeted by a dedicated denial of service (DDoS) attack that delayed paychecks for many local residents. Municipalities and banks are urged to

update their software and use web application firewalls to block potential DDoS attacks.

INDIAN NUCLEAR PLANT TARGETED BY CYBERATTACK

A troubling report from India revealed that the government confirmed its newest nuclear power plant was hit by a cyberattack. The Nuclear Power Corporation of India Ltd. (NPCIL), the government-owned agency responsible for generating nuclear power, announced that malware used for data extraction had recently been detected at the Kudankulam nuclear power plant. NPCIL noted that the threat was "isolated from the critical internal network," but cybersecurity experts believe crucial information may have been compromised in the breach. The malware used in the attack has been connected to the Lazarus Group, which has ties to two North Korean-backed organizations, and the situation highlights issues with Indian cybersecurity policies despite the Modi administration's efforts to aggressively digitize the nation's economy.

DEEPDIVE

HOW
RESHIPPING SCAMS DELIVER FOR FRAUDSTERS

The ongoing trade war between China and the U.S. appears to be doing little to dampen billions of consumers' holiday spirits. Recent data projects that global eCommerce spending will rise by 15 percent this year and total worldwide sales will reach $768 billion.

Major consumer shopping events like Black Friday and Cyber Monday attract deal-hungry customers, but such shopping holidays have the unintended effect of attracting fraudsters as well. These bad actors often take advantage of the chaos to steal credit cards, scam merchants and wreak other types of retail havoc.

Reshipping scams are one such nefarious activity that consumers must be wary of during the season. This fraud type covers for cybercriminals by tricking unsuspecting consumers into believing they have landed lucrative work opportunities even though they are actually participating in criminal enterprises. The following Deep Dive unpacks how reshipping fraud works and how both merchants and consumers can stay vigilant against it.

HOW SHIPPING FRAUD WORKS

Shipping fraud is relatively straightforward: Criminals have purchased items shipped to their own addresses rather than to the customers who supplied their payment information. These consumers may have intentionally made their purchases or had their data stolen.

Reshipping fraud is slightly more complicated, however. The criminal first steals payment data from a legitimate consumer and uses that information to purchase an expensive product. These bad actors then rope in unsuspecting assistants through job advertisements promising work flexibility. These victims are told

to accept shipments at their private addresses, repackage them and then reship them to fraudsters at different addresses that are often overseas.

The unsuspecting intermediaries make this fraud type hard to detect, and goods are very difficult to recover once shipped abroad. Accomplices could end up facing criminal charges for mail fraud and other crimes, and they are also unlikely to receive the paychecks their fake employers promised.

HELPING CONSUMERS, MERCHANTS AVOID RESHIPPING SCAMS

The United States Postal Service (USPS) has warned the public to stay vigilant against enticing fraud types. These schemes often originate on chat rooms, dating sites and job sites by scammers posing as representatives for fake charities, potential romantic partners or as employers offering work-from-home deals.

The BBB shared one cautionary tale of an individual who learned about reshipping scams the hard way. The organization outlined how a Mississippian applied for the position of "buyer" that promised him a salary of $98,400 plus commission to buy cell phones and ship them to an address in New York City. The man was told he could access a bank account to pay off his credit cards for the phones and himself, and he shipped the phones to a company specializing in sending packages to Uzbekistan.

The man's bank informed him a few days later that he lacked authorization to transfer funds from the account and reinstated the charges on his credit card, and the "employer" did not respond to his emails. This experience cost the victim $6,500 in money paid for the phones and resulted in his personal information being shared with the fake employer. The BBB urged the public to be wary of pursuing remote work opportunities that promise big payments, as they are unlikely to be legitimate.

Even Fortune 100 companies can be damaged by fraudsters' reshipping efforts. One such case involved a customer's credentials being stolen from a company and used to register large volumes of fake online accounts. The bad actors then reshipped packages or delayed deliveries and spammed legitimate users. These activities harmed the company's reputation and caused friction with legitmate users.

The USPS has an even more urgent warning for consumers about reshipping scams — that participants in these types of schemes are at risk of committing several felonies and are also likely to lose money to fraudsters in the process. Unwitting participants who are mailed checks or money orders are often told to deposit them, keep portions for themselves and wire the rest elsewhere. The USPS urges consumers to check whether checks or money orders are legitimate before depositing them, or else they could be liable for the full amounts, and to research any company making an unusual job offer without an interview process with the BBB the Federal Trade Commission and their state attorneys general.

Merchants can guard against this activity by comparing available data from Facebook, LinkedIn, Twitter and other social media networks to detect if there is a legitimate connection between online buyers and intended delivery addresses. Connections that cannot be verified should lead sellers to consider using anti-fraud solutions. Merchants should also consider implementing AI technology as well as unsupervised ML solutions that can proactively guard businesses against fraudulent activity, even before patterns become clear.

A busy holiday season will generate plenty of opportunities for fraudsters to end up on law enforcement's naughty list. Vigilance is imperative if consumers and merchants wish to ensure they are not pulled along on a cybercriminal's reshipping ride.

about

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

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 **digitalfraud@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.