DIGITAL FRAUD

TRACKER®

MAY 2022

FEATURE STORY

Mission Lane on preventing financial fraud in a connected age

PAGE 06

PYMNTS INTELLIGENCE

How eCommerce and financial services firms can reduce fraud risks for consumers using IoT-enabled devices for payments

PAGE 14

PYMNTS.com | DATAVISOR

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.

Read the previous edition

APRIL 2022

Digital Fraud Tracker®

TABLE OF CONTENTS

EDITOR'S LETTER

The pandemic not only accelerated the digital transformation of banking and payments but also solidified consumer demand for what has been called the Internet of Things (IoT). The IoT consists of a network of technology-embedded devices that allow for connecting and exchanging data, running the gamut from smartphones and laptops to smart speakers, TVs, streaming devices and more. The overlap of money and the IoT is now giving rise to new opportunities in the financial services sector.

Consumers exhibit a growing enthusiasm for technologies that can transfer money or pay bills at the touch of a button or the issuance of a voice command, and their use of IoT-enabled devices to conduct daily financial tasks is expanding rapidly. The global market for the IoT in the banking and financial services sector was predicted to grow by nearly $8 million from 2021 to 2026, marking a compound annual growth rate (CAGR) of 8%. North America alone will make up more than one-third of that increase, growing nearly 7% just this year.

As smartphones and IoT-enabled devices become the go-to method of doing business and making payments, however, the pressure is mounting on network providers and manufacturers to provide quick, seamless service and security. Inconsistent IoT standards make it difficult to mandate security safeguards on new devices, and legacy devices that lack up-to-date encryption can be easy prey for hackers. Users unfamiliar with the risks can also unwittingly introduce viruses and other online threats.

The good news is that consumers want to trust the devices that help make their financial lives easier and less complicated. Providers that leverage solutions to put security at the forefront of their service offerings can build trust with the customers who have come to rely on them. That trust can mean repeat business and an inherently safer connected economy.

This edition of the Digital Fraud Tracker®, a PYMNTS and DataVisor collaboration, takes a closer look at the proliferation of IoT-based devices and how consumers are currently using these devices for payments and financial services. It also examines how providers must work to gain the trust of cautious users and ensure the security of their payments and data.

THOUGHT LEADERSHIP TEAM

PYMNTS.com

Feature Story

Mission Lane On **Preventing Financial Fraud** In A Connected Age

AN INCREASING NUMBER OF CONSUMERS ARE USING CONNECTED DEVICES SUCH AS SMARTPHONES TO HANDLE THEIR DAY-TO-DAY ACTIVITIES, SUCH AS STREAMING VIDEO, ORDERING TAKEOUT OR HAILING RIDESHARES.

For the most part, consumers have become used to trusting their personal data to connected devices, but the risk of fraud is an ever-present concern, especially as more consumers use smart devices and the IoT to manage their financial lives.

A key problem for financial institutions (FIs) when consumers connect with their accounts via IoT devices is that even FIs with the best fraud protections in place have no control over whether the IoT-enabled devices accessing them do. Devices that lack encryption capabilities, for example, are vulnerable to fraud threats such as distributed denial-of-service attacks, which can overwhelm a server and take it offline.

The number of consumers demanding the ability to conduct quick and frictionless financial transactions on connected devices is growing, however, meaning that ensuring the security of customers' accounts when connecting with smart devices has become table stakes for FIs.

"It's good that we can interact and reach people [in] the space where they want to be in, which is with their device[s]. I think it's truly noble to say that we should try to educate customers, but really, you've got to make things simple," said Gaurishankar Gopalakrishnan, head of enterprise fraud, collections and recoveries at Mission Lane, a FinTech that has helped 1.5 million Americans with imperfect credit rebuild their financial lives.

THE CHOREOGRAPHY OF SIMPLE VERSUS SECURE

An FI's responsibility, according to Gopalakrishnan, is to give IoT-connected customers the same secure service they expect from physical banking. This begins with using authentication processes designed to identify customers while keeping hackers and bad actors out. Methods such as multifactor authentication (MFA) are critical, but asking customers for a six-digit code every time they log in may frustrate them to the point of taking their business elsewhere, he explained.

Consumers prefer solutions that recognize them when they log in, regardless of device, and many FIs have begun using artificial intelligence (AI) and machine learning (ML) to authenticate their customers as a result. These technologies use decisioning algorithms that build on previous interactions through pre-authenticated devices, and they work behind the scenes without customer interaction.

"My customer doesn't need to know that I have three layers of bot protection or whatever. They don't need to know that, and they don't mind. My objective is that when a customer is trying to log in, they just look at the phone, and the facial recognition picks it up, and they're done."

As fraudsters become more adept at cracking these safeguards, Gopalakrishnan believes it has become incumbent on FIs to use advanced biometric authentication methods, such as facial recognition and behavioral-based assessments as well as fingerprint and iris scans, to keep transactions safe.

THE FUTURE OF CONNECTED SECURITY

The potential for fraud will continue to increase alongside the growing number of digital "on-ramps" that can attract hackers.

Gopalakrishnan believes it is imperative that businesses and FIs become more digital to succeed in a world with more connected devices. At the same time, he said, providers must require built-in safeguards in the devices that consumers use to help keep information safe. For instance, he pointed out that Apple gives each device it sells a unique digital ID that allows the source of a data hack to be more specifically identified. In fact, he said, those device identifiers are much more accurate than even the IP address that a home internet address contains.

"[The digital ID] is unique to your device, and it can obviously be jailbroken, but for the most part, it's fairly good. It's more precise than IP because IP is your general location, your neighborhood or your area," he said. "It can help me build trust that it is indeed the same device that this customer logged in with last month, and they seem to be making good transactions, and I can build on that trust and build that into my knowledge for the next time you log in or the next time you access your product with a different device."

He said that FIs can also use AI technology and predictive analytics that "learn" users' digital behaviors to help determine whether they are potential fraudsters posing as legitimate customers — even on the same devices.

The companies that will thrive in the connected economy are the ones that find ways to use technology to make IoT-enabled transactions safe while keeping them simple.

"Those technologies will continue to improve, and we'll continue to get to a place where the trust factor increases," he said. "It's a constant battle that we fight. On the one hand, what's good for my customer — and good for my business — is to provide them more services and build that brand trust about using my products online, but at the same time, how do you keep protecting customers in an ever-evolving environment?"

As consumers become more connected, FIs' survival will depend on their willingness to adopt solutions that foster mutual trust with their connected customers.

Q&A

YINGLIAN XIE
CEO
DATAVISOR

What are some ways consumers are using IoT-enabled devices to enhance their experiences with payments and financial services?

It's interesting to see that the adoption of IoT payments is impacting multiple aspects of people's lives.

There are examples of people using IoT-enabled payments in their everyday personal lives. Amazon's Alexa and Google's Echo really paved the way for the adoption of IoT payments with small devices that can initiate transactions on behalf of their users, and other use cases like smart refrigerators are becoming more and more popular — especially in North American markets. It's exciting to think about how smart technologies will transform the homes of tomorrow.

Another example along these lines [is] IoT-connected automobiles that come loaded with full internet connectivity and impressive computing capabilities. New cars' software can be updated over the air, and owners can purchase goods and services from their manufacturers and third parties through in-car interfaces. These vehicles are highly capable IoT machines that will reveal an increasing intersection between this technology and financial services.

IoT and financial services are intersecting with people's professional lives as well. For example, industrial manufacturers are using IoT-enabled machinery to add to the operational efficiency of their production lines. When these machines are designed in ways in which they can initiate transactions to replenish inventories, secure output and perform other functions like scheduling their own maintenance, they begin intersecting with the world of payments.

In the realm of retail, large companies are increasingly relying on IoT technology to optimize their supply chains through, for example, smart shelves that can monitor stock levels with unparalleled accuracy and place replenishment orders at precisely the right moment, considering live lead times, sales velocity, seasonality and other factors.

Still within retail, but on the customer-facing side, "smart stores" are a good example of how IoT and payments intersect. Amazon Go stores rely on ML and cameras that can replicate human vision by capturing light with higher sophistication to enable computers to perform motion detection and object identification. These stores can recognize users and associate them with existing Amazon accounts, detect what they are purchasing and bill them without a checkout line. All the customers need to do is walk out of the store with their items in hand.

What are some of the fraud, risk and security challenges that need to be solved by providers, and what features must be included to ensure the safe use of connected devices?

The first issue I would highlight revolves around user authentication requirements. If IoT payments allow people to disengage from initiating transactions, then the question of whether or not merchants and FIs can tie them to specific identities becomes an interesting one.

The customer experience and value proposition of IoT (allowing people to disengage from certain transactions) hinge on providers' ability to trust the identity of the people who will be liable for transactions with creative and effective processes that do not require direct human contact. For example, most two-step verification measures would really damage the experience of IoT payments.

As a corollary to the above, existing payment liability determination frameworks are likely to be challenged. Disputes will inevitably arise, and retailers and FIs must navigate ambiguous situations and design policies that allow them to be settled in predictable terms. Well-designed delegation policies and authorization measures will be key to ensuring customer satisfaction and recurrent use of IoT-enabled payment technologies.

From a fraud prevention perspective, I believe that a higher number of IoT devices underscores the importance of incorporating advanced device intelligence into risk management strategies. In the near future, legitimate customers will be using dozens of devices to connect with payment systems, and fraudsters could too.

On a first level, this means using device identification tools that go beyond generating simple device IDs and can withstand reboots and other fraud techniques. But this is not enough, and good device intelligence must also provide fraud teams with actionable data about the behavior and activities of users and devices interacting with their applications or websites. This data will provide them with a big-picture view of their users' activities and devices and will enable them to make context-appropriate decisions in scenarios that challenge traditional customer interactions.

What can fraud and risk management professionals do today to prepare for a future where IoT devices will become increasingly popular?

There are many discussions that fraud professionals should initiate at an organization-wide level to prepare for the future of IoT transactions.

First, teams should pay special attention to the way they gather and use intelligence about their customer touchpoints for fraud prevention. FIs and eCommerce firms should secure greater control and understanding of the different interactions that customers have and the tools they use to retain control when these tools proliferate exponentially. This ties back to what we mentioned earlier about device intelligence.

Second, retailers and banks should also prepare for a future in which chargeback rates increase due to the number of purchases made without direct customer involvement. Purchases made without direct customer intervention can involve misunderstood voice commands or erroneous setting selection, thus leading to customers being surprised when items arrive at their doorsteps or when charges appear on their credit card bills.

For example, grocery orders initiated by smart refrigerators may lead to a higher chargeback rate than traditional ones. In these instances, having a team that understands IoT devices and the terms and conditions of the permissions that they operate under can prove very valuable for merchants and FIs handling these disputes.

The third angle of preparation is related to data management practices, which are a priority in most modern organizations. Their importance becomes more relevant with the proliferation of devices connected to the internet, as they are bound to generate increasingly large volumes of information for all parties involved — retailers, card issuers, payment networks, device manufacturers, etc.

PYMNTS Intelligence

Why Security Is Key To The Future Of IoT-Enabled Devices For Banking And Payments

The shift to remote transactions during the pandemic not only accelerated the adoption of digital banking but also firmly established the market for data exchange technologies and the devices connected to them, also known as the IoT. The convergence of money and the IoT has created a world of opportunities for the financial services sector. Consumers are eager to try new technologies that allow them to transfer money or pay bills with a voice command or click of a button. Security is always a concern with financial transactions, however, and providers must always mitigate the risks involved when subtracting human interaction from the equation.

The use of IoT-enabled devices and AI to help consumers save time on basic financial tasks continues to expand. The global market for the IoT in the banking and financial services sector was expected to grow by nearly $8 million from 2021 to 2026, representing a CAGR of 8%. North America will account for 34% of that increase, rising nearly 7% in 2022 alone.

AI-based chatbots and virtual assistants powered by services such as Alexa, Siri and Google Assistant will replace human tellers, but providers will need to invest in security processes and develop convenient interfaces to gain and keep consumers' trust. This month, PYMNTS Intelligence takes a close look at how payments and financial services are becoming more common on IoT-enabled devices, as well as consumers' perceptions and feelings about using these devices for payments and account access. It also examines how providers are responding to these developments, both to mitigate potential fraud and to make consumers feel secure when using IoT-enabled devices for payments and account access.

CONSUMER DEMAND FOR THE IoT IS HERE TO STAY

A March 2021 report found that the average United States household had 25 connected devices, including laptops, tablets, smartphones, smart TVs and other home devices, streaming or gaming devices and fitness trackers. This number was more than double that of 2019, and consumer use of connected technology grew by 50% within that time frame. Much of that growth owes itself to the pandemic, when consumers learned how to use these devices for virtual healthcare visits, remote working, fitness classes, streaming video services and, increasingly, shopping, paying bills and other financial tasks.

© 2022 PYMNTS.com All Rights Reserved

Nearly 40% of U.S. consumers say they will upgrade to newer models of their connected devices when these become available. A recent report also found that 57% of consumers in Germany, the United Kingdom and the U.S. already use voice assistants on devices in their hands, their cars and in smart speakers and other devices. Pressure, therefore, will be on manufacturers to develop devices that can handle everything from entertainment and communication to shopping and bill payment. Consumers also need help navigating this technology, however, with 46% of U.S. consumers in 2021 saying they encountered difficulties with their connected products and could use assistance from manufacturers with troubleshooting and connecting their devices to the internet. Nearly one-third said they find the process overwhelming.

SECURING THE FUTURE OF THE IoT

The IoT holds promise for use in payments and account access, but providers must work to ensure that transactions and personal financial data are secure. From a security perspective, the IoT can be viewed as a highway with many on-ramps, cars of differing ages or states of repair and operators of various skill levels. Hackers can find their way onto that highway through older devices lacking up-to-date encryption. Users unfamiliar with scams and security risks can unknowingly introduce viruses and other online threats. Inconsistent standards make it difficult to mandate security safeguards on new devices. Mass assaults through botnet attacks can simultaneously affect thousands of workstations, jamming traffic on the IoT highway.

Providers must ensure the safety of the IoT, including through the use of security solutions that can act as “traffic cops.” Such solutions work by assigning each device a unique ID that never changes, utilizing ML to help detect advanced online threats, such as rooted or jailbroken devices, emulators, app cloners, repackaged apps, VPNs and botnets, and putting a stop to them. Manufacturers must also work with providers and governments to introduce new legislation, such as the European Union’s cybersecurity strategy adopted in October 2021, which will require standardized security features in all new connected devices.

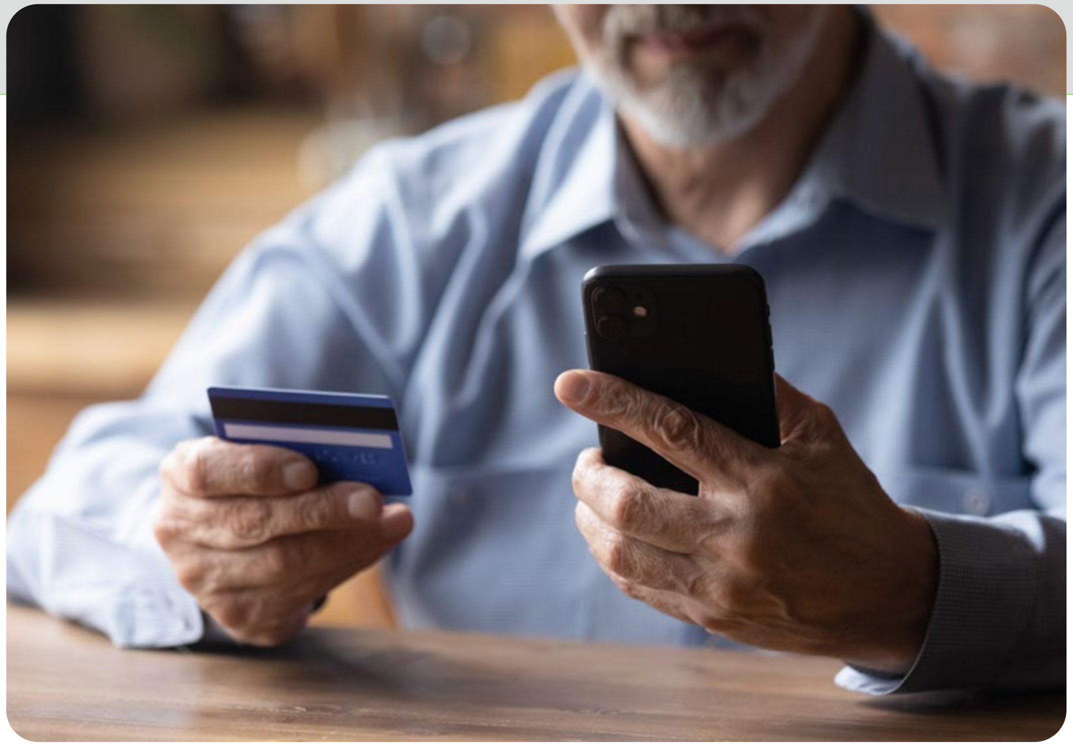
The opportunities that connected devices promise are only becoming apparent as consumers realize the benefits of using machines to make their everyday financial lives easier. It is now incumbent on providers to gain consumer trust and make sure the journey is both safe and convenient for them.

DIGITAL FRAUD TRENDS

STUDY FINDS FRAUD RISK VARIES BY GEOGRAPHY AND GENERATION

While anyone can be the target of financial fraud, a new study from IBM found that the frequency and impact of such fraud vary greatly depending on geographical location and generational differences. American consumers fall victim to debit card fraud more than any other country studied, costing U.S. consumers an average of $265 annually due to unauthorized charges from bad actors. Consumers in Germany lost the most significant amount of money, with consumers there losing more than three times the amount lost by consumers in Singapore, the second-most victimized country.

From a generational standpoint, millennials were the group most consistently targeted by fraudsters, likely due to their reliance on mobile and digital payments. Generation X consumers were the second-most targeted with fraud charges, frequently made on their credit cards and digital payment apps, and Generation Z came in third. Interestingly, most consumers surveyed said they feel that their FI or bank is responsible for preventing such fraud, and in the U.S., nearly one-quarter of consumers said they do not have confidence in their bank's ability to detect and prevent fraud. By comparison, roughly half of Japanese consumers said the same, showing even less confidence.



PAYMENT FRAUD ACTIVITY ON THE DECLINE AS ORGANIZATIONS GO DIGITAL, STUDY FINDS

The digital transformation that organizations have undergone since the pandemic began has increased the risk of financial fraud. The pivot to online and digital operations may be responsible for reducing successful fraud, however, according to a recent report from the Association For Financial Professionals (AFP). While 71% of organizations reported they fell victim to payments fraud last year, that rate was significantly less than the 81% reported in 2019 and was the lowest percentage recorded since 2014.

The report also found that remote work environments did not lead to increased payment fraud through email, owing much to the training and digital security efforts made to secure such channels. In addition, a decline in paper check usage was noted as a potential mitigating circumstance, as many organizations switched to digital payments in their business processes. Digital fraud incidents are on the rise, however, as 37% of organizations reported ACH debit fraud and 32% of organizations reported tampering with wire transfer payments.

GLOBAL FRAUD

WHATSAPP USERS TARGETED BY RUSSIAN PHISHING SCAM

Hackers intent on stealing personal information from app users are getting creative. A recent report warns that users of the popular messaging app WhatsApp are being targeted by email spoofing and fake voice messages in an attempt to get to their data. These attacks, originating from a group of Russian cybercriminals, can circumvent the security firewalls from Microsoft and Google using an email address that appears to be credible.

The scam occurs when WhatsApp users receive an email indicating they have a voice message waiting for them. The email contains a fraudulent URL directing them to a page with a play button, where the alleged voice message awaits. When the user clicks the button, they are prompted with a question asking if they are a robot. When they confirm they are not, the site downloads malicious phishing software onto the unsuspecting user's computer. The report noted that user skepticism could go a long way in prevention, as well as not reusing passwords with multiple accounts and employing MFA best practices.

DIGITAL PAYMENT FRAUD THREATS HIT THE APAC REGION HARD, SURVEY FINDS

Sixty-nine percent of consumers in the Asia-Pacific (APAC) region who use digital payments platforms report encountering at least one type of cyberthreat, according to a report from Kaspersky. While 85% of the more than 1,600 consumers said they used digital payments before the pandemic, just 15% started using them during the pandemic. Cyberthreats are no surprise, as 97% indicated they were aware of at least one threat against digital payment platforms. The most commonly encountered threats were social engineering scams, fake websites, fake offers and phishing scams.

The report revealed that 90% of APAC respondents had used digital means of payments such as mobile apps at least once in the past year, and their attitudes toward the inherent security hazards reflect a general distrust in providers to help protect them from fraud threats. For instance, 38% of consumers surveyed said they were concerned about financial loss when conducting transactions online or offline. Twenty-two percent said they get anxious when making online payments, and 60% said banks and FIs need to provide more incentives to get users to maintain better cybersecurity hygiene.

CONSUMER SCAMS

GIFT CARD PAYMENT SCAMS HIT ONE-THIRD OF AMERICAN CONSUMERS, SURVEY FINDS

Fraudulent payment scams involving gift cards are becoming more common. A recent AARP survey of more than 2,000 adults found that one in three adults aged 18 and older have been the target of scams asking them to pay a fake debt using a gift card. Interestingly, it found that most of the targeted individuals were under 50 years old, and 25% of them followed through with the purchase of a gift card, mistakenly believing they were satisfying a legitimate debt.

The scams commonly involve a targeted individual being asked to purchase a gift card to pay upfront for a service, pay a fee to claim a prize or do a favor for a friend. After buying the card, the target is asked to read the numbers on the back. Another scam involves consumers who receive "zero-value" gift cards, which, as their name suggests, are cards with no funds on them. The survey revealed that 23% of all U.S. consumers have given or received such zero-value gift cards, and when the victims called a number to receive a refund or credit, 54% of them were denied. Most respondents — 88% of consumers — feel lawmakers need to do more to protect consumers from these scams.

HACKERS USE DIGITAL MESSAGES AND PAYMENT APPS IN MONEY TRANSFER SCAM, FBI WARNS

The FBI has issued a public announcement warning consumers against a legitimate-sounding phishing scam asking them to make an instant money transfer using their bank's digital payment app. As more consumers turn to digital and mobile payment technologies for their financial activities, thieves are becoming more brazen by using stolen data to carry out scams.

The scam, which uses spoofed bank messages to gain the trust of victims, asks if they initiated a digital transaction through their bank's app. If the target responds, they get a phone call from what appears to be their bank's customer support number with a friendly-sounding agent, who asks them to initiate a funds transfer to reverse the fake transfer. The bad actors, who have gathered personal information such as account numbers, social security information and past addresses, can gain trust and talk the victim through the transfer process. Unbeknownst to the victim, the transferred funds get delivered to a bank account set up by the hackers.

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")