DIGITAL FRAUD

Tracker

January 2022

PYMNTS.com | DATAVISOR

TABLE OF CONTENTS

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.

WHAT'S INSIDE

Merchants and consumers alike are steadily realizing the many benefits of buy now, pay later (BNPL) options. BNPL plans can enhance the customer experience and reduce cart abandonment while simultaneously enabling consumers to extend their purchasing power with monthly installments that are typically free of interest. The payment method's growing success is reflected in the number of users who have incorporated it into their shopping habits: More than 45.1 million United States consumers were expected to use BNPL in 2021 alone.

When new digital payment methods become increasingly popular, fraudsters inevitably take note. Big banks and other well-established payment providers have exhausted resources innovating their fraud detection systems over the past decade to defend against sophisticated bad actors. BNPL providers are relatively new to the arena, however, and their cybersecurity measures may not match their more established predecessors'. As a result, BNPL providers are at greater risk of cyberattacks that stem from account takeovers (ATOs), fake accounts and security breaches.

BNPL transaction values continue to grow despite the specter of fraud, however, and BNPL is anticipated to account for 4.5% of all eCommerce payments in North America by 2024. This sustained growth makes it even more crucial for BNPL providers to equip themselves with robust fraud prevention tools to protect consumers and the merchants they frequent. Incorporating advanced technologies such as artificial intelligence (AI) and machine learning (ML) into their back-end processes and consumer-facing solutions can help BNPL providers successfully manage and prevent high-level security breaches.

Around the digital fraud space

BNPL's allure as a flexible payment method continues to grow, with a recent report finding that BNPL transactions rose 182% year over year in June 2021. The payment method's rapid growth, pared-back credit verification methods and straightforward repayment plans appeal also to fraudsters. Cybercriminals are cashing in on BNPL schemes by either opening fake accounts or hijacking existing customer accounts and paying only one installment before disappearing with the products. Still, some tools can help BNPL providers better fight fraud, and technologies such as AI and ML enable them to spot warning signs without bogging down legitimate customers' transactions.

Small to mid-sized businesses (SMBs) are another prime target for fraudsters as more business goes digital, but a large share remain unperturbed by the threat of cyberattacks, even as research suggests that they should be more vigilant. More than one-quarter of data breaches in the U.S. involved small businesses in 2020, yet a recent survey found that 56% of these firms were not concerned about potential security threats within the next year. The reality is that many of these SMBs could benefit from adopting more robust security measures or overhauling their existing anti-fraud systems, lest they risk the financial and reputational damage that can result from data breaches, cyberattacks and related fraud strikes.

Fraud prevention teams also are turning to cloud technology to halt cyberattacks. A recent survey of 700 IT professionals in the U.S. found that the majority considered ransomware and security risks stemming from remote work as key cybersecurity concerns in the year ahead. While these are not fraud issues, per se, fraud often occurs after security breaches. Many IT professionals are looking to the cloud to better safeguard their data, with 50% planning to ditch on-premises systems in favor of cloud-based ones within the next year.

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

Sezzle on keeping BNPL fraud-free as consumers popularize it

A rapidly growing number of consumers are turning to BNPL plans to fund purchases big and small, leading more merchants to offer the payment method to satisfy this demand. This trend has not gone unnoticed by fraudsters, however, emphasizing how important it is for BNPL providers and merchants to work together to keep these payments secure. In this month's Feature Story (p. 7), Charlie Youakim, co-founder and CEO of BNPL provider Sezzle, discusses how BNPL providers can incorporate AI-and ML-based fraud prevention tools to combat digital fraud schemes.

Deep Dive: Taking BNPL fraud prevention to the next level with AI and ML

BNPL provides consumers with an easy, low-friction method of paying for purchases over time, but many of the aspects that make it so appealing to consumers also attract fraudsters. This month's Deep Dive (p. 13) explores the factors that have made BNPL appealing to consumers and cybercriminals, the ways in which bad actors exploit the payment method and how providers and merchants can shore up their defenses using advanced technologies that harness AI and ML.

EXECUTIVE INSIGHT

How can advanced fraud prevention tools such as AI and ML help BNPL providers reduce cyberattacks without hindering the customer experience?

"The biggest draw of BNPL is precisely that smooth customer experience that retailers and lenders have worked so hard to perfect. ML-powered fraud detection [justifies] this effort by fighting fraud smarter: it uses data, advanced analytics and artificial intelligence to identify bad actors with efficiency and precision unthinkable for legacy systems.

Here's a real-life example:

In the old days, fraud prevention meant burdening good users with high-friction identification measures and saturating fraud teams with intensive manual reviews for each loan. At DataVisor, we arm fraud teams with advanced unsupervised machine learning technology that lets them look at millions of applications simultaneously and analyze them in real time to detect connections between them that are invisible to legacy systems — and the human eye. This intelligence, combined with a comprehensive suite of fraud detection tools, endows teams with a truly proactive fraud prevention mindset.

The secret lies in fighting fraud smarter, not harder. AI is the best tool for this."

Yinglian Xie
CEO and co-founder
DataVisor, Inc.

5 FIVE FAST FACTS

73%

Portion of eCommerce businesses that fell victim to promotion abuse over the past year

5%

Segment of consumers who reported being victims of payment fraud in December 2021

65%

Portion of digital shoppers likely to end their relationships with retailers after a single instance of payment fraud or data theft

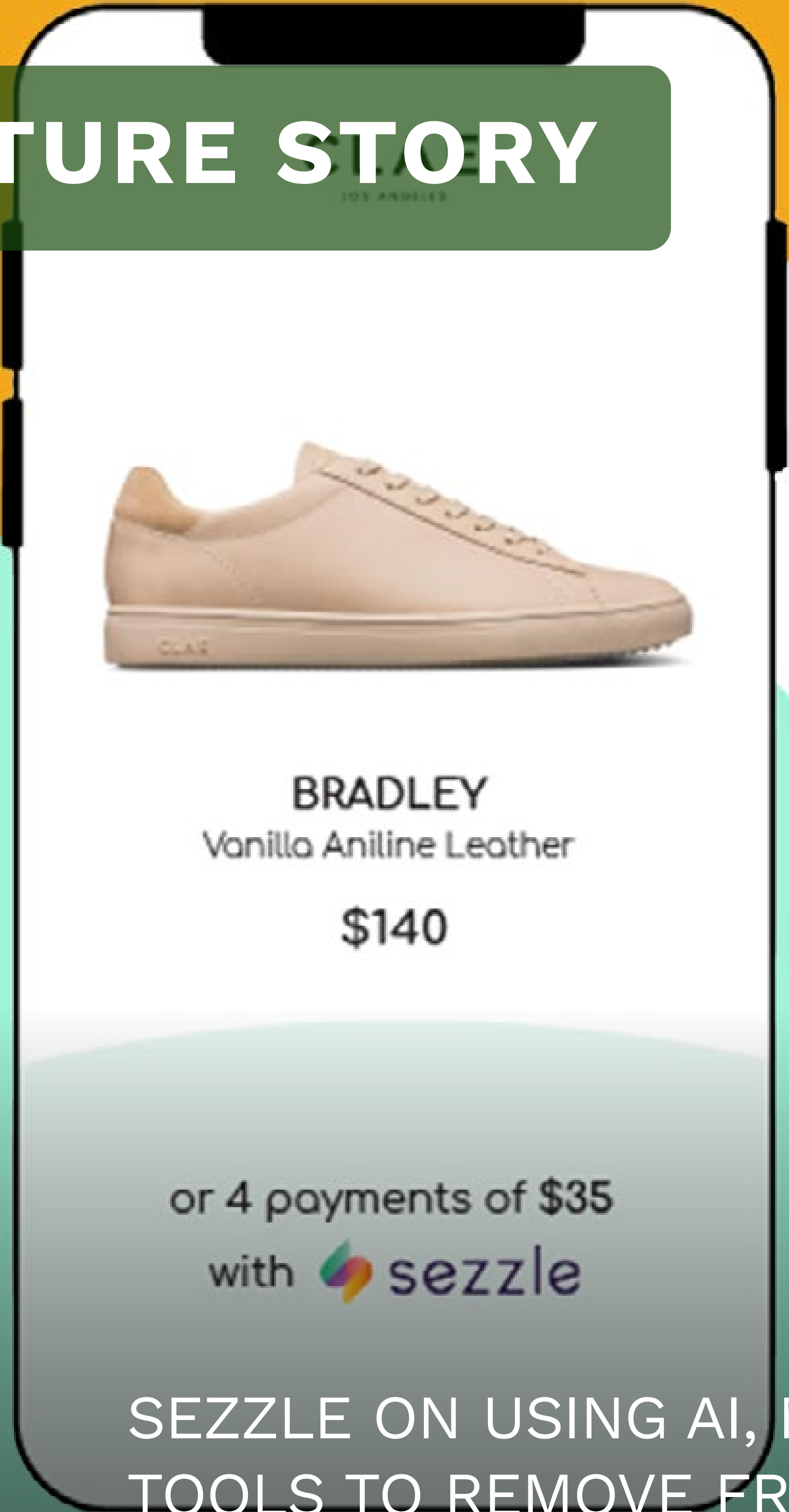
59%

Share of customers who were informed of a payment fraud incident on the same day it occurred

43%

Segment of payment fraud victims who filed claims for suspicious activity the same day they became aware of it

FEATURE STORY



BRADLEY

Vanilla Aniline Leather

$140

or 4 payments of $35 with sezzle

SEZZLE ON USING AI, ML TOOLS TO REMOVE FRAUD FROM THE BNPL EQUATION

BNPL's emergence within the broader payments market began just years ago, but the payment method has gained significant traction. Forecasts show that the number of U.S. BNPL users rose an impressive 81.2% year over year in 2021. BNPL's rapid growth can be attributed to widespread adoption by merchants and consumers' enthusiasm for its typically interest-free installment plans, which many see as a way to build credit.

Offering BNPL at checkout can lead consumers to alter their purchasing behaviors, giving them opportunities to shop for products that otherwise might be out of their price range, Charlie Youakim, co-founder and CEO of BNPL provider Sezzle, recently told PYMNTS.

"A consumer might have been shopping and seeing a product on your website and saying, 'I love that product. But I'm going to budget for it. I'm going to think about buying that in a few weeks,'" said Youakim. "[With BNPL], merchants saw customers [changing] their behavior, seeing that they could buy it today with automated budgeting through the tool. They would actually make that purchase decision today."

Millions of shoppers leverage BNPL plans each day, meaning merchants cannot afford to forgo BNPL adoption and risk losing out on substantial revenues. However, as demand for these plans increases and more merchants offer them, another party is beginning to take interest: fraudsters. BNPL providers will need to empower merchants to offer these payment methods without putting consumers' personal details at risk to halt the uptick in fraud BNPL platforms are facing.

Fraud: a major concern for BNPL providers

BNPL's popularity across digital channels can make the payment method an enticing target for fraudsters. Bad actors are targeting BNPL platforms using ATOs and synthetic identities, and providers' pared-back application processes can give cybercriminals more opportunities to bypass authentication methods. The stakes are high for retailers: PYMNTS' data shows that 65% of consumers are likely to terminate their relationships with a merchant after a single instance of data theft or payment fraud

Youakim explained that some of these increased risks are simply a natural part of the digital growth process. He noted that BNPL providers must focus on ensuring legitimate customers are signing up for services, pointing to advanced technologies as a key part of the solution.

"Fraud is always an issue for payment systems online," he said. "[Platforms] are always looking for ways to solve it because the bad actors are always there, so a key topic for us is focusing on fraud prevention. Because if you get the synthetic identities out of the way and get real people into the system, [it reduces fraud risks]. So that's why we have a big focus on fraud, and the systems and everything we do around that, which includes machine learning."

Fraud prevention is crucial to obtaining new customers and maintaining healthy relationships with existing ones. More than 48% of consumers have greater data security and fraud concerns now than before the pandemic began, in fact. Many BNPL providers and merchants they serve now are harnessing the powers of advanced fraud prevention tools and software, such as AI and ML, to enhance the customer experience by reducing fraud risks without adding friction.

"Machine learning programs have basically evolved over time," Youakim said. "Deep learning neural networks… start to come up with algorithms that [drive themselves]. And the trade-off is you lose a little bit of knowledge about the key indicators, like the key [fraud] scoring mechanisms. But the results speak for themselves."

The opportunity in offering secure BNPL plans

There is good reason for BNPL providers and merchants to offer robustly safeguarded installment payment plans. BNPL adoption is expected to increase from 45.1 million users in 2020 to 76.6 million by 2025. Consumers from all generations are drawn to the payment method, and Youakim explained that the upward trajectory of BNPL adoption and its repeated usage among consumers underscores its growing significance.

"I think [BNPL] definitely enhances the experience because customers love it," he said. "If you don't have buy now, pay later on your website today or in your retail store, I think you're really hurting your chances of the sale because customers are expecting it."

BNPL plans' growing appeal across sectors is undeniable, and merchants eager not to fall behind competitors would be wise to adopt this payment method. Keeping BNPL options simultaneously convenient and secure, however, will require an upfront investment in fraud prevention tools such as AI and ML.

BNPL providers stand to gain a lot from this investment in fraud prevention. As more and more lenders and payment companies launch BNPL solutions, offering a secure and fraud-proof product can act as a differentiator and ultimately serve as a competitive advantage for the most forward-looking BNPL players.

NEWS & TRENDS

BNPL FRAUD

How AI and ML tools can help BNPL providers battle back against fraud

BNPL plans are experiencing increased adoption around the globe, with the American market seeing exceptional growth. The number of BNPL users within the U.S. was expected to reach 45.1 million in 2021, and 30% of the nation's shoppers had planned to use the payment method during the holiday season. Consumers' increased interest in BNPL is getting fraudsters' attention, however, with many of them perpetrating their schemes with ATOs or by using stolen information to create fake accounts. Inadequately secured verification and checkout processes can lead to ATOs, while BNPL providers' failure to notice fraud indicators — such as applicant names that do not match given email addresses or phone numbers — can make companies vulnerable to fake accounts.

Several key tools, especially those that leverage advanced technologies, can help merchants and BNPL providers safeguard their operations from fraud. AI-based identity verification and authentication measures and ML algorithms can help providers spot behaviors that indicate ATOs and prevent purchases that raise red flags. Providers also can fight back against fraudulent account creation by ensuring their soft credit checks do not miss red flags.

Bot attacks ramp up as fraudsters set sights on BNPL space

Fraudsters targeting the BNPL space also are relying on more sophisticated attack methods for their schemes, prompting providers and merchants to pivot to advanced solutions. BNPL transactions increased 182% year over year in June 2021 as more consumers moved to online shopping during the pandemic. Many consumers value BNPL methods for the flexibility their installment payments offer, but fraudsters are drawn to the same features. Combined data from 28.7 billion online transactions between June 2020 and June 2021 showed a 41% increase in bot attack volumes, despite a 29% decline in human-initiated attacks.

One tactic favored among fraudsters involves using stolen information to open a fake account, make the first installment payment and then leave providers or merchants holding the bag. Providers will need to turn to advanced anti-fraud solutions of their own to spot these attempts without stalling purchases for legitimate customers. Improved verification methods that leverage multifactor authentication (MFA) can help reduce fraud; however, retailers should be aware that these methods introduce friction to their customers' checkout experience.

CYBERSECURITY CHALLENGES AND CONCERNS

Report finds 56% of SMBs are not worried about their cybersecurity

Cyberattacks are ramping up across all sectors, but new research shows that many SMBs are largely unconcerned about their cybersecurity — even though the data suggests that they should have concerns. A recent survey of 2,000 small businesses in the U.S. revealed that 56% were not concerned about security breaches over the next year, while almost one-quarter said they were not worried at all. This outlook could prove dangerous, however, as 28% of all data breaches in 2020 concerned small businesses. Furthermore, 60% of companies that suffer cyberattacks or data violations close within six months, emphasizing that these issues are not to be taken lightly, especially since an uptick in security breaches often leads to an increase in fraud attacks. Businesses of all sizes, but particularly SMBs, would be wise to implement anti-fraud solutions that harness advanced technologies such as AI and ML to avoid the financial and reputational blowback that a breach or cyberattack could create.

Half of Middle East organizations lack fraud awareness despite cybercrime rise

The uptick in digital fraud is not restricted to any one nation or region, new research has shown. A recent survey across multiple industries in the Middle East revealed an increase in instances of fraud during the pandemic, with 48% of respondents reporting a rise in fraud over the past year. Thirty-five percent said fraud has increased since the start of the pandemic, with remote work and greater reliance on technology cited as the top contributing factors.

While fraud is on the rise across the Middle East, many organizations still are reporting challenges when it comes to curbing cybercriminal activity: 50% of respondents said their organizations lacked fraud awareness and relied on legacy anti-fraud measures, static data and outdated infrastructure, and 41% said they lacked a dedicated fraud management team. The survey also found that 55% of respondents reported a lack of periodic training, senior management reporting and periodic fraud risk assessment, although those same respondents said their companies have a basic, policy-level fraud risk framework. These findings suggest that a sizable

share of Middle East organizations are long overdue when it comes to overhauling their anti-fraud methods.

Report identifies ransomware, remote work challenges as top cybersecurity concerns

Several trends are emerging as companies fight back against an uptick in digital delinquency, including the nature of the schemes they face. A recent survey of 700 U.S. IT professionals found that most believe curbing ransomware attacks and addressing the risks posed by remote workers will remain top priorities in the fight against cybercrime this year.

The cloud's advanced data processing technology enables companies to examine fraud patterns more quickly, reducing the time it takes to detect fraud. As a result, more IT teams are migrating their companies' data to the cloud rather than storing it on-premises: 50% said they intend to migrate to the cloud this year. Proponents say the move provides the flexibility to address and pay for fraud mitigation only when incidents occur rather than continuously. Only 8% of respondents said they intended to move their data from the cloud to on-premises solutions.

DEEP DIVE

WHY PREVENTING FRAUD IN BNPL TRANSACTIONS REQUIRES REAL-TIME SOLUTIONS

The growth in BNPL's popularity has made fraud prevention an increasingly important subject for both providers and the merchants that offer it. Twenty-five percent of U.S. merchants already accept BNPL payments, and 46% expect to implement it as an option within the coming year, expecting greater sales, customer loyalty and larger cart sizes at checkout. At the outset of the 2021 holiday shopping season, 12% of consumers said they planned to finance at least some of their purchases using BNPL, and many millennial, Generation X and Generation Z consumers planned to make BNPL their primary payment option for holiday purchases. A notable 45% of BNPL users — nearly half — said they intended to use BNPL for some or all of their holiday purchases, indicating just how popular it has become in recent months.

This month's Deep Dive examines how BNPL has attracted not just consumers but also fraudsters, and it illustrates the vulnerabilities these fraudsters are drawn to exploit. It also looks at steps BNPL providers and merchants can take to prevent fraud through proactive steps that stop fraudulent activity as it is happening.

Vulnerabilities to fraud present in BNPL transactions

Some of the largest BNPL players have experienced increased incidents of fraud as installment payment options have gained popularity. Individual fraudsters as well as organized criminal networks aim to exploit weak points in the processes through which BNPL loans are applied for and approved, and not just to purchase big-ticket items. Some fraudsters target small-dollar purchases such as pizza or alcohol. The increased popularity of BNPL also has attracted bad actors who expect to remain undetected in a marketplace awash in transactions.

BNPL fraud targets many of the same features that make it such a popular option for consumers, such as lenient authentication mechanisms that are meant to reduce frictions for legitimate transactions. Fraudsters create fake accounts to exploit default lines of credit, often making purchases with stolen credit card information. They can even deploy bots to scale up such attacks. Existing accounts can be even more profitable for bad actors, as a user with a good history can have a much higher credit limit with the BNPL provider. In those cases, fraudsters take over accounts through techniques such as credential stuffing, phishing and SIM swapping.

Securing BNPL transactions against fraud

One of BNPL's key vulnerabilities stems from providers, who have softer controls in place compared to the credit controls associated with banks and credit card companies. This can include a lack of credit checks prior to BNPL approvals. The method's installment nature also enables fraudsters to acquire merchandise for a fraction of the retail price up front, increasing the buying power of stolen credit cards used in transactions. During special events or the holiday shopping season, for example, merchants and BNPL providers also may lower security checks to prevent lost sales to false declines.

BNPL providers including Klarna and Afterpay have worked to outwit fraudsters with prevention capabilities in place. According to Afterpay, fraud made up less than 1% of its global sales in fiscal year 2020, while Klarna said it has protections in place that exceed those offered by credit cards and large banks. Afterpay attributed its fraud prevention successes to proprietary ML algorithms that adjust as fraudsters seek new points of entry.

Tools that would more quickly identify mismatched email addresses and phone numbers could help stem BNPL fraud, as criminals often seek to exploit the lighter identity and credit checks associated with the payment method. Such procedures could be implemented without adding friction to the transaction, as could better verification standards that look at a user's physical and digital attributes.

Replacing reactive solutions with proactive ones

Maintaining the positive customer experience that has contributed to BNPL's popularity while stopping fraud requires systems that can respond quickly to fraudulent activity. AI-based fraud prevention tools can respond to threats in real time, identifying fraudulent transactions while they are in the process of being completed. Along with methods powered by ML, such processes can help identify borrowers' personal documents and halt any suspicious activity before money is exchanged.

Providers may choose to partner with firms specializing in the use of AI for identity verification and authentication, and merchants can take their own steps to work with ML fraud prevention specialists to spot purchasing activity that follows fraudulent patterns. BNPL moves too quickly for fraud prevention methods such as labeling, writing rules and manual case reviews, with losses already showing by the time fraud is detected by such methods. Real-time detection is needed to effectively stop BNPL fraud. ML can recognize fraud patterns even as they are emerging, while automated systems can enable fast, low-friction transactions that also are significantly protected against fraud.

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, 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.