



OMNI

SECURITY

AND AUTHENTICATION

OCTOBER 2018

REPORT

PYMNTS.com

ca
technologies

Why Bank Security Is About More Than Preventing **Attacks**

Why stopping cyberattacks is only half the battle for Silicon Valley Bank

– Page 6 (Feature Story)

Facebook, Apple and the State Department each suffer data breaches

– Page 10 (News and Trends)

How 3D Secure 2.0 is pushing fraud protection forward

– Page 15 (Deep Dive)

TABLE OF CONTENTS



REPORT

03

WHAT'S INSIDE

The latest developments from around the omni security and authentication space, including a look at recent breaches and new security solutions that could prevent future attacks

06

FEATURE STORY

Why Bank Security Is About More Than Preventing Attacks

Silicon Valley Bank's chief security officer, Nick Shevelyov, explains how the financial institution prevents attempted cyberattacks from impacting the bank, and stops successful attacks from impacting customers

10

NEWS AND TRENDS

The latest headlines from around the space, including new debuts in the omni security and authentication industry

15

DEEP DIVE

How 3D Secure 2.0 Protects Banks And Their Customers

PYMNTS explores the latest version of 3D Secure

18

ABOUT

Information about PYMNTS.com and CA Technologies

ACKNOWLEDGMENT

The Omni Security and Authentication Report was done in collaboration with CA Technologies, and PYMNTS is grateful for the company's support and insight. [PYMNTS.com](https://pymnts.com) retains full editorial control over the findings presented, as well as the methodology and data analysis.

WHAT'S INSIDE

Cybercriminals are becoming craftier, and they're turning to more efficient and effective ways to target consumers and companies alike. Even the United States government isn't out of reach.

The U.S. State Department recently [confirmed](#) that it was the victim of a data breach that affected less than 1 percent of employee email inboxes. A report issued by the State Department noted that it had previously been knocked for its lax cybersecurity protections.

Apple, meanwhile, suffered a security scare of its own. Cybersecurity researchers from Duo Security discovered a [loophole](#) in Apple devices that could allow hackers to obtain corporate customers' WiFi and application passwords. The researchers claim that Apple's Device

Enrollment Program (DEP) exposes company passwords and other sensitive information if a "rogue" device becomes enrolled.

According to a report in [The Wall Street Journal](#), large U.S. banks are also seeing an increase in cyberattacks. The government is warning financial institutions (FIs) about bank cybersecurity and possible threats. Several big banks, including Bank of America, Citigroup, JPMorgan Chase and Wells Fargo are being called on to closely monitor traffic for hackers who might be searching for weaknesses in their networks.

Many companies from around the financial services industry are debuting solutions that will defend consumers and businesses alike from such security breaches.

AROUND THE WORLD OF SECURITY AND AUTHENTICATION

Payments platform provider Adyen, for instance, is putting its faith in 3D Secure 2.0. It recently [unveiled](#) a solution that is fully compliant with 3D Secure (3DS) 2.0 standards. The solution was created around EMVCo's 3DS protocols, and helps merchants reduce risk, protect against payments fraud and remove some of the pain points that plagued 3DS 1.0.





Adyen [partnered](#) with CA Technologies on the solution, which offers 3DS 2.0 authentication without interruption via frictionless flow transactions. This provides a more seamless experience to users and added value to merchants.

On the other hand, India-based payment platform and solution provider Paytm is focused on biometric authentication. The company is experimenting with a [facial recognition](#) platform that could enable digital payments. According to reports, Paytm plans to use facial recognition to allow customers to pay for merchandise using their face, which could boost the overall security of the app.

While Paytm is paying attention to facial recognition, KeyBank has its eyes on artificial intelligence (AI). It recently announced it would use Mastercard's Decision Intelligence system to protect its customers. The [integration](#) will increase the accuracy of real-time

transaction approvals and enhance the cardholder experience.

To read more about these stories and other headlines from around the security and authentication industry, check out the Tracker's News and Trends section (p. 10).

SVB WORKS TO BUILD BETTER BANK SECURITY

As fraudsters continue to develop more sophisticated methods of attack, stopping them is no longer enough, according to Nick Shevelyov, chief security officer at [Silicon Valley Bank](#) (SVB).

In this month's Omni Security and Authentication Tracker™ feature story (p. 6), Shevelyov explains how and why he and his team focus on not just stopping attacks before they happen, but also mitigating the impact of security breaches.

\$248.26 BILLION

Projected size of the global banking cybersecurity market by 2026

5 FIVE FAST FACTS

61,045

The number of mobile banking Trojans reported in Q2 2018 – a 300 percent increase over Q1

80%

Portion of mobile devices that will rely on biometric authentication by the end of 2018

66%

Share of consumers who are “very or extremely concerned” about data privacy when it comes to FinTech apps

10.2%

Expected CAGR of the financial services security space over the next seven years



WHY BANK SECURITY
IS ABOUT MORE THAN
PREVENTING ATTACKS

THE WORLD CAN BE A SCARY PLACE THESE DAYS,

especially for banks. According to recently released [reports](#), fraudsters are continuously targeting big U.S. banks, and these attacks are increasing in both frequency and sophistication.

Now, security providers and FIs are working to stop them from impacting banks' assets and customers by turning to new and emerging technologies like AI and machine learning (ML). Two-thirds of banks and 83 percent of FIs have [experimented](#) with this technology already.

[Silicon Valley Bank](#), according to Chief Security Officer Nick Shevelyov, uses AI and ML to rapidly analyze massive troves of data to find signs of suspicious or fraudulent transactions, malware or other indications that fraudsters are afoot.

"We've used [AI and ML] on the front side and the customer facing side of the bank," he said in a recent interview with PYMNTS. "[It analyzes the] behavior of clients to look for fraudulent and malicious activity, and we use that on the security side."

The company also uses firewalls to prevent fraudsters from gaining unauthorized access to customer records or bank assets. Yet, even when working together, techniques and tools designed to stop cyberattacks are no longer enough. The cybercrime market is growing more sophisticated and [producing](#) more than \$1.5 trillion a year. Therefore, efforts are turning to what can be done when — not if — an attack occurs.

"Maybe 20 years ago, the aspiration was really robust security, meaning you could stop all cyberattacks," he said. "Today, it's about how you remain resilient when things do impact your organization."

PREPARING FOR THE INEVITABLE

Shevelyov and his team don't just focus on stopping attacks before they happen — they also deal with the

“ Today, it's
about how
you remain
resilient
when things
do impact
your
organization.”

inevitable risks associated with conducting financial business in the digital age.

"It's not if the attackers are going to attack, or if they're going to get through," he explained. "It's when they do, and how you remain resilient."

Given the sophistication of the attacks and the rising number of incidents, the best defense for modern financial institutions is to be prepared in order to minimize potential damages. This means that technology and humans must work in sync to catch attacks as they're in progress.

"We've got layers of technology, and if it doesn't catch a particular attack because the attack is new, you need to have other layers in place, along with cybersecurity professionals that are always looking [out] for bad things [that might] happen, and [can] respond quickly," he said.

One of the reasons for this change in philosophy is the result of the rapid adoption of smartphones, mobile banking apps and other connected financial management tools. A massive amount of consumers around the globe rely on mobile devices to manage their money and interact with their FIs. While these innovations have given consumers more convenient and faster ways to access financial resources, they are also a top target for cybercriminals.

The demand for faster and simpler interactions with FIs can push some consumers to make poor security decisions, making them more vulnerable to phishing and other forms of fraud that rely on consumers willingly giving away access to accounts or security credentials.

"Today, the very technologies that empower us are also imperiling us," he explained. "Interestingly enough, most hacks still come through email phishing attacks, since



“We all want to move faster, we all want to reduce friction.”

we all use email on a daily basis. We're going fast, so attackers try to exploit that fact.”

THE FUTURE OF OMNICHANNEL BANK SECURITY

Despite the increased risk of falling victim to a cybercrime, most consumers don't appear eager to reduce their use of online, mobile and other connected banking channels.

Younger consumers, who have grown up in a connected world, tend to be the most common mobile and connected banking applications adopters, and it's likely that these tools will become even more popular in the coming years.

Bank customers have some simple steps they can take to strengthen their account security: using two-factor authentication, using biometric authentication over passwords or being more careful when communicating with financial institutions.

“We all want to move faster, we all want to reduce friction,” Shevelyov acknowledged. “But one of the things

we can do is just pause to read through emails, validating that the domain is someone that we know and trust, and even that the content of that email is legitimate. ”

Those steps may sound simple enough, but many consumers value convenience over security, even when it comes to their money. As a result, banks need to invest in not just AI and ML, but other emerging technologies and solutions that can serve as weapons in the fight against fraud.

This is especially important, considering how quickly fraudsters can create new methods that beat the latest cybersecurity defenses.

“You will always see cybercriminals evolve their tactics and focus on an area that has not been hardened or focused on more recently,” he said, “It's part of the cat and mouse game of the industry.”

Fraudsters won't stop targeting banks, and they'll continue to create more and more sophisticated attack methods. As a result, banks and FIs would be well-served to not only work toward preventing attacks, but also minimizing their potential impact.

NEWS & TRENDS



INDUSTRY INSIGHTS

BIOMETRICS TAKE CENTER STAGE IN IRELAND

The EU recently passed the European Banking Authority's Regulatory Technical Standards, which are new regulations on common and secure communication that require additional security measures and protocols, including mandating two-factor authentication. These standards will be implemented in about a year, but their impact is already being felt in countries like Ireland. According to [reports](#), a growing group of Ireland-based banks, FIs and other businesses are investing in biometric authentication tools to stay compliant with the regulations.

In the coming months, Mastercard expects to roll out 3DS solutions in Ireland en masse. Just 1 to 2 percent of transactions are currently subject to authentication using 3DS, but that number is expected to rise to about 25 percent.

WHY BUSINESSES SHOULDN'T PAY THE RANSOM

When biometrics and 3DS solutions fail, companies should not rush to meet the demands of cybercriminals, according to a recent [report](#) from Datto. Giving in to ransomware — malware that forces victims to pay a ransom to regain access to files or systems — doesn't guarantee system or file recovery. In its report, Datto discovered that 15 percent of SMBs were unable to recover data after paying the ransom.

The report claims that the most effective strategy to protect small businesses, and ensure that downtime is as minimal as possible, is to regularly back up data. Frequent backups can be an effective measure for businesses, even when they may lack adoption or even an understanding of sophisticated cybersecurity strategies and tools.

"Paying a hacker in these situations not only incentivizes further attacks, but it provides criminals with the vital funds they need to continue their operations," said Carl Herberger, vice president of security solutions at Radware.

GOVERNMENTS GET INVOLVED

BANK OF ENGLAND PLANS CYBER STRESS TEST

The Bank of England wants to make sure that British financial services firms are ready for not just ransomware attacks, but any threat that cybercriminals throw at them. According to [reports](#), the central bank will force financial firms in the U.K. to undergo cyber stress tests to ensure they could recover if they were hit by a major cyber breach. The tests ensure that banks have enough defenses built up to withstand a hit on their systems, and, more specifically, how long it would take for their key services, such as payments, to recover. The Bank of England contends that a disruption to a bank's payments systems could hurt the economy. That bank's customers wouldn't be able to make transactions or access their money.

The FIs subjected to the tests must show how they would recover in the event of an attack. If a firm fails the test, it must agree to remedial action plans that will improve its ability to handle similar situations, if they were to happen. The stress tests will start as a pilot in 2019, though it's still unknown which firms will face the tests.

TESCO, FCA SETTLE OVER CYBERATTACKS

One English FI — Tesco Bank — could likely benefit from such stress tests. According to a report from *The Guardian*, Tesco Bank, which was the victim of a cyberattack in 2016, recently paid out a [settlement](#) of £16.4 million (roughly US\$21 million) to the Financial Conduct Authority (FCA). The attack didn't result in theft or loss of customers' data, but it did lead to 34 transactions in which funds were debited from accounts. What's more, the bank said customers faced disruptions in normal service.



The FCA said the hackers in the case made off with £2.26 million by capitalizing on “deficiencies” in the design of Tesco Bank's debit cards, financial crime controls and its financial crime operations team. The FCA also noted that Tesco put a “comprehensive redress” program in place and spent significant resources to address the deficiencies that left it susceptible to the cyberattack. If Tesco had not cooperated with the FCA, it would have been fined £33.56 million.

BREACH BULLETINS

50 MILLION FACEBOOK USERS EXPOSED

Facebook recently [confirmed](#) a cyberattack of its own — one that affected roughly 50 million users. According to reports, Facebook employees discovered that attackers could take control of user accounts through a function in the platform's code. More than 90 million users were forced to log out of their accounts as a result of the breach — a typical measure taken with compromised accounts.

CEO Mark Zuckerberg said that the company was “taking it really seriously” and that it is currently working on a “major security effort.” Facebook had the vulnerability fixed and contacted authorities. This is not the first misuse of customer accounts and data that Facebook has had to face. It is currently dealing with allegations that Cambridge Analytica improperly collected personal data from Facebook users.

APPLE LOOPHOLE EXPOSES CORPORATE PASSWORDS

Apple is also in finding itself in hot water. Cybersecurity researchers from Duo Security recently [discovered](#) a security loophole in Apple devices that could allow hackers to obtain corporate customers’ WiFi and application passwords. Apple’s Device Enrollment Program (DEP) – a solution for corporate customers that enables them to manage multiple Apple devices used by their employees – exposes company passwords and other sensitive information if a “rogue” device is enrolled.

DEP provides user authentication when a new device is added, but companies are responsible for verifying the identity of the user of any added device. Businesses are also responsible for registering an enrolled Apple device onto their own mobile device management (MDM) servers. Analysts warned that if a business does not require such identity verification, hackers can access a DEP device’s serial number, as long as it has not also been added to the company’s MDM server. Hackers deploy employee social engineering to obtain that serial number.

The hacker can use the serial number to enroll that device on a company’s MDM server, if the legitimate employee who is actually using that device has not done so. With that complete, the hacker then passes as a legitimate user and, once on the server, can obtain information. The MDM server will only accept a device’s serial number once, but researchers warn that this is a relatively easy process.

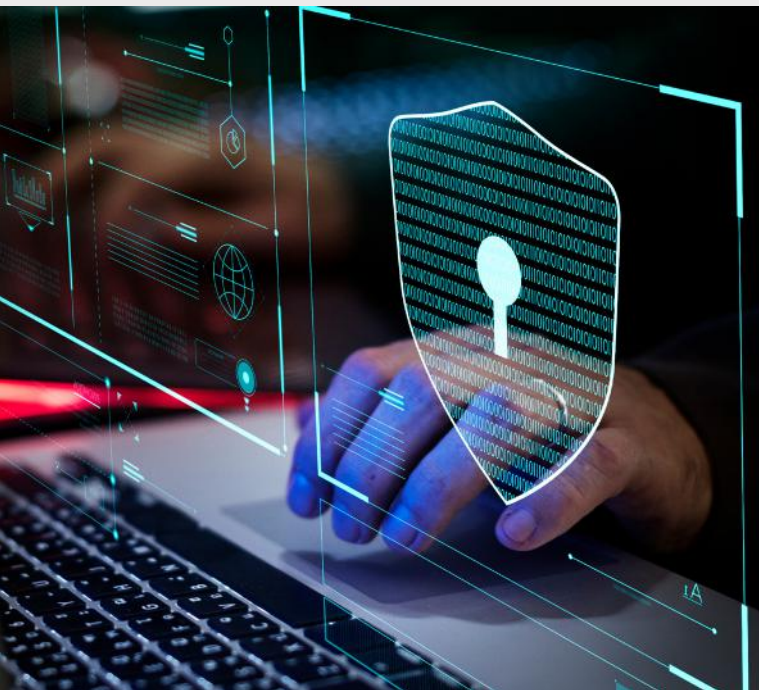
STATE DEPARTMENT CONFIRMS DATA BREACH

Even the U.S. government has to watch its back. The U.S. State Department [confirmed](#) it recently suffered a data breach in which personal information for some employees was exposed. The State Department informed affected employees, describing the breach as an “activity of concern” that affected less than 1 percent of employee email inboxes.

“We have determined that certain employees’ personally identifiable information (PII) may have been exposed,” the alert said. “We have notified those employees.” The State Department previously faced criticism for having soft cybersecurity protection. A bipartisan group of senators sent a letter to Secretary of State Mike Pompeo, asking how the department was responding to the criticism. Pompeo hasn’t responded.

This isn’t the first time the State Department has had to deal with the fallout related to security issues. In March 2016, a former employee was sentenced to 57 months in prison after committing an international phishing,





hacking and cyberstalking scheme that ensnared hundreds of victims in the U.S. and abroad.

FRAUDSTERS TARGET BANKING GIANTS

Cybercriminals may be targeting social networks, tech giants and even the U.S. government, but banks may be the most at risk. According to [reports](#) from *The Wall Street Journal*, large U.S. banks have recently seen an increase in cyberattacks. The government is increasingly warning FIs about cybersecurity and cyberthreats, requesting that banks such as Bank of America, Citigroup, JPMorgan Chase and Wells Fargo closely monitor traffic for hackers who might be looking for security weaknesses.

While some experts claim there has been “no heightened increase of cyberthreats to the financial services sector,” American FIs have long prepared for the possibility of massive cyberattacks. Last year, FIs quietly began [prepping](#) for an apocalyptic attack on their computers, hoping to prevent a run on banks should such an attack actually occur. The project, Sheltered Harbor, currently includes

banks and credit unions that, between them, hold about 400 million U.S. accounts. Each member bank is required to offer up its data, so it can be used by other firms in the event that their computers are disabled by a cyberattack.

DEBUTING DEFENSES

ADYEN UNVEILS 3DS 2.0 SOLUTION

Others in the financial services space are hoping to [provide](#) customers with a “next-generation authentication solution.” Payments platform provider Adyen recently [partnered](#) with CA Technologies and unveiled a new solution that is fully compliant with 3DS 2.0 standards.

Designed to help merchants reduce risk and protect against payments fraud, the solution will process EMV 3DS 2.0 transactions via the CA Payment Security Suite and work to authenticate them without interruptions. It also removes pain points that plagued 3DS 1.0 by improving the payments experience for customers, according to a press release — especially those using mobile devices.

The solution is the first to authenticate transactions in the background, too, without requiring customer intervention. Merchants can use it to provide customers with biometric security features like fingerprint, voice and facial recognition, as well as SMS-powered two-factor authentication.

PAYTM EXPERIMENTS WITH FACIAL RECOGNITION

While Adyen focuses on the next evolution of 3D Secure, Paytm, an Indian eCommerce payment system and digital wallet company, has its sights set on the future of biometrics. It recently started work on a [facial recognition](#) platform that enables digital payments. According to reports, Paytm plans to use facial recognition to allow customers to pay for merchandise, which could boost the overall security of its app.

"We have already started testing the facial recognition tool among our employees. Once live, Paytm users will be able to log in to the app by simply looking at their phone," a senior executive told *The Economic Times*. The executive, who wished to remain anonymous, added that the company is also developing additional security features to deter fraudsters.

The facial recognition capabilities are currently being tested on Google's Android platform and sources say it will soon launch via an app update. The move could be helpful to Paytm as it continues its fight for payments dominance in India by expanding its services and relying on its regional expertise. Already India's top digital payments firm, Paytm is expanding into banking, mutual funds and insurance.

MASTERCARD, KEYBANK COLLABORATE ON AI-BASED SOLUTION

U.S.-based KeyBank has also unveiled a security solution. It is now using Mastercard's Decision Intelligence system to increase the accuracy of real-time transaction approvals and enhance the cardholder experience, according to a Mastercard [press release](#). Decision Intelligence uses AI to boost the reliability of real-time transaction approvals and reduce false declines.

This collaboration is the latest in a long line of similar efforts from the two companies. They recently came together to offer Mastercard-branded debit cards to KeyBank's customers. Going forward, they plan to continue to collaborate on new product development initiatives.



DEEP DIVE.

HOW 3D SECURE 2.0 **PROTECTS** BANKS AND THEIR **CUSTOMERS**

Recent reports indicate an uptick in fraudsters [targeting](#) large FIs; and headlines surrounding security breaches and cyberattacks fill the news on a near daily basis. According to the International Monetary Fund, banks and FIs could lose as much as [\\$100 billion](#) to cybercrime every year. As fraudsters continue to chip away at profits and threaten firms' financial stability, security providers and banks alike are investing in solutions compliant with [3D Secure](#), which protects both consumers and the companies serving them.

Visa and Mastercard designed the 3DS protocols, providing them under the names Verified by Visa and Mastercard Secure Code. Both solutions provide increased fraud protection to online transactions made via debit or credit cards. 3DS was initially introduced

in 2001, and has continued to evolve over the past 17 years. Now, banks and merchants are looking to adopt the service's next generation: 3D Secure 2.0.

THE EVOLUTION OF PAYMENT PROTECTION

3DS 2.0 [offers](#) a seamless and convenient payment experience to customers. It eliminates many of the features that consumers found most interruptive or complicated, including pop-up windows that asked consumers to input information. Instead, these processes have been integrated into the site's existing shopping and payment experiences. The new protocols also better integrate with omnichannel features and loyalty programs, which have become popular with consumers.

76.3%
of consumers
now **prefer**
to bank via
mobile apps



Improving customer experiences was not the sole focus of 3DS 2.0's upgrades, however. The changes also [include](#) enhanced fraud protections for merchants. For example, 3DS 2.0 [uses](#) authentication data, artificial intelligence and machine learning to review, approve or flag transactions as suspicious in real time. What's more, merchants, FIs, payment processors and other players can share transaction data, allowing them to get a clearer picture of the traits that separate legitimate transactions from fraudulent ones.

MOBILE MOVEMENTS

Perhaps more important to the evolution of 3DS 2.0 was the migration of consumers to mobile shopping and banking transactions. Recently published [research](#) has found that 76.3 percent of consumers now prefer to bank via mobile apps. Other [studies](#) indicate that mobile and connected banking offerings are most popular among

millennials and other young consumers, meaning mobile banking apps' popularity is likely to continue — and increase — in the coming years.

Consumers expect these mobile transactions to happen without adding pain points, too, necessitating the use of frictionless flow transactions, or transactions uninterrupted by security protocols. This requires earlier risk evaluation and a richer collection of data, two elements provided by 3DS 2.0

3DS DRAWBACKS AND THE FUTURE OF AUTHENTICATION

3DS 2.0 may be an improvement over its earlier iterations, but it's not without imperfections. Some critics note that increased customer convenience will likely lead to growth in the number of online transactions. That might sound like music to eCommerce merchants'

ears, but an increase in the number of transactions can also make it easier for cybercriminals to slip fraudulent transactions in among the legitimate ones. Others point out that while 3DS 2.0 encourages brand loyalty and is easy to use, it still leaves merchants vulnerable to chargebacks.

Despite these downsides, 3DS 2.0 remains crucial in protecting payments and the customers making them. These issues can be mitigated by partnering with solution providers equipped to help the company with 3DS 2.0 protocols and solutions powered by neural network models, risk-based authentication, dynamic rules engines and other emerging tools and technologies.

With the right partners in place, the risk-based nature and data analytics of 3DS 2.0 capabilities can allow banks and FIs to review and verify transactions without requiring customer intervention. This will become increasingly important as more business is conducted online, where convenience and user experience are valued over almost all other elements.

As solution providers and other partners help in the fight against fraud, banks and other financial firms would be well-served to adopt 3DS 2.0 solutions going forward.



about

PYMNTS.com

[PYMNTS.com](https://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.



CA Technologies creates software that fuels transformation for companies and enables them to seize application economy opportunities. Software is at the heart of every business in every industry. From planning and development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate — across mobile, private and public cloud, distributed and mainframe environments. Learn more at www.ca.com.

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 omnisecurity@pymnts.com.

disclaimer

The Omni Security and Authentication Report 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.

You agree to indemnify and hold harmless, PYMNTS.COM, 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, from and against any and all claims, actions, demands, liabilities, costs, and expenses, including, without limitation, reasonable attorneys' fees, resulting from your breach of any provision of this Agreement, your access to or use of the content provided to you, the PYMNTS.COM services, or any third party's rights, including, but not limited to, copyright, patent, other proprietary rights, and defamation law. You agree to cooperate fully with PYMNTS.COM in developing and asserting any available defenses in connection with a claim subject to indemnification by you under this Agreement.