the PSD2 TRACKER

How SCA's Deadline
IS IMPACTING EU MERCHANTS' AUTHENTICATION APPROACHES

FEATURE STORY - PAGE 6

EKATA

table of
CONTENTS

PYMNTS.com

EKATA

ACKNOWLEDGMENT

what's
INSIDE

Merchants and partnering banks within the European Union are growing more comfortable with the initial changes the revised Payment Services Directive (PSD2) has wrought. These firms are now tackling the next PSD2 challenge: strong customer authentication (SCA), which will go into effect on Sept. 14, 2019. Financial institutions (FIs) are also facing changes regarding how they make their application programming interfaces (APIs) available to third-party players and FinTechs.

Technology providers and other companies are currently developing and launching solutions to better enable merchants that are still struggling with — or completely unaware of — SCA. Such offerings include designated toolboxes and products to help small and medium-sized businesses (SMBs) manage SCA requirements. Many of these smaller merchants are relying on their card acquirers and banking partners to ensure their compliance.

Larger merchants tend to be more aware of SCA compliance, but they still have their challenges. This group of businesses is still butting against the General Data Protection Regulation (GDPR), which requires significant changes to how merchants collect customers' data. Some, including Amazon, are still coming to grips with what these changes mean and how necessary they are. Noncompliance with GDPR is proving to be expensive, too, with the first big company fines recently being issued.

AROUND THE PSD2 AND GDPR WORLD

Merchants, banks and other EU corporate entities still have questions regarding exactly how PSD2, SCA and GPDR can affect them. Third-party players have been granted access to banks' APIs under PSD2, but what that entails is still a mystery to many. The European Banking Authority (EBA) recently published its fourth set of clarifications surrounding APIs under PSD2, focusing on mobile and biometric authentication measures, to address this issue.

Other EU regulators are also attempting to answer outstanding queries. The German Federal Financial Supervisory Authority (BaFin) is looking for ways to gain more flexibility and time for the country's merchants ahead of the SCA deadline. It hopes to offer methods that would let such merchants become more familiar with and prepared for SCA, ensuring losses stay at a minimum.

Online businesses in the United Kingdom are dealing with an increased wave of GDPR requests from consumers, with London merchants in particular [seeing](#) a spike in such inquiries. These requests, allowed under GDPR, enable customers to see how businesses are making use of their data and, in certain cases, ask them to stop using their personal data entirely.

For more on these stories and other PSD2 headlines, check out the Tracker's News and Trends section (p. 9).

HOW SCA'S DEADLINE IS IMPACTING EU MERCHANTS' AUTHENTICATION APPROACHES

SCA's deadline is Sept. 14, and merchants both aware and unaware will be equally affected when it comes time to authenticate their customers. Businesses are at the mercy of their card acquirers and issuers as SCA moves forward, but the rule will provide much needed support for EU-based end customers, said Paul Rodgers, chairman of payments forum [Vendorcom](#). For this month's Feature Story (p. 6), he discusses how merchants were approaching authentication and payment innovation leading up to the deadline.

DEEP DIVE: BIOMETRIC AUTHENTICATION IN A POST-SCA WORLD

Merchants need to stay on top of several SCA compliance requirements, most notable among them being that a single method of customer authentication is no longer enough. They must also ensure that knowledge-based authentication (KBA) methods such as passwords are paired with more stringent verification processes, such as biometric measures like fingerprints, voiceprints and iris scans. This Tracker's Deep Dive (p. 13) examines how merchants are dealing with authentication changes under SCA, as well as if — and how — biometric verification tools can play a part.

Executive
INSIGHT

What are some of the ways that merchants will have to adjust their fraud protection strategies once the SCA deadline passes?

"When India required two-factor authentication for online payments, conversions dropped for some businesses by 25 percent overnight. SCA poses a similar, very expensive problem, which is why merchants' fraud strategies need to become their customer experience strategies.

To protect themselves from a larger conversion loss than necessary, merchants should take full advantage of [SCA] exemptions … like utilizing real-time transaction risk analysis in a pre-authorization flow. This will allow merchants to identify and bucket consumers based on risk, not only speeding good customers through the transaction, but also personalizing the experience for low- to medium-risk consumers by offering benefits like instant fulfillment or promotions for branded cards.

For merchants that may not be large enough or have the resources to bring [transaction risk analysis] in house, the majority will be able to take advantage of SCA-compliant product offerings from their payment providers."

SPENCER MCLAIN
vice president, EMEA, at [Ekata](#)

5 FIVE FAST FACTS

30%
Portion of hotel payment authorization requests likely to be declined under SCA

62%
Segment of London businesses that are seeing a rise in GDPR requests since 2018

$57B
Amount EU businesses could lose in 2020 after the official launch of SCA

73%
Portion of EU businesses that state GDPR has encouraged them to change their use of customer data

66%
Share of EU businesses that have purchased tools to monitor enterprise communications and manage GDPR requirements

feature
STORY

How SCA's Deadline
IS IMPACTING EU MERCHANTS'
AUTHENTICATION APPROACHES

feature
STORY

The deadline to comply with SCA is Sept. 14, and European payment providers and merchants will have to either sink or swim. The former is unfortunately looking more likely for many businesses, especially those that want to transact internationally. These companies not only have to prepare for SCA, but also deal with a dizzying array of approaches from regulators, card issuers and acquirers — firms that determine countries' readiness as well as the authentication tools and methods merchants can use to meet the legislation.

EU merchants are at the mercy of the card acquirers and issuers that bracket online transactions and are responsible for determining how customers will be authenticated under SCA. These providers can choose from a number of verification strategies, including SMS passcodes and biometrics, as long as they fulfill two of the three SCA categories: knowledge, possession and inherence. Paul Rodgers, chairman of European payments membership forum Vendorcom, noted that merchants will be left with a flood of unanswerable questions until providers make their choices.

"The real challenge is, what do merchants communicate to their customers at the moment?" Rodgers said in a recent interview with PYMNTS. "Because merchants are essentially passengers in this process, they're passengers on somebody else's journey. Frankly, they've gotten onboard the SCA card payments Titanic."

SCA has been something of an "almighty iceberg" for EU merchants, even this close to the deadline, Rodgers explained, adding that the regulation is holding eCommerce merchants "below the waterline." This change in authentication standards is still necessary to protect customers from an increasingly complex online payments world, however.

SCA, AUTHENTICATION CHALLENGES AND THE DEADLINE PROBLEM

How merchants can approach authentication depends entirely on their home countries' approaches, which are highly fractured across the region. Some regulators have not responded to the EBA's most recent statement on the subject, while France and the U.K. have proposed

staggered rollouts over three-year and 18-month periods, respectively.

Both plans were designed to remain compliant with what the EBA has termed as a period of "supervisory flexibility" that enables countries to roll the rule out slowly in the face of massive non-preparation. There is not an exact definition for that term, Rodgers said, but it does allow regulators like the U.K.'s Financial Conduct Authority (FCA) to ease merchants and payment providers into compliance.

"If that period of supervisory flexibility is adhered to by the banks and the issuers, then hopefully we won't see a kind of payment Armageddon [on] Saturday," Rodgers said. "I'm fairly hopeful that will be the case."

The FCA's plan for authentication proposes a two-phrase rollout, with the first implementing one-time passcodes sent through SMS messages and the second involving slightly more secure methods, such as smartphone-based biometrics, Rodgers said. It is one of the more robust plans in Europe, especially considering regulators in other countries have yet to make even cursory statements on SCA. The FCA's rollout does not deliver on 2FA, however, which is required under the rule. The SMS phase also comes with a few problems. Approximately 2 million U.K. consumers will lack the ability to receive SMS messages at some point during the day due to the country's phone networks.

"Ironically, being based in the FCA's offices in London means that you can't receive SMS messages in most of their offices," Rodgers explained. "[The method] is very excluding."

Merchants will continue to wait on card acquirers and issuers, which can let end customers and card holders know what to expect from SCA — but even that is not yet standardized.

"What [end customers are] expected to do [to authenticate] isn't just a product of what the issuer decides they're going to have to do," he said. "It is also a product of how the acquirer, processor, gateway and … merchant implement the communications protocols that allow the authentication credentials to be transmitted. You could have as many different communications as there are issuers in Europe — and there are many hundreds."

BRACING FOR SCA'S IMPACT

This mess of payment regulations, rollouts and authentication requirements will be what payment providers, banks, FinTechs and merchants are going to have to deal with as the SCA deadline finally drops.

"To be perfectly honest, it is anybody's guess what we will see [on] Saturday," Rodgers said. "But, I do fully expect that we will see declined transactions that merchants will be surprised by, and I think most of those will happen in cross-border payments where the merchant is in one European country and the issuer is in another."

Protecting customers from the complexity of payments innovation is still a must as banks and regulators take charge of the payments ecosystem. Whether SCA will turn out to be a payments iceberg is still an open question, but it is clear that the EU payments world is bracing for some type of impact.

news &
TRENDS

SCA CHALLENGES AND SOLUTIONS

MERCHANTS, PAYMENT COMPANIES STILL UNPREPARED FOR SCA DEADLINE

The European Payment Service Providers for Merchants (EPSM) association has requested a delay in introducing SCA. It spoke up for the payment service vendors it represents, stating that many retailers are not ready to meet the required standards. The results of the request are unknown, but it appears the deadline is still in place for most of the EU. EPSM is not the only organization that has asked for an SCA delay, though: Regulators in the U.K. and France will unveil the rule over a staggered period.

Consumers also have their qualms about upping authentication on purchases, with a recent survey finding that 70 percent of adults in the U.K. think there are already too many identity checks required when buying online. Unfortunately, fraudsters are also satisfied with the current level of verification. One study found that there were 189,108 cases of fraudulent activity within the U.K. last year, costing £1.12 billion ($1.36 billion USD). The rising level of fraud across the EU is one of the key reasons regulators have remained firm on the SCA deadline.

BAFIN TO GRANT SCA FLEXIBILITY FOR GERMAN MERCHANTS

German regulatory body BaFin wants to give its merchants more flexibility to manage SCA, rather than push the deadline back. It expressed the concern that German merchants would not be able to accept credit card payments due to a lack of proper authentication, as outlined in a recent document, leading to a decline in transactions and customer conversions.

The regulatory body is looking to offer its merchants as much time to prepare as it can under the EBA's guidelines. The entity has not extended the SCA deadline, but has granted certain nations "some flexibility" when rolling out authentication measures. The regulator did not disclose how it would take advantage of this, nor did it state how prepared the country's merchants are for SCA.

UK FCA DEVELOPS 18-MONTH PLAN FOR SCA LAUNCH

The SCA deadline has arrived, but merchants and payment providers in many countries remain unprepared. The U.K.'s FCA released a plan to stagger its rollout in the region to give merchants and payment providers more time to adjust. The 18-month plan will impact the card issuers, payment firms and retailers in the U.K.'s eCommerce market and is a closely tailored response to the EBA's last opinion on the rule, released in June.

The staggered rollout does not mean the SCA deadline is not applicable, however. It instead means that noncompliance will not be strictly enforced among the providers and retailers that are following the FCA's plan. The EBA's June opinion acknowledged that many participants were unprepared, but did not move or waive the deadline. It instead added specific exemptions based on exceptional circumstances.

COMPUTOP LAUNCHES FIDO-COMPLIANT BIOMETRIC SOLUTION

The search for SCA-compliant authentication services is leading merchants and corporations to take a second look at biometrics. Payment processing company Computop recently announced a biometric authentication solution that merchants can utilize under SCA. The offering, Biometrics by Computop, is based on FIDO standards and allows merchants to run two-factor authentication (2FA) checks during payments. Merchants that adopt the technology can authenticate consumers through a number of smartphone-based biometric measures, including fingerprints and facial scans, vocal scans or voice prints.

Biometrics by Computop performs SCA in advance of the transaction, a move designed to help improve conversion rates. The company noted that it also avoids potential challenges or friction points during payment processes.

SIGNIFYD OFFERS PSD2-COMPLIANT PAYMENT SOLUTION

Computop is far from the only provider developing compliance solutions for merchants, especially as the cost for SCA noncompliance is estimated at $55.8 billion. eCommerce fraud protection provider Signifyd also launched a new payment solution, Signifyd Seamless SCA. The product allows retailers to authenticate customers with reduced frictions, fostering customer-merchant relationships, and is fully compliant with the EMV 3D Secure 2 (3DS2) protocol. It also creates more clarity and security
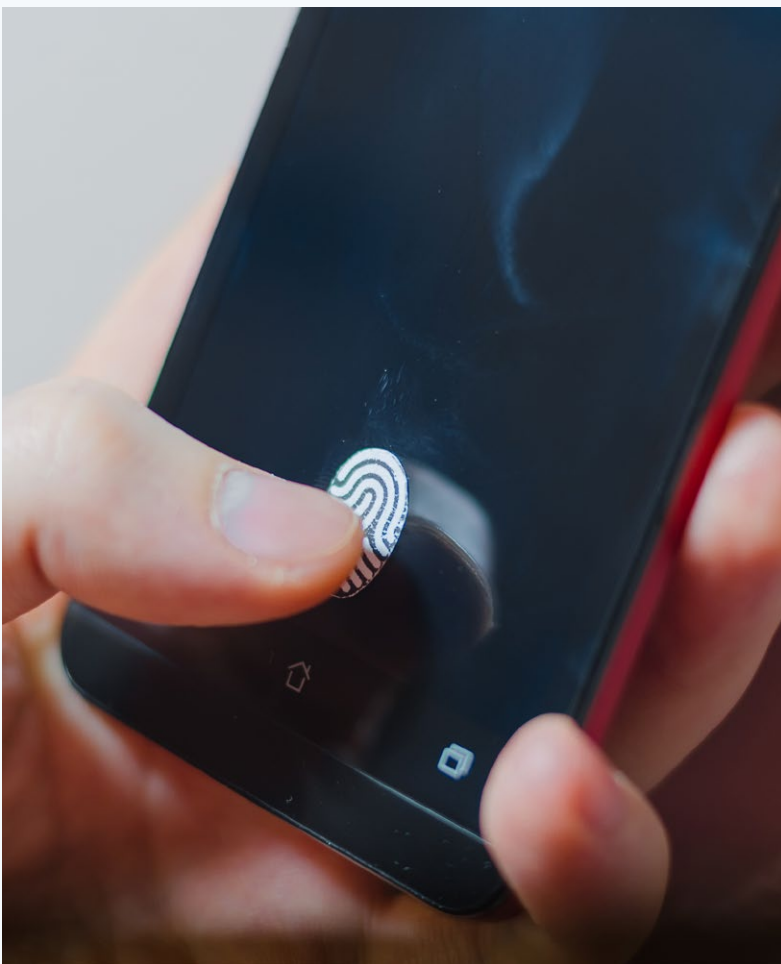
for payments under SCA. A press release explained that Signifyd Seamless SCA approaches PSD2 "holistically," rather than on an exemption by exemption basis, as other providers have previously done.

KONFIRMI RELEASES ID VERIFICATION TOOL FOR EU PARTNERSHIPS

Companies that want to interact with European businesses also have to comply with SCA standards and PSD2, even if they are not headquartered in the EU. Chicago-based technology company Konfirmi released a version of its platform with quicker and more secure authentication tools for businesses looking to remain compliant. The platform can support a range of customer verification methods that adhere to SCA, including 2FA through email and text message, KBA methods and single sign-on (SSO) options. Businesses using the service can tailor verification methods to suit specific needs, and Konfirmi plans to add support for additional authentication methods in the near future.

Businesses that wish to interact with European customers or otherwise work in the EU need to be sure that their authentication standards meet SCA's standards. SCA requires additional authentication measures for transactions that exceed a €30 limit, unless that particular transaction qualifies for a card acquirer-determined exemption.

PSD2 CHALLENGES AND INNOVATIONS

EBA PUBLISHES API CLARIFICATIONS

The EBA has published another set of clarifications on the use of APIs as PSD2 continues to change online banking and payment methods. This is the authority's fourth set of such clarifications published for its working group participants. The document offers explanations for issues involving authentication on mobile apps, biometric technologies and access to non-payment account information, and follows information published in March and April to further clarify PSD2 questions and concerns.

The working group, established in January, consists of 30 individual members representing API initiatives, account servicing payment service providers (ASPSPs) and others in the industry. The group identifies market challenges during the testing and usage of API interfaces.

WSO2 CREATES NEW PLATFORM FOR SCA, RTS STANDARDS

Open source integration vendor WSO2 recently released its WSO2 Open Banking platform, which supports Regulatory Technical Standards (RTS) and SCA compliance. The platform aims to allow banks and businesses to fully comply with PSD2 as standards shift and consolidate across the EU and the U.K.

Open Banking also supports electronic identification and other fraud detection measures for FIs, and the platform is compliant with Germany-based Berlin Group's NextGenPSD2 API 1.3 standard and the U.K.'s Open Banking U.K. API 3.1.1. standard. Both were created to help third parties, banks and merchants better comply with PSD2.

DUTCH NATIONAL BANK GIVES 2CHECKOUT PSD2 PAYMENT LICENSE

Other markets are moving forward with PSD2 plans even as SCA worries compound. The Dutch National Bank recently granted global monetization platform 2Checkout a PSD2 Payment Institution license. The license grants more flexibility when partnering with FIs and other institutions within the European Economic Area (EEA), and offers more consumer protections and security when it comes to payments.

2Checkout enables its partners to sell products and services through multiple communication channels, and the license will allow it to ensure transactions and payments sent on its platform remain compliant with PSD2. A press release noted that 2Checkout can use the license for compliance throughout the EEA.

GDPR NEWS AND DEVELOPMENTS

LONDON BUSINESSES STRUGGLE TO KEEP UP WITH GDPR REQUEST VOLUME

GDPR has been in place for more than a year, and 66 percent of businesses have responded by purchasing software to monitor communications under the rule. London-based businesses have already seen an uptick in the amount of data access requests customers are sending, with a recent study finding that 62 percent have seen a rise in such requests since GPDR's debut in May 2018. The same study discovered that most businesses are finding it hard to keep up with that volume, as 58 percent cite cost and 55 percent note GDPR's complexity as main obstacles to meeting demand. Businesses are tasked with responding to customer requests within a month, and consumers can use these requests to gain copies of all the data collected on them — including why it was collected and how it is being used.

GOOGLE'S GDPR STRUGGLES IN IRELAND CONTINUE

Technology company Google is among the entities seeing major impacts from GDPR, continuing its fight with Ireland's Data Protection Commission (DPC) over how it uses customer data within its ad system. The ongoing investigation is the result of a formal complaint alleging that Google's system relies on personal data for more

targeted ads and the ad traffic insights it provides partner websites and services.

A formal complaint from an executive of secure browsing service Brave also alleges that Google relies on and shares personal data through its real-time bidding ad system to create visitor profiles, despite the technology firm's own claims that it no longer shares "identifiable" data with these companies under GDPR. The DPC's investigation is ongoing and is not the only such issue Google has faced. French regulators fined Google $57 million in January for violating the rule. This also comes as 73 percent of companies state that GDPR has made them change the ways they approach customer data.

INDIA APPLIES FOR GDPR ADEQUACY STATUS FROM EU REGULATORS

The struggles EU merchants are encountering under GDPR are not dampening interest from other markets, with Indian regulators now seeking GPDR "adequacy" status. The country's data protection standards would be seen as equivalent to GDPR should EU regulators grant the request, allowing EU merchants to access data in India and vice versa. European technology companies would also be able to outsource projects to India while still keeping compliant with GDPR.

India needs to pass its own version of a GDPR bill before it can officially request this status, however. The EU has granted adequacy status to 13 other countries since GDPR first came into play, including Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States.

deep
DIVE

Biometrics And New Technologies In A Post-SCA World

SCA in its simplest form requires that customers be identified through methods that fall into at least two of three categories: knowledge, possession or inherence. The first refers to KBA methods like passwords or PINs, but the latter two categories are where merchants and payment providers will need to get creative.

Possession and inherence bring consumers more heavily into the authentication process because both rely on information that only they have. Possession can refer to the chip inside of a physical debit card, for example, while inherence refers to things that are even more personal — such as fingerprints.

Online merchants could collectively lose approximately $57 billion in 2020 due to SCA adjustments. Merchants that wish to stay compliant should search for methods that fit the inherence and possession categories. These solutions fall into the inherence bracket and can be

combined with KBA methods like one-time passwords, thus satisfying the standard.

One of the challenges yet to be faced is that only 25 percent of online merchants are aware of SCA, making compliance tricky for the remaining 75 percent. Another area of concern is that merchants are dependent on card issuers, which choose the verification categories and combinations consumers will need to meet when making online purchases. Merchants must therefore be prepared to support several verification and customer experiences.

BIOMETRICS AND AUTHENTICATION CHALLENGES

Merchant awareness and preparedness has been an ongoing issue since SCA was first proposed. Part of the confusion comes as a result of SCA being a legal

requirement and not a simple card payment standard upgrade, which would trickle down to merchants via the card networks. Merchants will bear the brunt of the consequences from noncompliance, however. All transactions over €30 are subject to SCA, meaning that purchases can be declined if the consumer cannot provide proper verification. Biometrics is emerging as one of the innovative solutions to this problem in a variety of industries, including retail, travel and hospitality.

Some studies predict that 30 percent of payment authorization requests in the hotel industry will be declined under SCA. Biometrics may be able to lower that percentage by combining tools like voice recognition or TouchID into customers' online purchases, ensuring that SCA standards are met. Hotels could also make use of digital wallets like Apple Pay that inherently authenticate payment through Face or TouchID, which satisfy authentication needs for the possession and inherence categories. The smartphone is in the customer's possession, after all, and face or fingerprint scans fit inherent verification.

Biometrics also have the advantage of simplifying customer experiences. Customers can be fully identified by providing fingerprint scans alone, reducing user frustration while also meeting heightened authentication requirements. This could come in handy for those looking to prevent sales losses post-SCA. Regulators are also closely examining biometrics as the deadline moves closer.

The U.K.'s FCA is among the entities that believe merchants need more time to prepare for SCA, and has come up with an 18-month plan to address shortcomings. The plan will help retailers balance both security and customer convenience with authentication measures like mobile text messages and biometrics in mind. Customers are already used to authenticating with their fingerprints to gain access to mobile banking apps or unlock smartphones, but it is unclear how acceptable this process will be for eCommerce purchases.

Merchants that wish to use biometrics still need to confront several problems, including that issuing banks and card acquirers will be the ones determining proper authentication methods under the rule. This puts the problem of biometric innovation on the shoulders of banks and payment providers.

SCA AND THE AWARENESS PROBLEM

Merchants and their partnering payment services will need to make sure that their chosen authentication methods measure up to customer preferences. They will have to determine whether customers prefer facial scans or fingerprints, for example, and see how these tools fit in with the methods users already prefer.

Merchants that want to have a say when it comes to customer authentication will need to work quickly, though. The lack of awareness about the regulation, its exemptions and its noncompliance consequences remain the most significant barriers. Those that want to succeed in keeping customers engaged and safe will need to confront the complexities of SCA as quickly as possible.

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.

EKATA

Ekata is an international identity data company that provides businesses with global identity verification solutions via enterprise-scale APIs and web tools to help companies identify legitimate customers, prevent fraudulent transactions, and smooth new customer creation.

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 psd2@pymnts.com

DISCLAIMER

The PSD2 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.