

The Future Of Authentication In Financial Services, a PYMNTS and Entersekt collaboration, examines authentication's role in financial services and illustrates how financial institutions can provide consumers with trusted and integrated banking experiences across multiple environments.

THE FUTURE OF AUTHENTICATION IN FINANCIAL SERVICES

Using Authentication To Build Trust



THE FUTURE OF AUTHENTICATION IN FINANCIAL SERVICES

TABLE OF CONTENTS

Introduction	04
Letting go of passwords	08
Managing consumer account access	12
Adopting new authentication methods	16
Building an experience grounded in security and trust	20
Conclusion	24
Methodology	25

PYMNTS.com



The Future Of Authentication In Financial Services was produced in collaboration with Entersekt, 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.

USING AUTHENTICATION TO BUILD TRUST

INTRODUCTION

The increased global penetration of mobile devices has transformed how consumers transact with their preferred financial institutions (FIs), merchants and service providers. Recent PYMNTS research finds that 69% of all consumers now bank using their FIs' mobile apps, and 47% of them use their FIs' apps at least once per week — an engagement level that is not matched by any other online activity.¹

Positively verifying end users' identities is now especially important, as consumers' lives have become more digitally connected. Many financial

services providers, however, still rely on password authentication as a primary method for their customers use to access their accounts and personal data. Stolen usernames and passwords thus remain a primary threat vector for cybercriminals who can engage in identity theft and fraud often before breaches are detected.

Our research shows that consumers use digital banking to access their accounts across multiple digital platforms, including mobile apps and mobile- and desktop-based browsers, but 64% of them use username and password combinations to access

their accounts. Consumers have high expectations for digital banking experiences that are both convenient and secure and, as a result, are increasingly interested in stronger forms of authentication, such as biometric fingerprint, face and voice scans.

Our data also finds that consumers who use multiple digital banking channels are most likely to feel comfortable with the security of their accounts when using alternative authentication methods. These cross-device users are also the most likely to believe that passwords will eventually be phased out as an authentication method.

The Future Of Authentication In Financial Services: Using Authentication To Build Trust examines consumers' preferences for different authentication methods when accessing financial services providers. We surveyed 2,719 consumers from Sept. 10, 2021, through Sept. 27, 2021, to learn more about the different types of authentication methods they use, how their preferences vary across devices, and how FIs can use authentication and secure experiences to build trust with their customers.

This is what we learned.

¹ How US Consumers Define the Super App. PYMNTS.com, December 2021. <https://www.pymnts.com/connectedeconomy/2021/how-170-million-us-consumers-define-the-super-app/>. Accessed January 2022.

01

USERNAME AND PASSWORD COMBINATIONS ARE THE AUTHENTICATION METHOD MOST USED TO ACCESS DIGITAL FINANCIAL ACCOUNTS. SIXTY-FOUR PERCENT OF CONSUMERS SAY THEY USE THIS METHOD AT LEAST ONCE A MONTH TO ACCESS THEIR DIGITAL FINANCIAL SERVICES ACCOUNTS.

Consumers who prefer to access their digital financial accounts with more than one device tend to use multiple alternative authentication methods. On at least a monthly basis, 36% use fingerprint scans, 28% use facial scans and 18% use voice scans.

02

SIX OUT OF 10 CONSUMERS ARE WILLING TO TRY LOGIN METHODS OTHER THAN PASSWORDS. THIS SHARE RISES TO 73% FOR THOSE WHO USE MULTIPLE DEVICES TO ACCESS THEIR ACCOUNTS.

Sixty-one percent of consumers are willing to log in to their accounts with alternative authentication methods, and 60% of those who use mobile apps and mobile- and desktop-based browsers say they would be “very” comfortable logging in using methods other than login IDs and passwords. Nearly half of these users believe passwords will eventually be phased out as an authentication method.

03

MORE THAN ONE-THIRD OF CONSUMERS ARE WILLING TO USE BIOMETRIC METHODS FOR AUTHENTICATION PURPOSES. ALMOST HALF OF CONSUMERS ARE WILLING TO USE FINGER-PRINT SCANS IN PRIVATE AND PUBLIC SETTINGS.

Forty-nine percent of consumers say they are “slightly” or “not at all” reluctant to use fingerprint scans in private settings, while 47% say the same about using them in public. A significant share of consumers are comfortable using facial scans and voice scans, with a slight preference to use them in private settings. Forty-four percent of consumers are “slightly” or “not at all” reluctant to use facial scans in private, and 41% report feeling the same about using them in public. Similarly, 43% of consumers are “slightly” or “not at all” reluctant to use voice scans in private settings, while only 37% say the same about using them in public.

04

ALMOST TWO-THIRDS OF CONSUMERS SAY THAT AN EMPHASIS ON DATA SECURITY HAS A “VERY” OR “EXTREMELY” BIG IMPACT ON THEIR TRUST IN A FINANCIAL SERVICES PROVIDER.

Sixty percent of consumers say that having information about how their transactions are secured has a “very” or “extremely” big impact on their trust in financial services providers. Forty-four percent of consumers say that the ability to log in without passwords is “very” or “extremely” impactful on their trust and 32% report that this has a “moderate” impact.



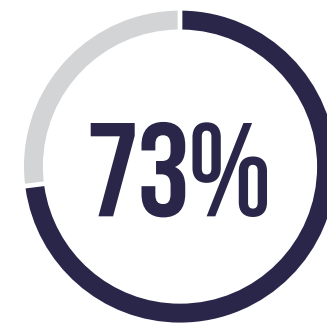
LETTING GO OF PASSWORDS

THE FUTURE OF
AUTHENTICATION
IN FINANCIAL SERVICES

PYMNTS.com



PYMNTS' research shows that login IDs and passwords are increasingly giving way to other forms of authentication across all common digital banking platform access points, including desktop- and mobile-based browsers and mobile apps. Our data indicates that the majority of consumers are comfortable logging into their accounts with alternative methods, including biometric ones such as fingerprints, facial scans and voice scans. This trend is especially prevalent among consumers who use multiple environments to access their account: 36% of this group use fingerprint scans, 28% use facial scans and 18% use voice scans at least monthly.



Share of consumers who mostly use multiple environments to access digital accounts and are willing to use login methods other than passwords

Sixty-one percent of consumers are willing to use login methods other than passwords, yet just 49% of consumers who most frequently access their accounts via desktop browser are willing to do so. Mobile device users are more willing to use alternative authentication methods: 68% of those who most frequently use mobile apps have willingness, compared to 54% of those who most frequently use mobile browsers. Seventy-three percent of consumers who mostly use multiple environments to access digital accounts are willing to use login methods other than passwords.

TABLE 1:
Consumers’ comfort with specific login methods

Share who agree with select sentiments, by most frequently used device

■ Highest percentage

	WILLING TO USE NON-PASSWORD LOGIN METHODS	VERY COMFORTABLE WITH SECURITY USING NON- PASSWORD LOGIN METHODS	PASSWORDS WILL EVENTUALLY NO LONGER BE USED
• Computer browser	48.5%	30.7%	36.1%
• Mobile device browser	54.3%	40.5%	41.9%
• Mobile device application	67.9%	50.0%	47.9%
• Multiple options	73.1%	60.1%	61.0%

N = 2,719: Digital financial account owners
Source: PYMNTS | Entersekt
The Future Of Authentication In Financial Services

Indicating growing confidence in the use of alternative authentication methods, 45% of survey respondents report being “very” comfortable with their accounts’ security when using login methods that do not require passwords. Mobile users are more likely to be “very” comfortable with their accounts’ security when using alternative authentication methods, with 40% of mobile browser users and 50% of mobile app users saying so. Only 31% of computer browser users report that they are very comfortable with their accounts’ security when using alternative authentication methods.



Share of cross-device users who believe passwords will eventually be phased out as an authentication method

Consumers who use multiple environments are most likely to feel comfortable with their accounts’ security when using alternative authentication methods, as 60% of respondent expressed this comfort. It is no surprise, then, that cross-device users are also the most likely to believe that passwords will eventually be phased out as an authentication method: 61% say so.



More than two-thirds of digital account holders would not oppose using biometrics to authenticate their identities.

FIGURE 1:
Consumers’ comfort with specific login methods
Share who agree with select sentiments



N = 2,719: Digital financial account owners
Source: PYMNTS | Entersekt
The Future Of Authentication In Financial Services



MANAGING CONSUMER ACCOUNT ACCESS

THE FUTURE OF
AUTHENTICATION
IN FINANCIAL SERVICES

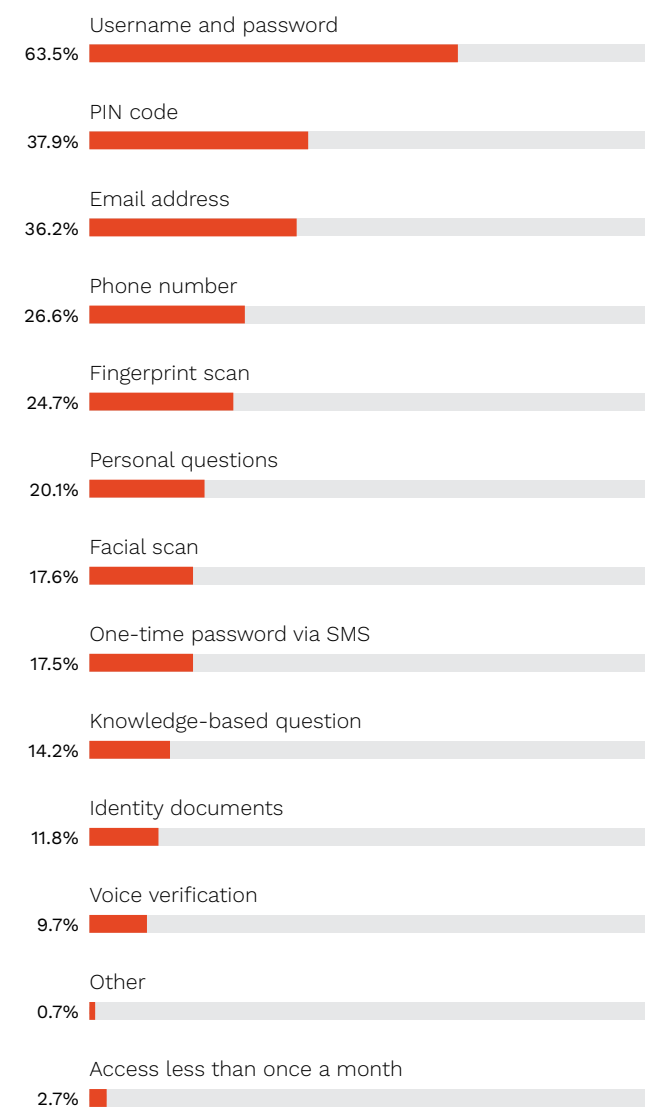
PYMNTS.com



FIGURE 2:

Authentication method usage

Share of consumers who use select authentication methods to access digital financial services accounts at least once a month



N = 2,719: Digital financial account owners
Source: PYMNTS | Entersekt
The Future Of Authentication In Financial Services

Username and password combinations remain the authentication method most commonly used when accessing digital financial services accounts. Our research finds that 64% of consumers still use username and password combinations to access their digital financial services accounts at least once a month, with consumers who access their accounts via computer browser the most likely to do so, at 77%. Sixty-one percent of those who access their digital financial accounts via multiple platforms use username and password combinations as well.

Consumers indicate they are ready to use alternative authentication methods, however, with more than half of account holders using some form of biometrics to authenticate their identities. Our research finds that 25% use fingerprint scans to access their digital financial services accounts at least once a month, 18% use facial scans this often and 10% use voice verification this often.

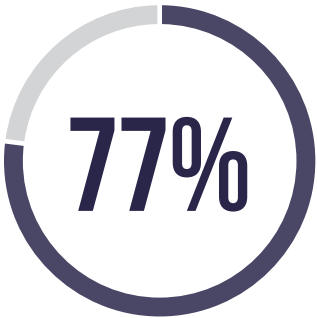
TABLE 2:
Authentication method usage
Share of consumers who use select authentication methods to access digital financial services accounts at least once a month, by most frequently used device

■ Highest percentage

	COMPUTER BROWSER	MOBILE DEVICE BROWSER	MOBILE DEVICE APPLICATION	MULTIPLE OPTIONS
• Username and password	76.8%	54.2%	57.7%	60.7%
• PIN code	27.7%	34.9%	45.0%	44.3%
• Email address	36.5%	37.1%	32.6%	39.4%
• Phone number	17.4%	28.5%	28.5%	34.3%
• Fingerprint scan	7.2%	25.7%	32.3%	36.2%
• Personal questions	25.9%	11.4%	15.6%	24.3%
• Facial scan	4.6%	15.8%	23.7%	27.5%
• One-time password via SMS	15.6%	11.6%	17.3%	24.3%
• Knowledge-based question	13.6%	10.5%	10.3%	22.1%
• Identity documents	5.8%	7.7%	11.8%	22.0%
• Voice verification	4.3%	11.6%	6.8%	18.1%
• Other	1.4%	0.4%	0.4%	0.4%
• Access less than once a month	4.7%	2.3%	2.8%	0.4%

N = 2,719: Digital financial account owners
Source: PYMNTS | Entersekt
The Future Of Authentication In Financial Services

Among mobile device browser users, 26% use fingerprint scans, 16% use face scans and 12% use voice scans to access their accounts regularly at least once a month. Mobile app users are more likely to use biometrics, our data shows. Thirty-two percent of those who most frequently use mobile applications say they use fingerprint scans and 24% use face scans, yet only 7% use voice scans to access their accounts at least once a month. This is not surprising, as many mobile apps are designed with easy-to-use interfaces that take advantage of the video and touch sensors that come standard with most smartphones.



Share of users logging into accounts from computer browsers with usernames and passwords

Consumers who access their digital financial accounts via multiple platforms are the most likely to use multiple biometric authentication methods to access their digital financial services accounts at least once a month. Our data finds that 36% of cross-platform consumers use fingerprint scans, 28% use facial scans and 18% use voice scans to access their accounts.



ADOPTING NEW AUTHENTICATION METHODS

THE FUTURE OF
AUTHENTICATION
IN FINANCIAL SERVICES

PYMNTS.com

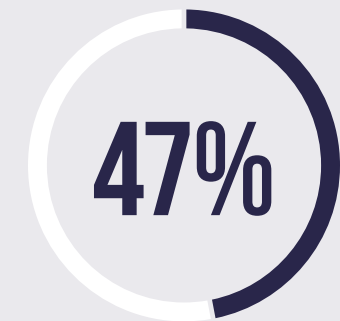
 Entersekt

Consumer confidence in new biometric authentication methods is strong enough that many are comfortable using the methods to access their digital accounts anywhere. We find that consumers are as willing to use biometric methods as they are to use username and password combinations for authentication in both private and public settings.

Sixty-one percent of consumers say they are “slightly” or “not at all” reluctant to use a username and password combination in private setting, while 48% are “slightly” or “not at all” reluctant to do so in public settings. Meanwhile, 49% of consumers say they are “slightly” or “not at all” reluctant to use fingerprint scans for authentication purposes in private settings, while 47% feel the same about using fingerprint scans for authentication purposes in public.

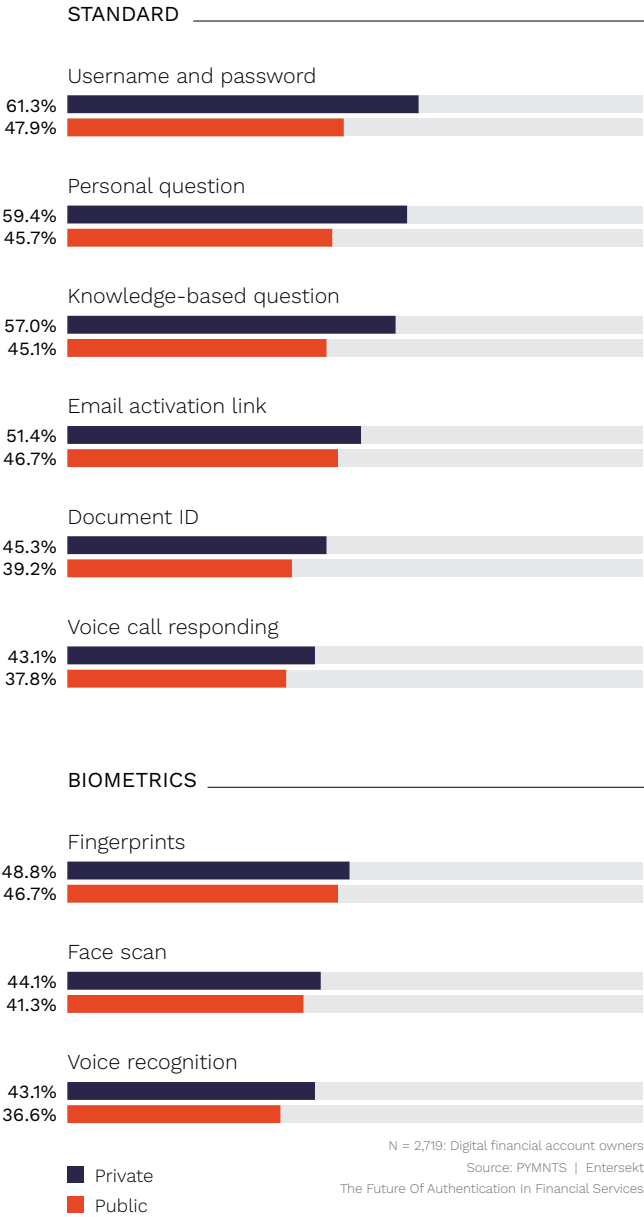


Biometric-based authentication is an appealing alternative to passwords for many consumers.



Share of consumers who say they are “slightly” or “not at all” reluctant to use fingerprint scans for authentication purposes in public.

FIGURE 3:
Willingness to use authentication methods
Share of consumers who would be “slightly” or “not at all” reluctant to provide information for authentication purposes in public or private settings



Share of consumers who say they are “slightly” or “not at all” reluctant to use facial scans for authentication purposes in public.

Willingness to use facial scans and voice scans is also high. Forty-four percent of consumers report they are “slightly” or “not at all” reluctant to use facial scans in private, and 41% say the same about using facial scans in public. Forty-three percent of consumers are “slightly” or “not at all” reluctant to use voice scans in private settings, and 37% are “slightly” or “not at all” reluctant to do so in public.





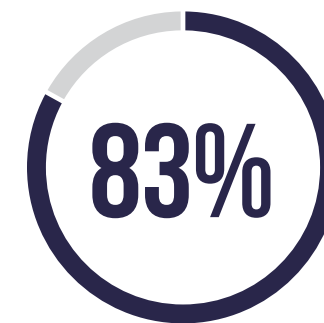
BUILDING AN EXPERIENCE GROUNDED IN **SECURITY AND TRUST**

THE FUTURE OF
AUTHENTICATION
IN FINANCIAL SERVICES

PYMNTS.com



PYMNTS' research finds that trusted user experiences are highly important to consumers accessing digital accounts via desktop browser or mobile device. It is no surprise that 83% of consumers say that their financial service provider having at least one feature that enhances security has a "very" or "extremely" big impact on their trust in that provider or that 65% of consumers say that providers that emphasize data security have the same level of impact on their trust. Sixty percent say that having information about how their transactions are secured has a "very" or "extremely" big impact on their trust, and 44% of consumers say that the ability to log in without passwords has a similar impact, while 32% report it has a "moderate" impact.



Share of consumers who say that their financial service provider having at least one feature that enhances security has "very" or "extremely" impact on their trust in that provider.

Our data also shows that 80% of consumers say that good user experiences have a "very" or "extremely" big impact on their trust in their financial service providers. Moving away from passwords to stronger, biometric-based authentication enables financial service providers not only to support secure logins and transactions, but also to simplify the consumer experience.

TABLE 3:

Why consumers trust or distrust financial services providers

Share of consumers who cite factors as having select levels of impact on their trust in financial services providers

■ Highest percentage

	EXTREMELY OR VERY BIG IMPACT	MODERATE IMPACT	SLIGHTLY OR NO IMPACT AT ALL
SECURITY			
• At least one option that concerns security	82.8%	13.4%	3.8%
• Emphasis on data security	65.3%	22.6%	12.1%
• Secure transaction information	59.9%	26.0%	14.1%
• Able to approve transactions before processing	56.4%	29.5%	14.2%
• Website quality	55.5%	30.0%	14.5%
• Login without password	44.2%	31.9%	23.9%
USER EXPERIENCE			
• At least one option that concerns user experience	80.2%	15.6%	4.1%
• Provide detailed data protection statement	55.7%	27.0%	17.3%
• Personalized real-time customer support	54.5%	29.6%	15.9%
• Consistent experiences across platforms	53.4%	31.2%	15.4%
• Marketing communication opt-out	50.3%	31.1%	18.6%
• Seamless communication channels	50.2%	32.5%	17.3%

N = 2,719: Digital financial account owners
Source: PYMNTS | Enterspekt
The Future Of Authentication In Financial Services



Share of consumers say who that good user experiences have a “very” or “extremely” big impact on their trust in their financial service providers.

Moving away from passwords to stronger, biometric-based authentication enables financial service providers

not only to support secure logins and transactions, but also to simplify the consumer experience.

CONCLUSION

As today's connected consumers move more of their interactions with their trusted financial services providers online, they are also growing more comfortable with alternative authentication methods regardless of whether they use computer browsers or mobile devices. They also expect best-in-class experiences defined by convenience and security. Digitally savvy consumers, especially those who transact via multiple devices, are looking for stronger authentication alternatives. They are comfortable with and willing to use biometrics, including fingerprint, facial recognition, and voice scan technology, for seamless and secure access to their digital accounts. Financial service providers can build trust by simplifying the consumer authentication experience and supporting frictionless and secure logins and transactions.

PYMNTS.com

 **Entersekt**

METHODOLOGY

The Future Of Authentication In Financial Services: Using Authentication To Build Trust draws from a PYMNTS survey of 5,578 American consumers who were asked about their preferences for different types of authentication when accessing their financial service providers across various digital environments (such as desktop/laptop versus mobile). We removed 563 responses from our original sample due to illegibility, inaccuracies or other issues, and we eliminated another 1,018 for incompleteness. This left us with 3,997 responses, of which 2,719 were from respondents who had bank accounts, owned mobile devices and used mobile banking apps. Our analysis considered the response data from this group, and our weighted sample was then census-balanced in terms of age, education levels, gender and income.

THE FUTURE OF
AUTHENTICATION
IN FINANCIAL SERVICES

ABOUT

DISCLAIMER ■

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.

 **Entersekt** Entersekt is a leading provider of strong device identity and customer authentication software. Financial institutions and other large enterprises in countries across the globe rely on its multipatented technology to communicate with their clients securely, protect them from fraud, and serve them convenient new experiences irrespective of the channel or device in use. They have repeatedly credited the Entersekt Secure Platform with helping to drive adoption, deepen engagement, and open opportunities for growth, all while meeting their compliance obligations with confidence. For more information, please visit www.entersekt.com or email info@entersekt.com.

The Future Of Authentication In Financial Services 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.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe, please email us at feedback@pymnts.com.