Socure

PYMNTS.com

DIGITAL IDENTITY

LIFESTYLE

CAPSULED

OVER **41%** aren't satisfied with their current authentication method due to a lack of data security.

OVER **91%** of consumers report using email addresses to authenticate new accounts.

eCommerce Edition | October 2018

DIGITAL IDENTITY

LIFESTYLE

CAPSULE

ACKNOWLEDGMENT

The Digital Identity Lifestyle Capsule is powered by Socure, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the findings presented, as well as the methodology and data analysis.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Businesses must be able to quickly and accurately determine that customers are who they say they are, something that is becoming increasingly important as more of them turn to digital to fulfill their needs.

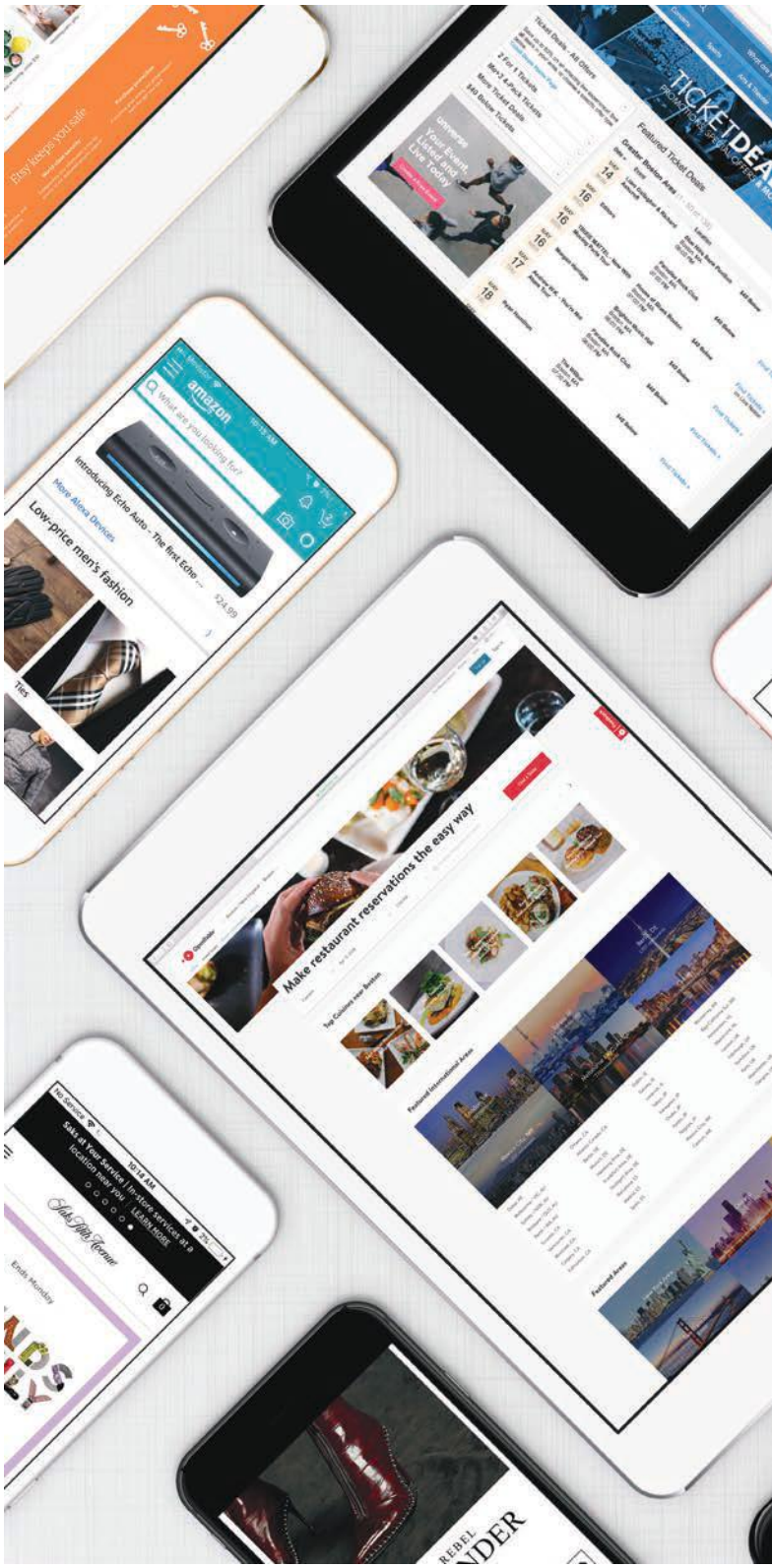
It's crucial that merchants do this *without* introducing frictions into the currently fast and frictionless experience. Authentication must be about customer preferences, but still secure interactions to protect consumers and the businesses with which they transact.

That customer who just ran out of milk and fabric softener, asking Amazon's Alexa to instantly add them to her shopping list, wants this exchange to take less than a minute of her time. So does the one stocking up on supplies while she's running out the door, adding groceries to her mobile shopping order so she can pick them up on her way home from work.

Even the customer impulse shopping on Amazon at midnight expects his transaction to be instantaneous, with or without Prime.

All these experiences are seamless for customers, but they require real-time authentication to keep them that way. Whether a password, PIN code, email address or biometric identification, consumers want to authenticate as quickly as possible and forget about it. The process must be fast, convenient and easier than any other way to authenticate.

Regardless of the device they use, most customers don't really think about authentication



and, for the most part, prefer sticking to the familiar. Passwords are still popular because they don't cause much friction, despite ongoing security concerns, and browsers like Google Chrome and Apple Safari keep caches of them for customer convenience. That means users don't even have to work to remember them.

No matter how a customer chooses to authenticate, the three things most important to customers — speed, ease of use and convenience — haven't changed. The PYMNTS Digital Identity Lifestyle Capsule Survey, a Socure collaboration, found that most customers are satisfied with the way they are currently authenticating their online purchases. This suggests that many common authentication methods have these three key virtues. Our research examined responses from more than 1,000 individual consumers in healthcare, financial services and eCommerce. This report will focus solely on eCommerce segment results.

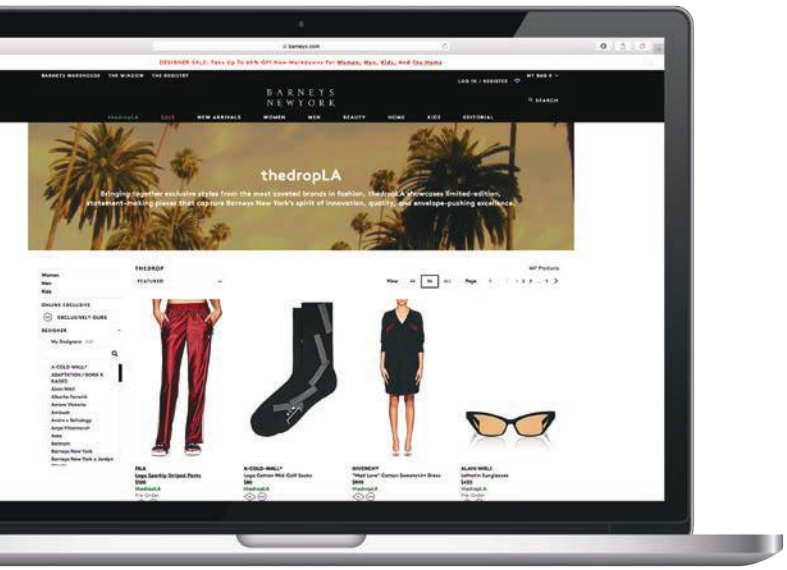
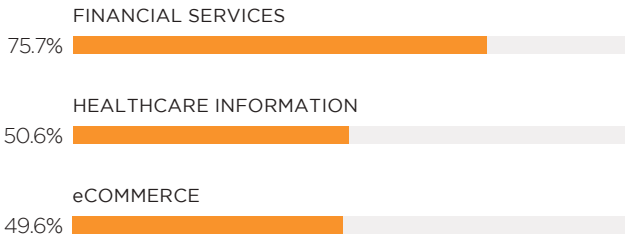


FIGURE 1:

How consumers across survey segments confirmed their identities

Frequency with which consumers were asked to authenticate, by industry



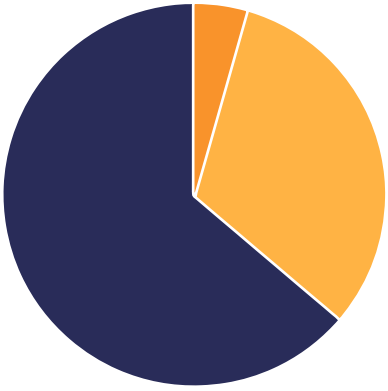
Passwords have been around for a while now. Consumers in their 40s and 50s tend to prefer them, as do lower-income users earning $25,000 to $50,000. Those in their 30s, 20s and teens have been primed by mobile technologies to adopt newer authentication methods, however, so long as they still provide a frictionless experience. These customers are thus much more likely to try emerging online identification tactics, including voice, facial or fingerprint biometrics.

Most customers become dissatisfied with authentication when it's slow, cumbersome or difficult to use. A growing number are also concerned about data security and fraud, a trend which might be contributing to growing interest in biometrics. A person's face or fingerprint is harder to hack than the online password retailers are storing on servers, after all.

That said, fewer eCommerce merchants authenticate their customers than those in

FIGURE 2:

How consumers confirmed their identities
Ways consumers authenticate,
by phone, online or via call center



Online**: 63.8%** Mobile device**: 31.8%** Call center**: 4.4%**

MORE THAN 31 PERCENT

OF CUSTOMERS

AUTHENTICATED

THEIR IDENTITIES

ON A MOBILE PHONE.

healthcare or financial services. Approximately 50 percent are authenticated for eCommerce transactions, compared to about 76 percent for online financial activities.

Consumers in their teens and 20s might be using their mobile phone when online shopping, but, for the most part, they're still using the computer to shop. Approximately 64 percent of them authenticated online, and about one-third did so through mobile. Call centers accounted for the remaining consumers.

Our survey findings revealed that passwords and email addresses are the most common ways consumers prove their identities. Consumers are largely satisfied with their eCommerce experiences, as 70 percent of eCommerce respondents cited being "very" or "extremely" so with such websites' required authentication methods.

The need to provide frictionless authentication in eCommerce transactions will continue to be important as younger consumers gravitate toward mobile shopping and begin using more innovative methods like biometrics.

Consumers are placing high emphasis on seamlessness and speed, meaning online merchants need to fulfill these values to remain competitive. Consumers also appear to be growing more concerned with data security, and online merchants will also need to show those across all age, income and education levels that their information is secure.

CONSUMERS' CURRENT AUTHENTICATION PROCESSES

How, exactly, are customers authenticating? To answer this question, we considered the types currently available to existing and new consumers loading up their online carts. In both cases, customers were most commonly asked to authenticate using email addresses and passwords.

Email was the most popular method, required 91 percent of the time for new account signups. Sixty percent of those accessing an existing account were required to input one, and 60 percent were required to provide a password.

FIGURE 3:

How consumers confirm their identities for eCommerce transactions

Ways consumers used to authenticate new accounts

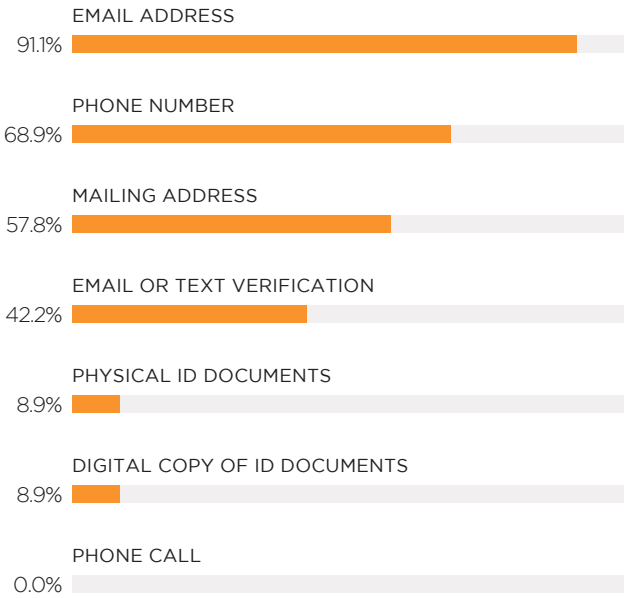
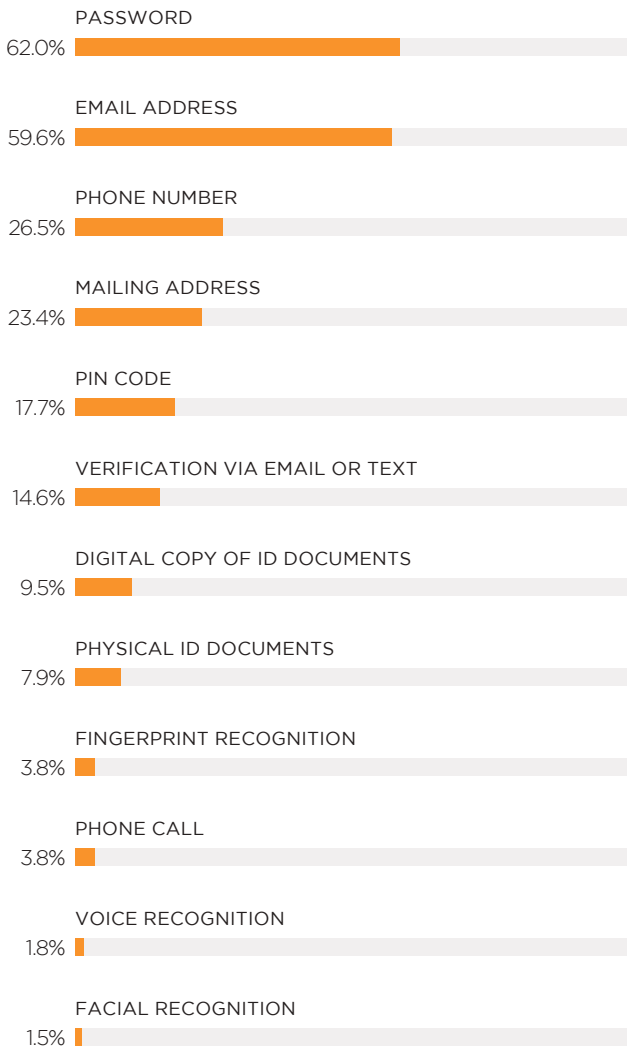


FIGURE 4:

How consumers with existing accounts confirm their identities for eCommerce transactions

Ways consumers used to authenticate existing accounts



Email and passwords weren't the only popular choices, either, as just under 60 percent of new account creators reported needing to give a home address. On the other end of the spectrum was biometrics, used by fewer than 2 percent of respondents when accessing an existing account for voice or facial biometrics (the use case for fingerprint ID was a little higher, approximately 4 percent). None of those in our sample reporting using biometrics to create a new account.

These are the methods consumers used for eCommerce transaction authentication, but which did they prefer?

OVER 60 PERCENT

OF CUSTOMERS

NEEDED TO PROVIDE

A MAILING ADDRESS

TO CREATE A NEW ACCOUNT.

AUTHENTICATION METHODS THAT

RESONATE WITH CONSUMERS

Consumers don't really think about how they'll authenticate a transaction to buy a shirt or purchase a throw pillow, but that doesn't mean they don't notice the process.

We considered the percentage of consumers who were satisfied with authenticated regardless of the method used, enabling us to get a sense of certain methods' popularity. Happily, 70 percent of them were "very" or "extremely" satisfied with online shopping authentication.

Some methods were more popular than others, however, and email addresses and passwords were at the top. Of the 70 percent who were satisfied, approximately half were highly so with using an email or password. Consumers were relatively neutral for most of the other methods.

Most consumers are satisfied with email and password, possibly because these are also two of the most common ways online retailers

TABLE 5:

Which authentication methods most satisfy consumers?
Customer satisfaction, by method

	Extremely satisfied	Very satisfied	Somewhat satisfied	Slightly satisfied	Not at all satisfied
Password	**50%**	**54%**	31%	17%	7%
Email address	47%	49%	**32%**	**44%**	14%
Mailing address	31%	16%	5%	34%	**29%**
Phone number	29%	20%	14%	27%	21%
Digital copy of ID documents	19%	7%	6%	17%	0%
PIN code	17%	26%	29%	17%	**29%**
Email or text verification	17%	24%	25%	17%	21%
Physical ID documents	11%	5%	4%	5%	14%
Fingerprint recognition	7%	9%	17%	20%	21%
Phone call	6%	7%	7%	7%	7%
Voice recognition	4%	2%	7%	7%	21%
Facial recognition	4%	1%	9%	10%	21%

authenticate them. Customers had mixed feelings about the options used less often, like providing identity documents at a physical store or fingerprint, facial or voice authentication. Identity documents saw lower satisfaction scores for both new and existing accounts, but biometric satisfaction was a little trickier to pinpoint.

Fingerprint biometrics boasted higher overall satisfaction than voice or facial authentication for new and existing accounts. Consumer interest appears to reach both extremes for the latter, with 43 percent of customers "not at all" satisfied and 43 percent "extremely" so.

Even as they become more comfortable with biometrics — some more than others — most consumers are happy with email and passwords.

FIGURE 6:

Which methods do consumers prefer?
Most popular required authentication method

	METHOD REQUIRED TO CREATE ACCOUNT					
	Digital copy of ID documents	Physical ID documents	Email or text verification	Mailing address	Phone number	Email address
METHOD PREFERRED						
Email address	**75%**	50%	**79%**	**81%**	**74%**	**78%**
Phone number	**75%**	**75%**	53%	54%	**74%**	59%
Mailing address	**75%**	50%	42%	62%	48%	46%
Password	25%	25%	63%	35%	39%	41%
Email or text verification	0%	0%	37%	23%	16%	24%
PIN code	0%	25%	37%	19%	26%	24%
Phone call	0%	0%	11%	15%	10%	10%
Fingerprint recognition	0%	0%	11%	12%	13%	10%
Physical ID documents	0%	25%	5%	4%	3%	7%
Digital copy of ID documents	25%	25%	0%	4%	6%	7%
Facial recognition	25%	0%	0%	4%	0%	2%
Voice recognition	0%	0%	0%	0%	0%	0%

WHAT'S DRIVING

CONSUMER SATISFACTION?

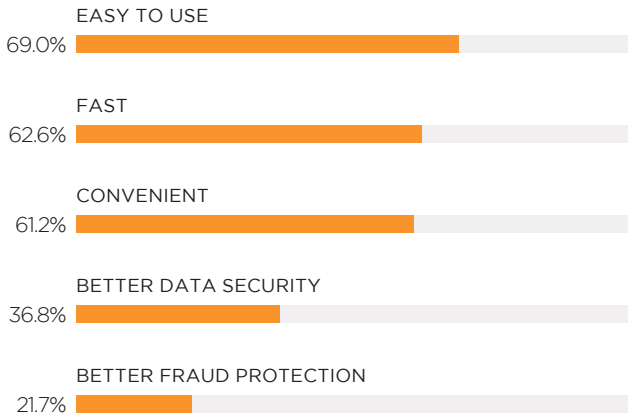
Offering consumers a seamless experience is the first step for merchants who want to keep up with competition, meaning authentication must be in the background as much as possible. Shoppers are satisfied with it for the same reasons involved in a physical transaction: it is quick, convenient and frictionless. Above all, they want their transactions to be easy.

Sixty-nine percent of consumers chose "ease of use" as the reason they're satisfied with their authentication processes, approximately one-third selected "data security" and more than 20 percent chose fraud protection. There are a few minor differences between users creating new accounts and those working with existing ones, but the key factors remain the same: Seventy-eight percent of those creating new accounts preferred to provide an email address, while 41 percent of those with existing accounts preferred passwords.

FIGURE 7:

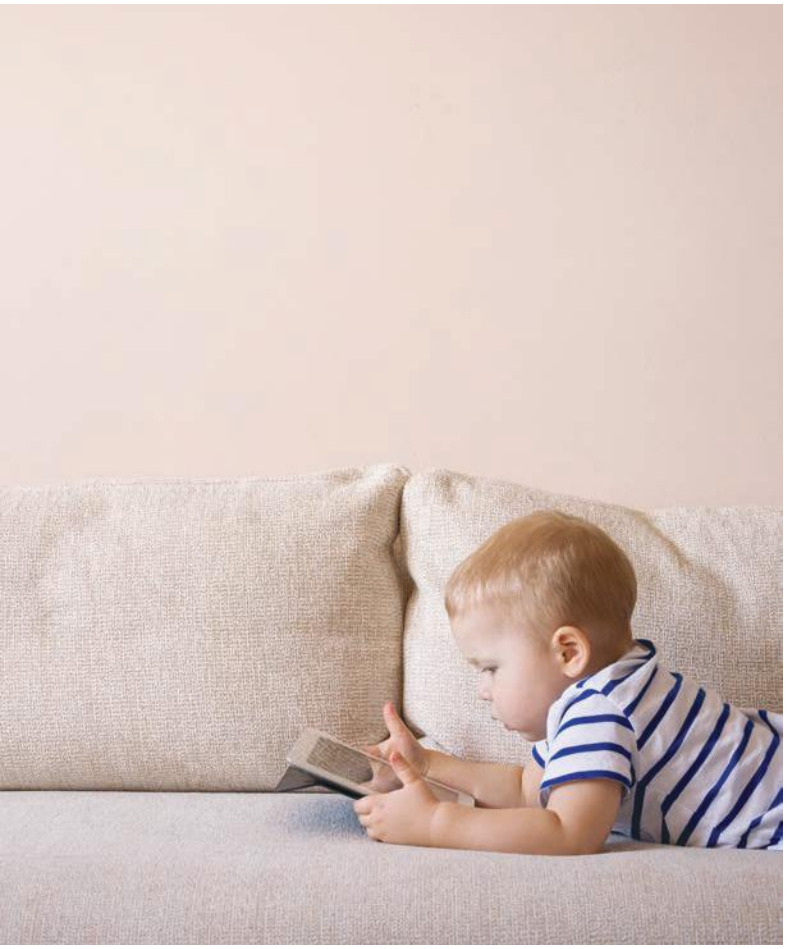
Top reasons consumers were satisfied with authentication methods

Consumers citing themselves as "very" or "extremely" satisfied with authentication methods



HOW AGE IMPACTS

USER SATISFACTION



We looked at gender, income and education levels, but the biggest differences we saw when it came to customer satisfaction could be attributed to age.

Consumers aged 55 or older are more worried about data security, while younger ones are more likely to be satisfied with faster authentication forms. Though consumers across all ages prefer email and passwords, the reasons for that preference differs in younger age groups.

TABLE 8:

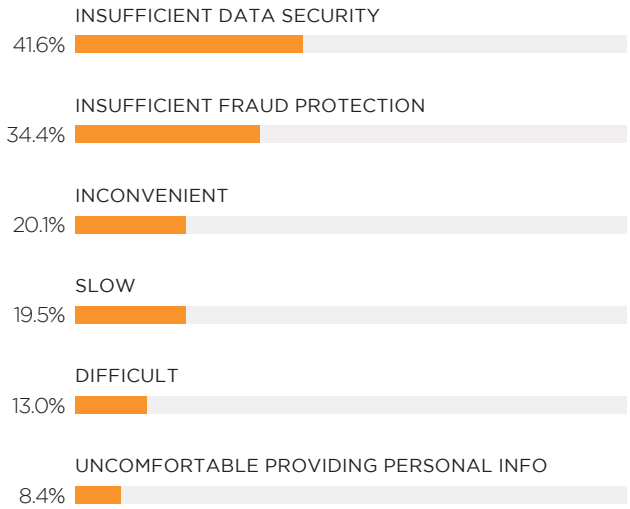
How do consumers authenticate and why do consumers prefer select authentication methods?
Consumers' preference and reason for an authentication method, by age

	18 – 34	35 – 54	55+
METHOD PREFERRED			
Email address	**55%**	45%	31%
Phone number	36%	21%	7%
Password	36%	**45%**	**51%**
Mailing address	34%	21%	2%
PIN code	24%	27%	20%
Email or text verification	21%	20%	26%
Digital copy of ID documents	18%	9%	3%
Physical ID documents	11%	7%	1%
Fingerprint recognition	10%	16%	8%
Phone call	7%	8%	4%
Voice recognition	6%	5%	3%
Facial recognition	3%	6%	6%
REASONS			
Convenient	**46%**	49%	**46%**
Better data security	37%	34%	43%
Better fraud protection	29%	33%	43%
Easy to use	45%	**50%**	42%
Fast	43%	40%	35%
Unobtrusive	10%	20%	19%

FIGURE 9:

Why consumers are unsatisfied with various authentication methods

Reasons for survey participants' dissatisfaction



CUSTOMERS WERE UNHAPPY WITH DATA SECURITY, **BUT 20 PERCENT** WERE ALSO UNSATISFIED WITH THEIR AUTHENTICATION AS INCONVENIENT OR SLOW.

Among the youngest customers, those aged 18 to 34, 43 percent chose speed compared to just 35 percent of those over 55. This younger group is also more likely to use mobile for their online shopping and authentication, and about twice as likely to prefer biometrics. Consumers over age 55 were much more likely to select data security as their top reason. Education and income had negligible effects here.

Why were customers left unsatisfied? In short, data security. For those who weren't satisfied with digital authentication methods, the biggest issue cited was whether their data was safe. Out of those who were dissatisfied, about 20 percentwere unhappy with the method's speed and convenience, respectively, while 42 percent with data security and 34 percent cited a lack of fraud protection.

Overall, approximately 20 percent of consumers choose "not very convenient" or "slow" as the top reason they were not satisfied. Even the 70 percent of those satisfied rated data security higher, though. When asked why they preferred an authentication method, approximately 38 percent chose data security.

As previously noted, consumers older than 35 are more concerned with security than younger consumers, and less likely to authenticate on a mobile phone or use biometric identification in eCommerce transactions. Most of them are also sticking to shopping online versus mobile.

MOBILE IS GROWING IN POPULARITY, BUT ISN'T AS

COMMONLY USED

Using a browser on a desktop or a laptop is the most common way consumers shop today, and nearly 64 percent of them typically authenticate themselves online during an eCommerce transaction.

That said, mobile is catching up. Nearly 32 percent of consumers reported using mobile to shop online. Among mobile shoppers, younger consumers, those between 25 and 34 years of age, reported being more comfortable using mobile for online shopping, making age a key distinction in terms of devices used to shop and thus, authenticate.

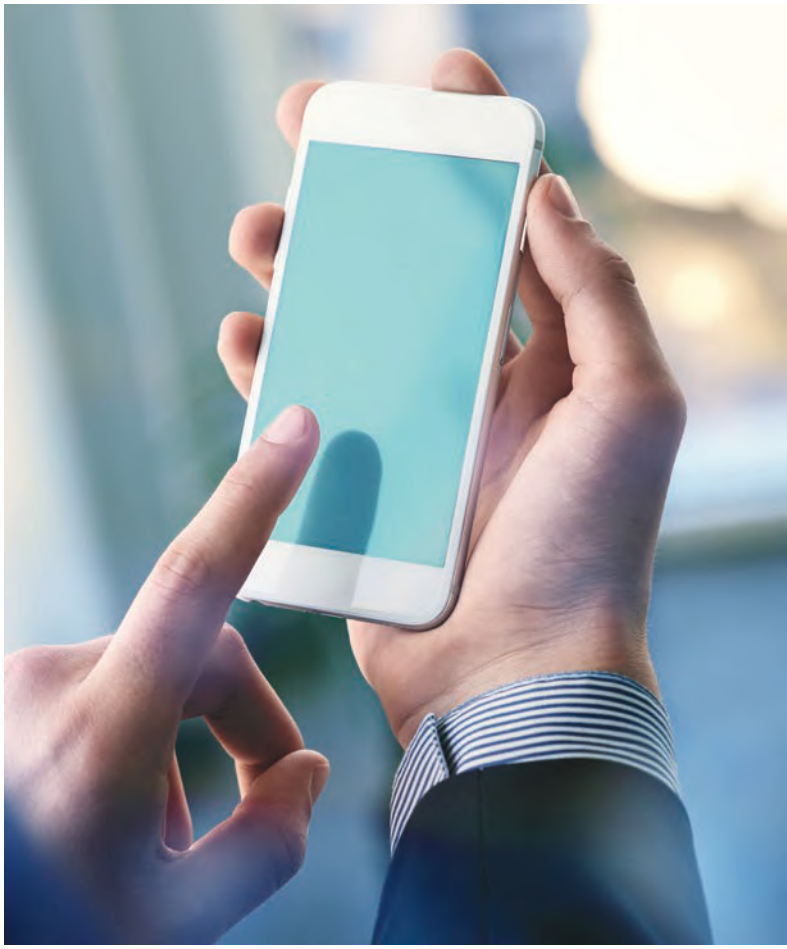
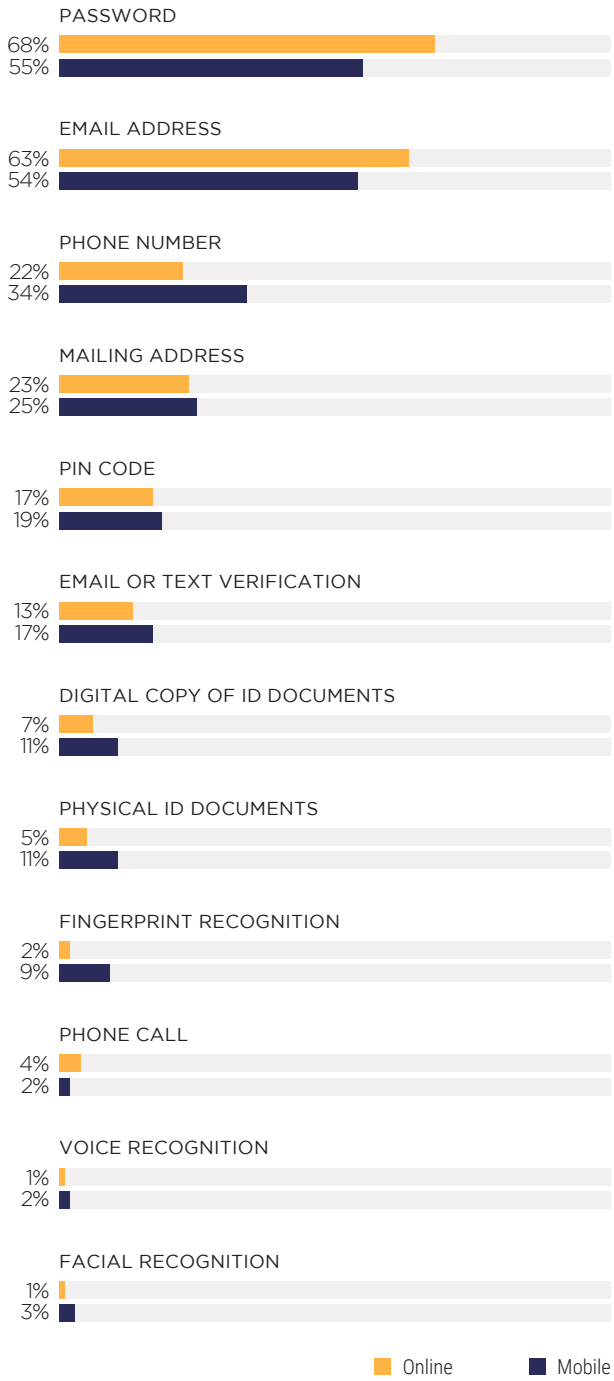


FIGURE 10:

How consumers are required to authenticate
Most popular consumer authentication methods, online and with a mobile device

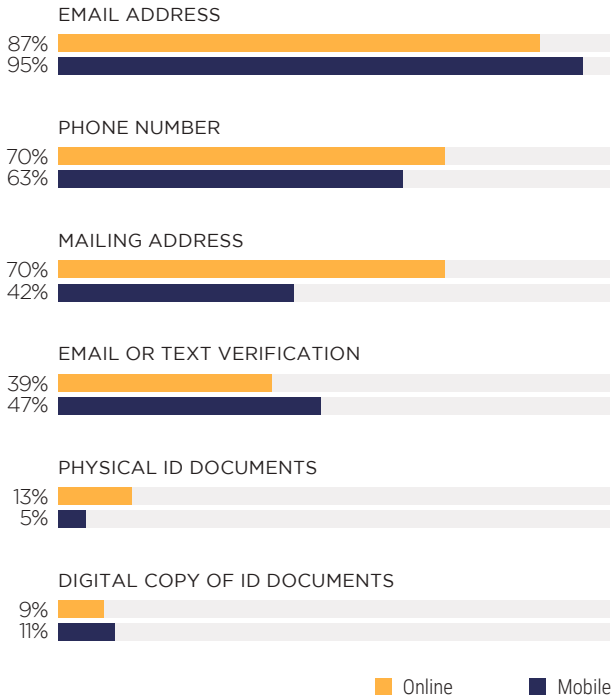


As one might expect, the most popular methods are email and password, regardless of the channel or longevity of account (new or existing).

Use of authentication methods tends to vary by channel, however. Consumers shopping via mobile are more often required to give a phone number (34 percent), compared to those in the online channel (22 percent).

FIGURE 11:

How consumers are required to authenticate new accounts
Methods required to create new accounts, by channel

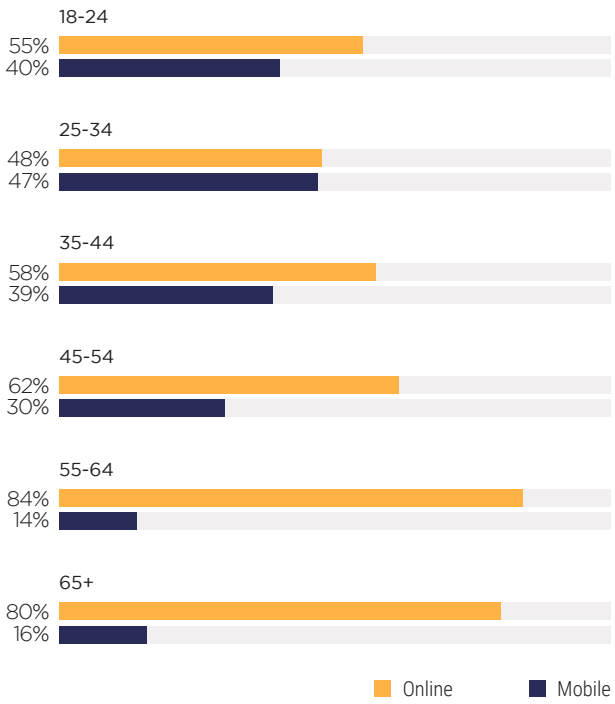


Once again, education, gender and income did not appear to influence the channels consumers use. As one might expect, younger users are much more likely to test out mobile shopping than older consumers. Older millennial users, those between 25 and 34, are most likely to choose mobile over online. That group was split almost 50/50: 47 percent used mobile to authenticate an eCommerce transaction and 48 percent used an online channel. The remaining percentage used a call center.

The online channel is still the more popular choice outside that age group. This could change as younger consumers gain more buying power and begin to rely on technologies like biometrics. Biometrics weren't particularly popular with consumers in either channel, but those shopping and authenticating with mobile seem more likely to try them.

FIGURE 12:

Channels consumers typically use
Online and mobile channel usage, by age



MORE THAN 50 PERCENT OF CUSTOMERS

PREFER TO CONFIRM THEIR IDENTITIES ONLINE WITH A PASSWORD.

FIGURE 13:

Methods consumers prefer
Top authentication methods for online and mobile, by channel

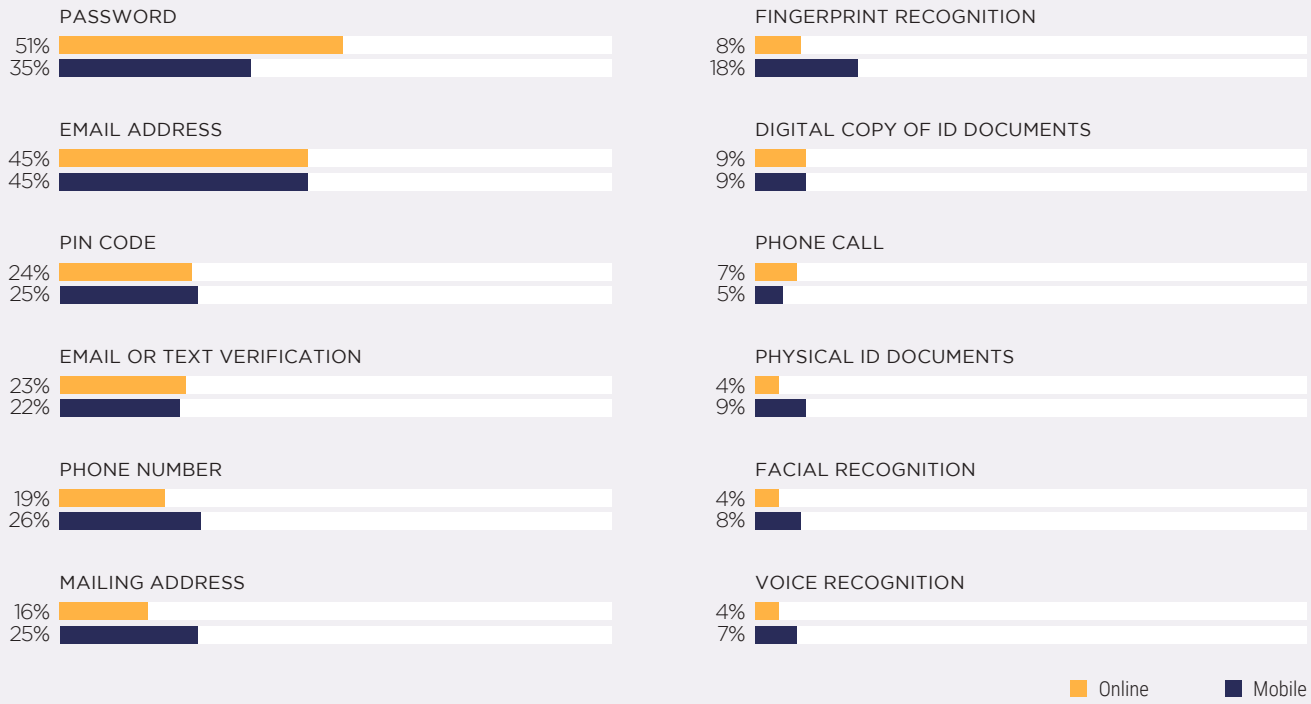
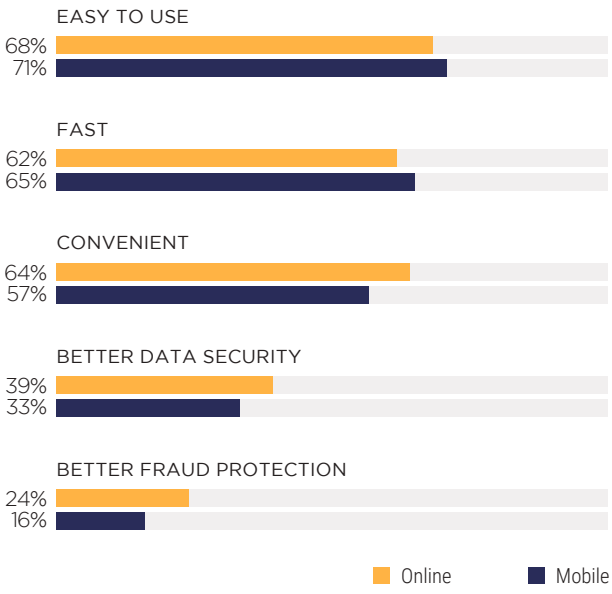


FIGURE 14:

Why consumers were satisfied with channels
Reasons for customer satisfaction, by channel



65 PERCENT

OF RESPONDENTS

CHOSE SPEED AS THE TOP REASON

THEY USED MOBILE TO

AUTHENTICATE THEIR IDENTITIES.

Consumers were satisfied with the online channel for their digital shopping because it's easy to use. Customers who authenticated via mobile thought the same: 68 percent of mobile users were satisfied because the channel was easy to use, compared to 71 percent of online users. . All are concerned with data security, and tend to think mobile is a less secure way to shop and authenticate than an online channel. Older consumers may be more likely to worry about security, but younger customers are more likely to shop via mobile. Those using mobile, regardless of age, were more worried about data security, according to our findings.

Mobile users were more satisfied with authentication speed than online users, however, with 65 percent citing this as their top reason compared to 62 percent of the latter. As mentioned, mobile users are more likely to be younger and to use biometrics to authenticate their digital transactions. Eight percent of them preferred facial biometrics, for example, compared to just 4 percent of those using the online channel.

Younger mobile users are also less satisfied with their data security. In fact, data security and speed are two of their top concerns when it comes to how they shop and authenticate. With an increasing number of users relying on their smartphones, mobile will likely soon become the top channel for eCommerce transactions. Biometrics will likely see more usage, too.

BIOMETRICS IN ECOMMERCE

Biometric technologies are positioned to become the most common customer authentication methods when shopping or using online services. This could lead to customer ID innovations across a variety of fields, particularly as more consumers begin to rely on their mobile devices.

Dozens of companies in both eCommerce and other industries are moving biometrics forward. Amazon is even exploring how the technology could impact delivery, testing a system in which couriers can place packages inside a home via unique biometric identifiers.[1]

Biometrics have captured the corporate and public eyes alike, and are sliding into physical store locations outside the U.S. as well as online purchases. The first store providing a way for users to pay via a fingerprint scanner recently launched in the U.K.[2]

Biometrics' potential future is clear, how fast it will arrive is less so. Some claim the technology will replace passwords, thanks to the popular assumption that consumers view passwords as clunky and cumbersome. Indeed, 86 percent of them are interested in biometrics-based payments, according to a 2018 Visa survey conducted.[3]

Online merchants have some work to do if consumers are going to get that chance, however. Biometric solutions are currently seldom required as an authentication method,

[1] Perala, Alex. Amazon adds biometric security to home unlocking app. Mobile ID World. 2018. https://mobileidworld.com/amazon-biometric-security-home-unlocking-app-903271/. Accessed September 2018.

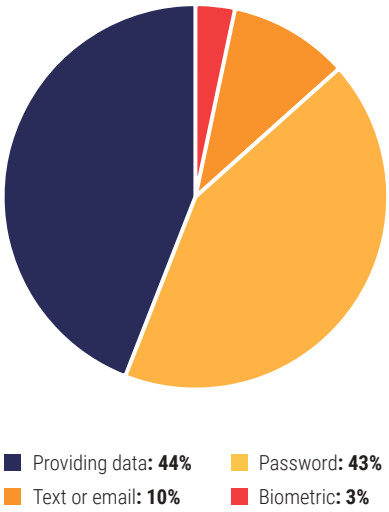
[2] Christie, Sophie. As shoppers start paying by fingerprint, what other changes like ahead for banking and spending? The Telegraph. 2018. https://www.telegraph.co.uk/money/future-of-money/shoppers-start-paying-fingerprint-changes-lie-ahead-banking/. Accessed September 2018.

[3] Chatzky, Jean. Biometrics are here: the crazy ways you're going to be paying in the future. NBC News. 2018. https://www.nbcnews.com/better/business/biometrics-are-here-crazy-ways-you-re-going-be-paying-ncna872336. Accessed September 2018.

FIGURE 15:

How customers were required to authenticate an account

Required account authentication, by biometrics, email, passwords and other data



ONLY 3 PERCENT

OF CUSTOMERS SAID THEY WERE "REQUIRED" TO PROVIDE BIOMETRICS FOR IDENTIFICATION.

especially for eCommerce sites. Just 3 percent of consumers surveyed by PYMNTS cited using them to authenticate an eCommerce purchase. Approximately 10 percent of that miniscule number preferred the method.

The good news is that these customers are highly satisfied with certain types of biometric authentication methods. The most popular appears to be fingerprints, which makes sense as mobile users are becoming more likely to unlock their phones with them.

Such identification for online shopping will depend on user adoption, so smartphone makers and online retailers will need to keep providing the technology. Some are forecasting that fingerprint scanning will sharply increase in usage by 2023, but others predict a possible dip as Apple and other providers move away from it.[4]

Still others, like Mastercard, are already making strides in increasing biometrics' popularity. The payment processor, with more than 600 million cards in circulation, announced in early 2018 that its users will be able to pay via biometrics by April 2019.[5] All businesses that accept Mastercard, online or otherwise, must also be ready to accept biometrics. Cooperation will be a must between mobile tech, card providers and Mastercard's bank network for this to happen.

[4] Author unknown. Fingerprint scanner tech to grow 500 percent in 2019. PYMNTS. 2018. https://www.pymnts.com/apple/2018/fingerprint-scanner-tech-biometric-mobile-payment-security/. Accessed September 2018.

[5] Author unknown. Biometric identification must be made available for all Mastercard users by April 2019. Mastercard. 2018. https://newsroom.mastercard.com/eu/press-releases/biometric-identification-must-be-made-available-for-all-mastercard-users-by-april-2019/. Accessed September 2018.

This works for bank cards and mobile phones, but Mastercard's approach makes it clear that mobile is going to be more popular for eCommerce and biometrics. Sixty-three percent of those who used the method did so on a mobile phone, according to PYMNTS' research.

Admittedly, it might be more difficult to use biometrics online simply because consumers lack the hardware. That it is limited by the number of devices equipped with the necessary tech isn't limited to eCommerce transactions.

Research shows U.S. consumers will also find it challenging to use biometrics for in-store purchases, largely because it relies on contactless technology, which is only available at about 1 million physical U.S. stores. Emerging offerings that don't rely on contactless, such as voice, might be a better fit for eCommerce once they become more widely available.[6]

Security is one of the biggest draws in using biometrics. It is being used by a growing group of U.S. consumers, a number predicted to increase from the 459 million to 1.5 billion by 2023.[7]

Biometric identification's future in eCommerce is a little murkier, though PYMNTS' research supports the idea that consumers see it as a more secure way to authenticate. Most preferred biometrics' protections against fraud, cited by 58 percent of those who prefer facial biometrics. Fifty-two percent of those who preferred voice authentication said the same.

The trendsetters using biometrics for online shopping are very satisfied with the technology, however. Growth in use will rely on embracing new user channels and responding quickly to new customer needs, especially as more consumers to digital shopping and purchases. Newer channels and methods must better protect their data as well as provide quicker eCommerce authentications and transactions, meaning biometrics will likely become more widely used.

[6] Chatzky, Jean. Biometrics are here: the crazy ways you're going to be paying in the future. NBC News. 2018. https://www.nbcnews.com/better/business/biometrics-are-here-crazy-ways-you-re-going-be-paying-ncna872336. Accessed September 2018.

[7] Author unknown. 1.5B mobile users to rely on biometrics security by 2023. PYMNTS. 2018. https://www.pymnts.com/authentication/2018/biometrics-smartphone-mobile-security-fingerprint-sensors/. Accessed September 2018.

CONCLUSION

Consumers are largely satisfied with the eCommerce authentication methods they're required to use, namely email addresses and passwords. Though mobile is rising, the online channel is still the most popular for digital identification.

Younger users are moving toward channels with faster authentication, but data security remains the reason consumers were not pleased with it. Despite the relative rarity of biometrics, it appears the stronger data security it provides will be key in continued adoption.

Regardless of age, gender, education and income, consumers prefer authentication tools that are quick, easy and convenient. Merchants in the eCommerce industry will need to innovate how they authenticate customers with these goals in mind.

METHODOLOGY

We conducted a survey of 1,822 respondents on whether they were required to provide a form of digital identity when authenticating an account or creating a new one in financial services, eCommerce and healthcare. They were asked if they used online, mobile or call center channels, which methods were required and if they were satisfied. Finally, we asked which methods respondents preferred and the reasons for these preferences.

The survey was constructed to reflect general U.S. population trends with respect to gender, age, education and employment. Fifty-five percent (1,009 respondents) completed the survey in its entirety. We only considered these 1,009 respondents in our analysis. We excluded respondents not required to authenticate themselves in the areas detailed above.

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 companies in payments share relevant information about the initiatives that make news and shape the future of this dynamic sector. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovations at the cutting edge of this new world.

Socure

Socure is the leader in high-assurance digital identity verification. The company's predictive analytics platform applies artificial intelligence and machine learning to trusted online/offline sources including email, phone, address, IP address, social media and traditional GLBA/DPPA data to authenticate identities in real-time. The Socure ID+ platform reduces fraud by up to 90 percent, lowers manual review/knowledge-based authentication (KBA) rates by as much as 80 percent, and automates Customer Identification Program (CIP) for over 90 percent of the U.S. adult population.
For more information visit www.socure.com.

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

disclaimer

The Digital Identity Lifestyle Capsule 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.