Socure

PYMNTS.com

DIGITAL IDENTITY

LIFESTYLE

CAPSULED

73%

Share of financial services consumers who are "very" or "extremely" satisfied with their authentication options

62%

Portion of eCommerce consumers who reported using online passwords for authentication

Authentication Satisfaction Edition | March 2019

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

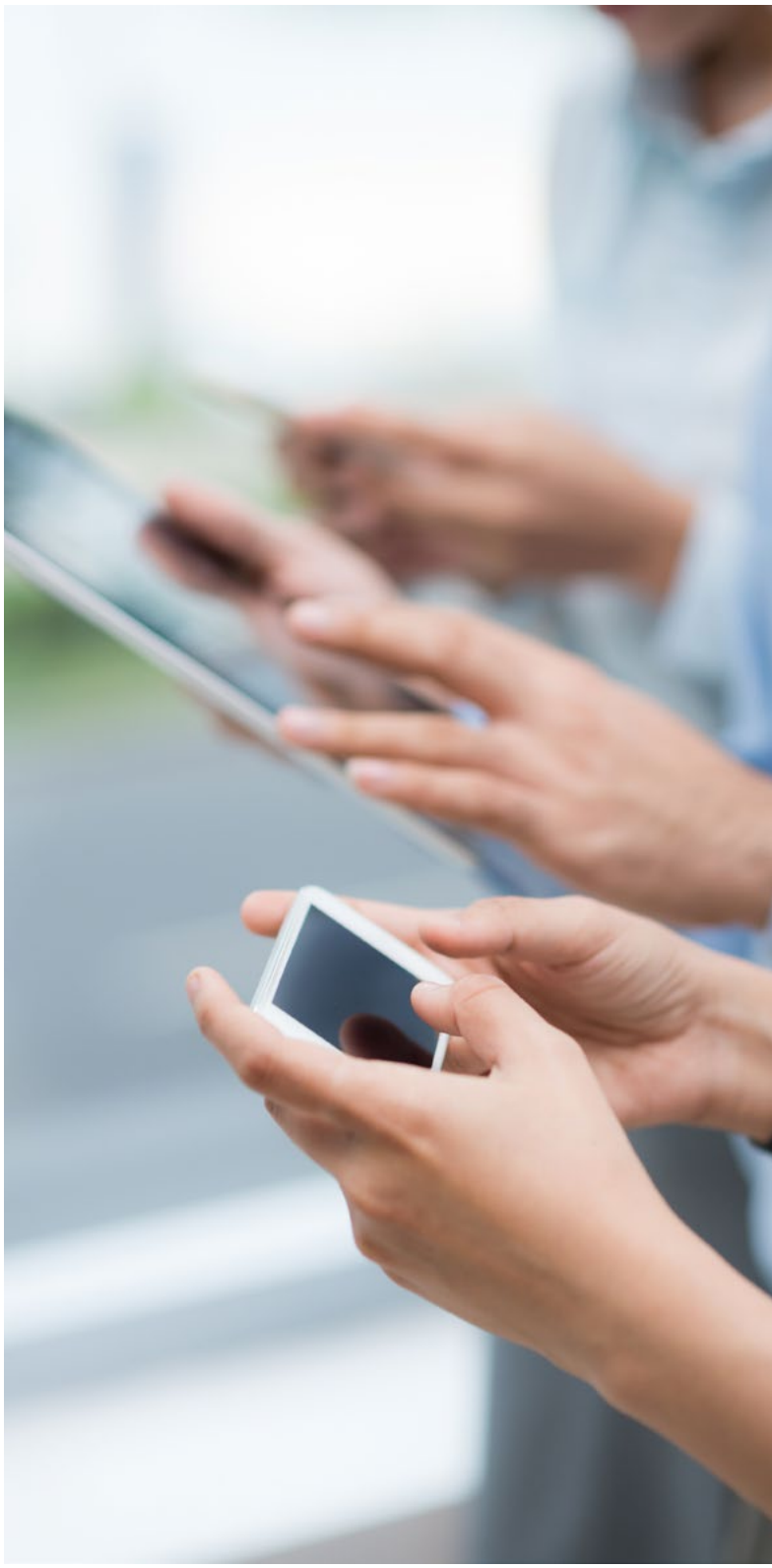
EXECUTIVE SUMMARY

EASE OF USE, CONVENIENCE WEIGH HEAVILY ON **AUTHENTICATION PREFERENCES**

Time is money for most consumers. Whether they're making ATM withdrawals, buying shoes online or going in for medical checkups, consumers want to complete transactions as smoothly and swiftly as possible – and without going to great lengths to confirm their identities.

But, regardless of the sectors with which they interact – eCommerce, financial services or healthcare – consumers need more than speedy authentication: They also want assurances that such businesses are safely and appropriately handling their personal information.

Companies across these industries must work to gain consumers' trust by striking a balance between seamlessness and security. Too-lax authentication processes could leave them worried that anyone could access and misuse their information. On the other hand, overly stringent options create frictions that ultimately deter consumers' interest in pursuing long-term relationships.



Certain authentication practices stand out as more favorable than others, however, like being asked for a phone number or email address. PYMNTS has followed eCommerce, financial services and healthcare firms' verification practices since September 2018. Each edition of the Digital Identity Lifestyle Capsule series, a Socure collaboration, measures customers' satisfaction with these institutions' authentication and fraud protection methods.

This latest edition compares consumers' contentment with authentication across all three verticals. The results are based on survey responses from more than 1,009 respondents, breaking down the methods consumers were asked to use by both industry and satisfaction.

Certain authentication methods proved more popular than others. Most consumers were asked to authenticate using passwords and email addresses, though those for eCommerce were particularly more likely to submit the latter than consumers from the other two. A smaller share was asked to provide digital copies of official identification or present said documents at physical locations.

Overall, consumers largely reported being "very" or "extremely" satisfied with most required authentication methods. Online passwords were top-of-the-list across all three markets, but other methods were more popular depending on the industry. Email addresses were preferred by eCommerce consumers more than those for financial services or healthcare, for example.

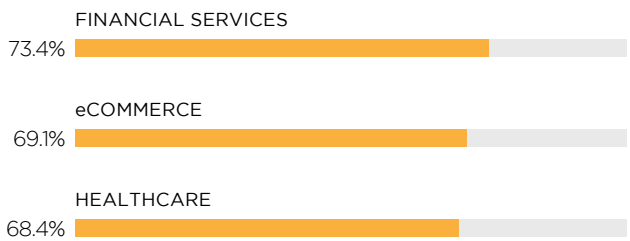
When compared side by side, financial services consumers expressed greater satisfaction with their authentication methods than those for eCommerce and healthcare. Nearly three-quarters (73.4 percent) were either "very" or "extremely" satisfied with their authentication options, better than the below-70-percent rates reported by the other two industries' consumers.

Most consumers pointed to financial services authentication methods' ease of use as a reason for their satisfaction. A higher share of those for healthcare expressed greater satisfaction with convenience — such as being asked to provide email addresses, passwords or phone numbers — and eCommerce consumers pointed to speed. Additional consumer satisfaction details will be outlined throughout this report.

This edition of the Digital Identity Lifestyle Capsule highlights how consumers authenticate their identities across these markets and the factors making some methods more appealing than others. It also includes an in-depth analysis of what sets the most satisfied apart from the least.

FIGURE 1:

Percentage of very or extremely satisfied users
Consumer satisfaction across the eCommerce, financial services and healthcare markets



“

68.4%

OF HEALTHCARE CONSUMERS

ARE **“VERY”** OR **“EXTREMELY”**

SATISFIED WITH THEIR

AUTHENTICATION OPTIONS

”

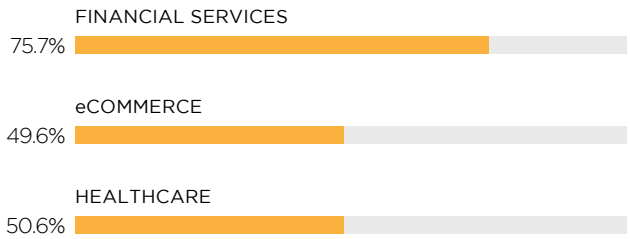
HOW CONSUMERS

AUTHENTICATE

Certain authentication methods were more widely used than others, according to our findings. Most eCommerce, financial services and healthcare consumers reported being asked to provide passwords and email addresses to verify their identities.

FIGURE 2:

Sample's authentication requirements
Frequency of implemented authentication practices by market



The financial services market appears to have the most stringent authentication requirements, as 75.7 percent of respondents reported having to confirm their identities when interacting with providers. This is a considerably higher figure than those found in the eCommerce and healthcare markets, indicating financial services businesses require comparatively more rigorous authentication procedures.

As for the channels through which consumers confirmed their identities, the highest share did so online. This method was the most widely used across all markets, though eCommerce and healthcare beat financial services at 63.8 percent and 63.4 percent, respectively. Just 59.7 percent of financial services consumers went online to confirm their identities.

FINANCIAL SERVICES

TD Bank provides financial services to approximately 9 million customers and is listed among the top 10 banks operating in the U.S. Serving a large consumer base requires it to offer a wide range of authentication options. Senior vice president and head of digital platforms Lino Catana outlines those TD Bank has employed, and explains how the FI uses them to adjust its digital user experiences.

"For online and mobile, customers can log in with their usernames and passwords. We've eliminated security questions and are instead using one-time security codes to authenticate users. With single-use security codes, we send a five-digit code to the phone number we have on file. Customers are then instructed to enter that code to confirm their identities. Single-use security codes eliminate the need to remember multiple security questions.

For mobile, we have Touch ID fingerprint log-in and Face ID facial-recognition authentication for iOS and fingerprint authentication for Android. This eliminates the need to remember usernames and passwords, as customers can use biometrics to [access their accounts].

If calling our contact center — which is open [24/7 year-round] — we've implemented TD VoicePrint, which analyzes more than 100 characteristics of a caller's voice to confirm [his or her] identity. It only takes a few minutes for a customer to enroll in TD VoicePrint during the course of a normal conversation.

Speed and convenience are important for many customers, so we find that the quicker authentication methods — biometric, VoicePrint — seem to be more appealing. However, for us, modern convenience means offering customers personalized experiences that feel customized to each individual's needs and preferences.

We regularly engage with our customers to ensure we're designing to meet their needs, and will continue to make significant investments in our online and mobile channels to make banking with TD even more convenient."

LINO CATANA,
senior vice president and head of digital platforms, TD Bank

PASSWORDS, EMAILS RISE TO THE TOP

OF THE AUTHENTICATION CROP

Regardless of industry, consumers clearly preferred personally identifiable information (PII) when authenticating their identities. Passwords and email addresses were the clear winners compared to other methods, possibly because consumers have become used to providing such information over the years.

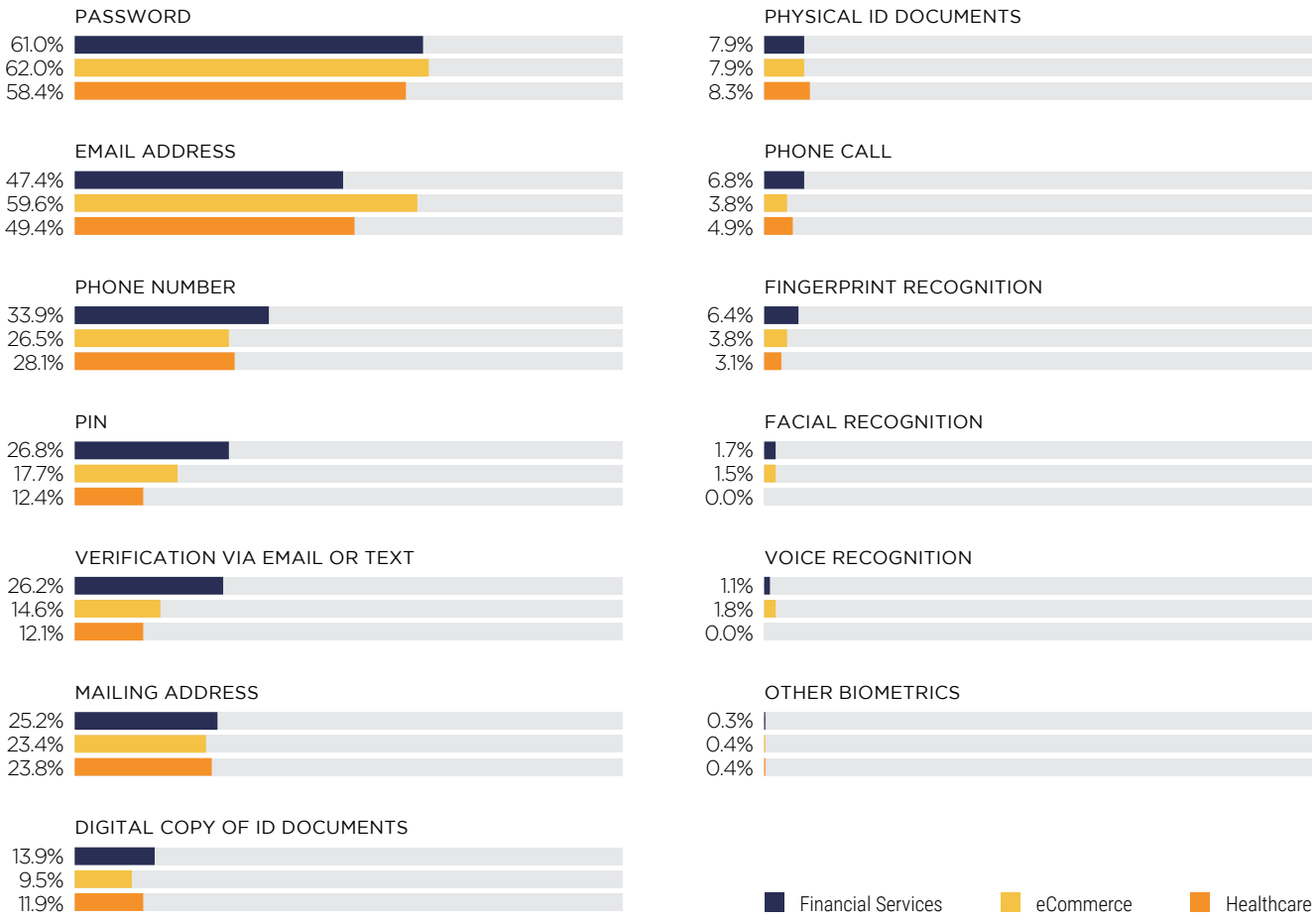
This is especially true for eCommerce consumers. This group reported the highest password usage at 62.0 percent, followed by 61.0 percent of financial services consumers and 58.4 percent of those for healthcare. At 59.6 percent, eCommerce users are much more likely to be asked for email addresses than others, however, and just 49.4 percent of healthcare and 47.4 percent of financial services consumers said the same.

In addition to providing online passwords and email addresses, financial services

FIGURE 3:

Identity confirmation methods

Most commonly requested PII authentication entries, by type and market



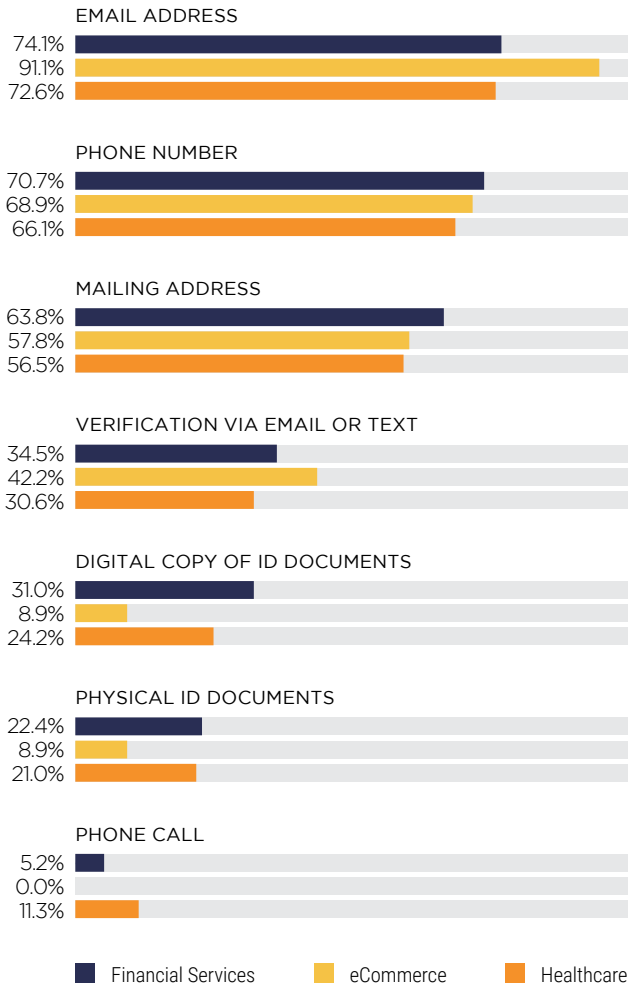
consumers were also more likely to submit other authentication types. This includes phone numbers at 33.9 percent, personal identification numbers (PINs) at 26.8 percent and confirmation emails and texts at 26.2 percent, all of which were required in financial services more often than in eCommerce or healthcare. The other two markets saw 17.7 percent and 12.4 percent for PINs, respectively, and 14.6 percent and 12.1 percent, respectively, for emails and texts.

Authenticating existing accounts is not the only scenario in which email addresses and phone numbers are preferred. They are also on top when confirming consumers' identities to create new accounts, a process known as verification.

FIGURE 4:

Methods required to create new accounts

Portion of consumers asked to provide personal data, by method and market



At 91.1 percent, email is the most-used identity verification method for eCommerce consumers signing up for new online accounts. This figure is considerably higher than those for financial services (74.1 percent) and healthcare consumers (72.6 percent), but is of little surprise: eCommerce is also more likely to rely on email to communicate about recent transactions.

Phone numbers ranked as second-most required method for account creation, especially for financial services consumers. More than 70 percent of financial services consumers reported being asked for phone numbers to confirm their identities when opening accounts. Prevalence was slightly lower for eCommerce and healthcare consumers at 68.9 percent and 66.1 percent, respectively.

The financial services market was also more likely to ask for home addresses than those for eCommerce or healthcare. Approximately 63.8 percent of its consumers reported being asked for home addresses when creating accounts, a share considerably higher than the 57.8 percent of eCommerce and 56.5 percent of healthcare users who said the same.

These findings indicate that certain PII lead the pack in existing account verification, regardless of industry. They also indicate that financial services consumers are more likely to be asked for additional authentication methods — including phone numbers, PINs, email and text response requests and home addresses — than other consumers, though.

This range of options is important for financial services, which appears to be the most engaged of the three observed markets based on Figure 1. If financial services is more widely used, a range of authentication methods is likely to contribute to consumers' overall satisfaction.

Email addresses stand out as more popular for initial verification in account creation, as a near-majority of eCommerce consumers reported being asked to provide theirs when first signing up. Phone numbers and home addresses show similar usage levels across all industries. Fewer consumers were asked to respond to emails or texts, provide digital or physical documentation or to receive phone calls for initial verification. This low usage pattern suggests such options could negatively affect their initial user experiences and contribute to broader dissatisfaction.

91.1%

OF eCOMMERCE CONSUMERS

WERE REQUIRED TO **PROVIDE EMAIL ADDRESSES**

WHEN SIGNING UP FOR AN ONLINE ACCOUNT

SATISFACTION

Online passwords are the most commonly used authentication method, as well as the most preferred across all customer types. Consumers in all three markets expressed the highest satisfaction levels with providing online passwords, regardless of whether they were asked for one. Healthcare consumers led with 45.2 percent, followed closely by those for eCommerce (44.2 percent) and financial services (41.0 percent).

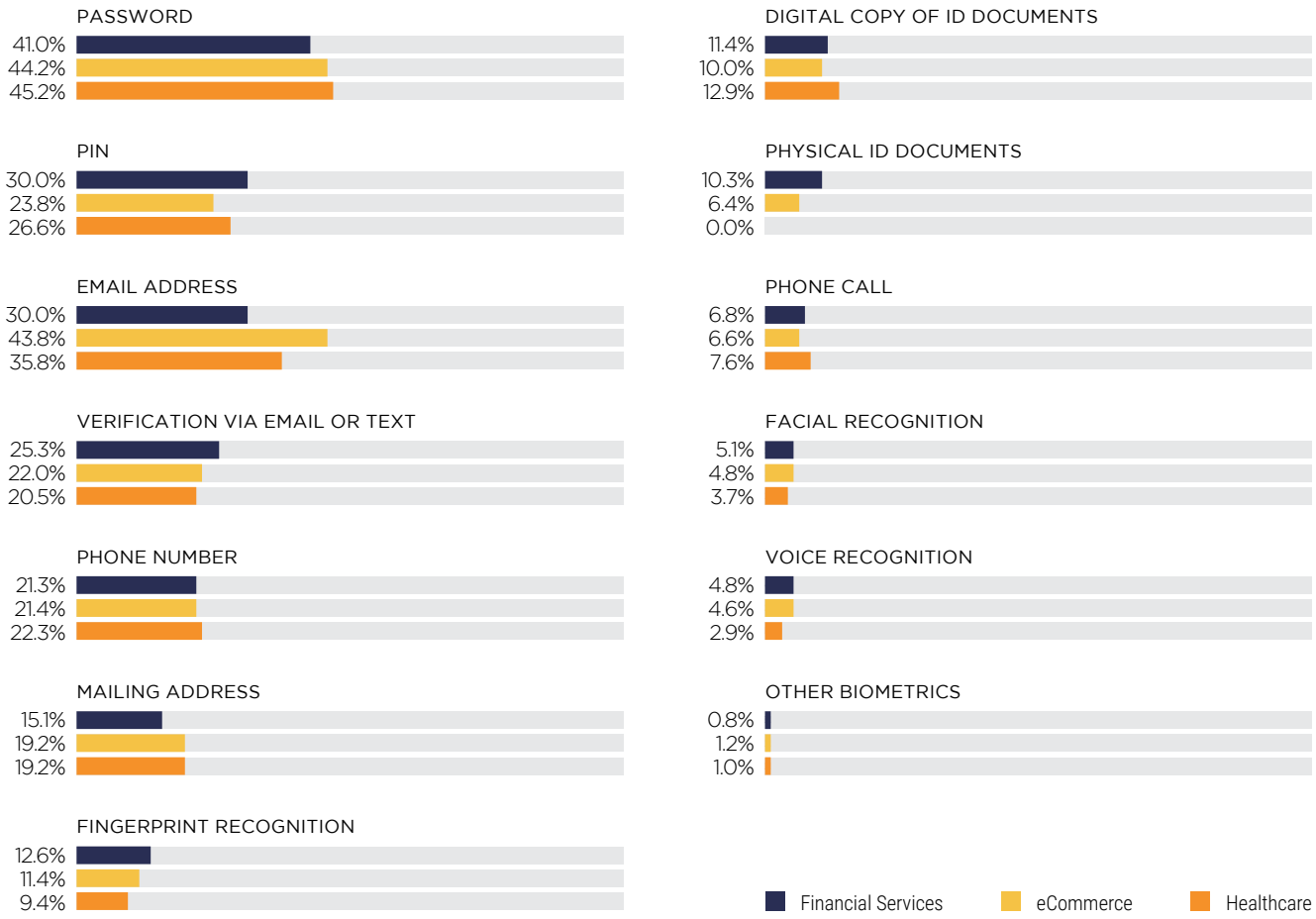
PINs were also popular, though there were clear satisfaction gaps. Thirty percent of financial services consumers were likely to prefer PINs, as were 26.6 percent of those for healthcare and 23.8 percent for eCommerce.

Email addresses are overwhelmingly preferred by eCommerce consumers, however, cited by nearly 44.0 percent as their method of choice. This is

FIGURE 5:

Methods preferred during account creation

How consumers rated online passwords, PINs, email addresses for verification



considerably higher than healthcare and financial services consumers' preferences at 35.8 percent and 30.0 percent, respectively.

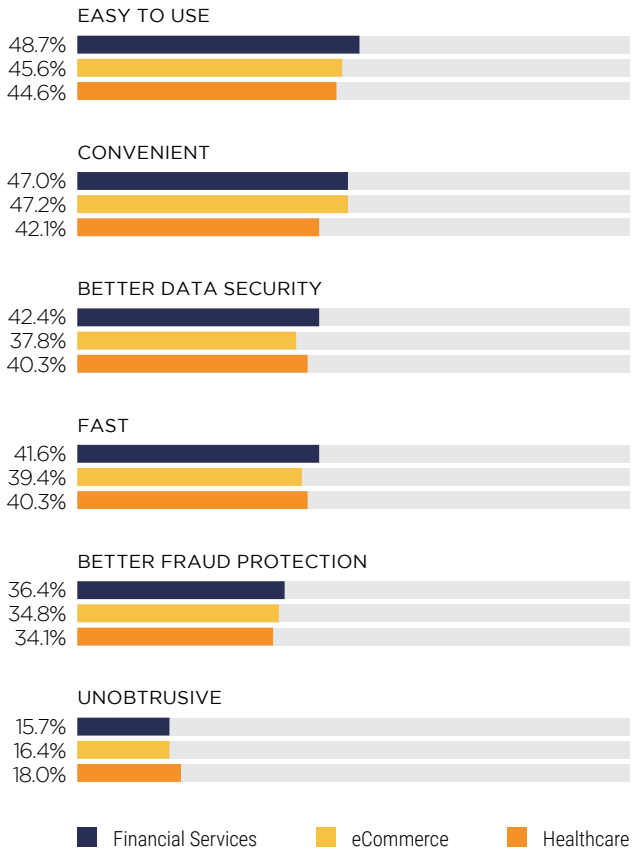
It's also worth noting that financial services consumers expressed higher satisfaction with a larger number of authentication methods. They were also more likely to prefer some of the less-popular options, including responding to text messages or emails, providing identification documents at physical locations and certain biometric solutions.

Why do consumers prefer these methods? Ease of use was appealing for a significant share across all three markets, identified by nearly half of our respondents. They also appreciated an authentication method's convenience.

FIGURE 6:

Reasons for preferring select methods during account creation

How ease of use, convenience, data security and speed affect consumers' preferences



Several satisfaction gaps can be seen in our markets of interest, however. eCommerce consumers were less likely to be satisfied with their preferred authentication methods' data security, for example, with 37.8 percent expressing satisfaction compared to 40.3 percent of healthcare and 42.4 percent of financial services consumers.

Meanwhile, healthcare consumers were less satisfied with convenience, facing a roughly five-point percentage gap compared to those for eCommerce and financial services. Those totals came out to 42.1 percent, 47.2 percent and 47.0 percent, respectively, indicating consumers already have certain authentication preferences — regardless of whether businesses choose to use them. Select methods have more appeal in certain markets, though.

Just about anything can be purchased or rented in the eCommerce space. Even maritime vessels — from kayaks to catamarans and yachts — can be reserved with just a few taps on a smartphone. Platforms like Boatsetter enable owners to list their vessels for rent and users to borrow said boats for their outings, but encouraging trust among the parties is no easy task — especially when they rarely meet in person. Julien Geffriaud, Boatsetter's chief growth officer, discusses how the boatsharing platform uses social media for authentication, and how the system offers smoother onboarding to more easily create trust among participating users.

"We use email, Google and Facebook for authentication. The purpose of using Google on our site is to get an email approved. So, if you sign up using a mobile phone, you're going to receive an email and will be asked to verify your email address. With Google and Facebook, the email address has already been recognized in the past, which allows us to skip a step.

That's easier because users do not have to fill out a form... You don't have to fill out a form, go to your email, click on a link and then return to the site. Google and Facebook [also] allow users to log back in without having to remember their passwords.

Consumers want convenience and a quick and easy sign-up [process]. They also want maintainability — the ability for the app to "remember" their password or social log-in so that future authentication is seamless — [and] also want security and for the site to use industry practices to keep their account information private. Speed is also part of the process.

For us, security is extremely important to protect all our users' data, whether it's the owner, the renter or even our captains. We have a lot of different users and a lot of data that needs to be protected, so authentication is very strict in that respect. Ease of use is extremely important as well, because we are an online product and a marketplace. We have to make sure the maximum number of users that come to our platform convert. So, the more flexibility and ease of use we can add to the process to reduce the number of steps, the better it is for them — and for us."

JULIEN GEFFRIAUD,
chief growth officer at Boatsetter

PREFERENCES

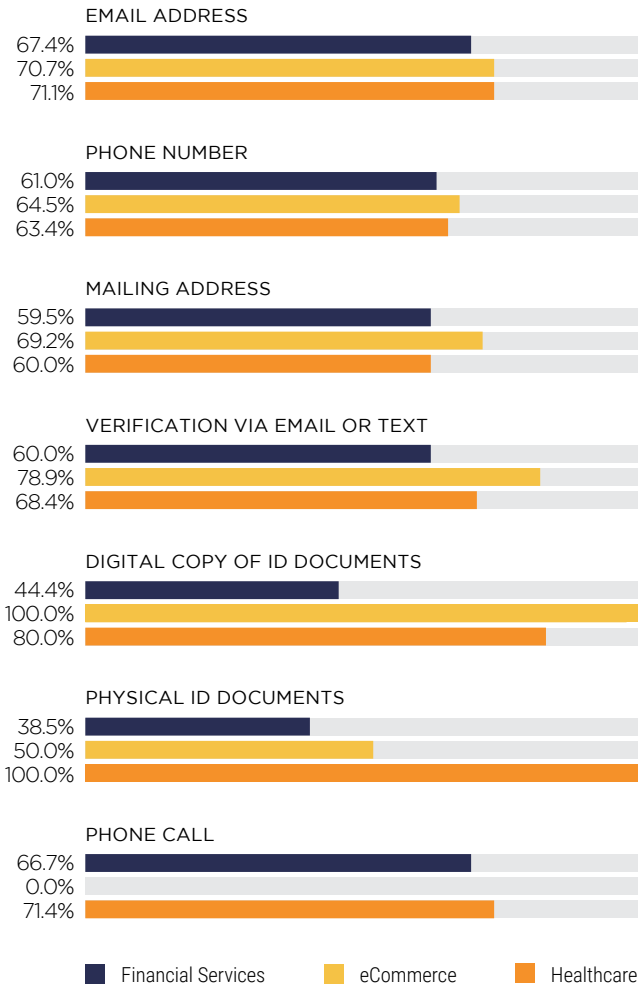
Consumers' satisfaction also varies depending on the authentication methods required to verify identities when creating new accounts or authenticate existing ones.

eCommerce consumers were largely satisfied with most of the required methods to initially verify their identities for new accounts. Among eCommerce consumers who responded to emails or texts to create a new account, 78.9 percent were satisfied with the requirement. This is a higher rate of satisfaction than the share of eCommerce consumers who were required to provide email addresses (70.7 percent), phone numbers (64.5 percent) or home addresses (69.2 percent). Meanwhile, 100 percent of eCommerce consumers who were required to submit digital copies of identification documents when creating accounts said they were satisfied with the requirement.

FIGURE 7:

Satisfaction with method used to create new accounts

Verification methods preferred by very or extremely satisfied users, by method and market



Financial services and healthcare consumers were also satisfied with available verification methods. Those for healthcare expressed the highest satisfaction with submitting identification documents at physical locations, reported by 100 percent compared to 50.0 percent and 38.5 percent for eCommerce and financial services consumers, respectively. The latter preferred to provide email addresses or receive calls.

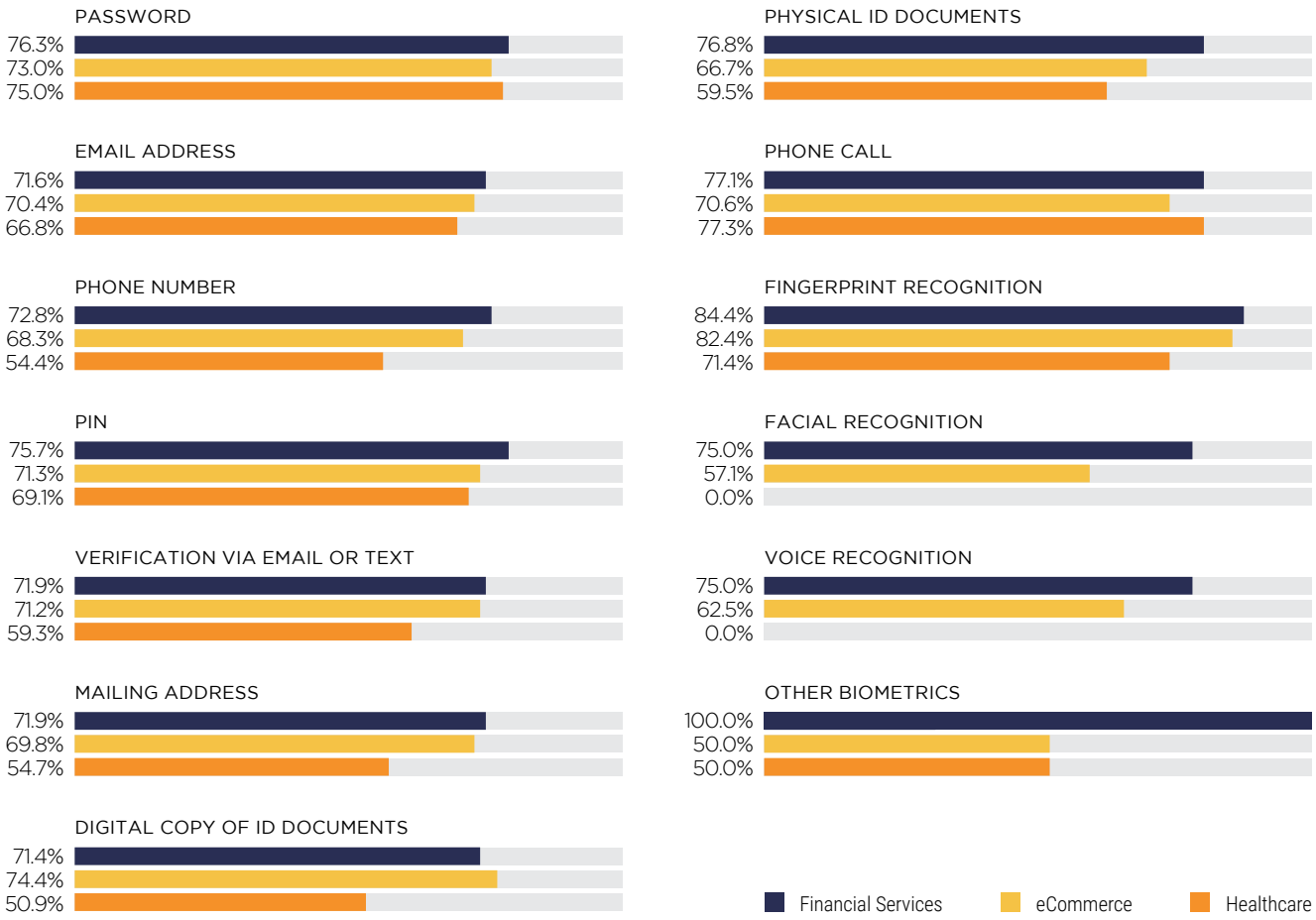
Consumers seemed highly satisfied with the methods available to authenticate existing accounts, too, like online passwords, email addresses, phone numbers, PINs or responding to texts or emails. Those for financial services appeared to be more satisfied with most offerings.

There appear to be notable authentication satisfaction gaps among healthcare consumers, however. This group was considerably less pleased with using phone numbers, responding to emails or texts and providing digital copies of identification documents than its eCommerce or financial services counterparts, for example. Financial services consumers were more satisfied with biometric-based authentications — fingerprints, facial recognition and voice recognition — though, which could indicate biometrics are more widely used in this market than in the others.

FIGURE 8:

Consumers' satisfaction with methods used to authenticate existing accounts

Consumers' authentication method preferences, by method and market



High satisfaction levels among consumers verifying their identities during new account creation could explain why methods like email addresses and phone numbers are so widely used across all three markets. Overall satisfaction is also high among the authentication methods used for existing accounts, but healthcare consumers appear satisfied with only a few of the methods provided. This trend could indicate they are less likely to embrace some methods over others.

BIOMETRICS HAVE ROOM

FOR GROWTH

Consumers reported single-digit usage of biometric authentication options like fingerprints, facial recognition and voice recognition. Fingerprints saw the highest, with 6.4 percent of financial services consumers reporting being asked to supply theirs to confirm their identities. This is approximately double the rates seen in the healthcare (3.1 percent) and eCommerce (3.8 percent) markets.

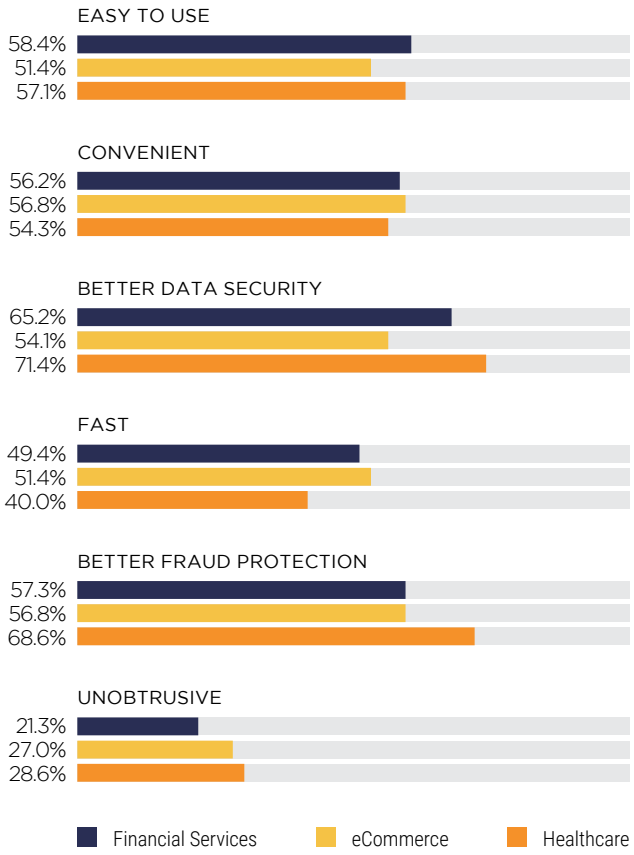
Such low usage indicates the solutions are so far not as widely embraced by as other methods. Consumers could be asked to use them more often as they become increasingly prevalent in identity verification and authentication, however.

Biometrics saw lower usage than other methods across all markets. The technology is still emerging as an authentication method but is preferred, to a greater extent, by financial services consumers. Even users in other markets expressed various reasons for preferring biometric

FIGURE 9:

Consumers' reasons for preferring biometrics

Why consumers choose select biometric authentication offerings, by reason and market



authentication, particularly pointing to potential usage growth in healthcare. A significant share preferred biometrics because it was convenient and easy to use, and an even higher share of healthcare consumers identified data security and fraud protection.

Biometrics was also preferred by eCommerce consumers, many of whom cited its speed. This market was more likely to prefer biometric authentication than the other two.

Financial services currently appear to be leading biometric adoption, but the technology might see greater adoption in healthcare and eCommerce. It could provide the data security and fraud protection consumers seek for their personal health information, for example, and eCommerce shoppers could use it to more quickly authenticate their identities and complete their online orders. Adopting biometrics could also boost consumers' overall satisfaction rates, a metric in which the financial services market is currently holding a lead.

HEALTHCARE

Recent smartphone technology developments enable patients to pay healthcare bills, consult physicians and book appointments from their smartphones. Among the players working toward that goal is digital healthcare network Carbon Health, which enables users to take greater control over their personal health. Improved digital access comes with greater data security and privacy concerns, however. Carbon Health CEO Eren Bali explains how his company balances smooth authentication with addressing patients' anxieties.

"At Carbon Health, patients are required to provide a verified phone number during the sign-up process. When patients use the Carbon Health app on new devices, they can use their email addresses and passwords to authenticate their accounts. For existing devices, they can unlock Carbon Health with native authentication options like Face ID or Touch ID. We support two-factor authentication for patients, but it's optional at this point. The authentication requirements are stricter on the patient web app since browsers don't provide the same level of protection as native mobile apps.

We see two very distinct customer segments when it comes to authentication preferences. Some patients want to log in once on their devices and never have to log in again, [and] unlocking the app with Face ID or Touch ID is perfect for this scenario. Patients would be choosing to opt out of some HIPAA restrictions if they opt for this.

The other segment of customers is more sensitive to privacy: They log out after each session and want to keep things as strict as possible.

For us at Carbon Health, an additional consideration is that sometimes patients want to be able to access care as soon as possible and we can't block their accounts for too long if they forget their passwords or if they're unable to do two-factor authentication. As a result, we had to build a tiered authentication system [through which] we sometimes allowed patients to book appointments without the full authentication requirements, but they weren't able to access their medical records, messages, profile, etc. When they visit the clinic, we check their government IDs — so the methodology works."

EREN BALI,
CEO of Carbon Health

DEEP DIVE

SATISFIED VERSUS

DISSATISFIED USERS

Consumers expressed wide satisfaction ranges when it came to required authentication methods. Reasons for satisfaction also varied by market. The following Deep Dive explores the reasons that make a big difference when addressing consumer satisfaction gaps.

Password requirements set most satisfied consumers apart from the rest of the sample, as those who were satisfied reported being required to provide one to access services. The trend held across all markets, although passwords were more common in eCommerce and financial services at 71.2 percent for each. That rate came in at 68.7 percent for healthcare consumers.

The highest share of dissatisfied customers reported being required to provide PII data as a means of authentication, a process that was most common in the healthcare

FIGURE 10:

Satisfied users' required authentication methods
Percentage of satisfied respondents that were required these authentication methods, by type and market

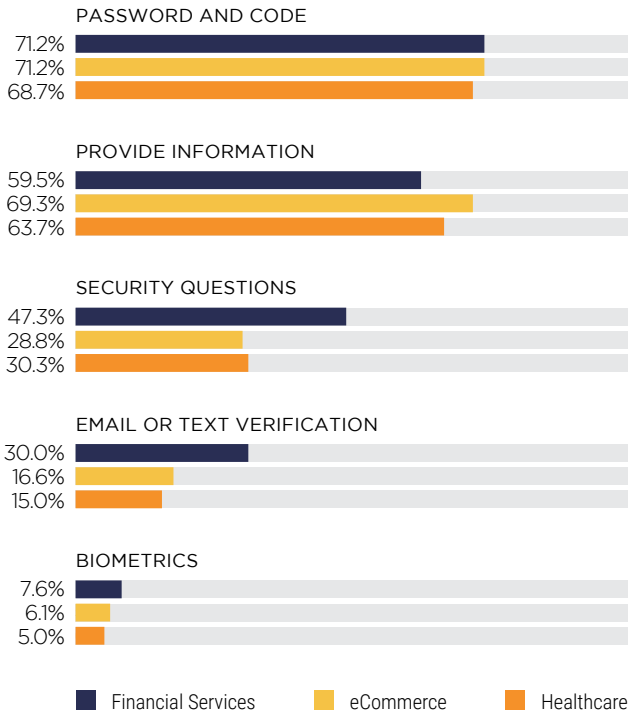
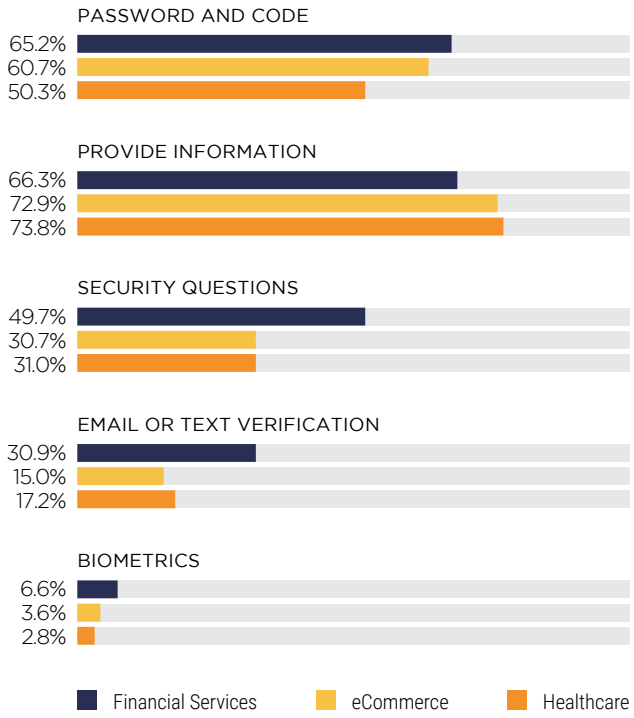


FIGURE 11:

Dissatisfied users' required authentication methods

Percentage of dissatisfied respondents that were required these authentication methods, by type and market



71.2%

OF BOTH FINANCIAL SERVICES AND eCOMMERCE CUSTOMERS EXPRESSED **SATISFACTION** WITH BEING REQUIRED TO PROVIDE PASSWORDS AND CODES FOR AUTHENTICATION

and eCommerce markets at 73.8 percent and 72.9 percent, respectively. Dissatisfied financial services consumers had the lowest rate at 66.3 percent, but these findings potentially indicate that requiring data as an authentication method is more likely to result in unhappy customers across all markets.

Financial services consumers were much more likely to be dissatisfied with required methods than those in healthcare or eCommerce. The more dissatisfied consumers in the market were required to provide passwords or PINs, answer questions, respond to texts or emails or use biometric solutions. This could be because financial services offers users a wider range of authentication methods, meaning they will likely prefer certain requirements over others.

In terms of channels used to access these services, satisfied and dissatisfied consumers alike logged in with desktops or laptops over mobile devices. Dissatisfied customers were more likely to use call centers to access their accounts than satisfied users, though, a finding that could present a call to action: It's time for all three markets to improve customer call center experiences.

FIGURE 12:

Channels through which satisfied users authenticate

Portion of satisfied consumers who used online, mobile and call center offerings, by market

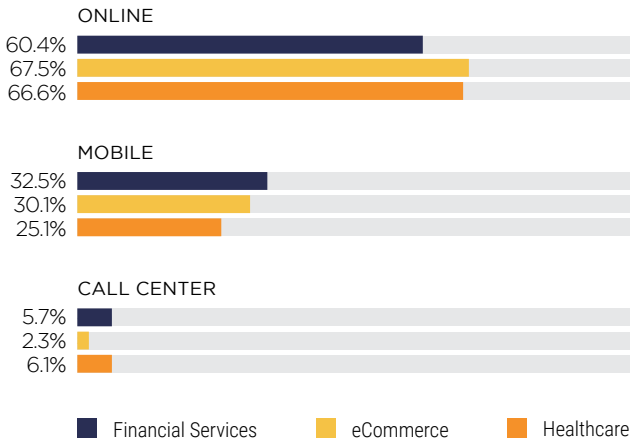
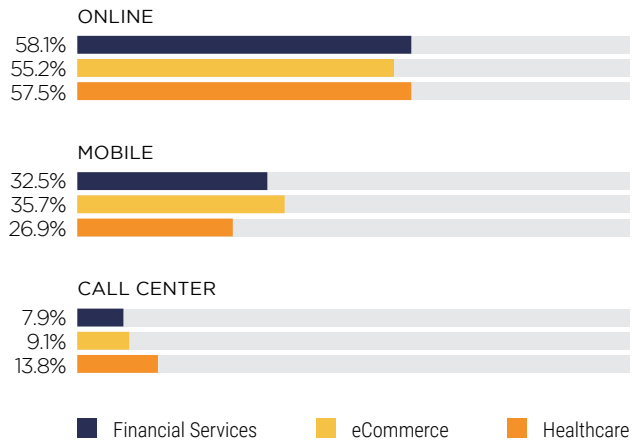


FIGURE 13:

Channels dissatisfied users used to authenticate

Portion of dissatisfied consumers who used online, mobile and call center offerings, by market



As for mobile authentication, financial services boasted more satisfied consumers than the healthcare and eCommerce markets: 32.5 percent for financial services, 30.1 percent for eCommerce and 25.1 percent for healthcare consumers. This indicates that the former's providers have likely developed a more satisfying mobile experience.

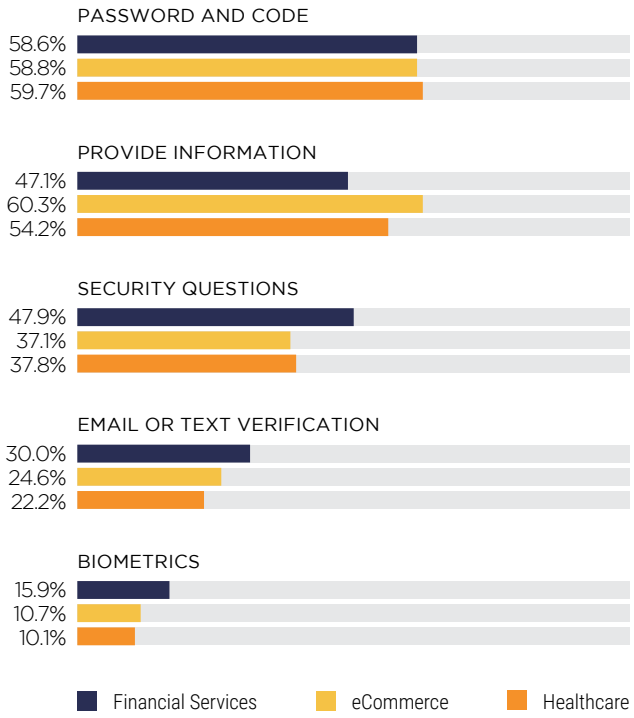
A different pattern emerges among dissatisfied users. It appears 35.7 percent of those for eCommerce logged into their accounts using mobile devices, as did 32.5 percent and 26.9 percent of financial services and healthcare users, respectively. In other words, eCommerce consumers are more likely to be dissatisfied with mobile experiences than their counterparts, a potential warning for the businesses that want to improve mobile authentication experiences.

Understanding why satisfied users preferred certain authentication methods could be the first step toward changing dissatisfied users' opinions. Passwords and PINs were preferred by satisfied users in both financial services and healthcare at 58.6 percent and 59.7 percent, respectively, while eCommerce consumers were more likely to prefer providing PII data. Like the rest of the sample, satisfied consumers in all markets indicated they looked for ease of use, convenience and speed when selecting their preferred authentication methods.

Passwords have won favor across all three markets because consumers find them to be convenient and easy to use. PINs and email addresses were also preferred, largely because

FIGURE 14:

Satisfied users' preferred authentication methods
Consumers' top choices when selecting preferred authentication options, by market



they offer the ease of use, convenience and speed customers appreciate.

Delivering the easy-to-use authentication process consumers have come to expect pushed financial services ahead of healthcare and eCommerce in terms of satisfaction. This was key to the market's appeal, cited by 70.5 percent of its consumers. The financial services market also appreciates convenience, with 63.6 percent of its users noting they were "very" or "extremely" satisfied by that of their preferred authentication methods.

eCommerce and healthcare consumers were highly satisfied with their authentication methods' ease of use. The former's reported the second-highest levels at 69.0 percent, and while healthcare consumers' satisfaction was lower, it was still significant at 63.4 percent. Healthcare and eCommerce were also close behind financial services in terms of consumers' satisfaction with convenience.

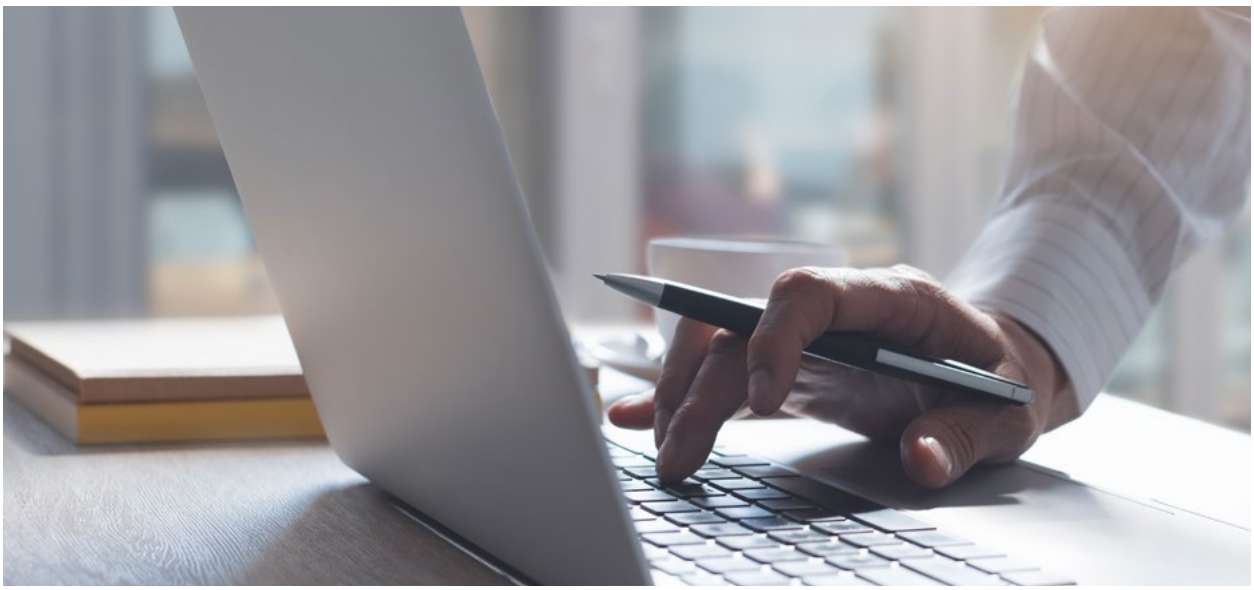


TABLE 1:

Reasons for consumers' satisfaction and dissatisfaction
Factors that drive consumers' satisfaction and dissatisfaction, by market

	Financial Services	eCommerce	Healthcare
REASONS FOR SATISFACTION			
Better fraud protection	32.0%	21.7%	21.0%
Better data security	44.6%	36.8%	40.9%
Fast	61.6%	62.6%	54.5%
Convenient	63.6%	61.2%	58.5%
Easy to use	70.5%	69.0%	63.4%
REASONS FOR DISATISFACTION			
Difficult to use	7.9%	13.0%	18.8%
Keep personal information private	16.3%	8.4%	12.5%
Insufficient fraud protection	24.1%	34.4%	29.4%
Insufficient data security	26.6%	41.6%	33.1%
Slow	29.6%	19.5%	25.0%
Inconvenient	34.0%	20.1%	24.4%

Financial services consumers prefer a wide range of authentication methods, suggesting the market is making multiple options available to them. One of those is biometrics, which appears to be more widely used here than in healthcare or eCommerce. Consumers prefer biometrics because of data security, fraud protection and speed, factors that could give it an advantage with healthcare consumers who are concerned about keeping their health information private.

Both healthcare and eCommerce users were more satisfied with their respective markets' data security protection, but only one-fifth of each market said the same about fraud prevention efforts. This low

“

34.0%

OF FINANCIAL SERVICES CONSUMERS INDICATED AN INCONVENIENT AUTHENTICATION METHOD

AS THE REASON FOR THEIR DISSATISFACTION

”

rate indicates both need to do more to ensure consumers feel protected from fraudsters.

Ease of use, convenience and speed have helped the financial services market outperform eCommerce and healthcare in terms of consumer satisfaction, but users across all three have also indicated which elements are least satisfying. Data security and fraud protection dissatisfaction was highest among eCommerce consumers, with 41.6 percent pointing to insufficiencies in the former and 34.4 percent reporting the same about the latter.

Data security was the top source of dissatisfaction among healthcare consumers, cited by 33.1 percent. Insufficient fraud protection was also a source of frustration for 29.4 percent of them, while 24.4 percent noted inconvenience with authentication.

On a similar note, 18.8 percent of healthcare consumers were more likely to be dissatisfied with difficult-to-use authentication methods. A difficult authentication method was less likely to be a point of friction among eCommerce and financial services consumers, however, cited by just 13 percent and 7.9 percent, respectively.

CONCLUSION

Consumers want to seamlessly engage with a variety of businesses' digital offerings as they go about their daily lives, and that is true whether they are checking their bank accounts, buying new watches or beauty products, consulting with physicians or checking medical test results online. These transactions all require authentication, meaning eCommerce, financial services and healthcare firms would be wise to focus on methods that deliver the ease of use, convenience and speed that consumers desire.

Certain authentication offerings can meet these criteria better than others. Consumers generally prefer passwords over other options, for example, while email addresses are the clear preference among those for eCommerce. This could be because consumers likely already have experience using these methods.

Of the markets surveyed, consumers expressed the highest satisfaction with the authentication methods used by financial services merchants. A significant share were particularly pleased with the offerings' ease of use. Financial services also holds an edge in biometric authentication options, although adoption still appears to be low. The technology could see greater prevalence among healthcare and eCommerce businesses, however, as consumers appreciate the speed, data security and fraud protection biometrics provide. With ubiquitous adoption would come a larger portion of consumers reporting satisfaction with how they securely access products and services.

Time is money for consumers, and loyalty is as good as gold for businesses. Merchants that utilize the right mix of authentication methods for easy, seamless and secure customer experiences will be sure to reap the benefits of a satisfied consumer base.

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 the financial services, eCommerce and healthcare industries. They were asked if they used online, mobile or call center channels, which methods were required and whether they were satisfied. Finally, we asked which methods respondents preferred and the reasons for their 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 considered only these 1,009 respondents in our analysis. We excluded respondents who were not required to authenticate themselves in the areas detailed above.

about

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 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.