Socure

PYMNTS.com

DIGITAL IDENTITY

LIFESTYLE

CAPSULED

68.0%
of respondents who used voice recognition authentication preferred it for its strong data security.

22.4%
of consumers are asked to provide physical identification documents to create a financial account.

Financial Services Edition | September 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

INTRODUCTION

FINANCIAL SERVICES AND DATA SECURITY

In September 2017, news broke that Equifax, one of the three major American credit-reporting agencies, had suffered a security breach. That attack exposed the contact information, birth dates and Social Security numbers of more than 147 million users, many of whom were not aware that the company had been retaining their personal information.[1]

This was far from the only major data breach to make headlines that year, however. Yahoo announced that its 3 billion user accounts had been hacked, Russian hackers' NotPetya ransomware spread globally like wildfire and a National Security Administration (NSA) hacking tool was leaked to the wider web.[2]

That string of cyber incidents demonstrated a harsh truth of modern life: that fraud and digital identity theft have fast become a major risk. It also introduced new pressures on companies like Uber, Amazon, PayPal and others that keep detailed customer profiles, forcing them to maintain a high level of security and keep those digital identities safe.

The implications of having digital identities are far reaching. Modern consumers rely on internet-based options for a wide variety of goods and services — including in healthcare, eCommerce and countless other markets — and their expectations of merchants' security features are rapidly evolving. For financial institutions (FIs), safeguarding consumers from bad actors means deploying secure authentication steps to verify users' identities and enable both account access and FI-provided services.

The PYMNTS Digital Identity Lifestyle Capsule survey, in collaboration with Socure, polled more than 2,600 consumers who had shopped online, paid their healthcare bills online or used digital banking services in the last three months, gauging their satisfaction with the authentication methods that protected their digital lives. Our inaugural study focuses on more than 1,800 digital banking

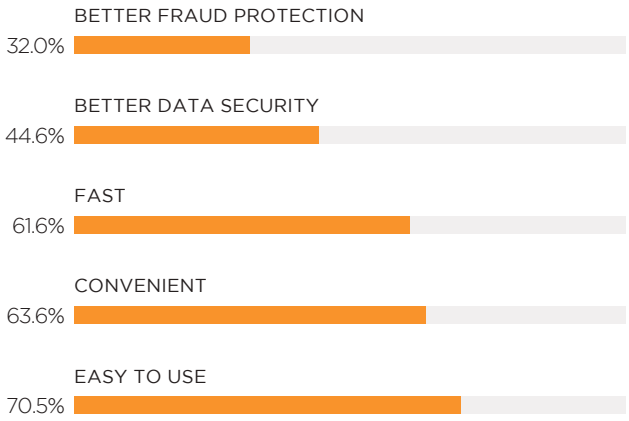
[1] Fung, Brian. Equifax's massive 2017 data breach keeps getting worse. The Washington Post. 2018. https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?utm_term=.20f9da6f4d6b. Accessed September 2018.

[2] Larson, Selena. The hacks that left us exposed in 2017. CNN. 2017. https://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html. Accessed September 2018.

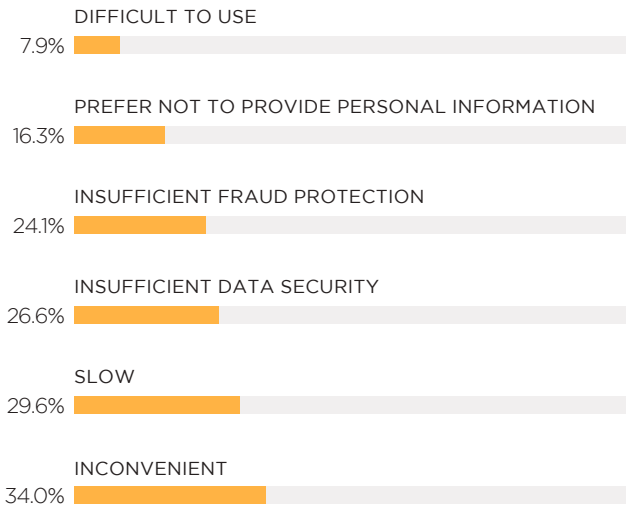
FIGURE 1:

What users like or dislike about an authentication process

Users who were satisfied with an authentication method, by select characteristics



Users who were dissatisfied with an authentication method, by select characteristics



customers' data, as well as the methods used to authenticate their online financial accounts.

We asked respondents about the elements that influence their decisions to rate any given authentication process as "good" or "bad." The results revealed several surprising trends, including an apparent preference for convenience and speed over security, especially in the financial services market.

Specifically, 71 percent of financial services customers reported valuing easy use, 64 percent cited convenience and 62 percent would prefer a faster authentication process. As seen in Figure 1, these three characteristics were most likely to result in a positive customer rating.

Meanwhile, just 45 percent of respondents said they would rate an authentication method's data security highly, as did 32 percent for its fraud protection capabilities. This is an odd finding, considering both attributes are, supposedly, the very reasons authentication methods exist.

The following sections will explore the technological, economic and cultural factors that may have contributed to these unanticipated results. After all, why would financial consumers, who entrust their life savings and intimate financial information to online accounts, care less about security than the ease with which they are able to access them?

The answer appears to stem from an unexpected source: that financial companies are entrusted to ensure the information's security at all.

70.5 PERCENT OF RESPONDENTS

ARE SATISFIED WITH

AN AUTHENTICATION METHOD

BECAUSE IT IS **EASY TO USE.**

CREATING VERSUS ACCESSING

AN ACCOUNT

Whether accessing services online or in person, there are two basic ways to identify customers: verification and authentication. These terms are used interchangeably in everyday conversation, but they have very distinct meanings.

Imagine that a customer walks into a bank branch to create an account. She is directed to a teller, who says she must fill out a few forms and present her state-issued identification to do so. This is identity verification. The customer leaves after the process is completed.

She returns two weeks later to access the funds in her account and is referred to a different teller who has never seen her before. He asks for her name and documentation, then presents a challenge question: "Which company provided the mortgage on your last house?" This is identity authentication, taking verification to the next level by asking questions with answers that are difficult to ascertain, usually regarding private information from a customer's past.

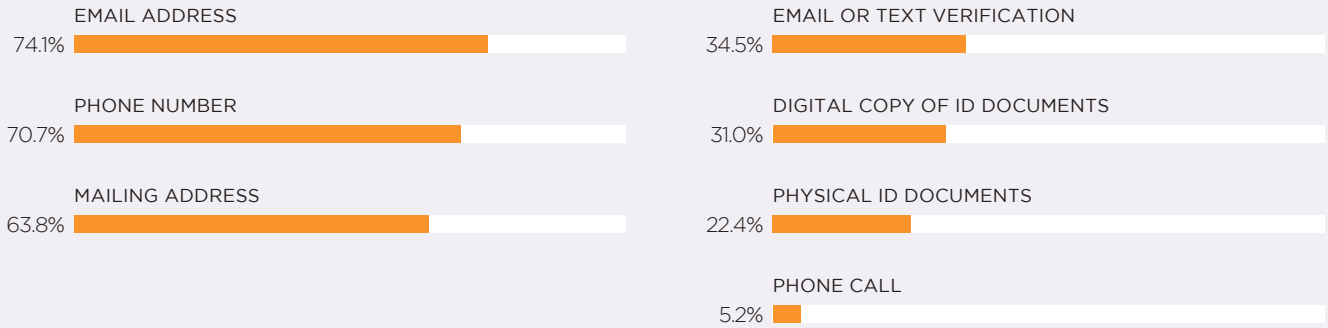
Very few modern consumers choose to manage their finances at brick-and-mortar branches. Online banking has become the norm, meaning the verification and authentication process has also changed. Rather than present identification documents to a teller, consumers must verify themselves on computers or smartphones using FI-dependent authentication methods.

To find out how consumers verify and authenticate their identities when engaging with online banking services — and gauge their satisfaction with these methods — we asked respondents about the information they were asked to provide when opening new online accounts. According to our survey data, the process tends to be lengthy and includes multiple layers of verification and authentication. The most common information for which respondents were asked was an email

FIGURE 2:

Information required to create an account

Percentage of companies requiring select information to create an account, by industry



address, cited by 74 percent, and 80 percent were asked for a phone number.

Providing publicly available information is just one part of the sign-up process, however. Many financial companies expect new customers to go a step further to verify their identities, with 40 percent of respondents saying they were asked challenging, customer-specific questions. These might include, "How, if at all, are you affiliated with this zip code?" or "Which company provided your mortgage 15 years ago?" This additional question is called a "backstop."

FIs also commonly use official identification documents — like government-issued IDs — as a backstop to verify new customers' identities before opening an account. Approximately 31 percent of applicants were asked to digitally provide ID documents, and 22 percent reported being required to do so in person.

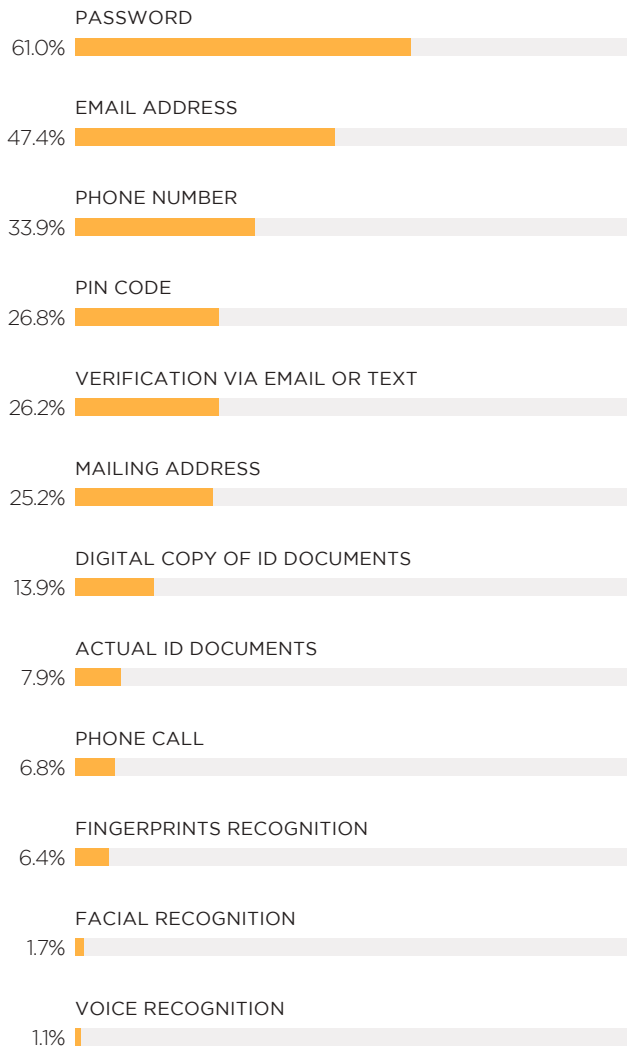
State-issued identification can be forged, copied or stolen, however, meaning it isn't always enough to unveil identity thieves posing as real customers. Fortunately, FIs have existing account authentication processes in place to help deter such fraud. When there is reasonable cause to believe a consumer might not be who he says he is, an FI can turn to personally specific questions to ensure accuracy.

We asked respondents about the ways they were authenticated when accessing an existing online account, giving us a better understanding of existing customers' process. In this case,

FIGURE 3:

Methods used to authenticate existing financial accounts

Companies requiring select information to allow customers access into a financial account



authenticating included logging into an online account by providing specific information.

Both email- and password-based authentications were popular, but the latter were more common. An FI might send a temporary code to a consumer's email address, for example, and he or she will then enter that code into the banking system. Sixty-two percent of financial customers used passwords to log in, but only 47 percent needed to provide an email address to do so.

Some FIs may choose to authenticate their customers with one-time passwords provided via email or phone message. Others may prompt for other additional information. Further, a customer might need to call an FI-supported customer service line through which he can verify that email address or phone number.

Our data suggests that financial service providers are more likely to use authentication factors like personal identification numbers (PINs) or responses to an email or text to authenticate their customers. Consumers were commonly asked to provide multiple pieces of information to authenticate their identities.

Considering the lengthy process required to verify and authenticate consumers' identities when creating an account or logging into one, it is not surprising that many respondents valued speed and ease above all else. In fact, our results suggested that consumers are more likely to prefer an easy-to-use or convenient security method over one that is simply secure.

As seen in Figure 4, 49 percent of consumers cited ease of use as a reason to be satisfied with an authentication method, while 47 percent noted convenience. Just 42 percent mentioned data security as logic for authentication method satisfaction.

Again, this likely relates to how time consuming it can be to open or log into an online financial account. A customer who forgets the basic information must verify his identity — often using his account password — then authenticate it by providing additional information. If that fails, he could end up locked out of his account.

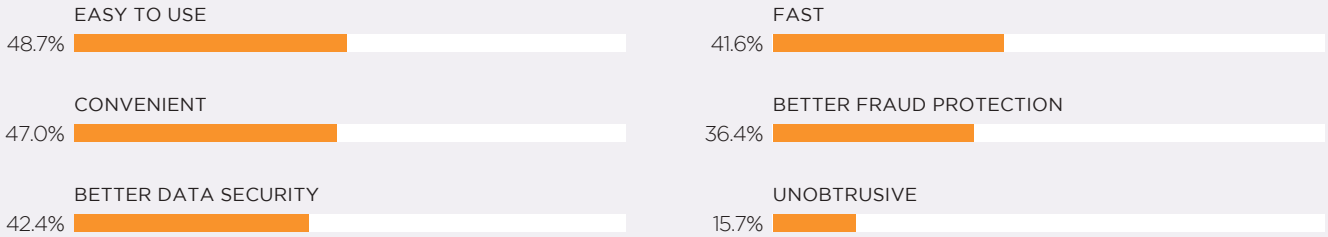
Consumers' experiences in these situations often shape their preferences for speed and convenience over security in identity authentication. That said, our data also demonstrates that some respondents do, in fact, value security over convenience and ease of use. This makes sense: Consumers are not homogenous, and therefore have unique security preferences.

We know which authentication methods financial consumers use, and a little about the processes they prefer, but what do they *actually* want in terms of digital security? The answer is a bit more complicated than one might expect.

FIGURE 4:

Reasons to prefer an authentication method

Respondents citing select reasons for preferring an authentication method, by type



HOW CONSUMER PREFERENCE FORESHADOWS THE BIOMETRIC FUTURE OF

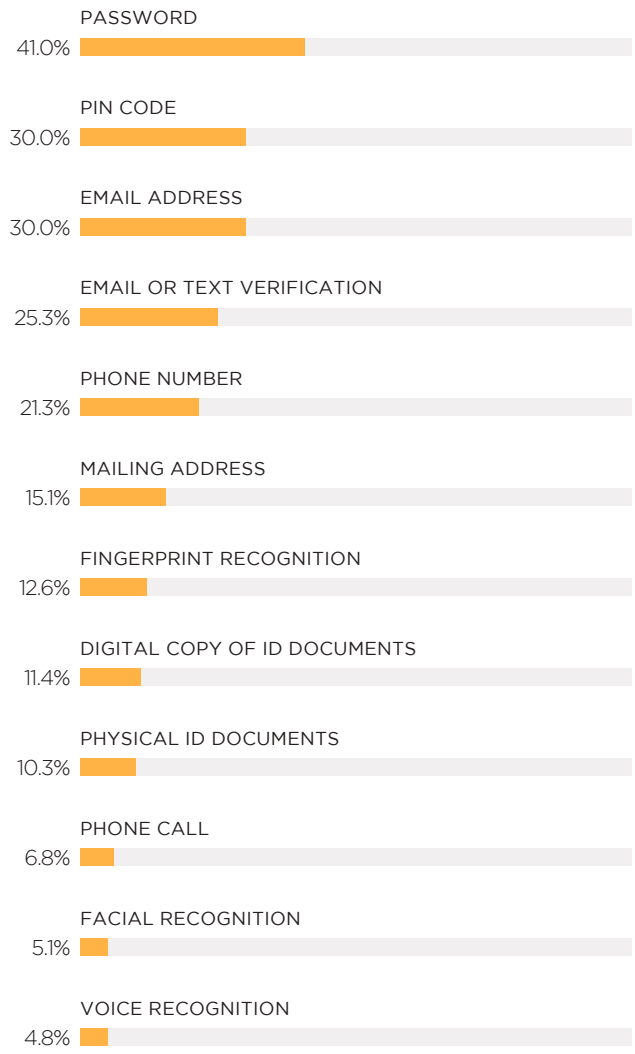
DIGITAL SECURITY

Modern consumers expect round-the-clock, easy access to online banking services, so it follows that they would also value speed and convenience. When authentication methods require passwords and security codes, though, such speed and convenience can be difficult to achieve.

Despite this, our respondents most commonly cited passwords and email addresses when asked which authentication methods they preferred, at 41 percent and 32 percent, respectively. That said, when we considered consumers' authentication preferences by age, we found those in the 18 to 34 bracket were more likely to value speed and convenience than older consumers. We will expand on this in greater detail later in the report.

FIGURE 5:

Digital identity and customer preferences
Respondents who preferred select authentication methods, by type



Few respondents in our sample had encountered biometric authentication, but those who had were extremely satisfied with it. As many as 83 percent preferred it for its convenience and tight security — a higher portion than reported for any other authentication method.

TABLE 6: AUTHENTICATION METHODS PREFERRED, BY REASON
Respondents who cited select reasons for preferring an authentication method

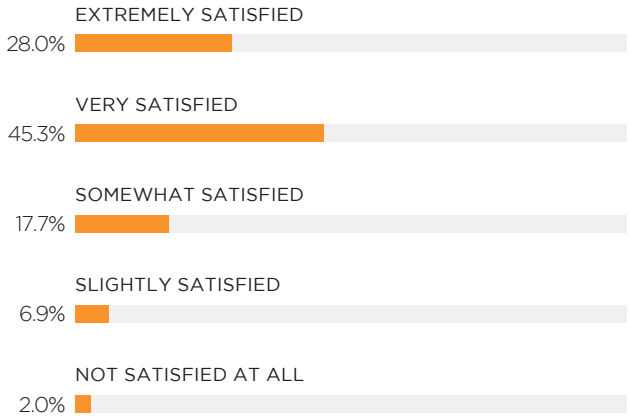
	Easy to use	Convenient	Better data security	Fast	Better fraud protection	Unobtrusive
Password	58%	58%	44%	49%	37%	22%
Security questions	57%	53%	57%	43%	50%	20%
PIN code	60%	54%	58%	46%	45%	19%
Email address	55%	50%	46%	53%	40%	16%
Email or text verification	54%	61%	45%	48%	44%	20%
Phone number	55%	51%	48%	59%	39%	17%
Mailing address	53%	49%	54%	53%	41%	15%
Fingerprint recognition	51%	50%	60%	41%	56%	23%
Digital copy of ID documents	46%	44%	54%	40%	46%	**11%**
Physical ID documents	48%	47%	48%	51%	47%	13%
Phone call	56%	56%	56%	48%	50%	23%
Facial recognition	41%	41%	67%	41%	62%	18%
Voice recognition	51%	54%	**68%**	46%	59%	16%

This must be taken in wider context, as most consumers had not previously encountered biometric authentication methods. This unfamiliarity is likely why biometrics ranked so low among available processes. People tend to accept that to which they are accustomed. Unless shown a viable alternative, they are unlikely to change how they manage their personal finances.

In fact, approximately 73 percent of consumers were either "very" or "extremely" satisfied with the authentication methods they used. They may hope their FIs' processes improve, but these consumers are also unlikely to close their accounts while they wait.

Regardless of how authentication methodology has been improved by technological advances, it appears users remain satisfied with the status quo. They may perceive biometric authentication to be too intrusive,

FIGURE 7: Consumers' satisfaction with FIs' authentication methods
Authentication process satisfaction, by level



45.3 PERCENT

OF RESPONDENTS SAY THEY ARE VERY SATISFIED WITH THEIR FIS' AUTHENTICATION PROCESSES.

too, and therefore opt against adopting. Not all users are comfortable using their faces or fingerprints to log into their accounts, something which may dissuade companies from employing the offerings.

This may sound understandable, but our data — seen in Figures 1, 3 and 5 — shows customers actually care very little about the intrusiveness of authentication methodology. They're more concerned with its security capabilities and convenience, meaning biometrics' perceived intrusiveness is unlikely to outweigh the potential speed- and security-related benefits.

Biometrics is no longer the stuff of science fiction, now becoming increasingly common in many industries. Most consumers are used to unlocking their phones with their fingerprints, and facial recognition is a prominent, popular feature of the iPhone X. As related offerings continue to become mainstream, they will likely develop into the new "status quo."

A FINANCIAL INSTITUTION'S

PERSPECTIVE

The prospect of biometric-based security systems' growing popularity has piqued many companies' interest. This raises yet another question: Which authentication processes do financial companies prefer and why? Do they tend to use biometrics, single-factor identification (SFA) or multifactor authentication (MFA)?

According to our survey, 72 percent of account providers used SFA to verify their users' identities.[3] Just 28 percent offered MFA, and 22 percent required additional authentication factors. These numbers are in line with financial industry observations, as approximately 24 percent of merchants required users to submit two factors to authenticate an existing account.

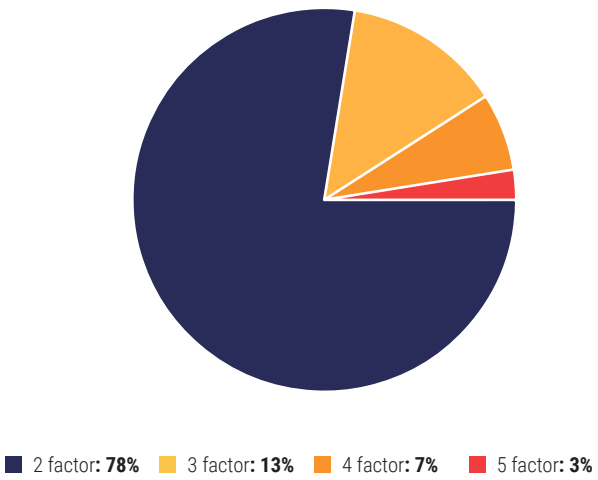
MFA includes any method which simultaneously uses several factors to authenticate an account. It is only used to prove ann existing customer's identity, one who had previously been verified and enrolled using biometric information.

This idea is quickly gaining traction, too. MFA usage may currently be in the minority, but the global two-factor authentication (2FA) market was valued at approximately $3.8 trillion in 2014. MFA is expected to reach $5.7 trillion by 2021, and 78 percent of that is projected to be generated by the 2FA technology market.

The financial services industry accounts for 42 percent of that multitrillion-dollar global market, and will likely continue to drive MFA growth in the coming years.

[3] Author unknown. Multi-factor authentication market size, share & trends analysis report…segment forecasts. Grand View Research. 2018. https://www.grandviewresearch.com/industry-analysis/multi-factor-authentication-market. Accessed September 2018.

FIGURE 8: **Global 2017 multifactor authentication market, by number of factors**
Portion of the market requiring a given number of authentication factors



MFA uses several authentication factors to identify a customer, but biometrics, offered by a mere 5 percent of FIs, is considered particularly secure.[4] This includes any method that authenticates using characteristics inherent to a customer, including fingerprint, voice or facial recognition technology.

If consumers are disproportionately satisfied with biometrics, then why does FIs' interest in it appear to be so low? It is currently neither as developed nor as familiar as mainstream methods like passwords and PINs, meaning customers may opt out of available biometric options. In addition, companies may prefer not to use it because biometrics is not yet commercially viable.

There is evidence to suggest that FIs are becoming more interested in biometric investments, though, with several testing the technology over the last few years to enhance their biometric authentication capabilities. Mastercard announced in early July that it is in talks with U.K. banks about introducing cards with built-in finger scanners that could verify users' identities, for example.[5] Just one year earlier, European-based TSB Bank announced it would roll out its own iris-scanning user authentication technology.[6]

The combination of biometrics and tokenization is also gaining popularity, geared toward returning customers whose information has been bound to the devices they use to access their accounts. Their digital identities would be tokenized and stored securely on special in-device chips to ensure data privacy.[7]

It appears companies are treading closer toward biometric authentication adoption, but whether their customers will be receptive to such innovations remains to be seen.

[4] Author unknown. Multi-factor authentication market size, share & trends analysis report…segment forecasts. Grand View Research. 2018. https://www.grandviewresearch.com/industry-analysis/multi-factor-authentication-market. Accessed September 2018.

[5] Browne, Ryan. Mastercard is in talks with UK banks about launching cards with fingerprint scanners. CNBC. 2018. https://www.cnbc.com/2018/07/09/mastercard-biometric-card-talks-with-uk-banks.html. Accessed September 2018.

[6] Cellan-Jones, Rory. TSB to roll out iris scanning tech. BBC. 2017. https://www.bbc.co.uk/news/technology-40663365. Accessed September 2018.

[7] Tode, Chantal. Biometrics, tokenization gain steam with MasterCard, Visa commitments. RetailDrive. 2018. https://www.retaildive.com/ex/mobilecommercedaily/biometrics-tokenization-gain-steam-with-mastercard-visa-commitments. Accessed September 2018.

DEEP DIVE

WHAT DRIVES USERS' SATISFACTION WITH AUTHENTICATION?

Humans are extraordinarily complex, and our genetic makeup, experiences and surroundings all play a part in determining our personal preferences. With so many variables in play, it is not shocking that our survey respondents' feelings about the authentication methods involved in accessing their personal financial accounts were more complex than might be necessary.

It also comes as no surprise that our survey results revealed consumers have mixed feelings about authentication. Most of those familiar with biometric authentication strongly prefer it over all other methods, but a very small percentage have used it. Considering its impressive user-satisfaction rate, one might assume a greater number of respondents would have adopted biometric technology, but our survey suggests they have not.

There are several possible explanations for this. What customers like in theory does not necessarily align with what they need in practice, for example, as the idea of hyper-secure authentication methods like MFA may *sound* appealing to ensure data security. In practice, though, it takes time for people to warm up to new, less-familiar technologies.

Yet, chances are that they eventually will. Most people tend to conceptualize the idea of liking or disliking something in relative terms. Consumer preference is shaped by choosing one subject over another. Consumers feel relatively satisfied with certain authentication methods' ability to enforce data security and are dissatisfied with their convenience. They, therefore, now prefer convenience, the trait they feel their current options lack.

It might be more accurate to say that consumers currently feel their most pressing grievance with authentication processes relates to convenience, for example, and not their security. This principle of relative satisfaction may help explain another observed trend: that older and younger consumers tend to have different authentication preferences.

We observed a correlation between consumers' ages and their reasons for preferring various authentication methods. Older consumers appeared to value speed less than their younger counterparts, for example. As shown in Figure 11, 54 percent of those between 25 and 34 noted their favorite authentication method's speed, as did just 30 percent of the 65-plus.

Younger users, "native netizens," appear comfortable with authentication processes overall, likely because most have never known any other way of managing their personal information. Users beyond a certain age, however — even if "tech-savvy" — experienced a transitional period between when online accounts were uncommon and when they became "normal." They are not native netizens, and have thus had to learn the language.

These findings are in line with industry buzz. Millennials and Generation Z, who have always had internet access and now live on their smart devices, are known for demanding speed and

TABLE 9: REASONS FOR CHOOSING A PREFERRED AUTHENTICATION METHOD, BY AGE
Respondents citing select reasons for preferring an authentication method

	18 - 24	25 - 34	35 - 44	45 - 54	55 - 64	65+
Easy to use	54%	55%	52%	47%	45%	42%
Convenient	40%	50%	48%	50%	44%	47%
Better data security	44%	44%	39%	38%	46%	43%
Fast	48%	54%	45%	40%	37%	30%
Better fraud protection	34%	36%	36%	33%	41%	38%
Unobtrusive	16%	11%	16%	13%	23%	16%

convenience in all aspects of their daily lives — especially in their digital ones. The desire to meet these modern consumers' demand for instant gratification has been an innovation catalyst in many sectors, including technology.[8]

Biometric authentication may be relatively rare compared to alternative authentication methods, but the consumers who use it are more satisfied with it than with anything else. Moreover, it appears millennials and Generation Z are more likely than other generations to have used biometric authentication and to report being satisfied with it.

It's no surprise that native netizens are supportive of faster, more innovative verification solutions. They have a strong toe hold in the evolving digital marketplace, pushing companies to continue to protect their digital identities. Both smart device use and security threats are only becoming more common, and the advanced technologies that make biometric authentication possible are now widely available, meaning consumers may soon find themselves gravitating toward financial companies that offer such options.

[8] Sorrentino, Frank. Millennials: More than an audience segment—it's a mindset. Forbes. 2018. https://www.forbes.com/sites/franksorrentino/2018/08/03/millennials-more-than-an-audience-segment-its-a-mindset/#bacef341eaa7. Accessed September 2018.

CONCLUSION

Authentication and verification technology has developed well past the need to rely on PINs, passwords and birthdays to securely access an online financial account. These factors may no longer even be viable as security devices, as consumer demand now considers longer, drawn-out verification and authentication methods unsatisfying.

This evolution appears to be leading to the rise of biometric technology and, more broadly, to MFA. Though still in its infancy, and though most consumers have yet to encounter it, MFA appears to provide the secure and convenient verification previously characterized by diametric opposition. Customers formerly had to choose between the two, but this no longer appears to be the case. The question, then, is not if the technology will take root, but *when*.

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% of the US 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.