PARTNER. ADVISOR. CATALYST.

Moving Beyond the Password: Consumers' Views on Authentication

MARCH 2017

Julie Conroy

Sponsored by:

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

IMPACT POINTS

- In this research effort, sponsored by iovation, Aite Group surveyed 1,095 U.S. consumers who use online and/or mobile banking in January 2017 to better understand their attitudes toward and understanding of various authentication mechanisms.
- With more than six billion data records compromised since 2013, the organized crime rings behind the majority of financial fraud have a vast amount of data at their disposal. Criminals are making ample use of this data, which is manifest in the rising account takeover (ATO) and application fraud losses that are hitting FIs and merchants alike.
- When Aite Group asked consumers about their key priorities for their financial institution's (FI's) online banking service, ease-of-use was the most important consideration for all age groups. Robust security and fraud prevention is also deemed to be very important by the majority of respondents; seniors give this equal weight with ease of use, with 76% of seniors saying both are very important.
- A key reason why consumers are comfortable with using passwords is because they are doing so poorly. The majority of consumers are only using a handful of username/password combinations across their online relationships. Millennials are the worst offenders, with 77% using between just one and five unique passwords across all of their online relationships.
- Forty percent to 45% of consumers report feeling extremely or very frustrated when they can't get into their banking website due to a forgotten password, with nearly one in three feeling that level of frustration when they can't login to an e-commerce or media site.
- When asked whether they would be willing to switch to an alternative identification method other than a password, there was a clear correlation between consumers' openness to change and their age. Forty-eight percent of millennials indicate that they are very willing to switch methods, with another 47% somewhat willing to change. In contrast, only 16% of seniors are very willing to learn new methods.
- While 51% of consumers say that they would be willing to proactively sign up for a variety of stepped-up authentication methods without any form of monetary incentive, an incremental 24% of consumers say that they would be willing to do so if the bank offers a cash bonus of US$10 to US$25.
- Given the clear differences in comfort level, understanding, and openness to new forms of authentication among the various age groups, FIs need to enable a variety of authentication methods and tailor their education and messaging to the consumer's demographic.

INTRODUCTION

Passwords are dead. This message has come from Google execs,[1] the U.S. government,[2] and myriad fraud and security experts (including those at Aite Group) for most of this decade. Yet passwords are very much still part of the fabric of online banking and commerce, so rumors of their death appear to be premature.

One reason for this is inertia; passwords are a well-understood mechanism among consumers and businesses. Moving to something different is not just a daunting task from an IT perspective; the far greater concern for many FI and merchant executives is the potential disruption of the customer experience.

This Impact Report analyzes consumers' perceptions of various forms of authentication. Based on the findings, the report concludes with a series of recommendations designed to help improve both security and the customer experience, which will hopefully speed the process of declaring the password truly and finally dead.

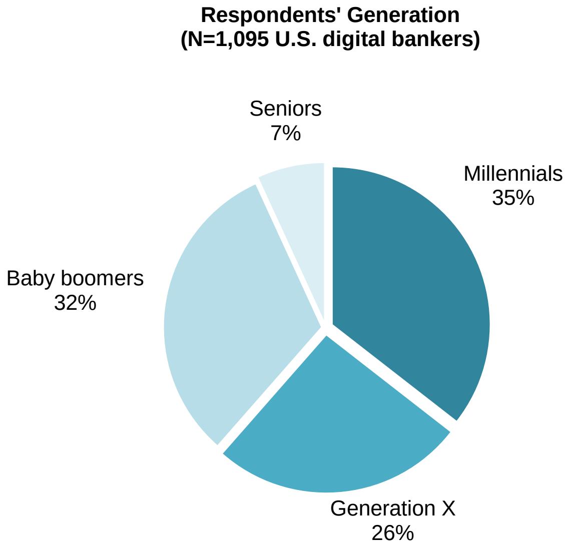
METHODOLOGY

In this January 2017 research effort, sponsored by iovation, Aite Group surveyed 1,095 U.S. consumers who use online and/or mobile banking to better understand their attitudes and understanding of various authentication mechanisms. The sample is in proportion to the U.S. population for age, gender, income, geographic region, and race. The data have a margin of error of three points at the 95% level of confidence. Seniors are defined as individuals who were born before 1946, baby boomers between 1946 and 1964, Gen Xers between 1965 and 1980, and Gen Yers or millennials between 1981 and 2000 (Figure 1).

[1] Daniel Terdiman, "Google Security Exec: 'Passwords Are Dead,'" CNET, September 10, 2013, accessed February 15, 2017, https://www.cnet.com/news/google-security-exec-passwords-are-dead/.

[2] Barack Obama, "Protecting U.S. Innovation from Cyberthreats," Wall Street Journal, February 6, 2016, accessed February 15, 2017, https://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003.

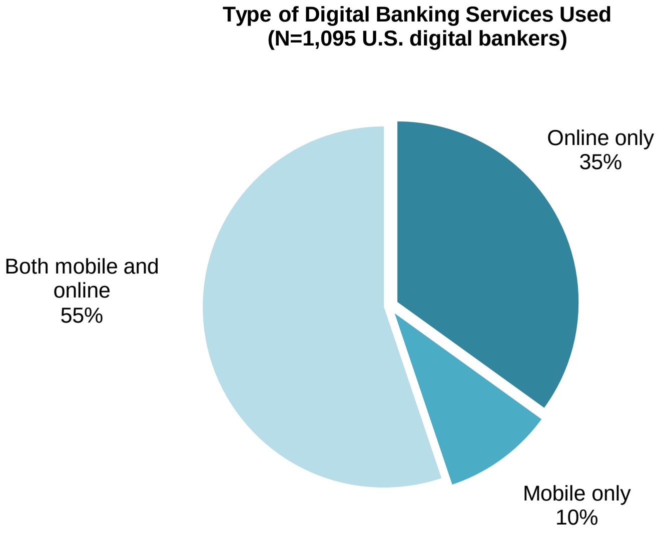
Figure 1: Survey Respondents by Generation



Source: Aite Group survey of 1,095 U.S. consumers, January 2017.

In terms of digital channel use, 55% of respondents use both online and mobile banking, 35% use online banking only, and 10% use mobile banking only (Figure 2).

Figure 2: Type of Digital Banking Services Used



Source: Aite Group survey of 1,095 U.S. consumers, January 2017.

THE MARKET DRIVERS

With more than 6 billion data records compromised since 2013, the organized crime rings behind the majority of financial fraud have a vast amount of data at their disposal. Criminals are making ample use of this data, which is manifest in the rising ATO and application fraud losses that are hitting FIs and merchants alike.[3] Table A highlights a handful of the notable data breaches announced in 2016.

Table A: Notable 2016 Data Breaches

Breached entity	Date announced	Data compromised
Yahoo!	December and September 2016	1.5 billion records including username, password, phone number, date of birth, and security questions and answers
AdultFriendFinder.com	November 2016	412 million records including username, password, and email address
Weebly	October 2016	43.5 million records, including username, password, email address, and IP address
VK.com	June 2016	171 million records, including full name, username, clear text password, email address, and phone number
21st Century Oncology	March 2016	2.2 million patient records, including name, social security number, diagnosis, and insurance information

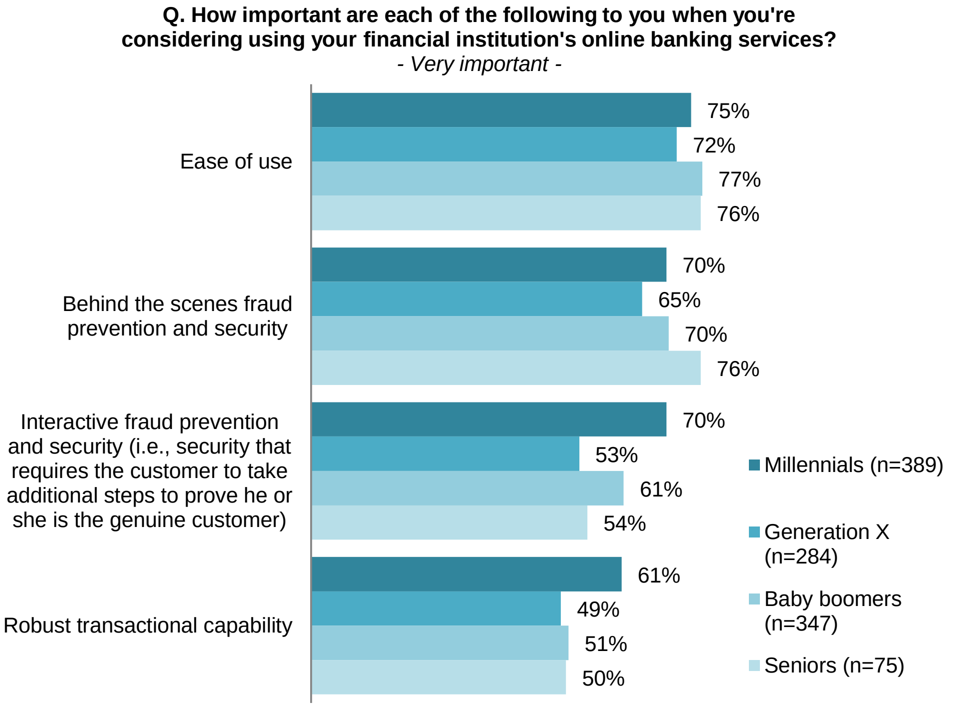
Source: Aite Group

At the same time that the threat environment is escalating rapidly, FIs and merchants struggle to find the right balance between security and the user experience. Consumers' expectations for digital interactions are being set by the elegant and largely friction-free user experiences provided by the likes of Amazon, Apple, and Uber. The ability to provide a satisfying and meaningful customer experience is increasingly a key competitive differentiator.

When Aite Group asked consumers about their key priorities for their FI's online banking service, the responses show that ease of use is the most important consideration on average. Robust security and fraud prevention is also deemed to be very important by the majority of respondents; seniors give this equal weight with ease of use, with 76% of seniors saying both are very important (Figure 3). Seventy percent of millennials believe interactive transactional security to be a very important component in their online banking experience, while this was less critical for the older age groups. Robust transactional capability in online banking came in last place relative to the importance of ease of use and fraud prevention; 61% of millennials say this is very important, while roughly one in two baby boomers, seniors, and Gen Xers believe it to be very important.

[3] See Aite Group's report *EMV: Issuance Trajectory and Impact on Account Takeover and CNP*, May 2016.

Figure 3: Consumers' Priorities for Online Banking Capabilities



Source: Aite Group survey of 1,095 U.S. consumers, January 2017.

Table B details some of the key trends shaping FI and merchant decisions around how to evolve their fraud prevention and authentication strategies.

Table B: Market Trends and Implications

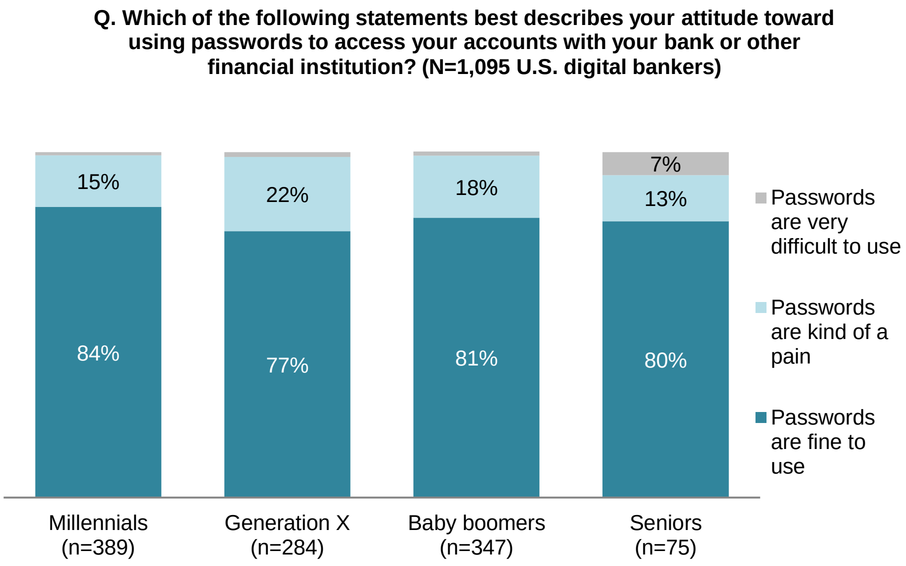
Market trends	Market implications
Usernames and passwords have outlived their useful life.	The combination of the data breaches and consumers' unfortunate tendency to use the same handful of username/password combinations across all of their online relationships have relegated the credential pair to a database look-up mechanism, with little security value.
Customer experience is a competitive differentiator.	FIs and merchants are working to remove friction from the customer experience in order to meet the rising bar of customer expectations for the digital user experience.
The threat landscape is evolving rapidly.	Criminals are adjusting their tactics rapidly; it's difficult for FIs to be equally nimble and keep pace.
There is an increasing ubiquity and use of mobile devices.	The increasing prevalence of smartphones and tablets provides new opportunities to deploy stronger authentication mechanisms in a customer-friendly manner. In addition, inputting usernames and passwords in a mobile device is a clunky user experience, so many consumers willingly embrace biometrics and other technologies that are both easier and more secure.

Source: Aite Group

PASSWORDS: EASY BUT INEFFECTIVE

Consumers are generally quite comfortable using passwords to access their online bank account, with very little difference in attitude across the generations (Figure 4). Part of this comfort level can be attributed to habituation; the username/password combination has been around since the inception of online commerce, and consumers are quite well trained in their use.

Figure 4: Consumers' Attitudes Toward Passwords



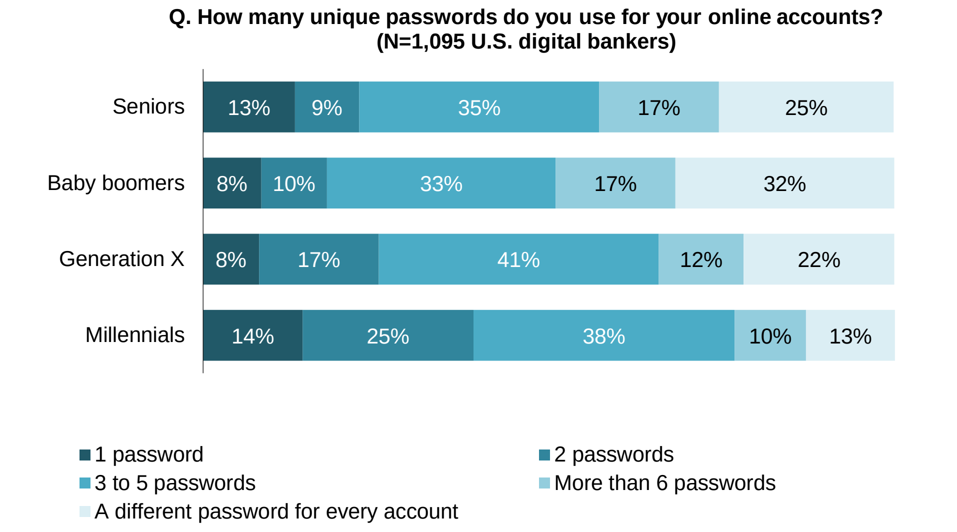
Source: Aite Group survey of 1,095 U.S. consumers, January 2017.

Unfortunately, another key reason why consumers are so comfortable with using passwords is because they are doing so poorly. The majority of consumers are only using a handful of username/password combinations across their online relationships. Millennials are the worst offenders, with 77% using between just one and five unique passwords across all of their online relationships. Sixty-six percent of Gen Xers and 57% of seniors use between one and five passwords across all of their online relationships. While the majority of baby boomers also use between one and five passwords across all of their online relationships, 32% of baby boomers use a different password for each of their online accounts (Figure 5).

Password managers, which enable end users to organize and store unique, complex passwords can help. These solutions face their own challenges, however, as criminals have recognized that they hold the proverbial keys to the kingdom. LastPass was successfully breached in 2015, and a recent report shows that a number of the other password managers have their own security vulnerabilities. The key lesson is that when it comes to security, there is never a silver bullet.[4]

[4] Roi Perez, "German Researchers Find Flaws in Nine Major Password Managers, SC Magazine, March 1, 2017, accessed March 6, 2017, https://www.scmagazineuk.com/german-researchers-find-flaws-in-nine-major-password-managers/article/640998/.

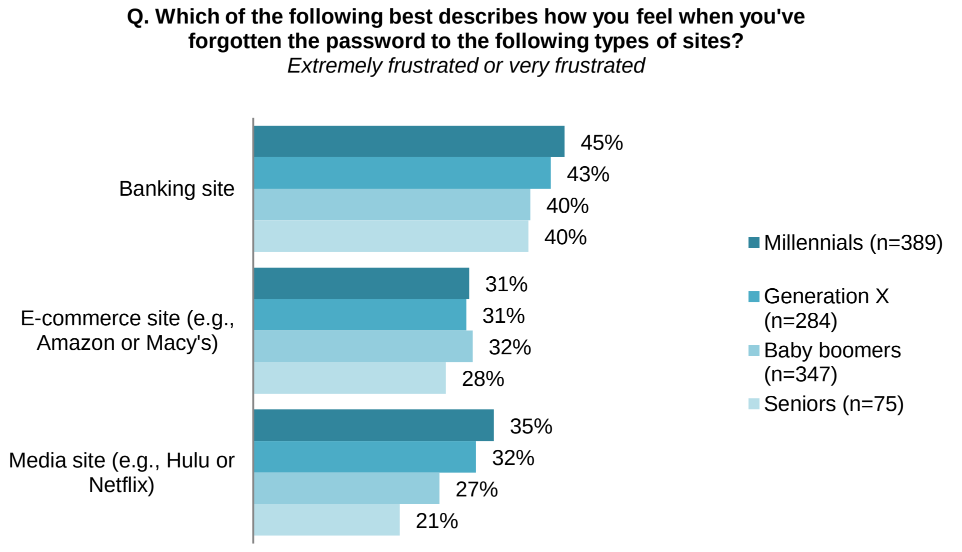
Figure 5: Number of Unique Passwords Used by Consumers



Source: Aite Group survey of 1,095 U.S. consumers, January 2017.

Part of the reason consumers are lazy about passwords is that it's hard to remember a different password for each site, and it's frustrating when a forgotten password prevents or delays access to a website and its services. As shown in Figure 6, 40% to 45% of consumers report feeling extremely or very frustrated when they can't get into their banking website due to a forgotten password, with nearly one in three feeling that level of frustration when they can't login to an e-commerce or media site.

Figure 6: Consumers' Response to Forgotten Passwords



Source: Aite Group survey of 1,095 U.S. consumers, January 2017.

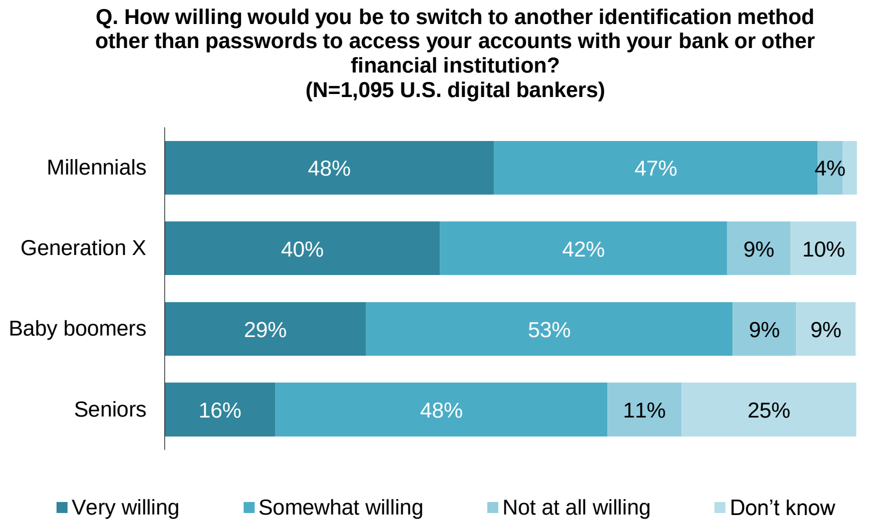
ONLINE AND MOBILE AUTHENTICATION METHODS

The username/password combination became the industry standard for online user identification more than two decades ago. Criminals have long since proven adept at compromising this capability, yet it still remains the predominant initial means of user identification. The increasing ubiquity of mobile devices, however, provides new opportunities to provide superior authentication capabilities with minimal impact to the user experience.

Within the mobile channel, replacing the need to enter a username/password with a biometric actually provides the opportunity to increase security while improving the customer experience. A number of large FIs, including Bank of America, U.S. Bank, Chase, and USAA, have already given their customers the choice of logging into the mobile app with their fingerprint.

When asked whether they would be willing to switch to an alternative identification method other than a password, there was a clear correlation between consumers’ openness to change and their age. Forty-eight percent of millennials indicate that they are very willing to switch methods, with another 47% somewhat willing to change. In contrast, only 16% of seniors are very willing to learn new methods (Figure 7).

Figure 7: Consumers’ Openness to Alternative Identification Methods



Source: Aite Group survey of 1,095 U.S. consumers, January 2017.

A number of viable alternatives to passwords are already in use, as described in Table C.

Table C: Authentication Methods

Authentication type	Description	Pros	Cons
Device fingerprint (or device identification)	Device identification technology examines a combination of identifiable hardware and software attributes associated with a computer or mobile device.	Transparent to the end user Can be used to provide recognition of devices associated with fraudulent activity as well as ongoing recognition of devices with trusted reputations	While highly reliable in the mobile app environment, the device fingerprint is less permanent in the browser environment.
Device location	It uses sensors native to the mobile device to identify the device's location.	Transparent to the end user Reliable risk indicator, particularly when used in conjunction with other layers of protection	Many businesses are concerned about a "big brother" stigma and enable this on an opt-in basis.
Eye vein biometric	It uses the device's video recorder to capture the end user's eyes, then applies pattern recognition to authenticate the eye veins.	Very accurate, low level of false positives and false negatives	It's less user-friendly than facial recognition or fingerprint, due to the need to capture a close-up of the eyes.
Facial recognition	It uses the device's video recorder to capture the end user's face and typically requires user to blink to perform liveliness check.	Works well with camera-enabled devices Good level of security if used in conjunction with device fingerprint	Some consumers will not want to enable their video. Liveliness tests are susceptible to spoofing.
Fingerprint biometric	It leverages a device's embedded fingerprint reader; remote channel use cases are currently focused on the mobile channel.	Decent level of security if used in conjunction with device fingerprint, certainly superior to usernames and passwords Easy to use	The sensors in mobile devices are cheap and lack liveliness tests. It is hard to get a good read on some consumers, particularly seniors or manual laborers, as fingerprints erode over time. Apple permits nine fingerprints to be associated with the device but doesn't tell the

Authentication type	Description	Pros	Cons
			FI whose fingerprint is in use.
Knowledge-based authentication (KBA)	KBA questions provide an additional layer of identity verification by establishing that the end user knows the answer to one or more personal questions.	Works with all device types and is understood by consumers	Due to data breaches and consumers' penchant for oversharing on social media, criminals have easy access to much of the data upon which the KBA questions are based.
Mobile network operator (MNO) data	Through direct, real-time interfaces with MNOs, this technology uses the same device hardware-based network authentication as MNOs to secure its own services. This enables positive verification that the device belongs to the person authorized on the mobile account as well as to provide notification if the device is lost or stolen.	Transparent to the end user Highly effective, given the reliance on source data from the MNO	Fraudsters have started perpetrating ATO attacks at the MNO level.
One-time password (OTP)	Sending a one-time password to a mobile device provides the ability to verify that the user has that device in his or her possession.	Used in an increasing number of use cases and well-understood by many consumers Secure when delivered by mobile app push to authenticate a transaction taking place online or in the contact center	If the transaction is performed in the mobile channel, then the OTP has limited value, since it does not provide a second factor of authentication. While OTP delivery via mobile app push is quite secure, SMS-based OTP delivery is vulnerable to SIM-swaps and malware-based attacks.
Two-way text	This is an SMS message sent to the consumer, to which they can reply, either approving or denying the transaction.	Ubiquitous—works for consumers with all types of mobile phones Provides an opportunity for a quick and easy dialogue between the business and its customer	SMS is susceptible to spoof, and delivery is not as certain as it is in the mobile app environment.
Voice recognition	It creates a unique biometric driven by the	Minimally intrusive on the user experience and can be completely	Technology is still subject to false positives.

Authentication type	Description	Pros	Cons
	characteristics of the end user's voice.	transparent if passive biometrics are used Applicable to a wide range of devices	

Source: Aite Group

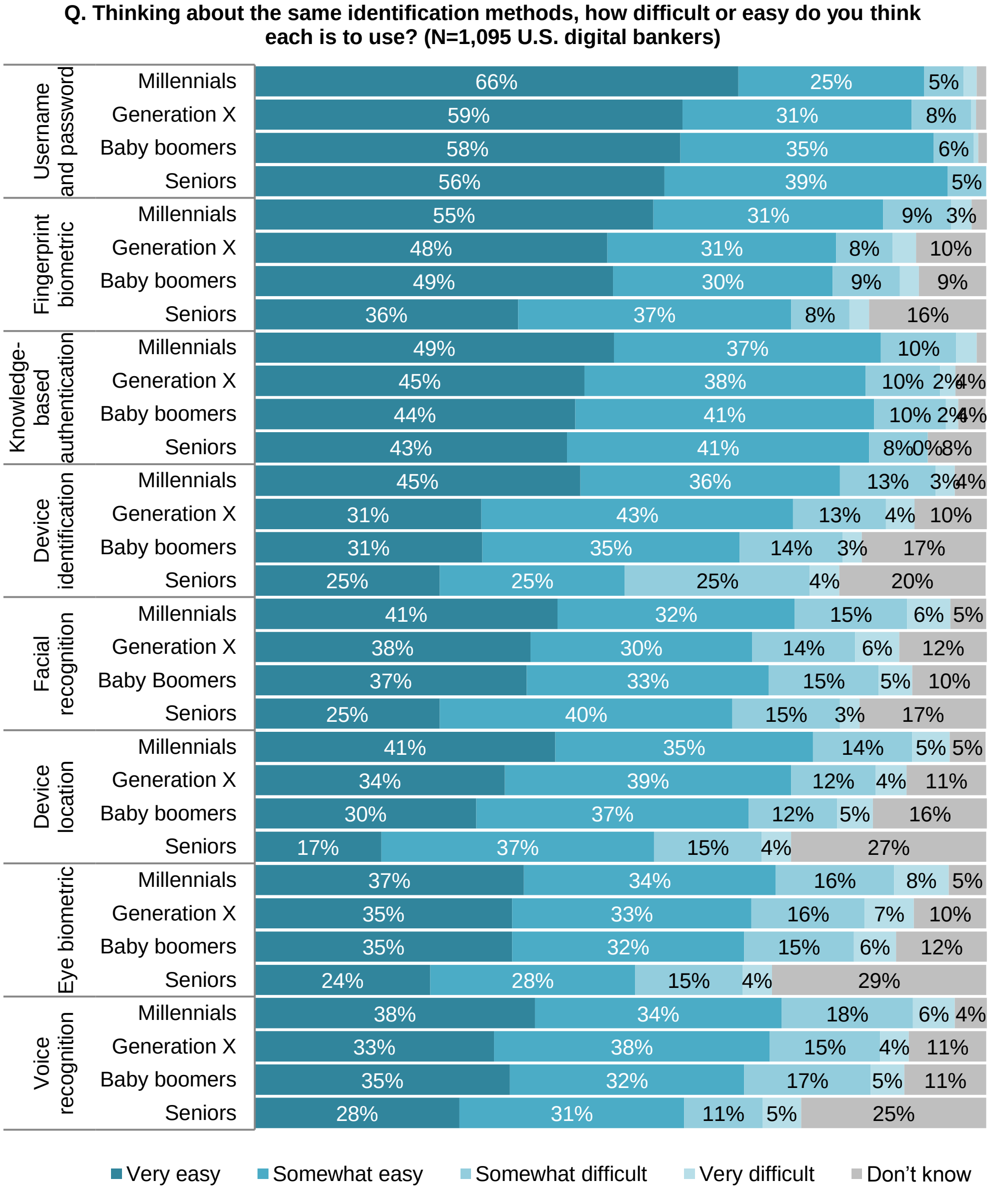
When Aite Group surveyed consumers about the ease of use and effectiveness of various forms of authentication (Figure 8), a few key learnings emerged:

- Familiarity equates to ease of use for many consumers; over 50% of all consumers deem username and password very easy to use (since most are using the same handful of usernames and passwords across all of their online relationships). Fingerprint biometrics come in second for ease of use, although seniors give it significantly lower marks than millennials, likely due to the fact that seniors tend to have lower read rates than younger generations.

- Consumers don't understand many of these concepts, even when provided with a brief description. Familiarity has a clear correlation with age—seniors are most likely to respond "Don't know" when asked about an authentication method, while millennials show the greatest degree of familiarity with the alternative authentication methods presented. The fact that device identification and device location—technologies that are completely transparent to the consumer—received relatively low marks for ease of use shows that these concepts are not well understood.

- While the millennials are stereotyped as being the "selfie" generation, only 41% believe that using the selfie as an authenticator is very easy. Username/password, the fingerprint biometric, device identification, and KBA all came in higher in perceived ease of use for this group. This could indicate that what works for social media does not easily translate to transactional activity without a concerted effort at education.

Figure 8: Perceived Ease of Use of Authentication Methods

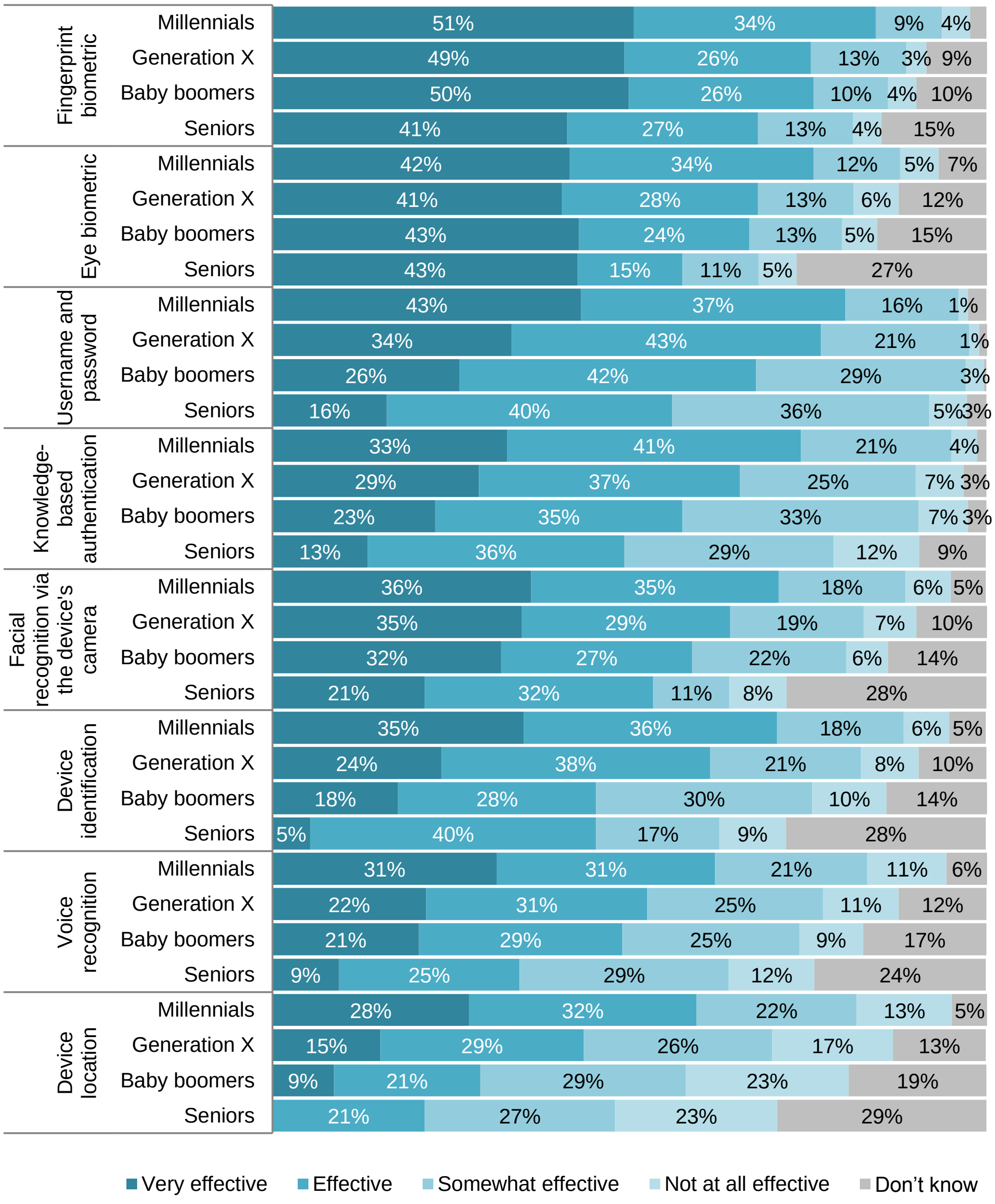


Source: Aite Group survey of 1,095 U.S. consumers, January 2017.

When asked about their perceptions of the effectiveness of each of these technologies, consumers clearly believe that the fingerprint and the eye biometrics have the edge (Figure 9). Opinions regarding the effectiveness of username/password were mixed; while 43% of millennials deem username/password to be very effective, only 16% of seniors share this opinion. Seniors are also more skeptical of KBA—while one in three millennials believe KBA to be very effective, that opinion is shared by just 13% of seniors (potentially meaning this group reads the news a bit more and is more aware of the vulnerabilities of both the password and KBA in this era of data breaches). While device identification ranked fairly low in terms of perceived effectiveness, many of the respondents also indicated that they didn't have a good understanding of the technology, which makes sense since it operates entirely behind the scenes.

Figure 9: Perceived Effectiveness of Authentication Methods

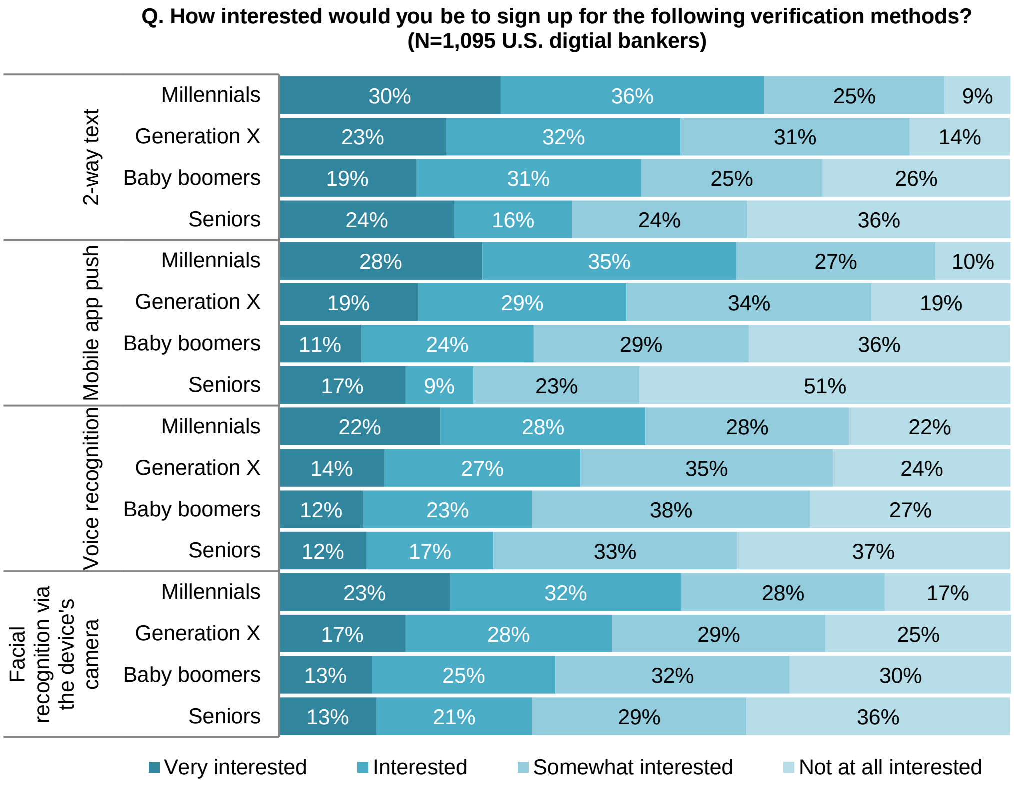
Q. How effective do you think each of the following is at accurately identifying you and preventing others from accessing your accounts? (N=1,095 U.S. digital bankers)



Source: Aite Group survey of 1,095 U.S. consumers, January 2017.

When asked about willingness to engage with specific authentication methods at the time of logging into an account, two-way text has a slight edge as the preferred method of interaction among all age groups, followed by mobile app push (Figure 10). SMS messages and mobile app push are already used by many FIs as a way to deliver alerts. This can serve as a path to habituation, that is, a way to train consumers to engage with these capabilities not only for notification of events, but for authentication as well.

Figure 10: Consumers' Willingness to Engage With Various Authentication Methods



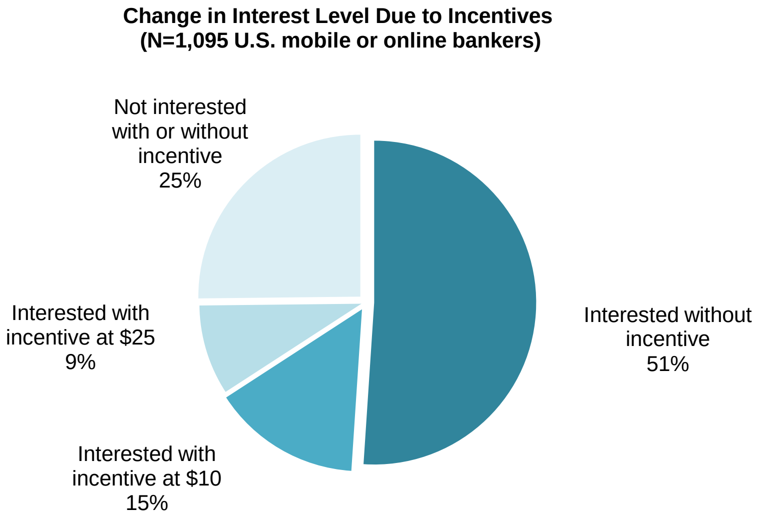
Source: Aite Group survey of 1,095 U.S. consumers, January 2017.

Consumers can be bought, and there is plenty of precedent that shows that incentives can go a long way toward influencing customer behavior. A prime example of this is the lukewarm reception that consumers have given open-loop mobile wallets such as Apple Pay and Android Pay. Fewer than 10% of U.S. banked consumers regularly use these open-loop mobile wallets, which provide little incentive for consumers to change their behavior aside from a "cool factor." In contrast, Starbucks now sees over 25% of its total U.S. payment volume coming in through its mobile app, which provides free caffeinated beverages in exchange for regular use.[5]

While 51% of consumers say that they would be willing to proactively sign up for a variety of stepped-up authentication methods without any form of monetary incentive, an incremental 24% of consumers say that they would be willing to do so if the bank offers a cash bonus of US$10 to US$25 (Figure 11).

[5] Rian Boden, "Mobile Payments Account for 25% of all U.S. Starbucks Transactions," NFC World, November 8, 2016, accessed March 1, 2017, https://www.nfcworld.com/2016/11/08/348311/mobile-payments-account-25-us-starbucks-transactions/

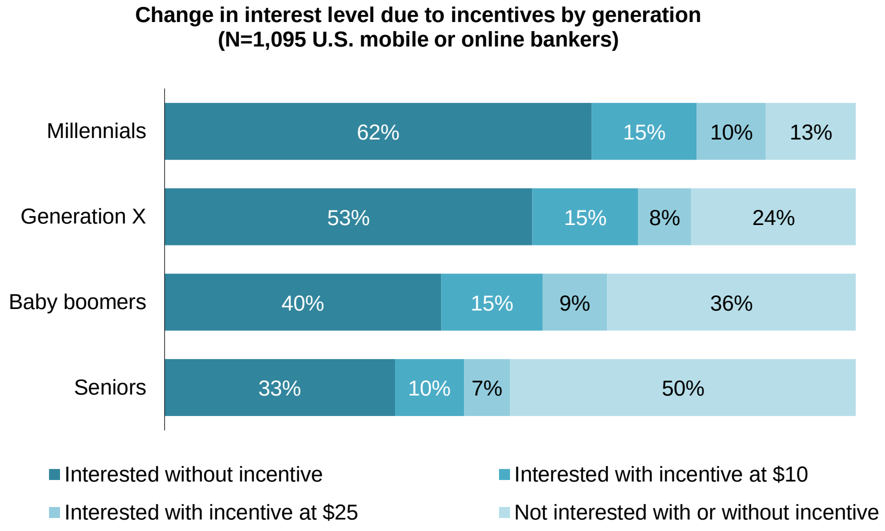
Figure 11: Incentives' Ability to Sway Consumer Behavior



Source: Aite Group survey of 1,095 U.S. consumers, January 2017.

Millennials are the most receptive to a new authentication experience, with 62% of millennials willing to engage with new authentication methods without the incentive, while seniors, at one in three, are the least receptive. The impact of the cash incentive on adoption is roughly equal across the generations, with the cash incentive increasing senior adoption by 17% and 25% for millennials (Figure 12).

Figure 12: Incentives' Ability to Sway Consumer Behavior by Generation



Source: Aite Group survey of 1,095 U.S. consumers, January 2017.

CONCLUSION

The need for FIs and merchants to move beyond a password for customer authentication is clear. Here are a few recommendations for executives as they are plotting their course.

- **Start with the mobile channel.** The mobile environment lends itself very nicely to expanding authentication methods, since keying the username/password into the tiny mobile keyboard is already a suboptimal user experience. Transitioning authentication to a biometric increases security while concurrently improving the customer experience.
- **Enable multiple forms of authentication.** A layered approach to authentication has long been a best practice—starting with technologies that are transparent to the end user, then selectively introducing stepped-up authentication measures commensurate with the context and risk of the transaction. Enabling multiple forms of stepped-up authentication provides flexibility—if criminals begin to exploit a vulnerability in a particular authenticator, then the FI or merchant can shift nimbly to another method. This approach also has the potential to give consumers the ability to choose the form of authentication with which they are most comfortable. The data shows that what works for millennials may not be the best option for baby boomers or seniors.
- **Leverage the complementary nature of notification and authentication strategies.** Consumers are becoming accustomed to receiving alerts and notifications from their FI via SMS and the mobile app. As that behavior pattern takes hold, it is a relatively small step to then move to using those channels for authentication as well.
- **Tailor education to customers' demographic group.** The data clearly shows widely differing comfort and understanding of the various forms of authentication. FIs and merchants need to take this into consideration as they are tailoring their messaging and educational efforts.
- **Consider providing incentives to shift behavior.** Changing ingrained habits is always difficult, and the use of passwords is certainly a comfortable habit for most consumers. As Starbucks has shown with the success of its mobile app, however, consumers respond to incentives, and the research shows that millennials will be particularly responsive.

RELATED AITE GROUP RESEARCH

Top 10 Trends in Retail Banking & Payments, 2017: Data Analytics Differentiate, January 2017.

Global Security Engagement Scorecard™, November 2016.

Biometrics: The Time Has Come, October, 2016.

2016 Global Consumer Card Fraud: Where Card Fraud Is Coming From, July 2016.

EMV: Issuance Trajectory and Impact on Account Takeover and CNP, May 2016.

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Julie Conroy
+1.617.398.5045
jconroy@aitegroup.com

Research Design and Data:

Sarah Fitzsimmons
+1.617.398.5039
sfitzsimmons@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com