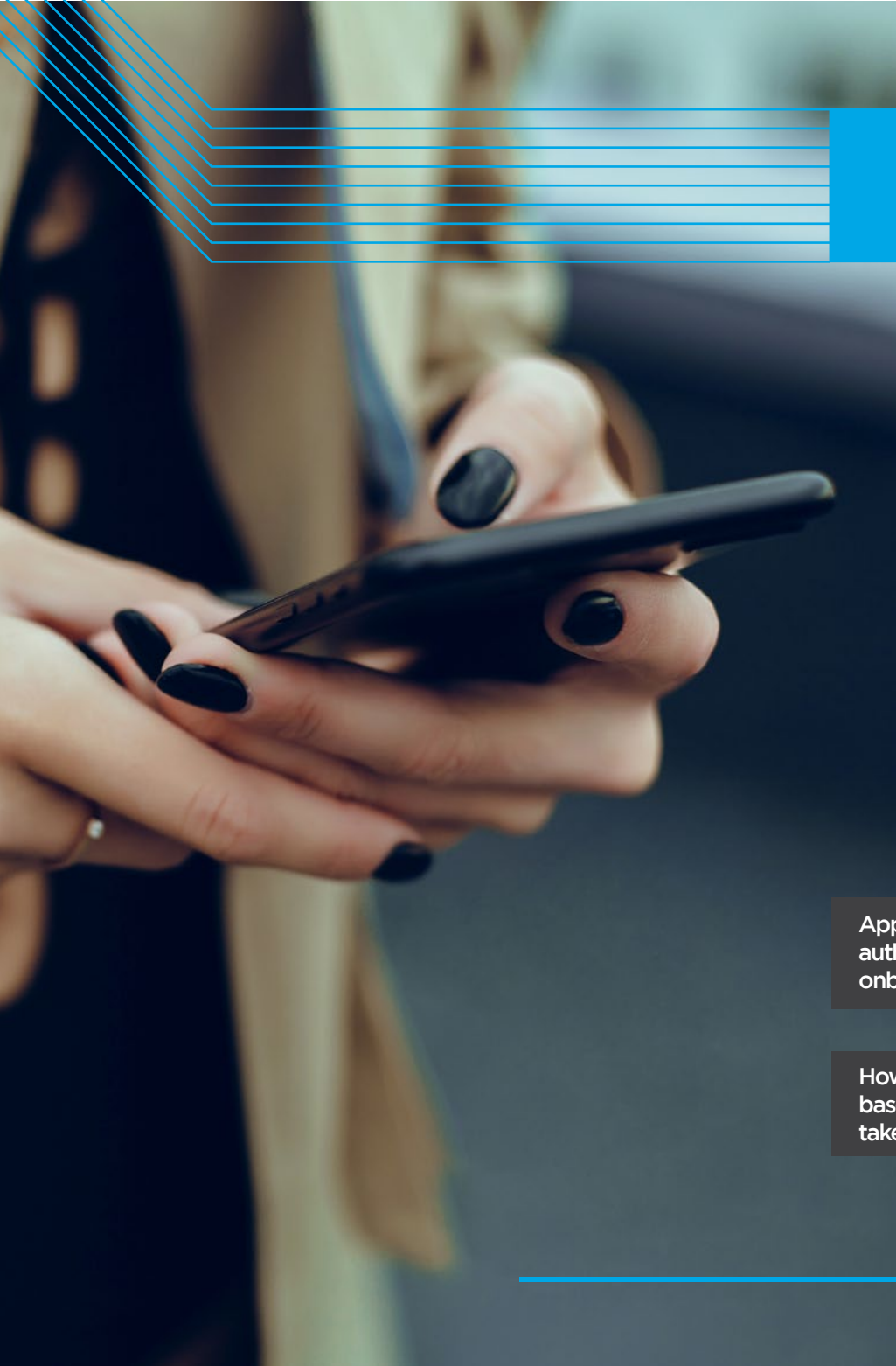


DIGITAL

CONSUMER ONBOARDING

TRACKER®



Embr Labs On Driving Customer Engagement, Checkout Conversion With SMS Services

PAGE 7 (FEATURE STORY)

Apple unveils “domain-based” SMS authentication feature for added onboarding, checkout security

Page 10 (News & Trends)

How organizations are turning to phone-based verification as more consumers take their digital shopping habits online

Page 15 (Deep Dive)

TABLE OF CONTENTS

03 WHAT'S INSIDE

A look at how retailers, banks and other organizations are utilizing 2FA – especially phone- or text message-based verification methods – to protect the growing number of customers transacting online

07 FEATURE STORY

An interview with Sam Shames, co-founder and chief operating officer of Boston-based thermal wellness startup Embr Labs, on fueling consumer engagement via text messaging to counter cart abandonment and unlock sales growth

10 NEWS AND TRENDS

Recent onboarding headlines, including Tesla's move to enable customers to sign in to their accounts using text message-based verification codes and a study's discovery that 51 percent of North American banks still require consumers to visit in person to complete account setups

15 DEEP DIVE

An in-depth examination of how various businesses and financial services providers are embracing text message-based verification measures even as some in the retail sector fear it will drive customers away

17 ABOUT

Information on PYMNTS.com and Melissa

ACKNOWLEDGMENT

The Digital Consumer Onboarding Tracker® was done in collaboration with Melissa, and PYMNTS is grateful for the company's support and insight. [PYMNTS.com](https://pymnts.com) retains full editorial control over the following findings, methodology and data analysis.

WHAT'S I N S I D E

More consumers are going digital during the COVID-19 pandemic than ever before, using online channels to sign up for various services, purchase groceries and transact with their banks while minimizing the risk of contagion. Many businesses and organizations were already observing a growing number of users migrating online, and the dramatic shift since the health crisis began in March has made them eager to invest in the channels and find ways to better safeguard customers' information.

Two-factor authentication (2FA) is getting considerable attention as an especially useful and effective method through which to protect consumers' personal and payment information, but this method has drawbacks. Many retailers are concerned that adding another authentication step could create undue friction and ultimately lead consumers to abandon their account sign-ups or

purchases. These worries are not unfounded, either, as one recent [survey](#) found that roughly 50 percent of consumers reported ditching onboarding attempts over the past year because they perceived them to be too cumbersome or untrustworthy.

There could be a solution that meets most customers' speed and security needs without significantly stalling onboarding or checkout processes, however. Many financial services providers and businesses are leveraging 2FA that relies on short message service (SMS) — or text message-based — verification to cater to an increasing number of consumers who are using mobile channels for their daily activities. This method comes with its own share of challenges, but some research suggests that it could help merchants, banks and other players safeguard their customers without slowing them down.



AROUND THE DIGITAL ONBOARDING SPACE

Ease, convenience and security were all factors that influenced Tesla to recently unveil 2FA for its car owners. The California-based electric vehicle company [announced](#) earlier this month that it would allow owners to sign up and sign in to their accounts using SMS-based 2FA, with consumers supplying their credentials and receiving verification passcodes via either a third-party authentication app or text message. Car owners can use their accounts to unlock their vehicles, locate them and turn on select features. This added security measure had been a longtime request from many consumers.

Businesses from all sectors are also turning to novel digital solutions – including those designed to streamline onboarding – during the pandemic. India-based startup WorkApps, which offers a video-based chat solution, recently announced that it would [boost](#) its communications network and help companies adopt various business functions and features, such as

video-based know your customer (KYC) verification. The company's co-founder and CEO, Rudrajeet Desai, said the moves are intended to help customers operate remotely and save time and resources on standard business operations.

Other companies are working together to enhance digital identity verification efforts and speed up consumer onboarding processes. Two digital verification companies recently announced that they were [partnering](#) to deliver more than 400 applicants per minute to the GOV.UK Verify platform, which allows consumers in the United Kingdom to access select governmental services. The pair's verification solution allows users to scan valid ID forms and snap selfies to authenticate themselves.

For more on these stories and other headlines from the space, read the Tracker's News and Trends section (p. 10).



EMBR LABS ON REDUCING CART ABANDONMENT, PROPELLING SALES GROWTH WITH TEXT MESSAGING

Global spending on SMS marketing is expected to [reach](#) \$83 billion by 2024 as more eCommerce merchants seek to directly communicate and engage with consumers at home. Text messages have proven to be an effective way to connect with potential customers, as 90 percent of consumers [open](#) and read their texts within three minutes.

Boston-based thermal wellness firm [Embr Labs](#), which produces a wearable device for controlling body temperature, is one such merchant leveraging SMS services in response to sales data revealing that a majority of orders were made from mobile devices. For this month's Feature Story (p. 7), PYMNTS spoke with company co-founder and chief operating officer Sam Shames on how the firm uses SMS to smooth checkout experiences, avoid cart abandonment and drive revenues.

DEEP DIVE: THE POSITIVES — AND CHALLENGES — OF SMS-BASED VERIFICATION

Droves of consumers are heading online to accomplish more of their everyday tasks digitally, prompting banks, businesses and other organizations to look for enhanced security measures like those offered by 2FA. Many are hoping to meet customers where they are by leveraging phone- or SMS-based authentication methods that offer the seamless, convenient sign-up and purchasing experiences consumers crave. This month's Deep Dive (p. 15) explores organizations' efforts to bring 2FA and phone-based verification methods into the security fold and spotlights the benefits and drawbacks that they present.

EXECUTIVE INSIGHT

What is the potential of using phone and SMS-based verification for improving the onboarding process and reducing shopping cart abandonment?

"Phone verification and cross-checking is an important part of a comprehensive way to verify identity quickly, [frictionlessly] and cost-effectively. Over 80 percent of respondents in a recent survey reported fake users as a significant problem. When you onboard a new customer, phone verification makes it easy to verify they are who they say they are — before they enter your database — by connecting with the mobile device associated with the entered phone number. Using multisourced data from national and international 411 directories and proprietary sources, you can get valuable data attributes and risk assessment indicators including number ownership, whether the number is active and callable, line type and geographic information like country of origin. Additionally, phone verification is a vital component of two-factor authentication. [Your company can] easily send a one-time verification code via SMS or voice message or through your mobile app to authenticate a known user or verify a transaction. Phone verification provides your business with the ability to provide an additional layer of security to assure your customers that their accounts are safe and secure — quickly and unobtrusively."

BUD WALKER
chief strategy officer at [Melissa](#)

5

Five Fast Facts

73%

Share of consumers who are frustrated by onboarding process inefficiencies



84M

Number of Americans who have signed up for services online that formerly required in-person completion since the pandemic began



8%

Share of financial services onboarding applications that can be completed on mobile devices



21%

Compound annual growth rate of the SMS market from 2019 through 2027



78%

Portion of consumers who claim that text messages offer more confidence when dealing with their banks



A hand holding a smartphone, with a blue tint overlay across the entire image. The phone is held in the lower left, and a finger is visible on the right side, possibly interacting with the screen. The background is blurred, showing what might be another person or object.

FEATURE STORY

EMBR LABS ON DRIVING CUSTOMER ENGAGEMENT, CHECKOUT CONVERSION WITH SMS SERVICES

More businesses are making moves to add text messaging services to their customer engagement and checkout conversion toolkits — and for good reason. Research [indicates](#) that 98 percent of consumers open and read their text messages, unlike marketing emails, which can easily get buried or fall into spam folders. This advantage highlights a massive missed opportunity: 61 percent of marketers still do not deploy text messages.

The chance to have customers' immediate attention is also possible through SMS, as typically 90 percent of such messages are [looked](#) at within three minutes. Text messages are an increasingly effective way to engage with customers, provide order updates, offer mobile coupons and share marketing pitches — ultimately driving revenue growth.

One company using SMS to reach its customers is Boston-based thermal wellness startup [Embr Labs](#), whose name is derived from an acronym for “environment, mind, body and resonance.” The company produces the Wave bracelet, which [harnesses](#) thermal sensations to deliver natural therapies and promises to cool or heat wearers with the press of a button. The wearable Apple Watch-like device and coordinating app allow users to essentially trick their brains into controlling their body temperatures, also helping to regulate the body to more easily drift off to sleep.

The wearable technology can warm or cool the body like holding a cup of hot chocolate or iced tea, according to Embr Labs' co-founder and chief operating officer, Sam Shames. The bracelet, originally named Wristify, was born out of necessity at MIT's Department of Materials Science and Engineering.

“We were in a lab space that was consistently over-air-conditioned, and it forced us to wear sweatshirts,” Shames said in a recent interview with PYMNTS. “I just said, ‘Man, there’s got to be a better way. Why can’t we cool ourselves directly?’ And we came up with the idea

as we brainstormed. It was really driven by the belief that temperature can be a tool to help people feel better and live better.”

Shames said the Wave serves a range of demographics, but its core userbase has turned out to be women between the ages of 45 and 65 who are menopausal or have sleeping issues.

“They’re in the prime of their lives, and they don’t want to let things like hot flashes or trouble sleeping slow them down,” he said.

HOW TEXT MESSAGING HELPS FUEL GROWTH

Shames said Embr Labs' strategy of text messaging to reach its customers came after its sales data revealed a majority of orders were being made from mobile devices. He said the finding motivated the team to provide customers with a more intuitive, simple way to communicate.

“Getting a text message with information is just fundamentally easier on your phone than email,” Shames said. “Ultimately, our North Star is the customer, and [we listen] closely to them.”

Embr Labs embraced text messaging as a way to more personally connect with consumers and help improve the checkout experience, counter cart abandonment and drive sales. Embr Labs will text customers who have abandoned carts recently with a promotion to entice them to complete their purchases.

Embr [works with](#) a third-party messaging provider to leverage not only text messaging customer service but also machine learning and artificial intelligence that offer customer insights.

“They invite customers who want the option to communicate with us through SMS,” Shames said. “Through that kind of market intelligence, we’re able to provide

special offers and identify things we can do to make the experience easier.”

SMS ADOPTION TO EXPAND

SMS’s range of benefits means that merchants’ use of it for customer outreach is expected to grow in popularity. Global spending on SMS marketing is [projected](#) to be \$83 billion by 2024. A recent research report also [predicts](#) that consumers will get more texts next year than ever before, with volumes increasing by 40 percent as brands strive for more direct relationships

with customers amid the COVID-19 pandemic’s economic fallout.

Consumers have relied more on online and mobile commerce since mid-March, so increasing communication budgets and engaging consumers via text message is a natural next step for companies like Embr Labs and merchants within the retail and technology spaces at large.



NEWS &

TRENDS

TEXT-BASED VERIFICATION DEVELOPMENTS

TESLA ANNOUNCES THAT CUSTOMERS CAN NOW PROTECT ACCOUNTS WITH 2FA

Tesla Inc. CEO Elon Musk recently made good on a promise regarding more robust consumer verification measures. The California-based electric vehicle company [announced](#) that customers would be allowed to safeguard their accounts using 2FA either by receiving and submitting codes sent to third-party apps or by inputting one-time codes sent via text to their smartphones. Tesla owners who enter their passwords and these one-time codes can access their accounts to unlock their vehicles, power numerous features, locate their cars and perform other tasks.

The decision to allow customers to use third-party apps or text-based messages to receive verification codes reflects the company's desire to ease consumers' security concerns, which are understandable, given the value of its vehicles. Tesla's lowest-priced model, the Model 3, retails for \$41,190, and its all-wheel-drive Long Range model starts at \$50,190.

APPLE UNVEILS 'DOMAIN-BOUND' SMS CODES TO BOOST SECURITY OF ONE-TIME PASSCODES

Many consumers appreciate SMS-based verification measures for the convenience and security they offer during onboarding as well as checkout, but some experts have warned that the unencrypted nature of these text-based messages can make them prime targets for fraudsters. Technology giant Apple recently [announced](#) a

format change to its SMS system that the company says could bolster the security of one-time passcodes sent to iPhones, however. It said that its iOS 14 mobile operating and macOS Big Sur systems would be compatible with "domain-bound" codes delivered via SMS. This technology will enable iOS and macOS to autofill these codes only for websites or apps with domains that are associated with the SMS messages that have been sent to users. The company said that this would make it more difficult for fraudsters to convince users to enter their codes on fake websites, and it urged developers to adopt the new standard to further safeguard one-time SMS passcodes.

DIGITAL ONBOARDING PARTNERSHIPS

IBM, FENERGO PARTNER TO OFFER AI-BASED ONBOARDING FOR FIs

Some solution providers are collaborating to unveil new digital onboarding technologies in various sectors. Tech giant IBM and Dublin-based client lifecycle management solutions company Fenergo, for example, have [partnered](#) to incorporate artificial intelligence (AI) and analytics on the IBM Cloud to help financial institutions (FIs) more easily sign up new customers. Recent research shows that it can take up to 12 weeks for FIs with limited onboarding capabilities to onboard clients, and banks face fines and other sanctions if their processes fail to take into account all relevant anti-money laundering (AML) and KYC regulations. Fenergo and IBM said the collaboration aims to help banks transform their digital operations and enhance customers' experiences.

MITEK, DIGIDENTITY WORKING TOGETHER TO SPEED GOV.UK ONBOARDING

Companies in the U.K. are also partnering to overhaul digital onboarding solutions and ensure that more residents register with [GOV.UK Verify](#), a public sector information website that allows residents to securely prove their identities online and access select government services. San Diego-based ID verification company Mitek and Dutch identity provider Digidentity [announced](#) that they have jointly delivered more than 400 applicants per minute to GOV.UK Verify since March, resulting in a total of more than 1 million verified accounts. Users are asked to scan their IDs and take selfies, then allow the firms' automatic authentication platform to verify them. In-person verifications are reserved for complex cases only, and multiple checks have been put in place to prevent fraud.

VIDEO KYC SOLUTIONS

FIRM'S VIDEO KYC PLATFORM ONBOARDS MILLIONS OF NEW CUSTOMERS FOR INDIA'S BANKS

India-based startup WorkApps, which provides video-based chat platforms for companies of all sizes, recently [announced](#) moves to improve its communications network and enhance key business functions, including onboarding processes. Rudrajeet Desai, the company's co-founder and CEO, said the upgrades will help banks conduct more of their processes remotely via video. Visits to branches are currently being limited to prevent the spread of COVID-19. The company said the development of video KYC on Amazon Web Services, the cloud-based platform that powers more than 1 million enterprises, enables banks to focus on product and feature development and dramatically reduces the time it takes to onboard customers from as long as two days to roughly 15 minutes. Desai said FIs can save approximately 90 percent on KYC costs when such processes are conducted via video.



INDIA'S PENSION SYSTEM ALLOWS SUBSCRIBER ONBOARDING VIA VIDEO

The Pension Fund Regulatory and Development Authority (PFRDA) of India recently announced that the country's National Pension System subscribers can [utilize](#) video-based customer identification to more easily open accounts and withdraw funding. Numerous pension system services have shifted online along with onboarding, but many pensioners must still appear in person to verify their identities and complete the process. The requirement has led to subscriber complaints and withdrawal delays.

PFRDA's announcement comes after the Insurance Regulatory and Development Authority of India [declared](#) that it had given insurance firms approval to use video-based authentication to ease KYC processes. The move allows these companies to join banks and mutual fund businesses in enabling their customers to complete video-based identity verification.

PANDEMIC-DRIVEN ONBOARDING SHIFTS

COMPANIES TURNING TO AI FOR ONBOARDING ASSISTANCE

Businesses are also turning to advanced technologies like AI to help them efficiently manage remote onboarding while protecting consumers from fraudsters during the pandemic. Such shifts are especially crucial because recent research [shows](#) that strict procedures for detecting and preventing money laundering as well as verifying consumers' identities can cause potential customers to abandon their sign-ups. One recent study showed that almost half of all U.S. consumers have ditched an online account opening attempt within the past year because they thought it was too complicated or could not be trusted, up from 37 percent the previous year. Two-thirds

of respondents also told researchers they fear companies will fail to protect their personal data.

Consumers in another recent [study](#) said that they preferred onboarding experiences that prioritize security ahead of speed, while 73 percent reported that their patience regarding account opening experiences had waned. Online merchants seem to be heeding these trends, leading some to utilize AI to determine how much friction to apply to the multitude of transactions that now occur digitally.



MORE THAN HALF OF NORTH AMERICAN BANKS REQUIRE BRANCH VISITS FOR ONBOARDING, STUDY SAYS

U.S. and Canadian consumers who have developed digital habits during the pandemic are more open to completing bank account sign-up processes digitally, but a recent FICO [survey](#) shows that many banks are not set up to allow them to do so. The study revealed that 51 percent of FIs in North America still require customers to visit branches to prove their identities or scan documents to complete applications. It also noted that just 16 percent of banks allow total digital onboarding and offer the tools necessary for customers to securely open accounts online.

North American banks' practices appear to be out of step with what consumers seek, however. Another FICO study [found](#) that 75 percent of consumers would be comfortable opening financial accounts online, though 23 percent of would-be customers said they would abandon their applications if they provided inconsistent identity verification processes. Liz Lasher, vice president of portfolio marketing for fraud at FICO, said that banks ultimately risk losing customers if their anti-fraud practices miss the mark and that FIs must be equipped to meet consumers' expectations for seamless and secure online experiences.



SURVEY SHOWS THAT 72 PERCENT OF FIRMS HAVE ADOPTED DIGITAL ID VERIFICATION DURING THE PANDEMIC

North American banks may be lagging in adopting seamless, wholly digital onboarding experiences, but this does not seem to be the case for the region's businesses. New research reveals that companies have [boosted](#) their identity verification processes to protect consumers during the COVID-19 pandemic, with 72 percent of eCommerce marketplaces adopting digital ID verification technology. The study suggested that online merchants had to quickly add the technology to serve customers and maintain safe operations. Ninety percent of U.K. and U.S. customers also said security is key to creating excellent account opening experiences, and 89 percent said online marketplaces must work to reduce cybercrime through any identity verification means necessary.

DIGITAL SALES CAPABILITIES CRITICAL TO FIS' HEALTH, REPORT FINDS

The pandemic continues to limit hours and customer capacity at bank branches, leaving many FIs dependent upon digital sales capabilities to keep their operations afloat. A [report](#) from one technology service and digital transformation consulting firm recently showed that banks are aiming to maintain digital sales for new customers, increase the number of digital products they offer and cross-sell to customers to increase returns on investment. Consumers also want local banks to provide the same frictionless experiences they receive from Big Tech companies, and numerous banks are adopting digital technologies and collaborating with third-party providers to boost customer service and stay competitive. The report recommended that banks invest in training to prepare their workforces for digital innovations and developments.



DEEP

D I V E

USING PHONE VERIFICATION AND TEXT MESSAGING FOR SECURE CHECKOUTS

Many banks, utility companies and government agencies have been leveraging two-factor authentication (2FA) for several years. This process requires consumers to provide not only their usernames and passwords to access services but also an additional form of verification, such as a biometric identifier or a code that can be emailed to them or sent via text message. The U.S. Social Security Administration, for example, requires recipients using its website to provide unique eight-digit codes sent via text to their smartphones in addition to their usernames and passwords when they sign up or log in.

It appears that these stepped-up verification approaches are warranted, too, as tales of security breaches that have ensnared unsuspecting internet users are rampant. Recent research [suggests](#) that more than two-thirds of consumers use the same passwords for all websites, which can be especially problematic when fraudsters deploy software that enables them to crack about 90 percent of passwords in less than six hours. Another recent report [underscored](#) these issues' pervasiveness, finding that 81 percent of data breaches three years ago were perpetrated using stolen or weak passwords and that this share had fallen only 1 percentage point by 2019.

A silver lining exists, however. A study [found](#) that businesses and other organizations could prevent roughly 80 percent of data breaches by leveraging 2FA. Numerous options are available to organizations determining the verification methods to utilize for 2FA, but phone-based verification has caught on for its ease of use and ubiquity. The process can be as [simple](#) as prompting a user to supply and verify a phone number during onboarding, which

enables organizations to either send text-based codes for additional authentication or ask consumers to input the phone numbers associated with their accounts when they attempt to log in or check out. This method is not without frictions, however, which are giving some businesses — especially retailers — pause.

The following Deep Dive examines businesses', FIs' and other organizations' use of phone-based verification and text messaging to help customers secure their accounts and ease the checkout process. It also outlines some of the frictions entities face when doing so.

LEVERAGING PHONE-BASED VERIFICATION

Phone- and text-based verification and authentication measures for consumers have been commonplace for several years, but the COVID-19 pandemic's dramatic acceleration of digital adoption is putting renewed focus on the technology. Recent research [found](#) that since the pandemic's onset, 84 million Americans have looked for services online that they had previously sought out in person, and 75 percent say they expect to maintain some of these new habits once the health crisis ends. A key facet of this shift has been an increased reliance on mobile phones. Reports show that the number of consumers who have used their smartphones to open accounts has increased 43 percent since March. Authentication measures that meet these customers where they already are — on mobile channels — could therefore be key to signing them up frictionlessly, keeping them engaged and safeguarding their checkout experiences.

Some experts have noted that text message-based measures are not as robust or fraud-proof as other potential 2FA factors, such as biometrics, but there is reason to [believe](#) that SMS verification offers enough protection for the average consumer. Many fraudsters' schemes rely on targeting customers whose information is relatively easy to obtain, and forcing bad actors to confront even minor obstacles in their efforts to snatch personal data can prompt them to abandon their tactics.

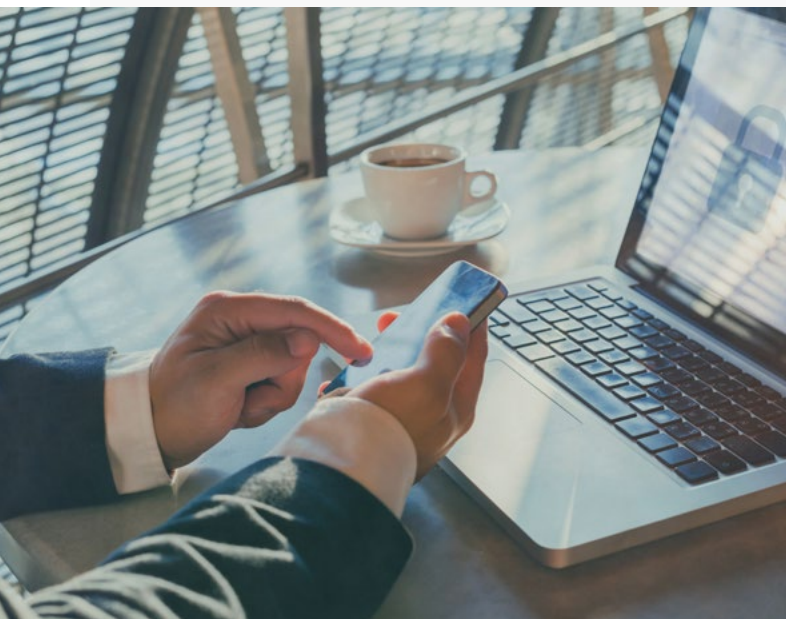
There are other reasons to speed up ID verification by using 2FA methods, including text- or phone-based verification, that minimize friction. Roughly half of consumers have [reported](#) abandoning online account sign-ups in the past year due to the process being perceived as too cumbersome or untrustworthy. That number appears to be rising, too, as just 37 percent of consumers said the same last year. The other factor to consider is that nearly two-thirds of consumers told researchers they are not convinced companies are protecting their personal data, leading an increasing number to opt for 2FA when such options are offered.

THE PITFALLS OF TEXT-BASED VERIFICATION

Social media, financial and email platforms have been relatively quick to adopt 2FA measures that leverage phone-based verification, but the retail sector has been slow to embrace the technology. These measures add security to the sign-up and checkout processes, but they do represent another barrier to purchasing that leaves retailers worried about their conversion rates.

Consumers have also expressed reservations about giving their smartphone numbers to businesses. One [survey](#) found that 58 percent say they already receive too many notifications from companies. The results suggested that consumers trust big-name companies such as Amazon or Uber to text them about deals or financial details, but they are likely to reject notifications from lesser-known brands, especially those perceived to be overly focused on marketing. Many consumers do appreciate receiving more information in key areas, however, with 71 percent noting that they liked receiving messages from retailers about a pending purchase and 73 percent saying they welcomed messages about potential fraud from their banks.

Consumers are flocking to digital channels in droves during the pandemic, and many businesses and organizations are eager to enhance their security measures by leveraging 2FA that incorporates phone-based verification. Evidence suggests that these moves can help retailers and others set consumers' minds at ease during onboarding and purchasing, but outreach could be necessary to allay fears.



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

melissa®

Bad data is bad business. [Melissa](#) helps organizations profile, cleanse and verify, dedupe and enrich all their people data (name, address, email and phone number) and more. With clean, accurate and up-to-date customer information, organizations can monetize Big Data, improve sales and marketing, reduce costs and drive business insight.

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

DISCLAIMER

The Digital Consumer Onboarding Tracker® 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. The Digital Consumer Onboarding Tracker® is a registered trademark of What's Next Media & Analytics, LLC ("PYMNTS.com").