melissa | PYMNTS.com

DIGITAL
CONSUMER ONBOARDING
TRACKER®

Digital-first Quontic Bank on upgrading its onboarding for enhanced customer service

PAGE 06 (FEATURE STORY)

COVID-19 advances global banks' digital onboarding efforts

Page 10 (News & Trends)

How outdated data can cause onboarding problems for FIs

Page 14 (Deep Dive)

APRIL 2020

TABLE OF CONTENTS

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 retains full editorial control over the findings presented, as well as the methodology and data analysis.

WHAT'S INSIDE

Businesses and financial institutions (FIs) alike face many challenges when enabling secure and seamless onboarding experiences — which, if not offered, can lead customers to abandon sign-up. Providing such processes is often easier said than done, however, as problems can arise when customers are required to submit physical paperwork for manual review or when the experience is not fully digital.

A one-step digital, two-steps paper experience can significantly contribute to customers' frustrations, especially with the ongoing COVID-19 pandemic, which is restricting customers from visiting physical bank locations. Many banks are thus taking closer looks at know your customer (KYC) and onboarding solutions that deliver both fast and secure onboarding experiences. Several players are hoping that biometric-based authentication procedures will provide seamless options for customers, while others are building and utilizing more reliable data sources for verification.

Enabling frictionless onboarding experiences is key for FIs looking to compete with FinTechs as well as for technological giants like Facebook and Google that are venturing into the financial services space.

PYMNTS' Digital Customer Onboarding Tracker® will cover these and more trends while also delving into the ways in which FIs and business-to-business (B2B) and business-to-customer (B2C) firms are leveraging digital KYC and anti-fraud innovations to streamline and optimize their onboarding processes. The inaugural issue of this Tracker will detail the lay of the land in the digital onboarding space, focusing on why businesses and FIs should utilize accurate data throughout their onboarding processes and how doing so improves customer conversions.

AROUND THE DIGITAL ONBOARDING WORLD

Many banks have made efforts to innovate their onboarding processes, but there are just as many that continue to rely on legacy solutions that require branch visits. Sixty percent of banks in the Asia-Pacific (APAC) region have yet to implement digital onboarding solutions, for example. This reliance on branch-based onboarding represents a significant weakness for banks, especially in the face of the ongoing pandemic, which has shuttered typical operations for most — if not all — FIs and other businesses. The need to find technologies and other solutions that could help bridge this gap is immediate and may lead many to accelerate their adoption of new tools.

COVID-19's spread may also result in wider biometrics and blockchain adoption, with two Canadian banks, including the Royal Bank of Canada (RBC), announcing the implementation of biometric identification tools in their mobile onboarding processes. This occurred just weeks before COVID-19 prompted stay-at-home orders and global closures of businesses and physical branch locations. RBC is also allowing its customers to scan their passports for quicker identification, which could prove to be particularly useful during the ongoing pandemic.

COVID-19 is also likely to have a long-term effect on how FIs handle their KYC collection process. Two separate economic entities in Dubai launched KYC platforms last month that use blockchain technology to enhance the speed and ease of access to crucial data FIs and third parties need for accurate and more secure onboarding. The platforms come as the government seeks to entirely eliminate paper-based processes within the region by 2021.

For more on these stories and other digital onboarding headlines, check out the Tracker's News and Trends section (p. 10).

HOW DIGITAL-FIRST QUONTIC BANK IS INNOVATING ONBOARDING FOR DIGITAL CUSTOMERS

Consumers expect quick digital experiences, but it can be difficult for FIs to provide the seamless, immediate engagement that many see with online retailers. The fraud protection and enhanced security measures FIs must take to ensure that new and existing customers are legitimate complicates authentication, as data used in onboarding must be up to date and corroborated with alternative sources. In this month's Feature Story (p. 6), Patrick Sells, chief innovation officer for digital-first, New York City-based FI Quontic Bank, explains why fast identity verification and robust data are critical to creating the frictionless onboarding experiences customers crave.

DEEP DIVE: FIs AND THE OUTDATED DATA PROBLEM

Enabling smooth onboarding experiences is often the most important step toward creating strong and long-lasting customer relationships. Clunky first interactions can prompt customers to look for new service providers, putting pressure on FIs to create fully digital account creation processes that do not take up much time. FIs must thus quickly verify users' identities, which often takes longer than any other part of the onboarding process. Those looking to remain competitive must examine how they authenticate users and which data they are using, as outdated information can add friction to already frustrating processes. This month's Deep Dive (p. 14) analyzes how outdated data can cause significant onboarding and security problems as well as the steps that can be taken to ensure FIs have access to the details they need to make onboarding as effortless as possible.

EXECUTIVE INSIGHT

How important is current and accurate data in the onboarding experience and what are some of the common errors FIs typically make?

"FIs are under increasing pressure to successfully balance the regulatory mandates for compliance, like the EU's 5AMLD that became law in January, with the need for fast, seamless onboarding. Inefficient onboarding is a key driver behind a 56 percent abandonment rate for banking customers. This means FIs must ensure that the ID verification process takes place in real-time. A real-time process has to mitigate the … data entry errors that are common during the application process, which include manual data entry and duplicate data.

Fat fingers are a big fat problem for mobile users, resulting in erroneous information being typed into online applications, including mistyped street addresses or postal codes. One must also determine if a new customer is a duplicate record before it enters your system, but similar records can be hard to identify as duplicates. For instance, is Elizabeth Riley Smith at 123 Elm Street the same person as Liz Smith at 123 North Elm Street?

FIs can look to build in autocomplete functionality to prompt users as they type with suggested complete and standardized addresses. This not only helps speed up the sign-up process but ensures only accurate information enters the system to reduce manual data entry errors and prevent duplicates."

BUD WALKER
chief strategy officer for Melissa

5 Five Fast Facts

60%

Share of banks in the Asia-Pacific region that lack fully digital onboarding processes

40%

Portion of consumers who abandon their mobile bank applications due to the time it takes to complete them

38%

Share of consumers who believe user experience is the most important factor to consider when picking digital banks

35%

Portion of FIs that believe their KBA tools are cumbersome and add frictions to their onboarding processes

40%

Portion of consumers who rescind their bank applications before completing them

FEATURE STORY

BEHIND QUONTIC BANK'S **DATA-DRIVEN APPROACH TO FASTER ONBOARDING**

FIs must continually focus on providing seamless and secure customer onboarding experiences. Those with too-stringent authentication measures risk losing customers behind locked digital doors, while those with weak verification tools are holding those doors open for fraudsters.

FIs are out of options, however, as they have an obligation to create and maintain a balance that enables customers to securely complete onboarding processes without pushing them toward abandonment, Patrick Sells, chief innovation officer for digital-first FI Quontic Bank, said in a recent interview with PYMNTS. They must also keep up with digital banking innovations to ensure their platforms can both oust fraudsters — who often have access to equivalent technologies — and keep customers satisfied.

Quontic Bank recently upgraded its digital onboarding solution to that end, focusing further on identity verification and eliminating many common authentication and fraud protection friction points. The crucial change is not how it is authenticating these customers, Sells said, but the data it is now using to do so.

"That [onboarding] process at most banks takes eight, nine, 10 minutes and is slow and cumbersome," he explained. "The process we [rolled out] takes about … three minutes. It is much easier for the consumer and much safer for the bank. The key to how we have been able to shorten that experience and process is by using data [regarding] who a customer is to verify [their identities]."

Seamless onboarding requires current data, Sells added. Making sure customers can authenticate quickly allows them to begin communicating with their banks and interacting with financial services as soon as possible. This is particularly important because consumers expect the same instant services from FIs that they receive from other businesses online.

THE PROBLEM OF THE RETAIL EXPERIENCE

A large share of U.S. consumers quickly transact through digital and mobile channels, meaning they now expect banks to do the same — even at their first point of contact. FIs must thus be prepared to onboard potential users the way large-scale digital retailers would: in a few minutes and with minimal questioning.

Most FIs are well-acquainted with these expectations and are searching for technologies that can bring eCommerce-style onboarding to the financial space. Quontic Bank operates just one branch in New York City and pivoted to focus on its digital experiences approximately a year and a half ago. The decision largely involved abandoning its brick-and-mortar services, and the FI learned that creating retail-like experiences requires extensive and accurate data.

"Technology is an example in which we can use Big Data to create better experiences for customers, and you see that in our lives as consumers," Sells said. "When we shop, we go online and Amazon knows exactly what we want. [It is] doing the same thing and using data to drive that experience, and that is one of the key things that we are doing: … using data that is available to us to not only make the experience of interacting with [us] better but also more intuitive and easier."

Using alternative data streams such as geolocation, online shopping behavior or mobile app analytics is much easier after customers have already onboarded, but banks can also use them to help build out more detailed customer profiles and differentiate legitimate users from bad actors. Their access to this information during onboarding has been limited to keep that process as seamless as those of online retailers, however.

Amazon and like businesses onboard users in an instant with an email address and password — and sometimes verification codes sent to these addresses for two-factor authentication (2FA) — but that is

the critical point at which banks must deviate in their approaches. Amazon does not need personal identifiers like Social Security numbers or home addresses up front because those can be verified at the point of purchase if necessary. These key data points can help FIs determine if users' identities are real, however, meaning they are needed to match retail's onboarding times with greater security.

Legacy onboarding processes cannot keep up with the number of digital applications consumers submit daily, making digital onboarding even riskier. Accepting these applications at speed could result in inadvertently approved fraudsters gaining access to FIs' platforms. Blocking identity theft, IP address or new account fraud is thus a challenge for banks before, during and after onboarding, Sells said. Data is the key to making sure FIs have the information they need to protect against fraudsters at every step, because one data point can be cross-referenced with multiple others to ensure legitimacy.

"The key with third-party data is to not overly trust any one data point but to understand the totality of the picture being painted," he explained. "It is easy for a false positive data point to exist, hence the need for the large data set."

Larger data caches are thus critical, because more information is better for banks as they build out cohesive online customer profiles. Voluminous data caches contain more specific customer information that helps FIs distinguish between real and illegitimate actions, while those based on weaker or smaller data sets do not have enough points available to ensure certain online activities fit consumers' typical patterns, making onboarding processes more vulnerable to fraud.

DATA AND THE SECURITY GAME

Utilizing these large data sets for seamless onboarding processes allows FIs to use diverse information about consumers' online lives to verify them. This may help stop fraudsters, but banks must be sure to keep seamlessness in mind.

Quontic Bank's onboarding solution uses several third parties to ensure this balance is met, including those that provide verification technologies to ease security burdens. Such partners' expertise and data caches provide

FIs with alternative perspectives on customers' online behaviors and are essential to stopping cybercriminals from gaining access. Banks need expansive back-end data sources, such as digital receipts and security metrics like biometric authentication, that will help them achieve both efficiency and security during onboarding. These databases allow FIs to build more transparent views of their customers and stay one step ahead of fraudsters, especially as large-scale data breaches and hacks grow cybercriminals' information pools.

"There is probably an immeasurable [number] of data breaches, so the combination of that and just the nature of our lives [means] we have much larger data footprints," Sells said. "Bad actors out there … have a plethora of self-generated data. They have data they can get from these breaches and they can manipulate that data to try to commit bank fraud … That is probably the area we see the most activity, if you will."

Banks must be sure to safeguard their platforms against fraudsters using stolen data to perpetrate attacks. Doing so can be especially difficult during onboarding if FIs do not have access to alternative sources of information, like consumers' typical online browsing habits or spending patterns that showcase their normal activities. Fraudsters rely on such gaps to convince banks they are legitimate with only one or two pieces of stolen information, but banks that can quickly and seamlessly authenticate legitimate users, without adding too much friction to the experience, will likely gain savvy consumers' loyalties.

NEWS & TRENDS

RECENT ONBOARDING CHANGES

COVID-19 PUSHES DIGITAL ONBOARDING

COVID-19's spread is forcing many FIs to fit their legacy solutions into the digital sphere, enabling them to carry on with business. This deeply affects customer onboarding, as many banks around the world still require in-person onboarding processes. Sixty percent of banks in the Asia-Pacific region do not yet have digital onboarding procedures in place, and banks in Germany or Switzerland may ask for customers to appear in person to complete the process. Such requirements have become challenging to meet due to the ongoing pandemic. Consumers still need access to banking products and services but cannot visit physical branches.

Implementing digital onboarding can be difficult, especially for those that need to significantly overhaul their infrastructures. These FIs must examine their KYC processes and identify digital verification tools that can help improve their digital onboarding processes. Such systems ensure that customers are properly identified and that their onboarding experiences are as effortless as possible.

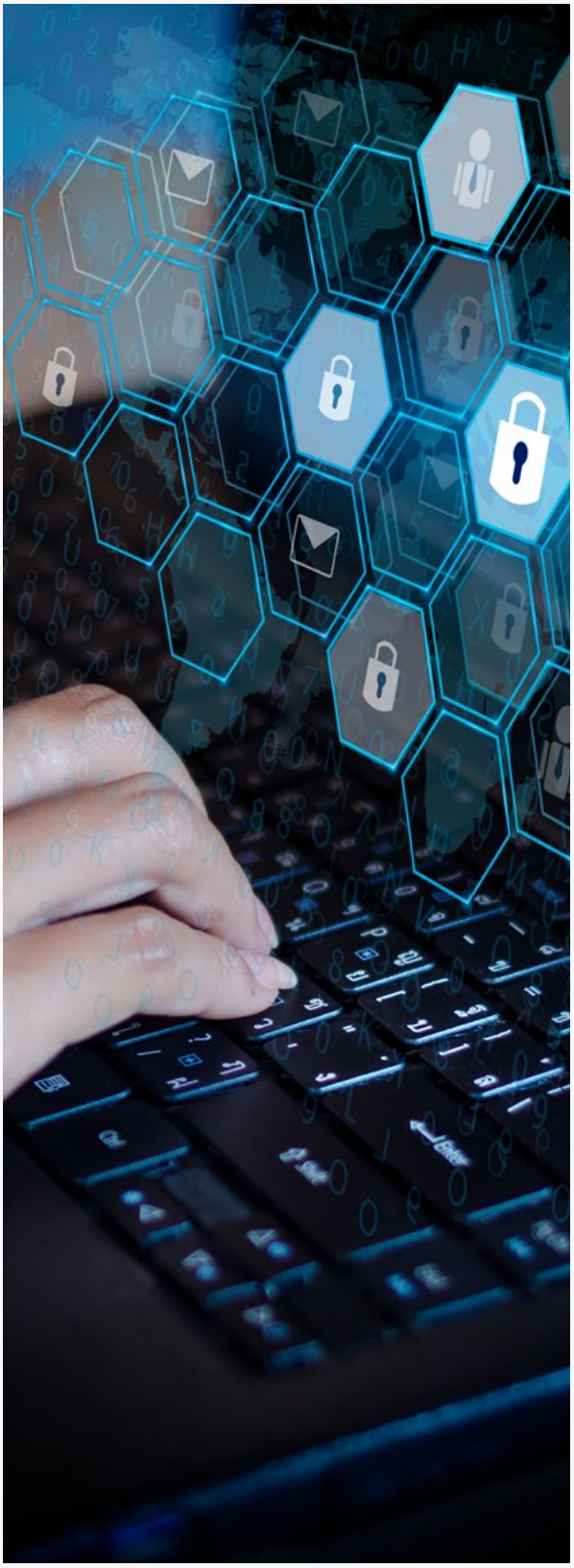
IMPROVING DIGITAL ONBOARDING EXPERIENCE IS FIs' TOP PRIORITY IN 2020

A significant share of FIs are focusing on improving their account opening procedures as they look to boost their customer experiences. A recent survey of more than 100 FIs in North America noted that 80 percent of FIs identified improving their customer experiences through better onboarding as their top business objective for 2020. Many of these FIs are thus looking to reduce their reliance on manual procedures and are instead focusing on automating their digital account opening processes, cited by 90 percent of FIs. These entities are also putting their money where their mouth is, with 99 percent of FIs increasing their budgets for improved digital onboarding experiences.

Allocating the appropriate funds is critical, but FIs still have several challenges that must be overcome. Forty-nine percent of FIs said that their systems are still tied to legacy, manual identity verifications processes, and 35 percent said that their knowledge-based authentication (KBA) tools are cumbersome and add friction to the onboarding process. FIs also cited being unable to safeguard against bad actors attempting to open fraudulent accounts and lack of funding as challenges.

EXAMINING DATA'S IMPORTANCE FOR FASTER ONBOARDING

One way to ensure that banks' onboarding processes can keep up with expanding customer bases is by ensuring that accurate and relevant KYC data is being collected during the account creation stage. This is true for both businesses and banks, which must safely onboard new clients at speed. A recent PYMNTS report found that 58 percent of business leaders think enhanced data insights are critical to compliance and customer identification, for example. Relying on outdated data or assessments that take too long to finalize — such as background checks — can drive up costs and increase the likelihood of potential clients abandoning the process entirely. Finding the necessary data to both verify clients' identities and provide them with swift onboarding experiences is difficult, however, and many are examining how automated technologies could bridge this technological gap.



FIs AND ONBOARDING NEWS

FINTECH TONIK ADAPTS NEW BIOMETRIC SOLUTION

FIs are finding customer verification critical during the pandemic, which is pushing more consumers to use mobile and online banking options. Digital-only bank TONIK has implemented a cloud-based identity verification solution from solution provider Daon to keep up with this shift. The FI will utilize the latter's IdentityX solution, which uses face, fingerprint and voice biometric features to authenticate users, to manage identity verification needs and maintain compliance with changing anti-money laundering (AML) and KYC regulations.

TONIK has yet to officially launch, though it is expected to first roll out its services in the Philippines, which boasts a tech-savvy young population, later this year. Competition in this market is fierce, and TONIK is looking to stand out with this partnership and bring more users to its platform.

APEX GROUP DEVELOPS ONLINE PLATFORM FOR ONBOARDING

Other entities are hoping that digital onboarding will speed up processes for asset managers and bankers by steering them away from manual, paper-based offerings. Global financial technologies group Apex Group has developed a digital onboarding platform for asset managers that will allow them to finalize account openings in a five-day period. The platform will first be available for clients in Luxembourg, through Apex Group's subsidiary, the European Depositary Bank (EDB). The company plans to expand this offering to Ireland and the U.K. later this year.

The online onboarding solution was developed to help asset managers — as well as others in the space, such as corporate firms or trusts — move away from paperwork. Digital onboarding experiences can quickly process information that can finalize accounts, realizing benefits for all involved parties.

BIOMETRICS AND ONBOARDING

UTILIZING BIOMETRICS FOR ONBOARDING DURING THE COVID-19 PANDEMIC

Biometrics have been championed as a next-gen authentication tool for years, but their adoption has been slow, as the technology needs further experimentation before it can be implemented at scale. COVID-19 is pushing many players in the financial services space to once again consider how face, fingerprint or voice identification can be best utilized in onboarding and identity verification, and one digital identification provider reported a 21 percent increase in sign-ups since the pandemic's onset.

Enabling seamless onboarding processes has become imperative. Banking customers are often quick to abandon these processes if they are too lengthy or friction-filled. Thirty-eight percent of customers say that user experience is the most important factor when they choose digital banks, meaning these entities must find ways to keep authentication as seamless as possible. Biometrics are an attractive tool for this purpose and will perhaps see more adoption after the pandemic thanks to the rise of remote, digital onboarding in the wake of non-essential business closures.

FINAX OFFERS ONBOARDING WITH FACIAL RECOGNITION

Securities broker Finax is looking to use biometrics, offering clients online biometric identification tools when onboarding to improve their experiences. The company is utilizing a digital onboarding platform from technology provider Innovatrics that uses facial recognition during the onboarding process. Finax first partnered with Innovatrics in 2019, and the latter's platform is meant to replace the former's existing verification tools, which had human employees match customers' uploaded photos with those on their government-issued identity documents — a lengthy process given that these photos also needed to be cross-referenced with bank statements.

Clients signing onto the platform will now use the Innovatrics platform to photograph their faces and their IDs, and the software will automatically compare and verify the two pictures. Finax plans to further innovate its use of this solution, including mobile integration for iOS users.

ZENOO TO USE FACIAL BIOMETRICS FOR SECURITY

Onboarding technology provider Zenoo is another player in the space that is utilizing facial recognition. It recently partnered with biometric securities firm ID R&D to bring biometric capabilities to its onboarding solution, allowing Zenoo clients to identify themselves with photos or videos that would undergo "liveness checks" to ensure they were taken in real time by the correct individuals. This is meant to mitigate fraud by adding security while also minimizing the time available for fraudsters to create false videos or photos.

Real estate sales platform Homepie will be the first of Zenoo's clients to make use of this offering, according to Zenoo. Homepie is hoping the platform will ensure that prospective buyers' identities are properly authenticated before they embark on virtual tours of certain properties.

CANADIAN BIOMETRIC LAUNCHES OCCUR PRIOR TO PANDEMIC

Several Canadian banks also recently made efforts to implement biometrics for onboarding and mobile verification. The RBC is now offering biometric identification features on its mobile app, as is fellow Canadian bank Bluink. RBC is also allowing its clients to scan their passports, licenses, permits or other identity documents during the onboarding process.

Bluink has rolled out a mobile identity app called eID-Me, which its customers can use to authenticate themselves

when engaging in healthcare- or government-related processes as well as financial transactions. These tools were both introduced just a few weeks before the COVID-19 lockdown and could prove critical to continued relationships with banking customers during this period.

KYC AND FRAUD

DUBAI GOVERNMENT CREATES KYC CONSORTIUM

Dubai's Department of Economic Development believes that while biometrics are important, the real issue is ensuring that FIs have access to accurate and secure data that such tools can rely upon. The department recently announced the creation of a regional KYC blockchain consortium with six member banks, enabling more secure onboarding with the data FIs need to ensure verification can occur as quickly as possible. Consortium members include Abu Dhabi Commercial Bank (ADCB), the Commercial Bank of Dubai (CBD), Emirates NBD, Emirates Islamic, HSBC and Rakbank. Each member will look to share authenticated KYC data between members to further innovate onboarding processes and leverage blockchain for security.

The consortium will further develop the technologies and tools it offers members as 2020 progresses and plans to launch an "Instant Bank Account" product later this year to speed onboarding. The product will allow consumers and FIs to create new bank accounts in as little time as possible.

DUBAI BLOCKCHAIN, KYC EFFORTS CONTINUE

The Dubai International Financial Centre (DIFC) is also looking at new innovations, developing a KYC blockchain platform focused on helping licensed businesses and other corporate entities open digital bank accounts instantly. DIFC crafted this platform in collaboration with Mashreq Bank and online software solutions FinTech norbloc. It prevents FIs from having to rely on outdated, paper-based KYC processes and instead provides them with up-to-date KYC data.

The offering was tailored to assist with an existing proposal meant to make the government fully digital by 2021. DIFC's platform also uses blockchain technology to this effect to better store and categorize data on digital channels. The solution is now available to any FI operating within the United Arab Emirates, according to the DIFC.

DATA-DRIVEN KYC PROCESSES DRIVE IDENTITY INNOVATION

Accurate KYC requires more robust data — obtained in real time — so banks can continuously provide the best experiences possible. The need to constantly update which data they are collecting and why to keep up with KYC trends could end up giving banks an unexpected edge on a different playing field — that of digital identity, according to Oliver Diaz, chief technology officer for financial platform services company Covault.

Banks need to reference a growing number of key data points to ensure their KYC procedures are up to date with digital consumers, Diaz explained, and that means they are uniquely suited to becoming the wardens of digital identity as more daily tasks start and end online. Developing digital identities is critical, but protecting them is even more important, and FIs already have much of the information necessary to determine if users are who they say. That means banks must ensure that their security measures for guarding user data are tighter than ever, especially when onboarding.

DEEP DIVE

THE NEED FOR REAL-TIME DATA TO KEEP ONBOARDING FAST AND SECURE

Onboarding is typically the first interaction customers have with FIs, which leaves a lot riding on the process. Banks are jostling for space in the market because an expanding number of FinTechs and large-scale technology companies are competing for the same set of consumers.

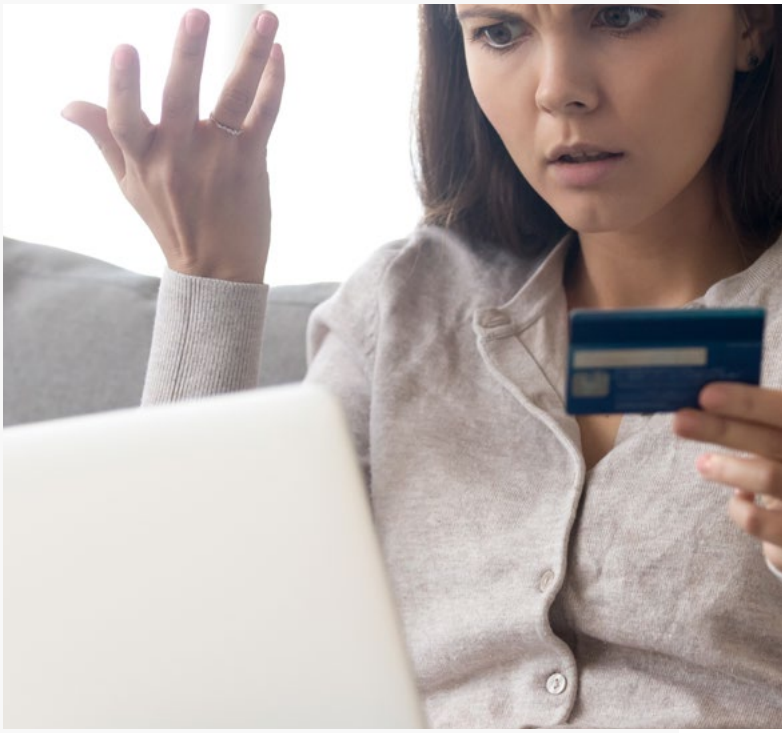
Banks must enable fast and seamless onboarding experiences, but these processes should also be secure. New account fraud is a significant problem for FIs, with 48 percent of values generated from fraud attempts coming from accounts that have only been open for one day, according to a recent report. FIs do not really have the choice to make onboarding's security procedures less stringent, however.

Security processes must be effortlessly grafted into onboarding processes, however, as 38 percent of consumers value user experiences above all else. FIs must find ways to maintain this balance that go beyond simply enabling onboarding through faster and more convenient channels such as mobile.

There has been greater interest among FIs for tools that can provide the same level of service and satisfaction regardless of channel, with 88 percent of banks' fraud executives stating that key use cases for risk assessment tools are ones that improve onboarding experiences. FIs should thus consider which details they are utilizing during this process, as access to valid and current data is critical, and its impact on authentication and customer sastifaction has grown as more users start asking for digital banking services over in-person ones. FIs that are reliant on data caches that are just a year old are at a distinct disadvantage, not only for fraud protection, but also for successful onboarding. Having quicker or real-time access to data means these entities will be able to verify potential customers' identities much faster, cutting down on the friction points many customers experience when asked to authenticate themselves.

DATA AND AUTHENTICATION FRUSTRATIONS

One of the most frustrating parts of any onboarding experience is the time it takes for customers to complete the process, even via channels designed for ease of use



like mobile banking apps. One recent report found that 40 percent of consumers abandoned applications on mobile banking apps because of the time involved to sign up. Identity verification is one of the longest parts of the onboarding process because customers must provide numerous details such as their addresses, bank statements or Social Security numbers and also wait for FIs to validate their details and approve their applications.

This often causes customers to abandon onboarding, meaning that banks looking to remain competitive must shave time off of their onboarding processes. Consumers are searching for instant access to new services, with their experiences on platforms like Netflix and Uber setting customer expectations across various industries. The key to seamless authentication is always having access to the right data, making FIs' sources for their KYC processes extremely important.

Banks pull data from various sources to fulfill financial requests, but much of this information is only collected after consumers have already created accounts. This is why new account fraud is so hard to detect, but risks can be mitigated if FIs take different approaches to which sources they use during onboarding.

Crafting KYC processes that combine customer data from credit agencies, governmental sources, utility companies or even social media sites with banks' previously siloed data is one way they could potentially enhance their onboarding processes' security while maintaining speed and seamlessness. Access to varied data sets can help FIs check potential customers' information against multiple points for any possible red flags without further involving those customers. Using biometrics in place of old-school KBA procedures and passwords can also help improve the overall onboarding experience.

BIOMETRICS AND ONBOARDING

FIs have been interested in biometrics ever since fingerprint-based login became a common functionality on smartphones and other devices. The use of fingerprints, facial recognition or voice prints for banking is not uncommon, but most FIs use these factors to replace passwords, which customers use to sign in to preexisting accounts — not as identifiers for new customers.

Biometric tools can present their own challenges, however, as it can be difficult to verify customers' biometric indicators when they are not collected during onboarding. Other types of biometric indications, however, may provide unique ways for FIs to maintain the seamlessness users seek when creating new accounts. Behavioral biometrics can be implemented entirely on the back end and used throughout online banking interactions to ensure consumers are legitimate. Tracking consumers' keystrokes or typing speeds can help indicate the presence of a bot or other automated technologies fraudsters may use for account takeovers (ATOs) or new account fraud attempts, for example. The same is true for biometrics that track how consumers interact with online or mobile websites, such as taking too long when typing in personal details or comparing their behaviors to those of existing customers whose identities have already been verified.

These technologies are not yet widespread, however, and it will likely be some time before they are commonly used for onboarding and authentication procedures. Banks must examine if biometric tools could work for their onboarding experiences as well. Those that choose not to implement these tools will need to find other ways to expand which data they use, however, and those that cling to KBA and other static data to authenticate and onboard users will quickly find themselves ousted by competitors that have made the effort to innovate.

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.