Online Banking in the U.S.

Part 1: How 20 of America's Top Banks Are Balancing Security with Usability for Onboarding

Executive Summary

How easy is it for a consumer to open a bank account in the United States?

It sounds like a simple question. Yet two seemingly opposing forces are making the onboarding process challenging for financial institutions and their customers. Those two forces - security and usability - bring different demands to the table:

> **Customer Experience:** COVID is driving more consumers than ever before to bank online. Many are doing so for the first time and will be looking for an online experience that is straight-forward and intuitive. Customers want some sort of 'ceremony' as they onboard - a bank with no security at all will not inspire confidence. But too many hoops to jump through and the experience becomes frustrating, which means the customer will take their business elsewhere - and the choice of alternatives is far greater online.
>
> **Security**: Banks want to provide a simple user experience, but security is critical - especially with the increase in COVID-driven cybercrime. The financial sector stands on the frontline in the fight against money-laundering and organized criminal networks. New account fraud (NAF) losses increased to $3.4B in 2018. This is achieved by criminals using victims' identities to create bank accounts or apply for credit cards, or through synthetic identities created using potentially valid social security numbers. Know Your Customer (KYC) regulations demand that the financial sector carries out due diligence on every new customer and this has implications for the user experience.

Until now, financial institutions have had to choose between security and usability when verifying customers, or at least strike a careful compromise between the two. Today, iProov's remote identity verification technology enables the highest levels of security with the most effortless user experience, allowing banks to achieve both.

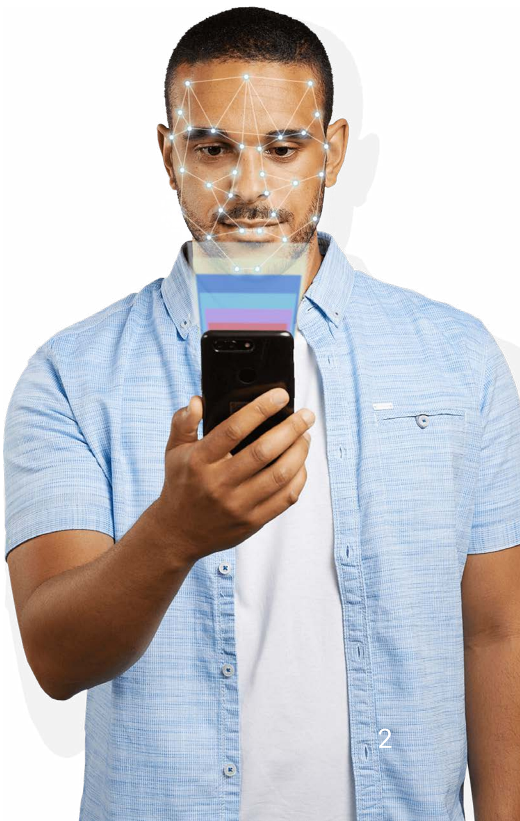
iProov wanted to see how U.S. banks were managing the onboarding process. From August 3–31, 2020, we attempted to open a personal account online at 20 of the largest retail banks in the U.S., as determined by asset value. Our objective was to evaluate the process, from opening the website or app through to account creation and funding, to determine how easy it was for a customer to navigate.

Three banking security drivers:

- New account fraud (NAF) costs $3.4B annually, affecting 3.2M consumers in 2018.
- Large-scale data breaches increased 273% in the first quarter of 2020. 63% of Americans say they have had data stolen in a data breach.
- In the first half of 2020, banks paid $706M in fines for AML failures, versus $444M for 2019.

Digital experience essentials:

- 46% of U.S. consumers had used at least two online financial services in 2019, up from 17% in 2015.
- 36% of financial institutions say they have lost customers due to inefficient or slow onboarding processes
- Onboarding costs could be reduced by 90% by using digital ID-enabled processes.



The Future of Online Banking Verification: iProov Biometric Authentication

Financial institutions in the US are turning to biometric technology for online identity verification to:

1. **Support remote customers securely:** COVID is bringing more customers online. Criminals want to take advantage. Biometric authentication makes the customer experience easier and deters fraud.
2. **Increase the speed of KYC:** Customers onboarded in under 60 seconds? It's already being done.
3. **Deliver a great customer experience:** With success rates of >98%, biometric identity verification maximizes completion rates and reduces frustration faster and more securely than anything else.

The iProov Approach

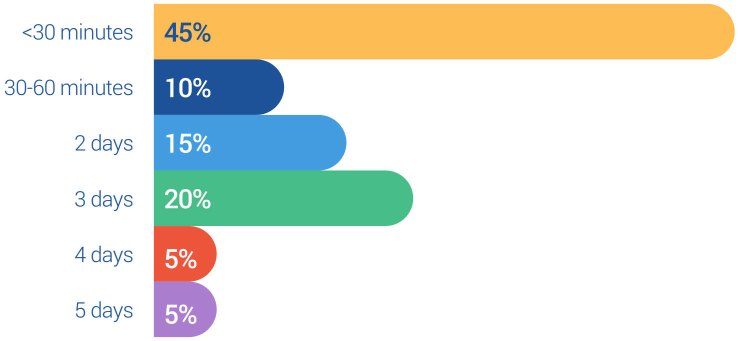
Each of the financial institutions we tested has an opportunity for **enhanced security** and improved **customer experience** with iProov products.

Onboarding Essentials	Current Bank Protocol	iProov Approach
Identity verification/KYC	Knowledge-based information is used to verify identity - SSN, state/gov't ID numbers, or credit history. All are either obtainable by criminals and/or hard to remember.	Customer scans their government approved ID on a mobile device, computer or kiosk. A brief scan of their face is then matched with the document image to confirm identity. See it in action.
Assuring Genuine Presence of customer	If issues arise in identity verification, customer is asked to travel to a branch or to speak to a bank representative on the phone. This leads to inconvenience for genuine customers and to accounts taking days to open.	Customer's facial scan confirms within seconds that the individual is the **right** person (and not an imposter), a **real** person (and not a stolen photo or video), and authenticating **right now** (and not a deepfake or other synthetic media).
Account setup and ongoing authentication	Customer is asked to create and remember passwords with varying requirements in complexity.	Customer uses a face scan as a factor for simplified authentication, either to access their account or to complete high risk activities.

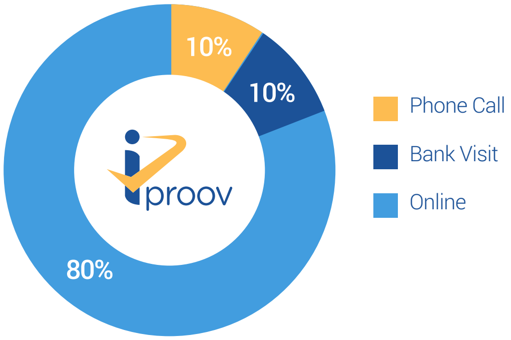
Key Results

How easy was it to open a bank account with 20 leading U.S. banks? The key results show how the experience varied greatly, in terms of time taken, amount of information required, and simplicity of process.

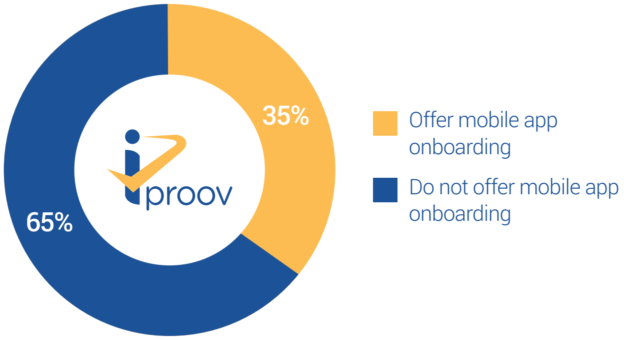
Time to Open/Fund Account



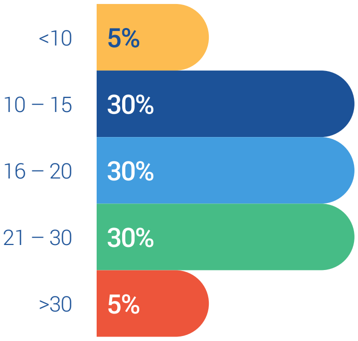
Ability to Open Account Fully Online



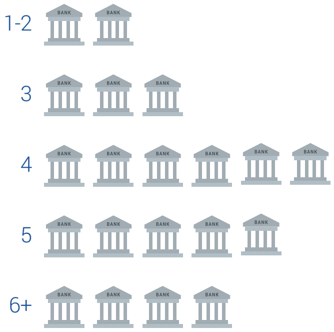
Ability to Open Account on a Mobile App



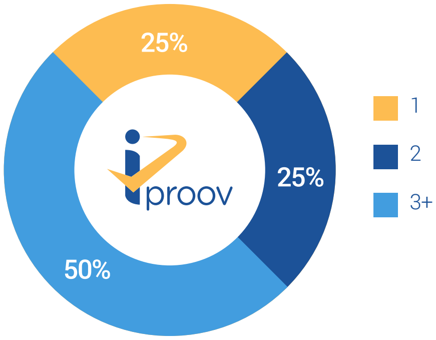
Number of Clicks to Open Account



Number of Password Requirements



Number of Proofs of Identity Needed



Research Results

Research Results

Digital banking is growing. In 2019, 46% of U.S. consumers had used at least two online financial services, up from 17% in 2015. Savings, payments, borrowing and budgeting are all moving online.

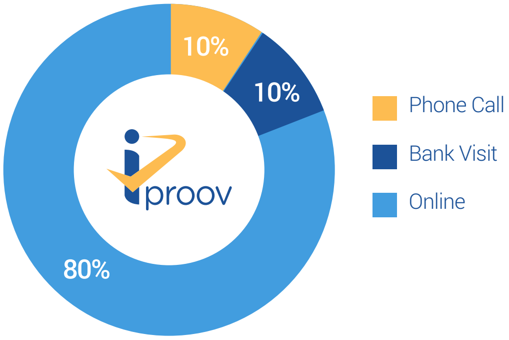
This report details how 20 of the largest U.S. banks are currently striking a balance between security and usability during the customer onboarding process.

80% of banks enabled an account to be opened online

20% of banks required a phone call or branch visit to open an account.

When consumers choose to do their banking online, they likely do not expect that opening the account requires a visit or call to their local branch. And, for 80% of account applicants, the entire experience from initial click to new bank account was a totally remote, digital exchange. Of the remaining 20%, half of the banks (2) required a call or in-person visit due to being flagged during the funding process.* The other 2 gave no exact reason for the added steps.**

Ability to Open Account Fully Online



The test included 5 attempts to fund accounts from an account not belonging to the applicant. The logic was that some first accounts may be funded by a parent or employer. In 2 of these instances, this initiated personal interaction with the bank.

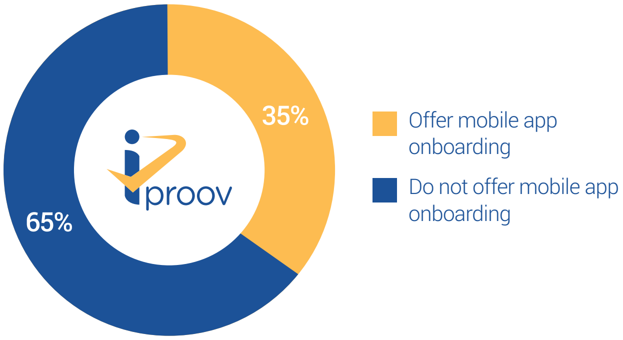
*** In one case, the test administrator believes the additional step(s) may have been a result of IP address identification; the applicant resided in a different state from where the administrator was logged in. In another case, the bank may have heightened security because of multiple recent fraudulent accounts being opened.*

35% enabled an account to be opened via mobile app

65% of banks did not offer onboarding via mobile app.

According to a Pew Research study, a growing share of Americans use smartphones as their primary means of online access at home rather than a computer and traditional broadband service. However only a third of the banks offered a mobile app that enabled secure onboarding.

Offer Account Onboarding Via Mobile App



45% of accounts took 2 days or more to open and fund

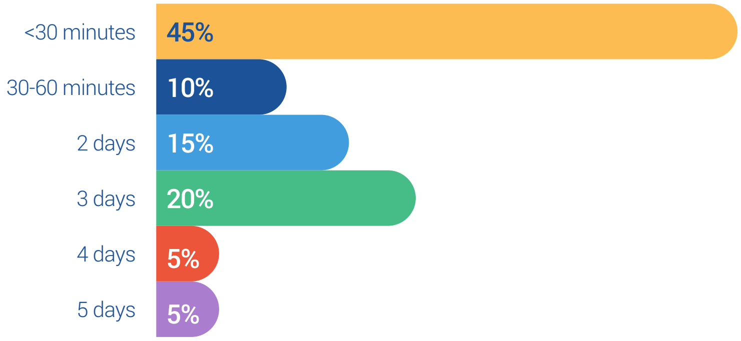
55% of accounts were open and funded on the same day.

For busy consumers, digital banking is attractive because it offers convenience and speed. 9 of the banks tested provided a time-efficient process that resulted in the applicant having a new account open and funded in under half an hour. Another 10% took between 30 minutes and 1 hour.

45% of accounts were not open/funded for several days.

While half of the accounts were complete in an hour or less, the remaining half took 2 to 5 days. Of those, slightly more than half used trial deposits to verify the applicant's funding source, which took an average of 2 business days. However, funding was not always the issue - the remaining banks required applicants to call or visit a branch to complete the opening process.

Time Taken to Open and Fund Account

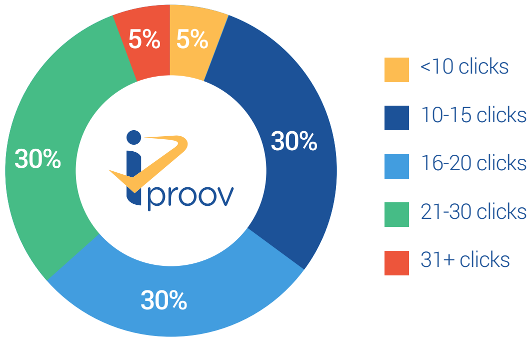


65% of banks required 20 or fewer clicks to onboard

In one case, 39 clicks were needed.

The online customer journey, from opening the app or website to completing the account set-up, varied greatly from bank to bank. At one end of the spectrum, one of the banks required fewer than 10 clicks to get from start to an open bank account. At the other end, another applicant had to make their way through 39 clicks to complete the process. The institutions with longer processes tended to have multiple pop-ups and required document reading along with information gathering. 90% of banks required 10 to 30 clicks to establish an account.

Number of Clicks to Open Account Online



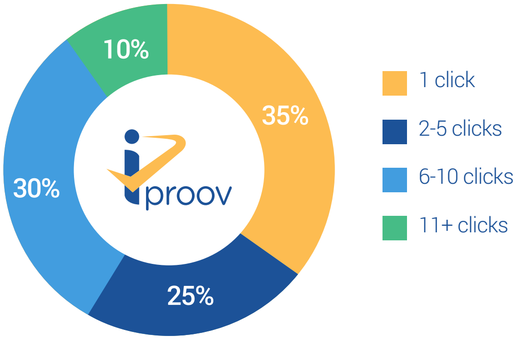
35% of user profiles were created with one click

The account creation process typically involved the set up of a user profile, followed by gathering of information for the application, followed by funding of the account.

The process of establishing a user profile varied a lot from bank to bank. 35% of the largest U.S. banks made this straight-forward — a set of fields followed by a single click to move to the next stage.

Conversely, for 30% of the banks, the creation of the user profile required between 6 and 10 clicks.

Clicks Taken to Create User Profile



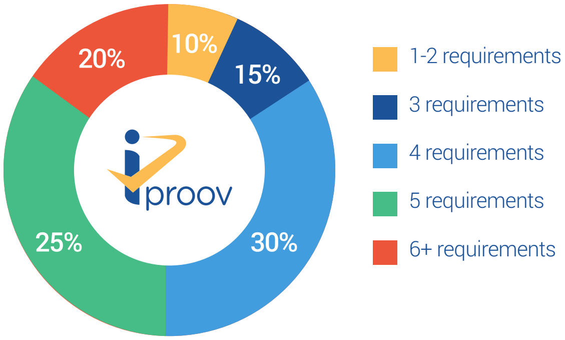
75% of banks had 4 or more password requirements

At the other extreme, 10% of banks had only 2 stipulations for password format.

Password frustration is real: an iProov study from 2020 found the average American abandons an online purchase 16 times a year because they forget their password. For financial institutions, password resetting can cost money.

Yet 45% of the banks asked customers to meet 5 or more criteria for their passwords, making them potentially hard to remember. There was a lot of variation in what was required, from 4 asks (usually upper case, lower case, special character, and number) through to more complex instructions involving not using the same character three times in a row.

Number of Password Requirements for Online Account

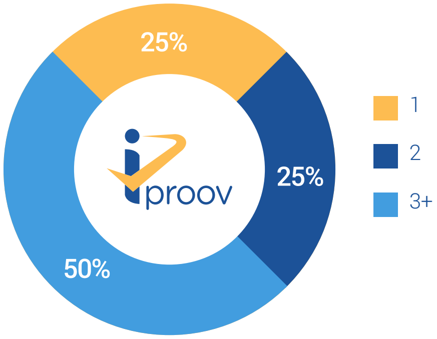


50% of banks required 3 or more proofs of identity

How are consumers confirming and proving their identity for the largest U.S. banks? 13 banks required the unique numerical sequences of 2 government-issued forms of identification: a Social Security number issued by the federal government and a state-issued driver's license or identification card. (Most – but not all – allowed substitutions of military ID or passport in lieu of state ID). 25% required only the Social Security number.

50% of the banks required three or more forms of identification, which included government issued IDs, as well as questions about the applicant's credit history and/or presenting an ID in person at a branch.

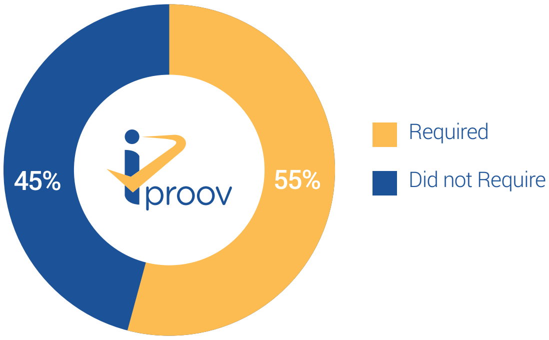
Number of Proofs of Identity Needed to Open Account Online



55% of banks required credit history to confirm ID

Some banks are digging deep into an applicant's financial past to confirm their identity. 55% of the banks tested presented the user with 1–5 multiple choice questions about prior addresses and phone numbers, prior mortgage or automobile loans and prior names used. Sometimes, no correct answers were available and "none of the above" was an option. Responses were required within a given time frame or they were incorrect. Interestingly, several of our test consumers were not able to remember these financial moments from their own past.

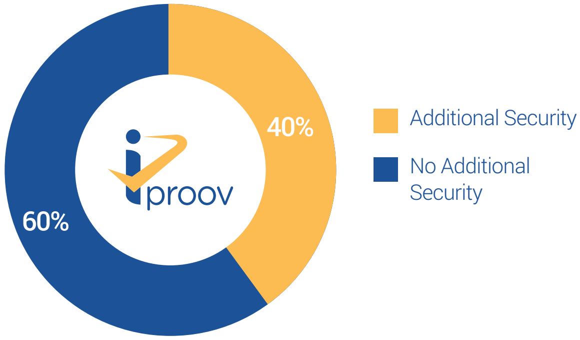
Require Applicants to Answer Credit History Questions to Verify Identity



40% requested additional security at time of funding

More than one third of our test accounts required additional security when the time came to add funds. These included: credit history questions, trial deposits of small amounts in the account where funding was coming from, confirmation that the funder resided in the same ZIP code as a bank branch, or requiring that the initial deposit be made in-person only at a bank branch location.

Additional Security Procedures at Time of Funding



Summary and Conclusion

Banks and other financial institutions have much to gain from using biometric authentication technology to automate and simplify the onboarding process:

- **Win the business of every bona fide prospective customer** - never lose out on genuine business
- **Reduce onboarding costs with online completion -** phone or in-branch verification carries an expense
- **Reduce fraud -** using Genuine Presence Assurance deters criminals and new account fraud
- **Comply with regulations -** KYC guidelines can be met using face authentication

This research shows that many banks can do more to ensure high levels of security without disrupting the customer experience. In summary:

- **Most of the banks made it possible to open an account online** but 4 of the 20 did not. Even in these COVID times, 2 banks insisted that the customer visit a branch to complete the onboarding process. This suggests that there is still work to be done in automating the processes involved in verifying identity. Improvement of the security process will ensure that bona fide customers are not turned away, it will save customers the time and costs involved in driving to a branch to wait for an hour, and it will reduce the costs involved in calling customers or dealing with unnecessary in-branch visits.
- **Onboarding through a mobile app is not always possible.** 35% of the banks had a mobile app that permitted account onboarding but two thirds of banks did not. As digital natives increasingly use their smartphones as their main means of going online, this is something for banks to consider.
- **Opening an account can take anywhere from 30 minutes to 5 days.** There was a huge difference in how long it took to create and fund an account. The fact that almost half of banks managed to onboard the customer and fund the account within 30 minutes suggests that this is the benchmark that all should aspire to. But half of the banks are not there yet.
- **10-39 clicks needed to open an account.** An online user experience can vary from website to website but a 39 click process is very different to one involving 10 clicks. Some banks may need to simplify.
- **More than half of banks asked for SSN and state ID as proof of identity.** Others also asked credit history questions or required presenting ID in person.
- **Credit history questions were used by half of the banks.** Anecdotally, this is where many of the testers struggled - questions about former addresses or phone numbers, prior mortgage or automobile loans and prior names often proved challenging, particularly if the questions timed out.
- **More than half of the banks required more security information for funding.** The onboarding process was just the start for 40% of the banks - more security checks were required to fund the account. Technology to support a cohesive onboarding and ongoing authentication is essential.

By using iProov's Genuine Presence Assurance, banks can be confident that a new customer is the **right person**, matching their ID document, a **real person**, not an imposter waving a photo or video in front of the camera, and authenticating **right now**, not a synthetic deepfake or replay attack.

For more information on iProov's Genuine Presence Assurance technology for secure online onboarding or to request a demo go to www.iproov.com.

About iProov

iProov is the world leader in providing facial biometric authentication technology to financial institutions, governments and other enterprises that need to securely verify customer identity online. Used for onboarding and authentication, iProov customers include the US Department of Homeland Security, the UK Home Office, the UK National Health Service (NHS), Singapore GovTech, Rabobank, ING and others.

iProov's unique patented Genuine Presence Assurance technology enables banks and other financial enterprises to ensure that an online customer is the **right person** (not an imposter), **a real person** (not a photograph, mask or video presented to a camera), and **authenticating right now** (not a deepfake or synthetic media attack injected into a sensor). This provides unique protection against sophisticated replay attacks and the emerging threat of deepfakes. Read more at www.iproov.com.

Next Steps

For more information on the research:
If you would like to know more about the research, please contact enquiries@iproov.com.

For more information on iProov:
To find out more about iProov's services and how we help banks around the world with remote customer onboarding and authentication, please contact enquiries@iproov.com.

Report Methodology

From 3 August to 31 August 2020, we attempted to open a personal account online at 20 of the largest retail banks in the U.S., as determined by asset value. Our objective was to evaluate the entire process, from opening the website or app through to account creation and account funding to determine how easy it was for a customer to navigate the process.

33 data points were included in the research, including the steps involved in the user profile creation, the identity verification procedure, the funding process, and the overall length of the onboarding experience.

Ally Financial
Bank of America Corp.
Bank of the West
BBVA USA
Branch Banking and Trust Company (BB&T; now Truist Financial)
Capital One Financial Corp.
Charles Schwab Bank
Citigroup, Inc.
Citizens Bank
Fifth Third Bank
Goldman Sachs Group, Inc.
HSBC Bank USA
JPMorgan Chase Bank
KeyBank National Association
Regions Bank (BNP Paribas)
PNC Financial Services Group, Inc. (PNC)
SunTrust Banks, Inc. (now Truist Financial)
Toronto-Dominion Bank (TD Bank)
U.S. Bank National Association
Wells Fargo & Co.

For more information on how to assure the genuine presence of the **right** person, **real** person, authenticating **right** now contact us at:

enquiries@iproov.com