# Online Banking in the U.S.

## Part 2: How 20 of America's Top Banks Are Balancing Security and User Experience For Digital Account Access

# Introduction

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.

Just as online banking creates opportunities for banks, it also presents challenges. The need for an effortless user experience, to maximize customer inclusion and reduce frustration, must be balanced with the security required to protect against fraud and comply with regulations.

iProov's face verification technology achieves both the highest levels of security and the simplest, most inclusive user experience. We commissioned research to look at how banks are striking that balance currently.

- Part 1 looked at the online onboarding process.
- In this Part 2, the focus turns to ongoing authentication and how bank customers are able to access their accounts, carry out transactions and update personal information.

# Executive Summary

Having set up an account online with 20 of America's largest banks for Part 1, the researchers were then asked to carry out a number of activities to establish how easy it is for a customer to manage their account. The researchers noted that the balance between security and usability was often uneven:

**Too much security?**

- Banks are losing revenue by making it hard for customers to access new products and services. A third of banks asked the customer to re-onboard from scratch to set up a savings account to go with their checking account. If banks have securely assured the identity of a customer during onboarding, verifying their identity for new bank products and services should be simple. Instead it often turns into a lengthy application process.
- Debit cards and PIN replacements still require offline intervention. Half of the banks did not enable a PIN to be changed online and half did not allow customers to request a new debit card online. By verifying that an online customer is the right person, a real person, authenticating right now, banks can avoid sending customers to ATMs or into branches to make such requests.

### Who is responsible for security?

Banks are putting the onus on customers to report potential breaches.

- The researchers reported that it was often possible to update an email address, password, home address or cellphone number with just a username and password.
- Many banks then sent email or text alerts to the customer, confirming a change had been made and asking them to get in touch if they had not made it. This is potentially very stressful for the customer, as well as being a security risk if fraudsters have redirected the phone number first.
- By putting additional, simplified authentication in place, banks can verify the genuine presence of the customer making the change and avoid putting them under stress.

### How does Genuine Presence Assurance solve these challenges?

iProov's unique face authentication technology enables banks to assure the genuine presence of an online customer in a way that is highly secure and effortless to use. A face scan lasting a few seconds verifies that an online customer is the right person (not an imposter), a real person (not a photograph or mask), and that they are authenticating right now (not a digitally injected attack using deepfakes).

Banks can therefore enable customers to complete the most secure transactions online in a way that is fast, reassuring and maximizes user privacy.

## The iProov Approach

| Account Management Essentials | Current Bank Protocol | iProov Approach |
|---|---|---|
| Upsell Products / Services | - Customer must re-enter all information (30% of banks)<br>- Customer must re-enter some information (35% of banks) | Genuine Presence Assurance maximizes completion rates |
| Updating PIN/Debit Cards | - Only 10 of the banks allowed a PIN to be changed online<br>- Only 40% of banks enabled the customer to cancel a debit card and request a new one online | Genuine Presence Assurance is highly secure |
| Changing Personal Details | - Password reset when forget (85% require 2-3 forms of info) | Genuine Presence Assurance improves the user experience |

# Key Findings

### Section 1: Logging In

- Nearly all the banks asked for additional identity verification for the customer's first login to a new account, and for any subsequent logins made on a new device.
- The methods included a one-time text or email code (60% of banks used these), the use of security questions (20%), a choice of both (10%), or the use of a hardware token (5%).
- All of the banks enabled customers to access their accounts via mobile app, with Face ID and Touch ID on offer if supported by the customer's device.

### Section 2: Carrying Out Transactions

- 75% of banks required additional security verification if the customer wanted to transfer funds to an external account – trial deposits, login to the other account, debit card numbers or one-time passcodes were most popular.
- Only 40% of banks enabled the customer to cancel a debit card and request a new one online.

### Section 3: Adding New Services

- 30% of banks asked the customer to complete the onboarding process entirely from scratch if they wanted to access an additional product or service.
- 35% of banks pre-populated some or most of the information required to complete an application for an additional service, asking the customer to add some extra details. 6 banks pre-populated all the data needed for a savings account.

### Section 4: Updating Information

- 85% of the banks allowed the customer to change their primary email address online and most did not ask for additional information beyond username and password.
- Most banks sent an email notification after a change had been made.
- 90% of banks allowed the customer to update a password by confirming their old one. One bank required no verification and one sent a code.
- 60% allowed a customer to change personal information, such as address and cellphone, without additional verification beyond the initial username and password login.
- Only 10 of the banks allowed a PIN to be changed online. 2 of these sent a text/email verification code prior to making the update, and 1 required the current PIN to be entered to make the change. The others allowed the change with just the initial username and password at login.

### Section 5: Security

- All of the banks allowed passwords to be reset online but some made it very difficult – 2 banks required 4 or more pieces of information for this to be completed.

# Research Results

# Research Results

In Part 1 of this research, we looked at how 20 of the largest U.S. banks are onboarding new customers online. In this section, we focus on how those 20 banks enabled the customer to access their accounts online, carry out transactions and update their personal information. How did the banks balance security with usability to ensure an effortless yet reassuring experience?

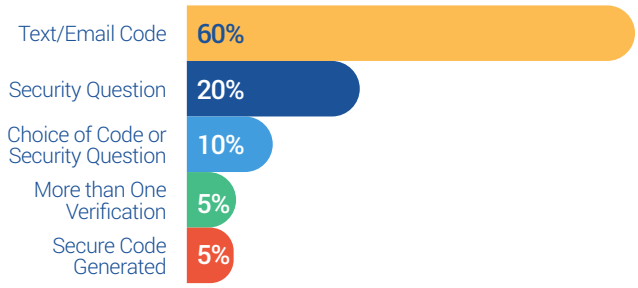
## SECTION 1 – LOGGING IN

### 95% of banks used multi-factor authentication at first login

Nearly all the banks applied additional security for the customer's first login to their new account. Having provided their usernames and passwords, the customers were then either asked additional security questions or sent a one-time text or email code to verify identity.

One-time text or email codes were most popular, with 60% of the banks using these. 20% used security questions, while two banks (10%) offered a choice of code or question. One bank (5%) used a hardware token device to send a code to the customer.

Type of ID Verification at Login

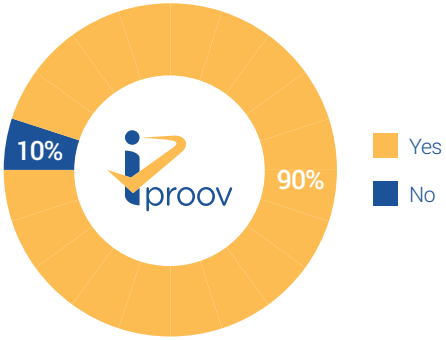



Only 1 bank (5%) continued to use multi-factor authentication for every subsequent log-in as default. Almost half of the banks (40%) gave users the option to turn on security verifications for all logins.

## 90% of banks used multi-factor authentication for login from a new device

Once a customer had completed their first login on a device, most banks only required username and password for subsequent logins. However, if the customer accessed the account from a new device, 90% of banks required additional identity verification using text codes or other methods mentioned in question one.

Verification for New Device Login



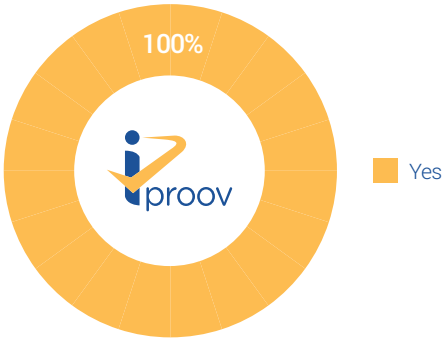

## 100% of banks supported face or touch login to their app

In Part 1 of this research, we noted that 65% of banks did not allow the customers to open a bank account via the bank's mobile app. However, when it came to accessing an existing account, all of the banks offered access on a mobile app using three options for logging in: password, Face ID (where supported on the device) and Touch ID (where supported on the device).

It is worth noting that all three of these options are ultimately using passwords to access an account. Neither Face ID nor Touch ID verifies the customer's biometric with the bank itself. Face ID and Touch ID enable the customer to be recognized by the device, which then populates the saved password without the customer having to type it in.

What it does show is that U.S. bank customers are already using face verification or fingerprint verification to access their bank account digitally.

Face & Touch ID if Supported on Device

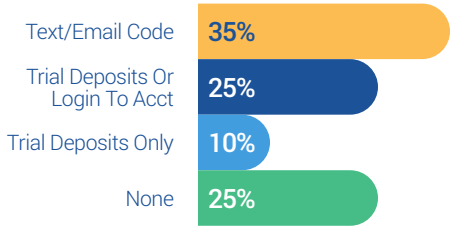


## 75% of banks used multi-factor authentication before linking to an external account

Having accessed the account online, the researchers then attempted to link it to another existing external account, owned by the same customer, with a view to transferring funds between the two.

15 of the banks added additional security steps to verify the customer's identity during this process. The most common method was a trial deposit or asking the customer to login to the other account. Text/email codes were used by 35% of banks to verify linking an external account. 25% of banks required two levels of verification to link an external account, such as text codes or verifying the account holder's debit card number.

Type of Verification to Link External Account

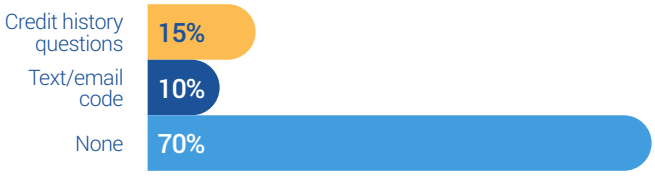



4 banks did not require further security verification beyond the initial username and password account login. 1 of these did use text code verification to activate an external transfer but no authentication to link an account. 1 bank is unknown, as the account was closed before funding for suspected fraud.

## 25% of banks used multi-factor authentication before a transfer of funds

With the accounts linked, 70% of the banks then allowed a transfer of funds to take place between the two without further security checks. 25% of banks on the other hand required additional authentication for transfers, using credit history or text codes to verify the customer. 1 bank carried out extra authentication if the transfer was over $1,000.

Type of Verification to Make a Transfer




The banks varied greatly in terms of transfer limits, from $1,000 to $250,000, with some limits defined per day and others per month. The lack of consistency across banks may lead to confusion for a customer with more than one account. 85% of the banks offered Zelle for payments to other people.

**5% unknown due to one bank closing account before funding for suspected fraud.*

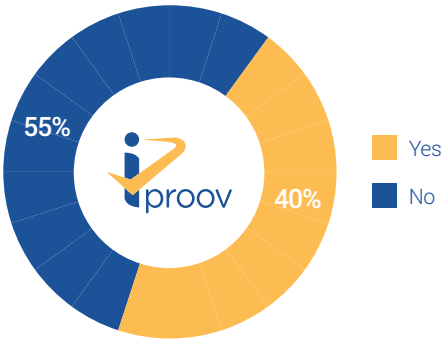
# 40% of banks allowed a customer to request a new debit card online

40% of the banks enabled the customer to cancel their debit card and request a replacement online. The other banks required the customers to go into a branch or contact the branch by phone or letter to request a new card.

The convenience offered by the 8 banks was appreciated; however, as will be seen on page 12 below, it is also possible to update addresses and other personal details without multi-factor security checks. If a fraudster gained access to a username and password, they could change the address and request a new card to be delivered there.

The ability to verify the genuine presence of an online customer would prevent fraud and enable the other 60% of banks to offer debit card replacement online.

Request New Debit Card Online



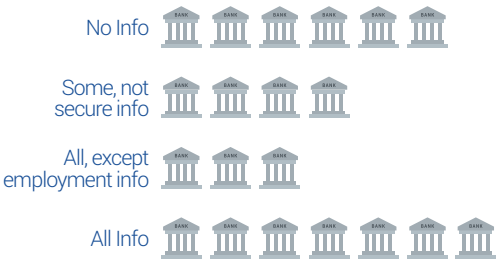

*One bank tested did not have a debit card

## 65% of banks required a customer to 'reonboard' for additional services

One of the advantages of in-person interaction is the ability for bank staff to advise customers of new services or offers that might benefit them. Finding ways to cross-promote products online should be a focus for banks looking to extend that capability.

It was therefore surprising that almost a third of banks made it very hard for an online customer to add a savings account to go with their checking account. In 30% of cases, the customer had to go through the entire onboarding process again, which could deter them from doing so.

Pre-Populate Personal Information when Adding Additional Account




35% pre-populated some or most of the information but required the customer to provide some additional details to complete the application process.

6 banks pre-populated all the data needed to apply for a saving account so that the customer only needed to add funds. 1 bank authenticated the customer with a text code, then pre-populated all information.

Of the banks that asked for additional information, 4 banks required secure information to be re-entered (e.g. SSN and/or driver's license), while 3 others required customers to verify their employment information.

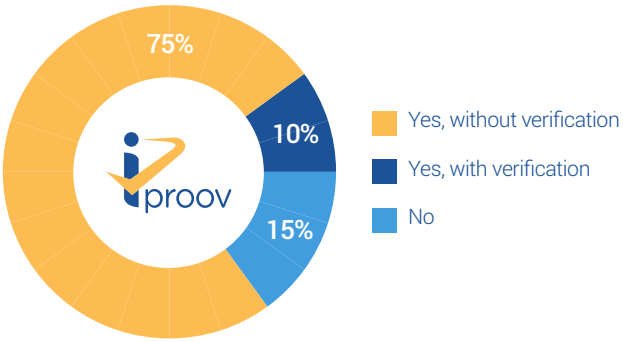
There is a huge opportunity for banks to cross- and up-sell additional products and services to customers who have a main account with them. By making it easy to verify the genuine presence of the account holder submitting the new application online, the customer experience could be greatly improved.

## 75% of the banks allowed the customer to change their primary email address online without multi-factor authentication

85% of the banks allowed the customer to change their primary email address online. Of those, one bank required the customer to confirm the last four digits of their SSN before making the change, and one sent a one-time text code. The other 15 banks allowed the change to be made with only a username and password.

Most banks sent an email notification to the original email address after a change had been made. The researchers noted that many banks seemed to be working on the basis that a customer would alert them if a breach had occurred, which would be stressful for the customer and potentially too late if a fraudulent transaction was being made.

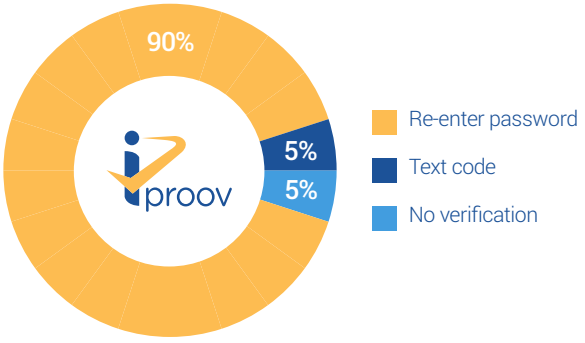
### Changing Primary Email Address Online




## 95% of the banks allowed the customer to change their password online without multi-factor authentication

90% of the banks allowed the customer to change their password online by re-entering their current password, while 1 bank required no verification – the customer only had to enter the new password. Only 1 bank required a code to be generated on a secure device prior to making a change to the customer's password.

### Changing Password Online

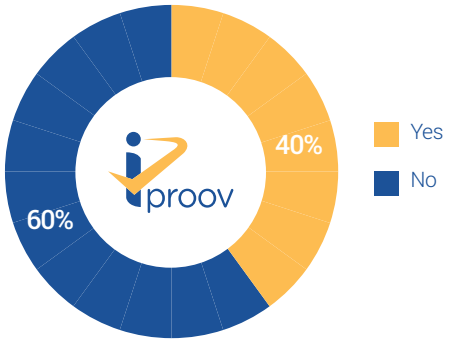


## 40% of banks required additional security before updating personal information online

60% of banks allowed the customer to change personal information, such as their address or cellphone number, online without additional verification beyond the initial username and password login.

The banks that required additional verification either asked the customer to answer a security question, enter a portion of their SSN or account number, or use a text verification code.

Require Verification to View/Update Personal Information




Some banks (20%) allowed customers to edit their personal information through a web browser but not on a mobile app. This is interesting, as web and apps present the same levels of risk. The misconception is often that web security is stronger than an app, so banks build 'simple' apps and ask customers to use a browser to complete more sensitive activities. This could be frustrating for customers who use smartphones and apps for everything.

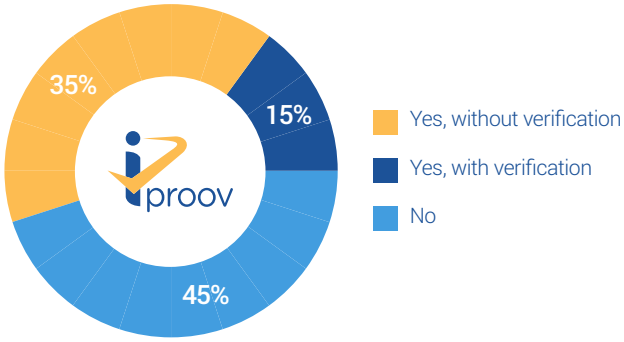
---

## 50% of banks allowed a customer to change their PIN online

Of the 19 banks that provided a debit card with a PIN, 10 allowed customers to change their PIN online. The other 9 banks asked customers to change their PIN at an ATM, by phone, or in a branch.

Only 2 of the banks that allowed online PIN changes sent a text/email verification code prior to making the update, and 1 required the current PIN to be entered to make the change. The others allowed the change with just the initial username and password at login.

Changing PIN Online




**One bank tested did not have a debit card*

Although it is convenient to be able to change a PIN online, if a fraudster gains access to an account, changes the address and requests a debit card, this poses a risk that a new card and PIN will be available to that fraudster without the knowledge of the customer. The ability to verify the genuine presence of the online customer would reduce the fraud risk while enabling PIN changes to be made online.

## 55% of banks required 3+ pieces of security information to reset a forgotten password online

All of the banks allowed forgotten passwords to be reset online. However, the amount of information required to do so varied greatly. At the low end, 1 bank posed a single security question. 8 banks requested two additional pieces of information – the combinations varied but included knowledge-based info, such as an SSN and date of birth, or verification via physical artifact, such as a one-time text/ email code or a portion of the debit card number. 7 banks required 3 pieces of information, while 2 banks needed 4 or more (e.g. debit card number, PIN, last four digits of the SSN, last digits of the account number and a security question).

# of Forms of Data Required to Retrieve Password


The chances of a customer having 5 pieces of information on hand to reset a password are quite low, especially if they were on the move. This could restrict them being able to gain access to their account when needed.

The number of login attempts before an account was locked also varied. In 9 cases it was unclear how many attempts were permitted. Of the others, 4 banks allowed 5 attempts, 1 bank allowed 4 and 6 banks allowed 3 attempts.

# 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 or data stream). This provides unique protection against sophisticated digitally injected 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 contact@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 contact@iproov.com.

# Report Methodology

In Fall 2020, we attempted a variety of secure actions online with the personal accounts opened in August at 20 of the largest retail banks in the U.S., as determined by asset value. Our objective was to evaluate the security and usability of the digital banking experience once we were an account holder. 39 data points were included in the research, including login verification process and alerts, changing personal information, linking and making transfers to external bank accounts, and adding additional accounts.

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:

**contact@iproov.com**