Online Banking in Canada

How Are Canada's Top Banks Balancing Security and User Experience for Online Customers?

Introduction

Digital banking is growing. In 2019, 70% of Canadian consumers had used digital channels to access their banking services. 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.

Executive Summary

iProov wanted to see how Canada's largest banks were delivering online services to customers. As part of this research, we opened a checking account with 5 of the largest retail banks in Canada, as determined by asset value. Once the accounts had been created, the researchers then carried out a number of activities to establish how easy it is for a customer to manage their account online. Throughout, the researchers were looking at points where authentication may be required or expected, and how each bank approached the balance between security and usability.

Opening a bank account online was not possible at 3 of the 5 banks

Only two of the banks enabled the customer to fully complete the onboarding process online. In the other cases, an in-person visit to a branch was required. This stood in contrast to similar research in the U.S., where only 20% of banks failed to offer a full online onboarding experience.

None of the banks enabled an account to be opened via a mobile app

All of the banks provided customers with an app for mobile banking but none of the apps supported the opening of an account. This again stands in contrast to the U.S., where a third of banks offered onboarding via app. Additionally, in a separate study, iProov found that 23% of Canadian consumers have completed all of their banking on a mobile device in the past 12 months.

It took more than a week to open an account with 80% of the banks

The fastest onboarding process among the Canadian banks was 5 days. This is in stark contrast to the U.S., where 5 days was the longest that any bank took - almost half of the American banks onboarded the customer within 30 minutes.

Changing a PIN and requesting a new debit card required offline intervention

The researchers found that the most secure transactions could only rarely be completed online. Only one bank enabled a new debit card to be requested and one made it possible to change a PIN.

Resetting a forgotten password could be done online but it took effort by the customer

One bank required seven pieces of information, including employer's name and mother's maiden name, before the password could be reset online.

The iProov Approach

Onboarding and Account Management Essentials	Current Bank Protocol	iProov Approach
Identity Verification / KYC	- Every bank had a different approach, requiring different forms of identity.	iProov's Genuine Presence Assurance enables an online user's identity to be verified against a government-approved photo ID within seconds.
Account Setup and Ongoing Authentication	- Most banks used debit card numbers as username, which delayed account setup - All banks required multi-factor verification at first login	Genuine Presence Assurance does not require the customer to remember any information. It can be added as an additional verification factor to bolster existing processes.
Upsell Products / Services	- Customer information was automatically populated in application process for new services.	Genuine Presence Assurance ensures the legitimate account holder is applying for additional products, such as credit cards.
Updating PIN/Debit Cards	- Only one bank allowed the PIN to be changed online - Only one bank enabled customers to cancel and request a new debit card online, but the process was onerous	Genuine Presence Assurance provides the security to manage PIN changes and new debit card requests while protecting against account take over.
Changing Personal Details	- Most personal information could be updated with username and password. Password resetting usually required 3+ pieces of information.	Genuine Presence Assurance enables the identity of the user to be verified before an email address, home address or other personal account info can be updated.

Effortless Security for Banks with iProov

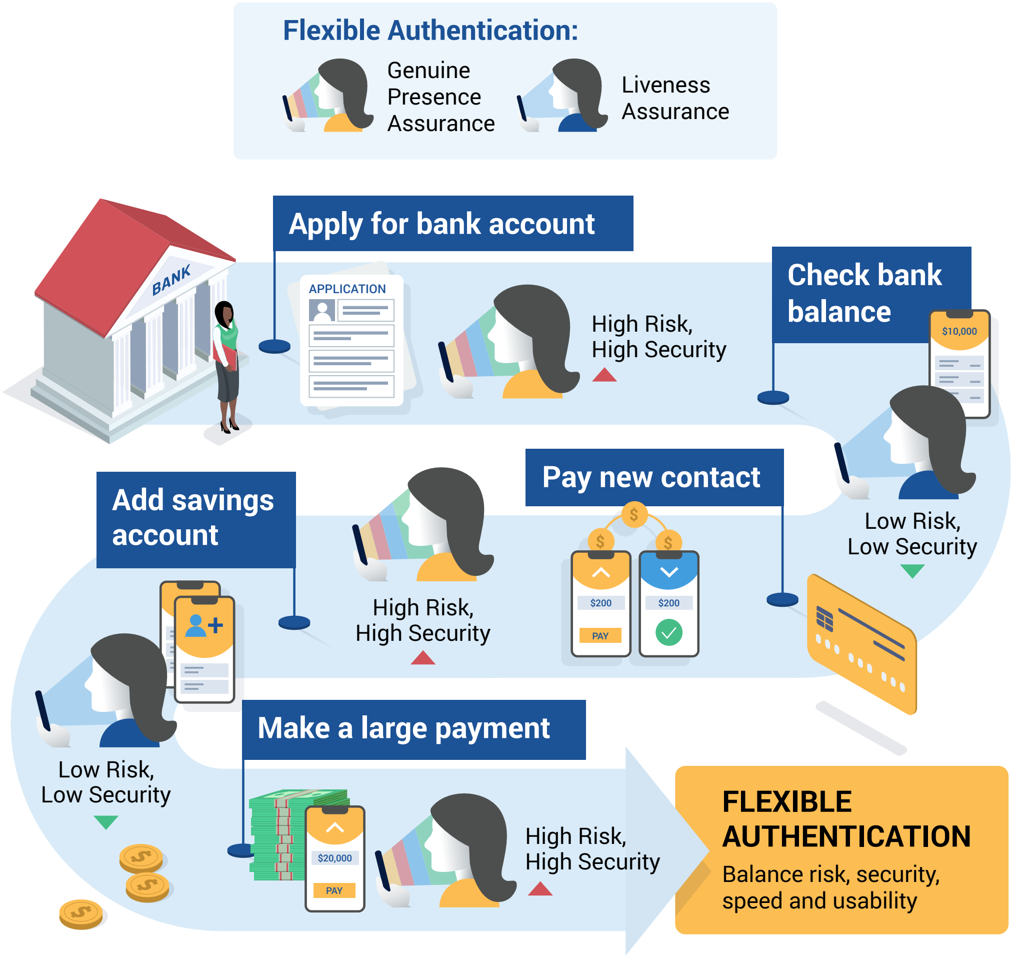
iProov is the world leader in enabling financial institutions and governments to securely verify the identity of online individuals using face biometric technology.

Our Flexible Authentication solution enables banks to balance risk, security, convenience and reassurance throughout the customer lifecycle.

Flexible Authentication combines two iProov technologies in one SDK:

> **Genuine Presence Assurance™:** iProov's flagship technology enables banks to verify that an online user is the **right** person (not an imposter), a **real** person (not a presented photograph or video or mask), and that they are authenticating **right now** (not a digitally injected attack using deepfakes or other synthetic media). Ideal for onboarding and step-up authentication, it offers the highest levels of security in high-risk scenarios with an effortless face verification.
>
> **Liveness Assurance™:** For lower threat activities, Liveness Assurance technology can be used, particularly for activities such as checking a balance or making low value payments. This technology provides protection against physical and digital artifact attacks.

Find out more about how Flexible Authentication can protect against fraud and improve completion rates – email contact@iproov.com or visit www.iproov.com



Key Findings

Section 1: Onboarding

- Only 2 banks allowed accounts to be fully opened online.
- None of the banks offered account opening via mobile app.
- It took over a week to open accounts at 4 banks. In comparison, half of US banks enabled account onboarding to be fully completed within 30 minutes.
- 4 banks required more than 18 clicks to open an account.
- Every bank had a different process for verifying the customer's identity at onboarding, ranging from no verification at all to asking for 4 proofs of identity.

Section 2: Online Account Access
Logging in:

- All banks used multi-factor authentication for the customer's first login to their account, and subsequently for new device logins.
- 3 banks used one-time text codes as an authentication method, while the other 2 used security questions.
- All of the banks' mobile apps could be accessed with face or touch verification.

Transactions:

- No bank required additional identity verification beyond a username and password when transferring funds to another account.
- Only one bank allowed customers to request to cancel or replace their debit card online, with all others requiring a phone call or visit to branch.

Adding New Services:

- All banks made it simple for customers to access other services from the bank, such as setting up a savings account.

Updating Information:

- 4 banks allowed the customer to change their primary email address with no additional verification beyond username and password.
- All banks enabled the user to change their password online as long as they knew the existing one.
- All banks enabled personal information, such as a home address, to be updated online without further verification beyond username and password.
- Only one bank allowed the PIN to be changed online - all others required a visit to a branch or ATM.

Security:

- 4 banks required a call or visit to a branch to reset a username.
- 4 banks required 3 or more forms of verification to reset a forgotten password, including text codes, debit card number and personal information.

Research Results

Onboarding

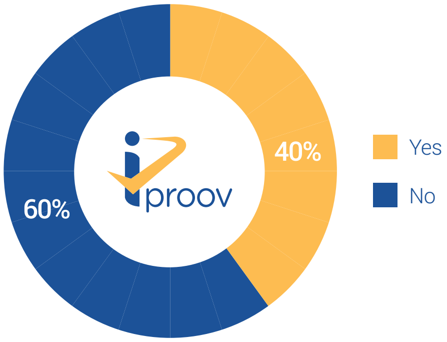
Research Results - Onboarding

Only 2 banks allowed accounts to be opened online

While all of the 5 banks included in the research offered initial steps to open an account online, only 2 permitted the complete process to occur digitally. One other bank offered a full online process (with documentation submitted via photos), but verification failed and a visit to a branch was required. The remaining 2 banks required visits to branch as standard for opening an account. These visits were scheduled upon receipt of an online application.

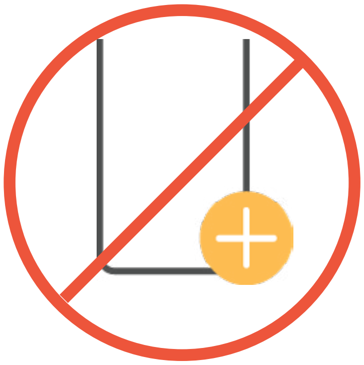
Canadians are increasingly banking online, with more than 80% of Canadians preferring it over traditional in-person banking. There is an opportunity to streamline the process of account opening to meet this demand.

Banks that Allowed Online Onboarding



None of the banks allowed accounts to be opened via mobile app

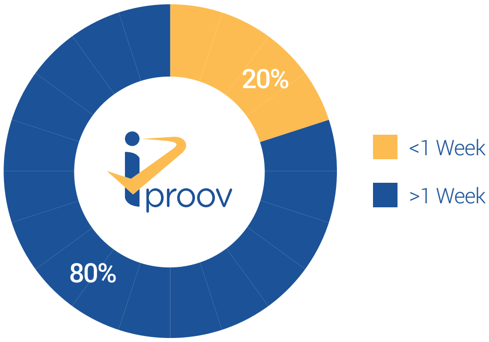
While all of the banks had a mobile app that can be used for mobile banking, none allowed the account application process to take place through the app. Consumers are increasingly using their mobile devices as their main way of accessing the internet. In a separate study, 23% of Canadian consumers surveyed told iProov that they had done all of their banking on a mobile device in the last 12 months. For those mobile-first customers, the ability to onboard via an app could be a benefit and therefore a competitive advantage to any bank that can offer it.



4 banks took more than a week to finalize account opening

Just one of the banks enabled a new customer to open and fund an account in less than one week - and that still took 5 business days to complete. This is in contrast to the U.S., where almost half of the largest U.S. banks were able to onboard a customer online within 30 minutes. The lengthy process can be attributed to the banks sending a debit card to a new customer, which is then needed to complete the onboarding process whether online or in person. The bank with the quickest process allowed the customer to visit the bank to pick up their debit card in lieu of mailing it – but still required an appointment to do so, and there were limited appointment times available due to COVID-19.

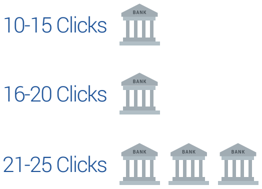
Time to Open/Fund Account



It took more than 18 clicks to open an account with 4 of the banks

It took an average of 19 clicks to open a bank account online in Canada. The shortest user journey required just 13 clicks from opening the website to completing the application process, while the longest took 22 clicks. The average in the U.S. research was also 19 clicks.

Number of Clicks to Open Account

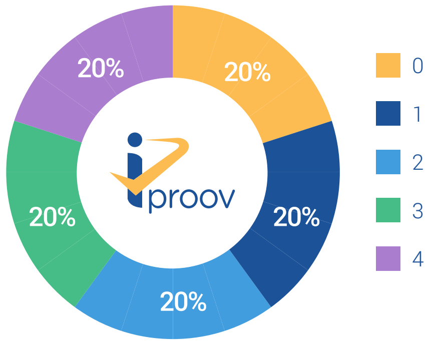


Forms of identity verification varied greatly

Each bank employed a different system for checking the applicant's identity, ranging from no verification to four different proofs of identity:

- 3 of the banks asked for a Social Insurance Number (SIN) but made it optional for applicants.
- One bank used only a text code to verify identity.
- One bank offered the option to provide a picture of a driver's license or passport along with a "selfie" to verify identity, with an in-branch visit if online verification failed.
- Some banks required a mix of online verification like SIN plus some in-person ID verification, delaying the account opening process.

Number of Forms of Identification Required



Research Results

Online Account Access

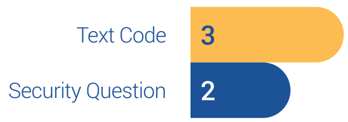
Research Results: Online Account Access

SECTION 1: LOGGING IN

All banks required authentication at first login and for new device logins

Every bank asked the customer to complete multi-factor authentication when they logged into their account for the first time. One-time SMS codes were popular, with 3 of the banks using this method, while the other 2 banks asked for the answer to a security question. All of the banks used MFA if the customer logged in again from a new device. 2 of the banks enabled the customer to make MFA a necessary step for every log-in to their account.

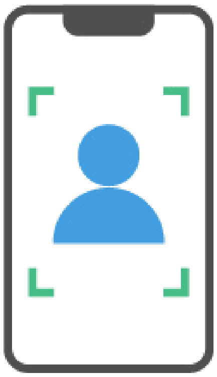
Type of Verification at Login



All of the banks' mobile apps could be accessed with face or touch verification

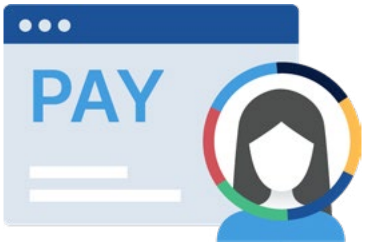
While none of the banks enabled customers to create an account on a mobile app, they all allowed the customer to check balances and complete transactions via app. In every case, the customer was able to log in to the app by using face or touch verification technology if it was supported on their device.

Face ID, Touch ID and other device-based biometric systems only enable the customer to be recognized by the device, which then populates the saved password without the customer having to type it in. The customer is not verifying themselves directly with the bank, as they do with iProov technology. What it does show is that Canadian bank customers are already using biometric verification to access their bank account digitally.



None of the banks required authentication when transferring funds

Once the customer had logged in using a username and password, they were able to transfer funds to another account in their name within the same bank, or to process a transfer to a third party using the Interac e-transfer service or Visa Direct. Transferring funds to a third party required only the name and mobile phone/email address of the recipient for 4 of the 5 banks. One bank required account details of the recipient to make the transfer, but no additional authentication. Most of the banks had a daily transfer limit of $3,000.

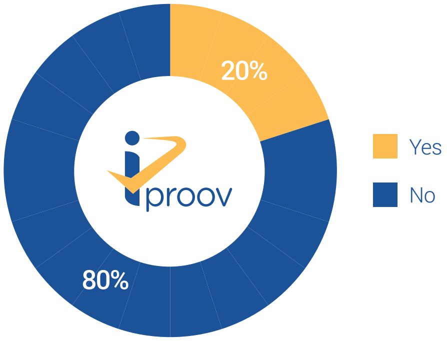


With Genuine Presence Assurance, banks are able to verify that the person making the transfer request on their mobile device or computer is the holder of the account and not an imposter or criminal.

Only one bank enabled a debit card to be canceled or replaced online

Only one of the banks enabled a debit card to be canceled or replaced without a call or visit to a branch, although it wasn't a straightforward process. The account holder had to have the debit card information and send a secure customer service message with the request. This level of security is understandable, as debit card numbers acted as the default username for 4 of the 5 banks.

Can Request New Debit Card Online



With Genuine Presence Assurance, however, banks have access to the high levels of security needed to deliver this service online. By verifying that an online individual is the right person, a real person, right now, the banks could offer additional convenience and simplicity to the customer while reducing the manual administration involved in processing card requests.

SECTION 3: ADDING NEW SERVICES

All banks made it simple to add additional services

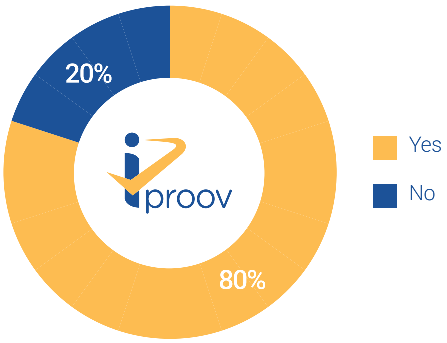
All of the banks made it simple for the customer to access additional services from the bank online. When the researchers attempted to open a savings account to go with their checking account, every bank pre-populated the application details with the customer's data without requiring additional verification beyond username and password. This made it very easy for the customer to take advantage of new bank products but does raise a question about security if a customer's username and password had been compromised. Genuine Presence Assurance would verify the identity of the person making the request, providing additional security.

SECTION 4: UPDATING INFORMATION

4 banks allowed the primary email address to be updated online

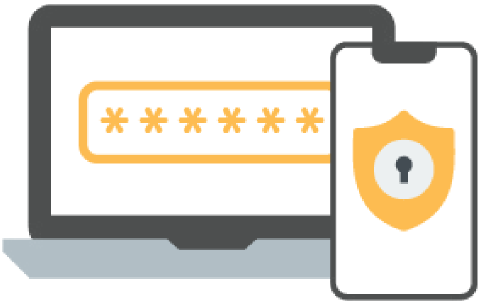
Most banks allowed the user to change the primary email address associated with the account once they had logged in using a username and password. Only 1 bank did not allow the change without further interaction with the bank.

Primary Email can be Updated Online



All banks allowed password changes without authentication

All of the banks enabled an account holder to change their password once they had logged into their account, as long as they reentered their password during the process. One bank required the new password to be different from the last 5 passwords, which is quite demanding on a customer that needs to create something memorable. If a fraudster had access to a customer's username and password, changing that password would be easy.



None of the banks required additional identity verification for personal information updates

All of the banks enabled an account holder to update personal information such as a phone number or mailing address once they were logged in, without additional authentication beyond username and password. If a fraudster was able to acquire a customer's login credentials, they could change personal information relatively easily. By requiring verification with Genuine Presence Assurance, banks could make this more secure.

✓ Only one bank enabled a PIN to be changed online

Only one bank enabled the customer to change their PIN online. The others required the account holder to visit an ATM or bank branch. Genuine Presence Assurance provides the secure online identity verification needed to ensure that the account holder is genuinely present and requesting such a change. This provides convenience to the customer, enabling them to change a PIN in the privacy of their own home, while reducing administration for the bank.

SECTION 5 – SECURITY

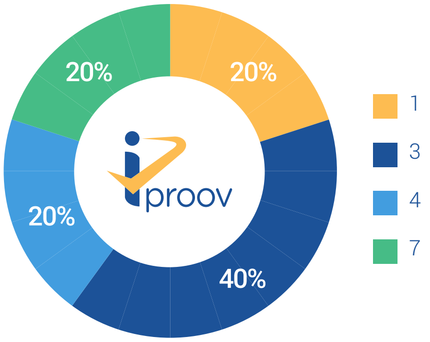
✓ 4 banks required the debit card number to reset the username

Because an account holder's debit card number is the default username for 4 of 5 banks, it is not surprising that changing the username is a secure process. In those cases, a call or visit to a bank branch was required to reset a forgotten username. Two of the banks allowed customers to change their username to something easier to remember; one required the customer to enter their name, email and debit card to retrieve their username, the other required a phone call. The remaining bank asked for the security code created during onboarding to retrieve their username.

4 banks required 3+ forms of verification to reset a forgotten password

The banks differed in how many pieces of identity information were required to reset a password online. A typical approach involved a one-time SMS code, the full debit card number and the customer's last name or postal code. One bank asked the customer to provide 7 pieces of information, including date of birth, employer's name and mother's maiden name.

Number of Verifications to Reset Forgotten Password



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, the Australian Taxation Office, 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.

Further Research

Two other reports are available in this series:

- Online Banking in the U.S.A. - Onboarding
- Online Banking in the U.S.A. - Online Account Access

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 early 2021, a team of researchers commissioned by iProov opened a checking account online at 5 of the largest retail banks in Canada, as determined by asset value. Our objective was to evaluate the onboarding process and see how easy it was for a customer to open an account digitally. Once the account was open, the researchers then attempted to carry out a number of transactions, including transferring funds and requesting a new debit card. The objective was to assess how the banks were balancing security with user experience. The banks included in the research were:

Bank of Montreal (BMO)
Bank of Nova Scotia
Canadian Imperial Bank of Commerce (CIBC)
Royal Bank of Canada (RBC)
Toronto-Dominion Bank (TD Bank)

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