PARAMA CREDIT UNION

Two-Step Verification FAQ

Increased Authentication

What to expect, how to login to Online Banking, FAQs

- How to register screens
- How to add additional email or text numbers
- Password vs code and member vs you

F.A.Q. - Frequently Asked Questions

Q: What is Increased Authentication?
A: Increased Authentication is a security feature that strengthens online and mobile banking security by using 2-Step Verification during high-risk activities. It uses a risk engine to assess user activities and identify high-risk situations where stronger authentication is required. When suspicious interaction is determined, the member will be prompted to enter a one-time password sent through SMS (text) or email.

Q: What's in it for our members?
A: Protection – your finances and personal information are safe with you
Peace of mind – You're being protected them privacy and cyber security breaches
Control – You have control over your personal information
Awareness – Keeping you more informed to make better decisions to protect yourselves

Q: How does a member register for Increased Authentication?
A: Once Increased Authentication is in place, members will be prompted to sign up for 2-Step Verification on the Online Banking or Mobile app login screen. Members will be asked to register an email or SMS text enabled phone number to receive a one-time password when the risk engine detects suspicious login activity.

Q: How does Increased Authentication work?
A: Increased Authentication works by establishing typical member usage patterns by device, location and other habits and makes it easier for fraudulent behaviors to stand out. When a new login location or device is used , the member may be prompted to enter their one-time password.

Q: How does a member log in to their online banking with Increased Authentication?
A: Members log in to online banking as they always have. The risk engine works invisibly in the background so that only suspicious activity is challenged by entering a one-time password to let the system know the login has been authenticated and can proceed normally.

Q: What happens when a member enters their one-time password incorrectly?
A: Members will be given three attempts to enter the one-time password correctly. If the temporary code is input incorrectly three times, the member will be locked out of online banking and will need to contact the Parama Helpdesk (416-532-8723 or Helpdesk@parama.ca) to unlock the account.

Q: What happens if I do not use the temporary password right away?
A: Members will have a 10-minute window to enter the temporary password. After 10 minutes, the temporary password will expire. Members will have to request a new temporary password by selecting **"We can send you a new verification code."**

Q: What happens if I defer my enrollment?
A: Members will be given 90 calendar days to enroll for Increased Authentication and will be prompted to enroll at every login. At the end of the enrollment period, the member will be presented with the enrollment page that no longer includes an option to defer. Members must complete enrollment to continue to log in to online or mobile banking.

Q: Can a member register for Increased Authentication via both SMS and email?
A: Yes. During your initial enrollment, you can only register only one of either a mobile phone number or an email address to receive 2-Step Verificiation notifications. However, after enrollment, you can update your contact information through

- Online banking: the Profile and Preferences page
- Mobile banking app: the Settings on your mobile device

to add the second notification channel.

Q: Will duplicate verification codes be sent by both SMS text and email when both mobile phone numbers and email addressed are registered?
A: No. During each stepped-up authentication where the member has multiple notification channles registered, the member will be presented with a Select Verficiation Method page where they must select which channel they wish to be notified through.

Q: Can I register for more than one phone number or email address?
A: No. 2-Step Verification is linked to a single mobile phone number and a single email registraion

Q: What should I do if I did not receive the SMS text message or email with the verification code?
A: After waiting a reasonable amount of time, try re-sending the code using the "send new code" option on the Enter Your Verification Code page.

Q: How long should I wait for the SMS text message or email to arrive?

A: In most cases, notifications should arrive almost immediately, but a member should wait several minutes before requesting a new code. If after several attempts a code is still not received, please contact the Parama Helpdesk (416-532-8723 or Helpdesk@parama.ca).

Q: Will enrollment in 2-Step Verification affect my current configurations or settings?
A: Yes. Member configurations or settings for Touch ID and QuickView on the mobile app and enabling memorized accounts (the “Remember Me” option selected during a login) must all be re-configured by members after enrollment in 2-Step Verification.

Q: What if I lose my mobile phone or my email has been compromised?
A: Call the Parama Helpdesk (416-532-8723 or Helpdesk@parama.ca). You will be required to re-enroll for 2-Step Verification at your next login.

Q: What if I am travelling internationally?
A: There is no limitation on sending verification messages internationally to mobile phones under 2-Step Verification. Members should receive their texts while travelling if their mobile phone plan provides international roaming and they are in an area with good mobile service.

Q: What if I have multiple Member Cards for login?
A: Each Increased Authentication enrollment is linked to one Member Card. If a member has multiple Member Card numbers with unique logins, they must register for Increased Authentication with each Member Card.

Q: What if I get a new Member Card?
A: If a member changes their Member Card (due to, for example, a lost card), Parama will use the migration tool so there will be no impact to members when they get a new card.

Q: What is the “Register this computer” checkbox used for?
A: If a member checks the “Register this computer” checkbox, a cookie is placed on their computer (browser) for identification purposes and marked as a “trusted” computer. Although there is no limit to the number of computers that can be registered, a member should register their computer only if they are the owner of the computer (such as a home PC).

Q: Why does the member see the “Register this computer” checkbox even though they checked/registered it previously?
A: Every time the member clears their computer browser’s cookies, they are prompted to register their computer again.

Risk Engine & Case Manager

Working seamlessly with Increased Authentication, Risk Engine & Case Manager use an advanced Bayesian algorithm to detect suspicious activity. Establishing typical member usage patterns by device, location and other habits makes it easier for fraudulent behaviors to stand out.

Q: How does Risk Engine & Case Manager work?
A: Risk Engine creates profiles for each member that includes device, location and a series of behavioral patterns. Risk Engine automatically evaluates and scores every member transaction against this profile, assigning a score between zero to 1000, where a score of zero is least suspicious, and 1000 is the most. Suspicious logins will automatically trigger additional authentication steps to verify the member's identity,

Risk-Based Authentication

The Risk-Based Authentication improves the member's login experience and their online banking security, and it makes the Fraud-Reactive, Fraud-Fighter and Fraud-Conqueror models even more effective.

FAQ - Frequently Asked Questions

Q: What is the transition period Increased Authentication is run for?
A: The Increased Authentication transition period is run for 90 calendar days.

Q: When does a member get locked out of Online Banking?
A: Members will be locked out of Online Banking if they fail to enter the correct temporary verification code three times.

Q: When logging in the member sees the error "Sorry, your account has been locked out. For assistance, please contact your institution". How do we unlock the member?
A: The FI staff can unlock members through the MemberDirect Authentication Admin tool. It is important to note that if a member is locked out, they are not automatically reset after 24 hours. For those members who lock themselves out the FI can expect higher call volumes during and outside its normal operating hours.