Multi-factor Authentication

What is multi-factor authentication (also know as MFA)?

Multi-factor authentication (MFA) is an added layer of online account security that couples a time sensitive one-time PIN (OTP) with standard login credentials (user ID and password).

Why is MFA important?

When combined with fixed login information, dynamically generated one-time PINs provide greater account security. Fraudsters are out there and we all need to take steps to stay ahead of them! Utilizing MFA is one such step.

When will MFA be triggered?

MFA will be triggered each time you log into your online retirement account. You will also be sent a one-time PIN in the case of sensitive account transactions, such as personal information changes or loan requests.

What is a one-time PIN (also known as OTP)?

A one-time PIN (OTP) is a dynamically generated code that must be entered, in addition to your user ID and password, when accessing your online retirement account. The OTP is generated after you enter your login credentials and is sent to you either by text message or email. The OTP, which is only valid for 5 minutes, must be entered before you can access your online account.

How will my OTP be sent to me?

The first time MFA is triggered on your account, you will be presented with all phone numbers and email addresses we have on file as well as Google Authenticator. You can choose which you would like to use for your OTP delivery. If selecting a phone number, please be sure that it is one for a text-enabled device, such as a mobile phone. Your preferred OTP delivery method will be saved and you will not be required to re-select it on subsequent logins. For details and instructions on using Google Authenticator app please go HERE.

How can I update the phone number or email address on file or change my preferred OTP delivery method?

If you wish to update the phone number or email address on file or change your preferred OTP delivery method, you can do so from the Personal Info section of your online account. If you need further assistance, you can also contact our Service Center.

Why did I receive an OTP at a time of day when I wasn't trying to access my online account?

An OTP will be generated when an attempt is made to log into your account using your user ID and password. If you receive an OTP when you were not attempting to access your account, this means that either someone or some automated process was attempting to access your account at that time. Most often, this is being driven by a third-party financial management service for which you signed up and provided login credentials (i.e. mint.com, eMoney, MoneyGuide Pro, etc.). When these sites attempt to log in to gather the account details, they are encountering our MFA process and, if they do not have a fully deployed MFA solution, an OTP is being generated. Connections to a third party vendor are controlled by that third party's protocols and we suggest that you open a ticket with them to request that this be resolved. You will continue to receive OTPs as that vendor attempts to log into your account on your behalf until the connectivity issue is resolved or you terminate that connection within your account with the third party.

I received my OTP but when I enter it online I get a message saying the code is invalid.

Why?

When you trigger the MFA a one-time PIN is generated and delivered to your preferred device. You will have 5 minutes to use the OTP provided. If you trigger the MFA again before the first one is delivered, the PIN you receive will be invalid and you will need to wait for the second code.

Why didn't I get my OTP?

You will need to confirm the information and device selected is valid. If you need to update the phone number or email address on file or change your preferred OTP delivery method, you can do so from the Personal Info section of your online account. If you need further assistance, you can also contact our Service Center.

I am already logged into my account and I received another request for a OTP. Why?

An OTP will be generated when an attempt is made to log into your account using your user ID and password. Multi-Factor Authentication will also be triggered by specific online transactions. You will be required to enter a OTP with the following changes:

- Password Changes
- Changes to Security Questions
- Personal Information Changes
- Beneficiary Changes
- Loan Requests
- Forgotten Password

Will I have to enter a OTP every time I log in?

A OTP is required at each login by default. You do have the option to choose "remember this device". This will allow for the OTP process to be skipped at login if you again access the account from the same trusted device within 30 days. Please note that the "remember this device" feature is controlled by cookies. If cookies are disabled within your browser settings or if you clear your cookies, you will be prompted to enter your OTP at login.