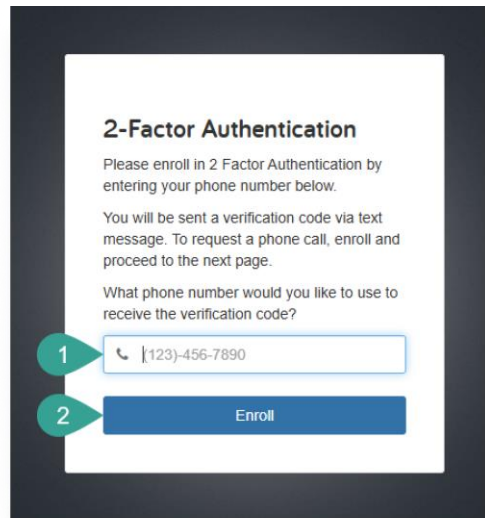


The 2-Factor Authentication (2FA) feature is integrated into your Personal Financial Management Website. It is an important security measure to safeguard your personal financial data. 2FA sends a PIN to your phone to use when logging in.

Initial Enrollment

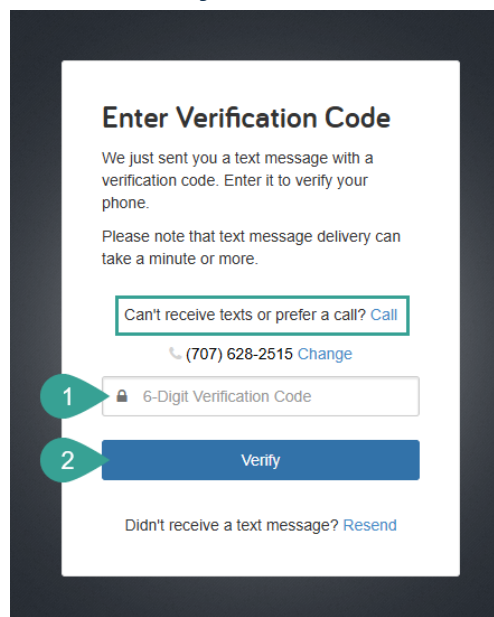
As you register for your personal Client Portal, you must enroll in 2-Factor Authentication.

1. Enter your primary mobile **phone number** and click **Enroll**. International phone numbers are supported. You must enter + and the country code before your phone number.



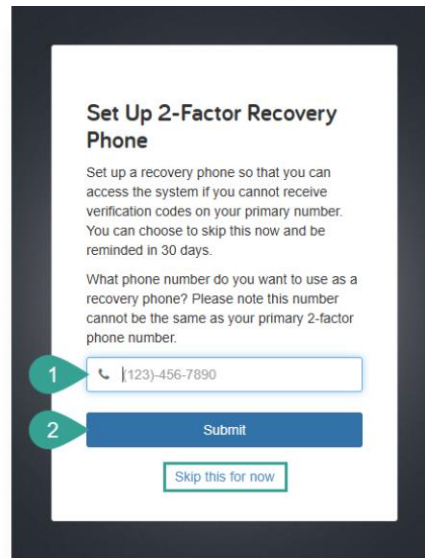
The screenshot shows a dark-themed window titled "2-Factor Authentication". Inside, the text reads: "Please enroll in 2 Factor Authentication by entering your phone number below." followed by "You will be sent a verification code via text message. To request a phone call, enroll and proceed to the next page." and "What phone number would you like to use to receive the verification code?". There is a text input field containing "(123)-456-7890" with a phone icon on the left. Below the input field is a blue button labeled "Enroll". Two green callout boxes with numbers 1 and 2 point to the input field and the "Enroll" button respectively.

2. By default, the system will attempt to text a 6-digit code to the number you entered. You can click the **Call link** to have the code delivered via an automated phone call. Obtain and enter the **6-Digit Verification Code** and click **Verify**.



The screenshot shows a dark-themed window titled "Enter Verification Code". Inside, the text reads: "We just sent you a text message with a verification code. Enter it to verify your phone." followed by "Please note that text message delivery can take a minute or more." There is a link "Can't receive texts or prefer a call? Call" in a box. Below that is a phone number "(707) 628-2515" with a "Change" link. There is a text input field labeled "6-Digit Verification Code" with a lock icon on the left. Below the input field is a blue button labeled "Verify". At the bottom, there is a link "Didn't receive a text message? Resend". Two green callout boxes with numbers 1 and 2 point to the "6-Digit Verification Code" input field and the "Verify" button respectively.

3. If you cannot access your primary phone number, you can set up a 2-Factor Recovery Phone number. Enter your desired **phone number** and click **Submit**. Note that you cannot use the same phone number as your primary phone. If you do not want to set up a recovery phone number, you can use the link to **skip this for now**.



The screenshot shows a form titled "Set Up 2-Factor Recovery Phone". The form contains the following text: "Set up a recovery phone so that you can access the system if you cannot receive verification codes on your primary number. You can choose to skip this now and be reminded in 30 days." Below this, it asks: "What phone number do you want to use as a recovery phone? Please note this number cannot be the same as your primary 2-factor phone number." There are two numbered steps indicated by green circles: Step 1 points to a phone number input field containing "(123)-456-7890", and Step 2 points to a blue "Submit" button. Below the "Submit" button is a link that says "Skip this for now".

Settings

Through your Client Portal, you can select between two levels of 2-factor Authentication security or update your primary or recovery phone numbers.

Standard Security

Requires PIN entry when "at-risk activity" has been identified. Select this option if you prefer only to be prompted with a PIN when our system detects a potential threat, like a login from a foreign country.

High Security

This option requires you to enter a PIN every time you log into the system. Select this option if you prefer to use the highest level of security available.

Note

Depending on your application's version, you may not be able to switch between standard and high security.

2-Factor Authentication

1. To change your 2-factor Authentication Settings, click **Settings** and then **Security**. In the Two-Factor Authentication section, select the radio button for your desired security level or enter a new **Primary Phone** or **Recovery Phone** number. Click **Save**.

Home Organizer My Plan Spending Investments Vault Reports My Advisor

Help Settings Sign Out

Settings // Alerts **Security** Privacy

Change Password

Old Password

New Password

Verify New Password

Save

Two Factor Authentication

Enable two factor authentication to increase your security. Enter a primary phone number to receive SMS, and optionally a recovery phone number for two-factor authentication.

Security Level

☒ Standard Security

☐ High Security

Primary Phone

(707) 628-2515

Recovery Phone

Save

Troubleshooting

If you cannot access your primary phone number, you have the following options.

1. On the Enter Verification Code screen, click **More Options**.

Enter Verification Code

We just sent a text message to you at
(**) ***-**-15 with a verification code. Enter it
to verify your identity.

Please note that text message delivery can
take a minute or more.

6-Digit Verification Code

Sign In

More Options

Didn't receive a text message? [Resend](#)

- Here, you can select **Call Me** or **Text Me** to your **Primary Phone** and/or **Recovery Phone**, if you have one. If you cannot access your established phone numbers, click the link to **Contact [your Advisor] for One Time Access**.



2-Factor Sign In Options

Receive verification code at:

Primary Phone: (*-***-***15**

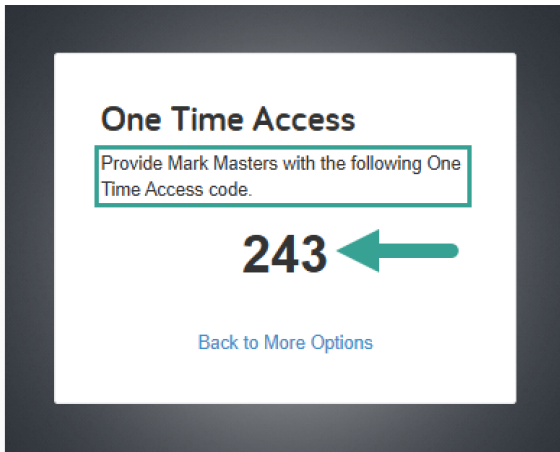
[Text Me](#) [Call Me](#)

Recovery Phone: (*-***-***12**

[Text Me](#) [Call Me](#)

[Contact \[redacted\] for One Time Access](#)

- When using the link for One Time Access, you will see a **code** on screen that you must provide to your Advisor or their applicable staff to approve your login.



One Time Access

Provide Mark Masters with the following One Time Access code.

243

[Back to More Options](#)

Note

If you enter your PIN incorrectly 3 times, your account will become locked. Contact your Advisor or their applicable staff to unlock your account.