

Enrolling in Multi Factor Authentication (MFA) to Access the TRAQS Website

JANUARY 31, 2022 – VERSION 1.2

The information contained herein may not be copied, retransmitted, disseminated, distributed, sold, resold, leased, rented, licensed, sublicensed, altered, modified, adapted, or stored for subsequent use for any such purpose, in whole or in part, in any form or manner or by any means whatsoever, to or for any person or entity, including the purchaser, without FINRA's express prior written consent (unless such use constitutes fair use under the Copyright Act).

Multi Factor Authentication (MFA) enhances the security of accounts by adding an additional layer of security beyond the Username and password. All users of the TRAQS website are required to enroll in MFA using their mobile device or landline. Sharing account credentials is not recommended.

The following enrollment steps only need to be completed once per user account. For more information about MFA please see our TRAQS MFA website

The TRAQS website uses a combination of Transport Layer Security (TLS) encryption and an Okta cloud based authentication platform referred to as the NASDAQ MFA Service to protect data that is being transferred from the client to FINRA and back. To access the TRAQS website for trade reporting, the user must be entitled to use the product, have an assigned Username and password, answer the security questions and have at least one second factor authentication method. The available second factor authentication methods include Okta Verify, Google Authenticator, SMS Authentication, and Voice Call Authentication



Note: This guide covers information specific to MFA. Review the TRAQS User Guide for the trade reporting product for questions about navigating the TRAQS website.

Table of Contents

Section 1: How to Enroll and Choose Authentication Method(s) to Access the TRAQS Website	4
Okta Verify	9
Installing Okta Verify	9
Google Authenticator.....	14
Installing Google Authenticator.....	14
SMS Authentication	20
Setting up SMS Authentication	20
Voice Call Authentication	24
Setting up Voice Call Authentication	24
Section 2: Profile Page	28
How to Edit the User Profile	30
How to Remove My Verification Devices.....	33
How to Unlock your Account.....	37
Section 3: How to Login to the TRAQS Website Using MFA.....	41
Section 4: How to Access the API Download	47
Section 5: Common Questions	48
Section 6: Revision History	51

Section 1: How to Enroll and Choose Authentication Method(s) to Access the TRAQS Website

1. To establish a new TRAQS Username, please use the **Participant Data Management System**, ~~a person with administrator access to the FINRA Order Form must complete the **FINRA Order Form**.~~
~~Please Note, step 1 is not necessary for existing users of the TRAQS website. Existing users will be emailed automatically when Multi Factor authentication is implemented.~~
2. An email will be sent to the user containing an invitation to access the NASDAQ MFA service.

This is an automatically generated message from Okta.fokta.com. Replies are not monitored or answered.



FINRA TRAQS - Welcome to Okta!

Hi John,

FINRA is using Okta to manage the Multi-Factor Authentication for TRAQS.

An Okta account for FINRA TRAQS access has been created for you.

Click the link below to activate your Okta account:

Activate Okta Account

This link expires in 30 days.

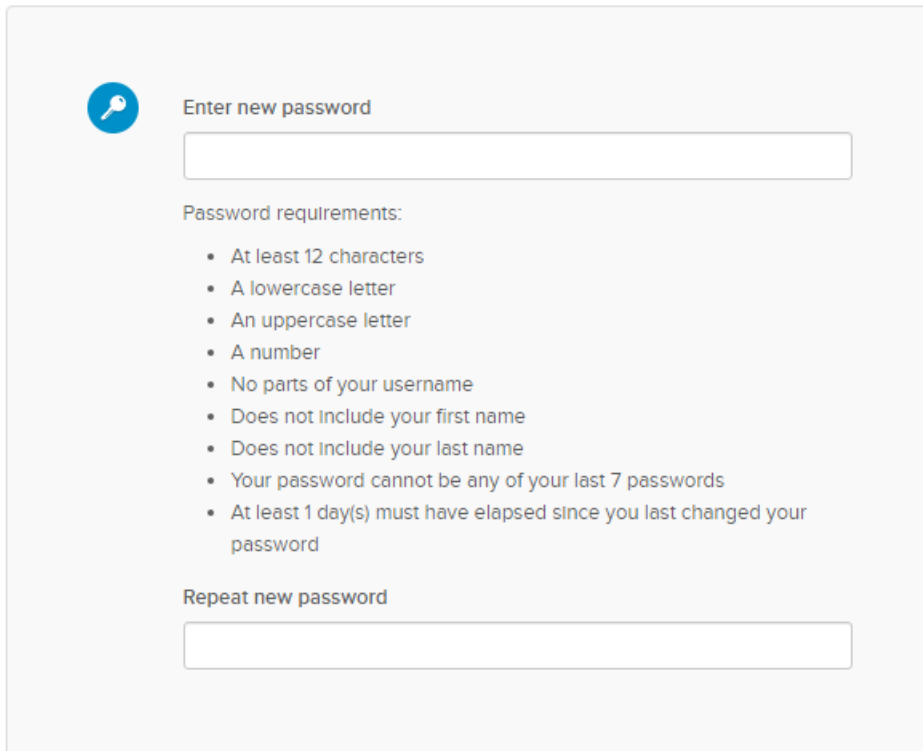
Your Username (email address) is John.smith@yourfirm.org

FINRA's Okta Account for TRAQS access sign-in page is <https://sign-inpage.com>

For further information regarding MFA for TRAQS please click [here](#)

3. Click on the **Activate TRAQS Account** link in the email. This will allow you to set up your Okta Account. The Okta account set up involves entering a new password, setting up a forgotten password question/answer and selecting a security image.
4. Enter a **New Password**. Confirm your password in the **Repeat New Password** field.

Welcome to FINRA TRAQS **John!**
Create your FINRA TRAQS account



The screenshot shows a form titled "Enter new password" with a key icon. It includes a text input field for the password, a list of password requirements, and a "Repeat new password" field.

Enter new password

Password requirements:

- At least 12 characters
- A lowercase letter
- An uppercase letter
- A number
- No parts of your username
- Does not include your first name
- Does not include your last name
- Your password cannot be any of your last 7 passwords
- At least 1 day(s) must have elapsed since you last changed your password

Repeat new password

5. Choose a **Forgotten Password Question** and enter an **Answer**. The answer must be at least 3 characters.



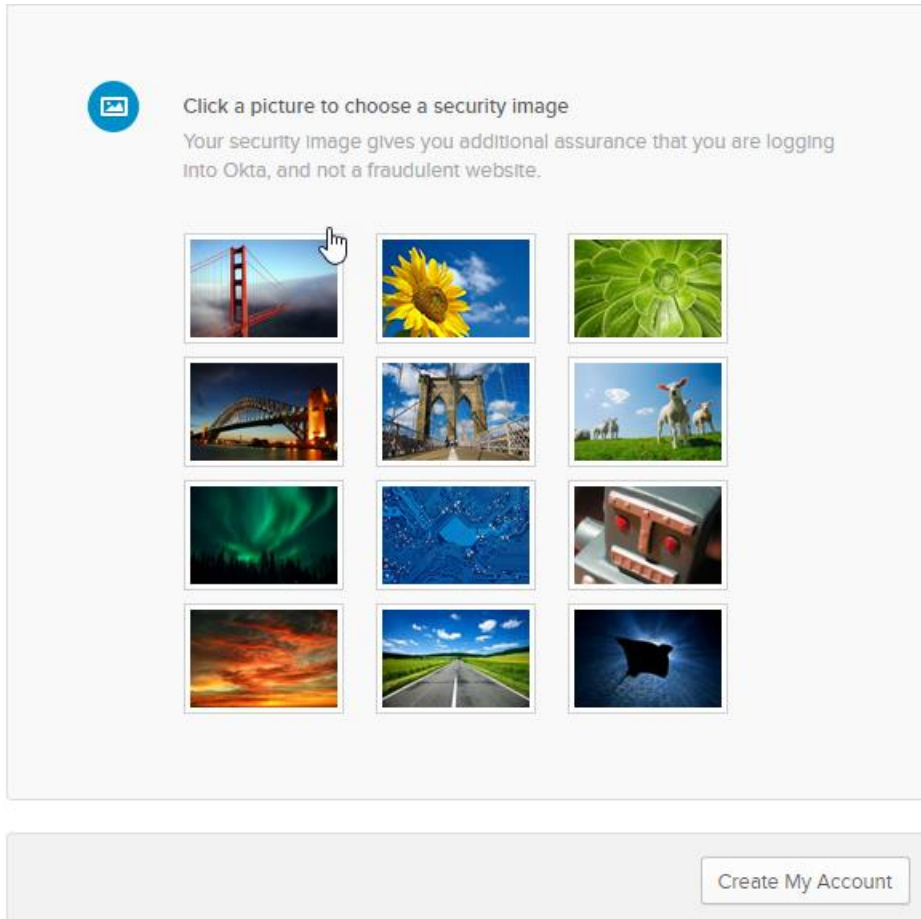
The screenshot shows a form titled "Choose a forgot password question" with a padlock icon. It includes a dropdown menu for the question and a text input field for the answer.

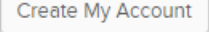
Choose a forgot password question

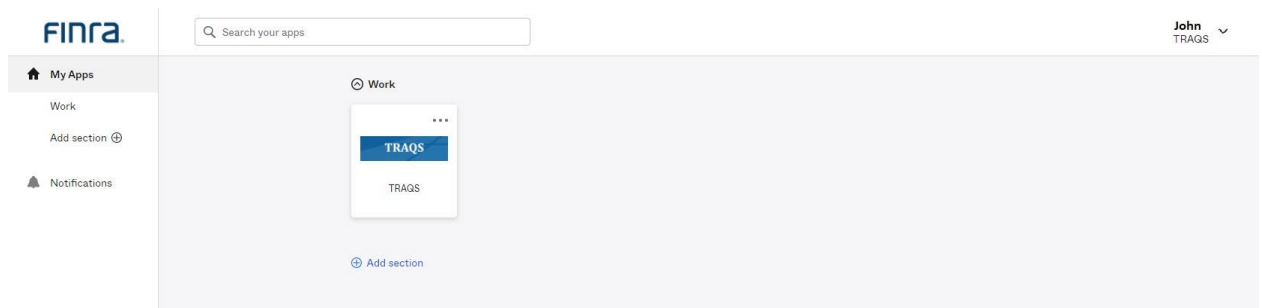
What is the food you least liked as a child? ▼

Answer

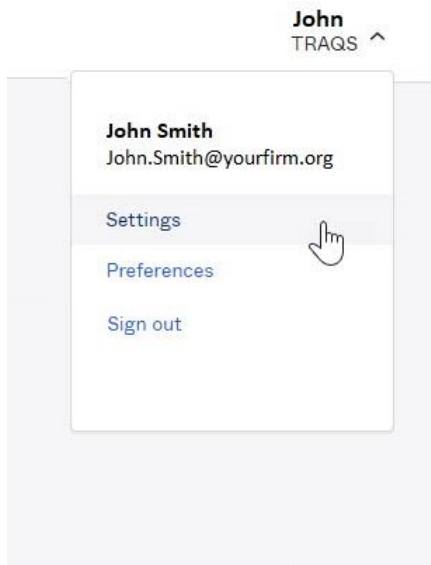
6. Select a **Security Image** for additional assurance your logging into your Okta account. On future visits to the site, the security image will display after entering your email to let you know you are logging into the correct website.




7. Click on **Create My Account** button.  This will create your Okta account and will take you to your **Profile Page**.

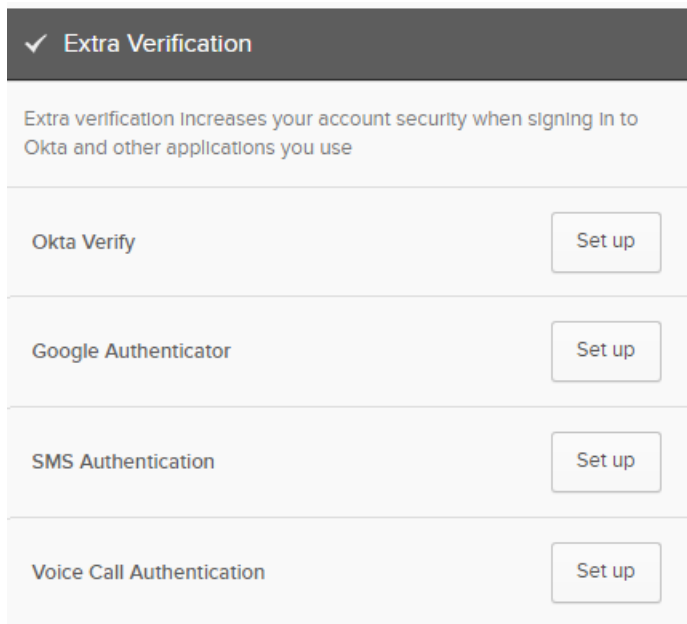


8. Click on your **Name** and select **Settings**. This will open the Account page.

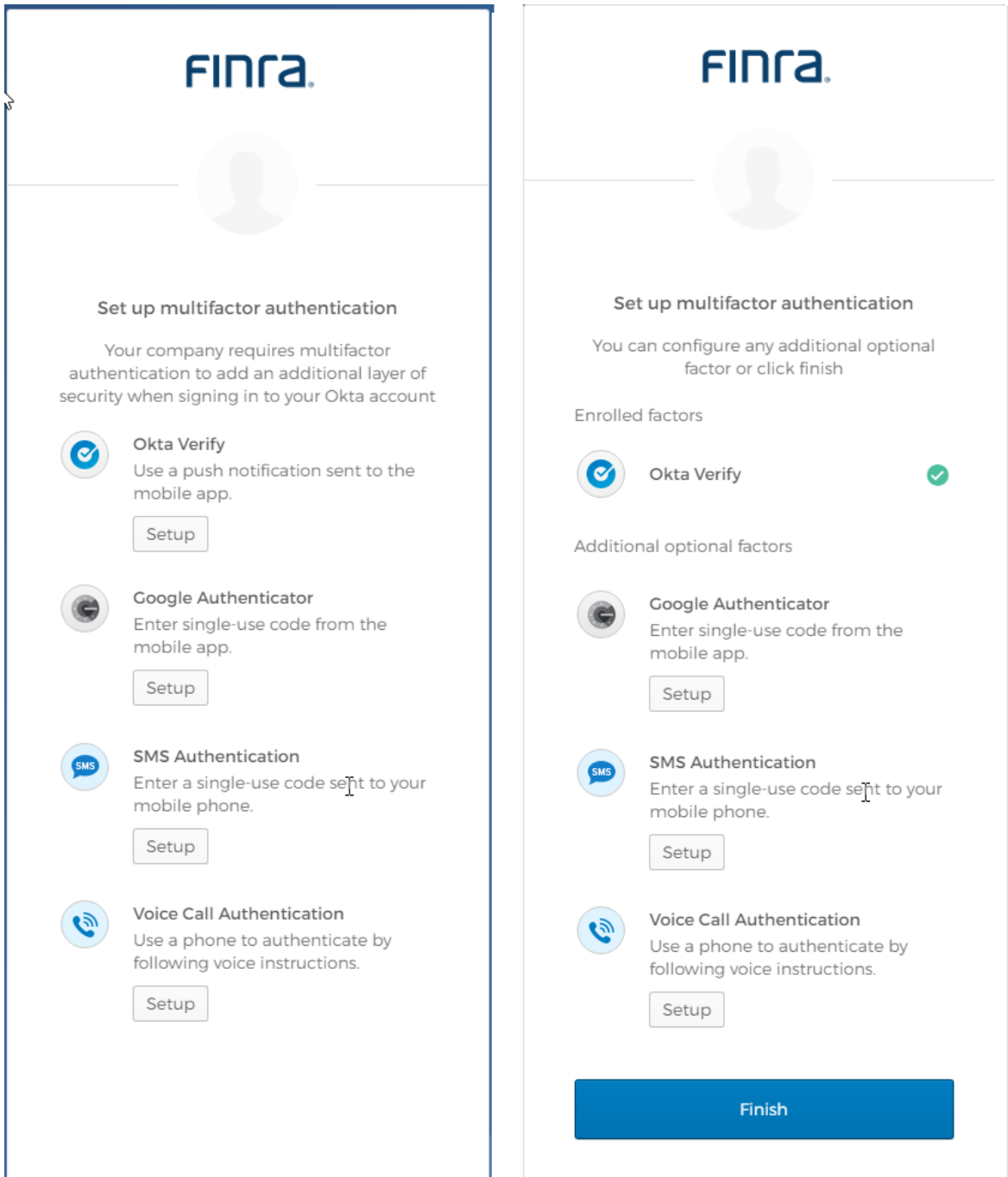


9. Click the **Edit Profile** button , then verify your **Password** if prompted. This will allow you to edit your Account.

10. In the **Extra Verification** section, select the **Preferred Authentication Method** from the list of available choices including [Okta Verify](#), [Google Authenticator](#), [SMS Authentication](#), and [Voice Call Authentication](#). Click **Setup** next to the factor you want to use. Please continue reading for a description of each validation method and instructions for enrollment.



Note: Users are required to set up an Extra Verification. Users will receive the authentication method enrollment screen below (on the left) when trying to access the TRAQS website without at least one authentication method set up. Once you select an authentication method, from the choices below, follow the instructions, and when completed, the authentication method will have a green check box next to it (screen on the right). Users can choose to add additional authentications or proceed directly to the Account page by selecting **Finish**.



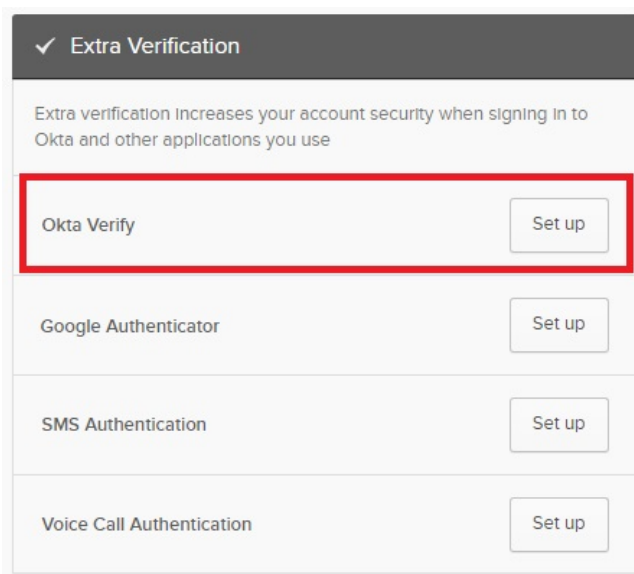
Okta Verify

This is a mobile app that verifies your identity in one of two ways. Okta Verify can send a push notification that you approve on your mobile device. Alternatively, Okta Verify can generate a 6-digit code that displays for users to type into the Sign In screen.

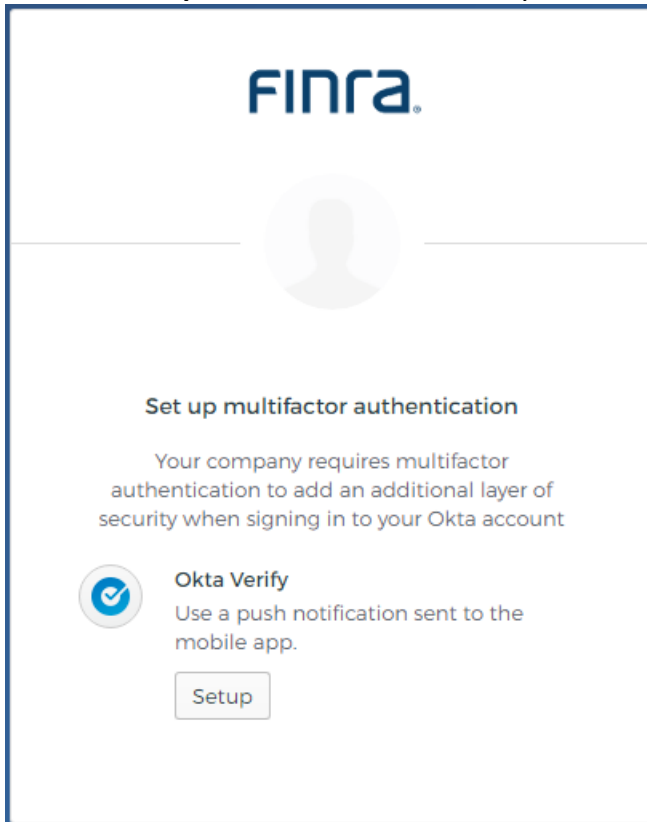
Note for iPhone users: If you would like to use Okta verify, you must have face id/touch id (iPhone 5 and higher) enabled on your phone. If you do not want to enable face id/touch id please use another verification. Also you must be on the latest iOS.

Installing Okta Verify

1. Click the **Setup** button next to Okta Verify option

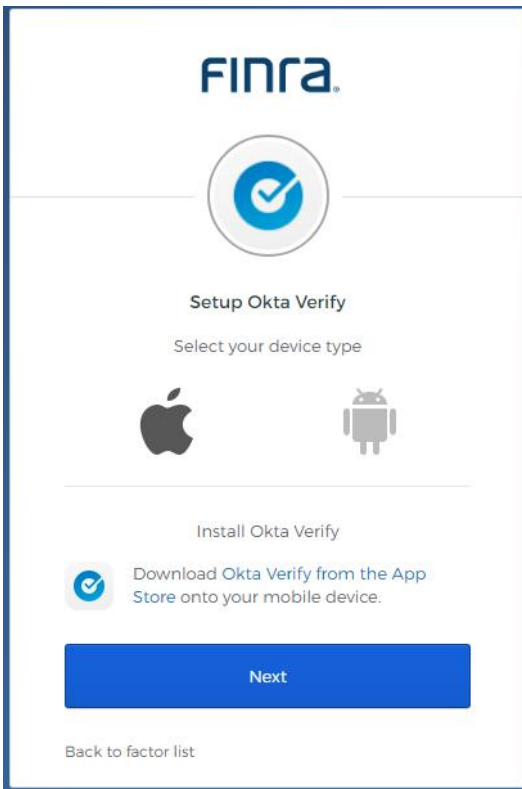


2. Click the **Setup** button under Okta Verify

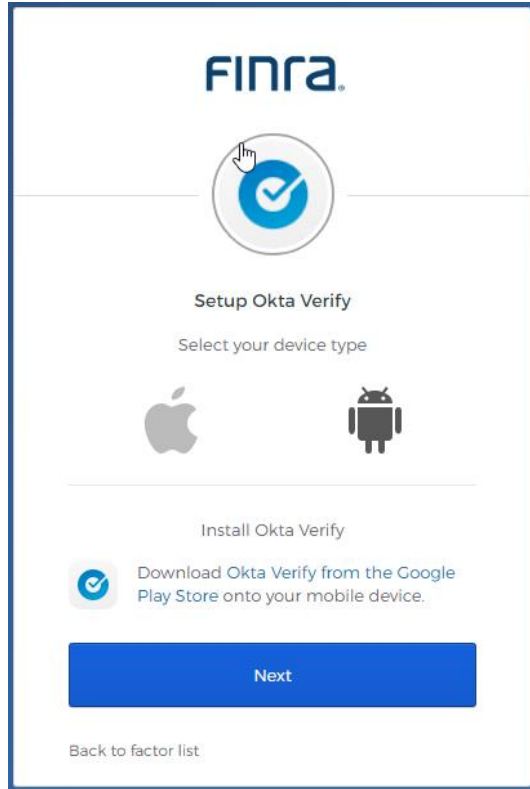


3. Select **Device Type**: iPhone or Android from the list
4. **Download** the **Okta Verify App** from the App Store or Google Play Store onto your primary mobile device. Click **Next** once the download is complete..

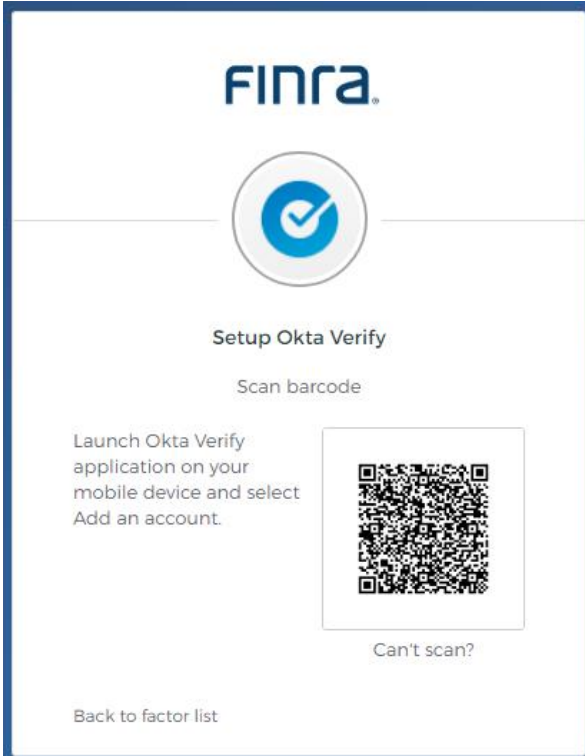
iPhone



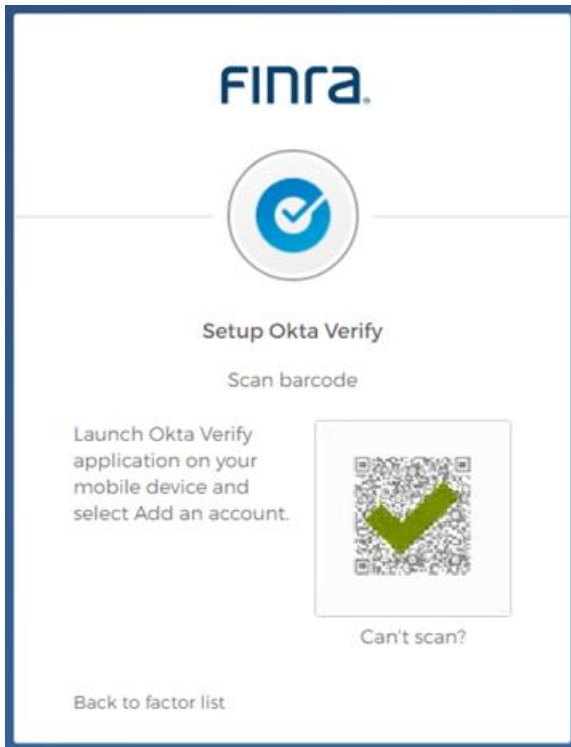
Android



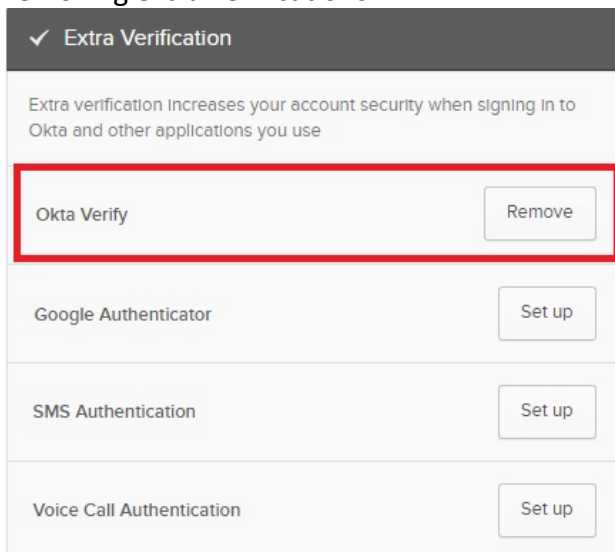
5. A screen with a **QR code** will appear on your computer monitor.



6. **Open the Okta Verify App** on your mobile device.
7. Follow instructions on your mobile device to add FINRA's MFA.
8. **Scan the Barcode** using the **Okta Verify App**. If it was successful you will see a green checkmark.

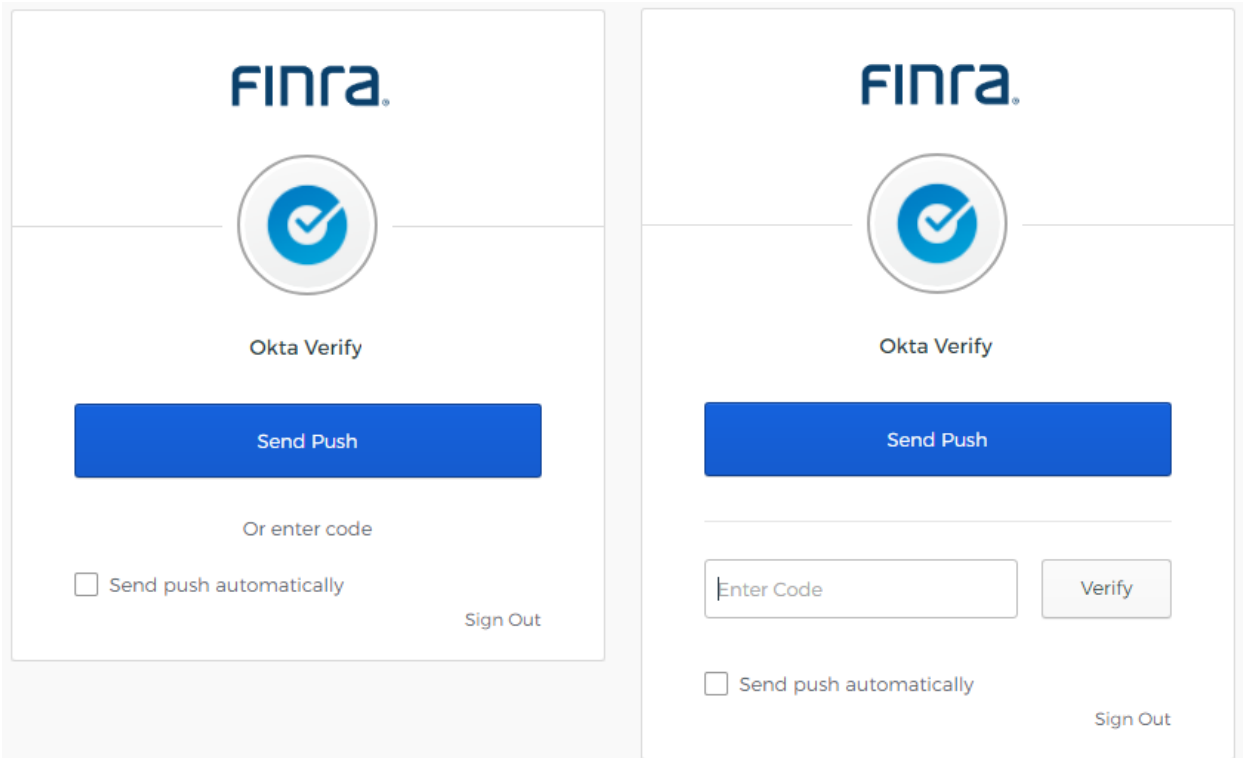


9. Once you have completed the set up for a verification, you will be directed back to the profile page and the Okta Verify button will now say "Remove". In some cases, Okta Verify will have a green check box next to it. Select **Finish** to return to the Account page. Please see [How to Remove My Verifications Devices](#) below for information about removing extra verifications.



10. Users can choose to add additional factors or proceed directly to the TRAQS website.
Please see [Section 3](#) below for instructions on logging into the website using MFA.
11. The website will prompt you to use your chosen validation method(s) to login.
12. Going forward users of the Okta Verify App will be prompted to select between a push notification or a passcode notification.

<p>Push: Access the Okta Verify app on the associated device and approve the request.</p>	<p>Passcode: Use an auto generated Okta verify passcode. Users must enter the code contained in the App into the entry box and click Verify. Note: The code changes every 30 seconds. If you fail to enter a code within 30 seconds please enter the next generated code.</p>
--	--



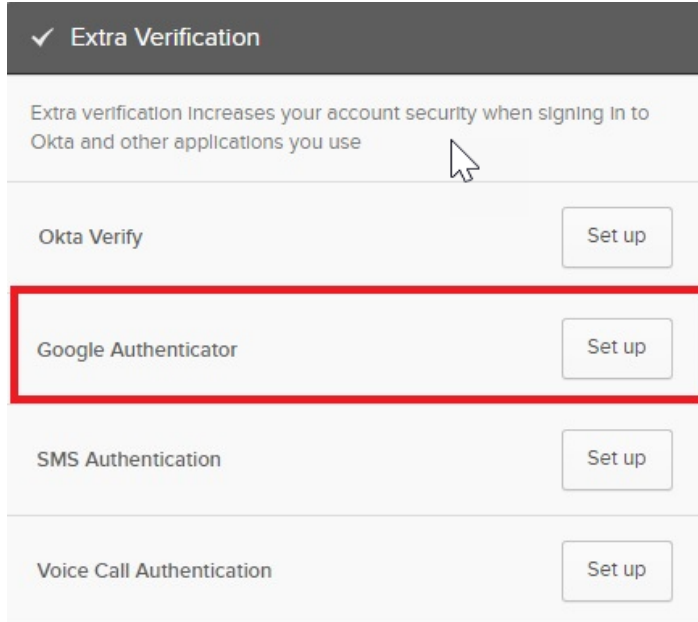
Note: If users would like an automatic push notification, please select the **Send Push Automatically** check box.

Google Authenticator

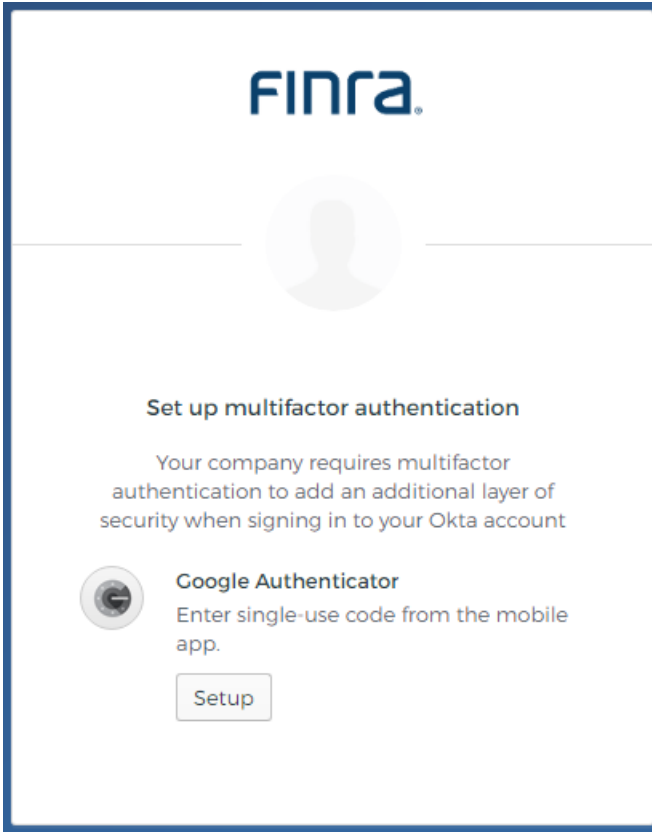
This method of verification uses a third-party app to generate a 6-digit code for users to type into the Sign In screen. Users will have 30 seconds to input the code before it generates another.

Installing Google Authenticator

1. Click the **Setup** button next to the Google Authenticator option



2. Click the **Setup** button under Google Authenticator



3. Select **Device Type**: iPhone, Android or Blackberry from the list
4. **Download** the **Google Authenticator App** from the App Store, Google Play or Blackberry World Store onto your primary mobile device. Click **Next** once the download is complete.

iPhone

The screenshot shows the FINra mobile application interface for an iPhone. At the top is the FINra logo. Below it is a circular icon with a 'G' and a keyhole. The text reads "Setup Google Authenticator" and "Select your device type". Three icons are shown: Apple, Android, and BlackBerry. Below this, it says "Install Google Authenticator" and "Download Google Authenticator from the App Store onto your mobile device." A blue "Next" button is at the bottom, with a "Back to factor list" link below it.

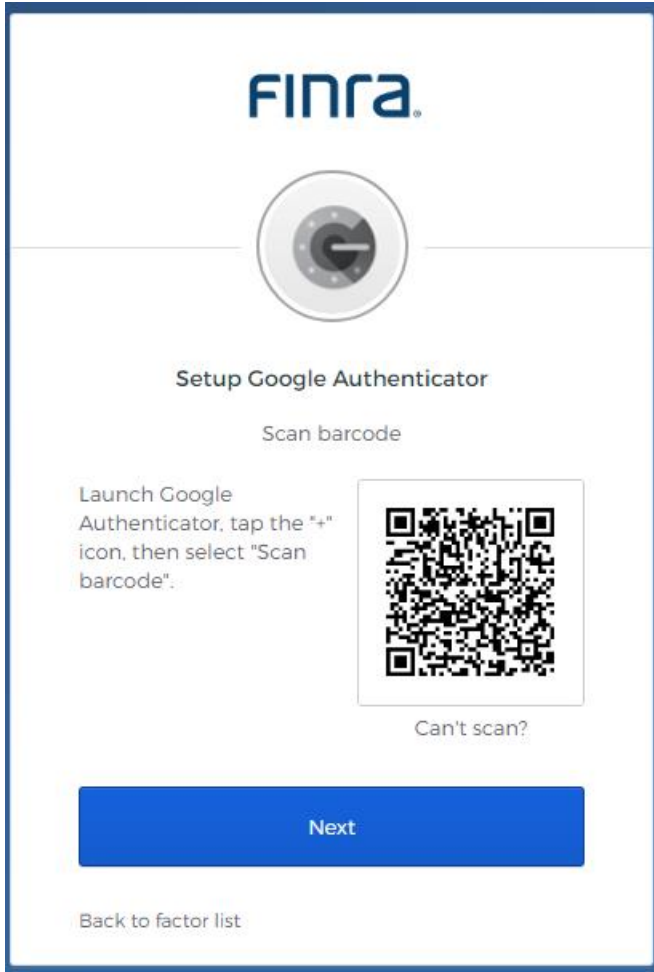
Android

The screenshot shows the FINra mobile application interface for an Android device. It features the same FINra logo and circular icon as the iPhone version. The text reads "Setup Google Authenticator" and "Select your device type". Three icons are shown: Apple, Android, and BlackBerry. Below this, it says "Install Google Authenticator" and "Download Google Authenticator from the Google Play Store onto your mobile device." A blue "Next" button is at the bottom, with a "Back to factor list" link below it.

Blackberry

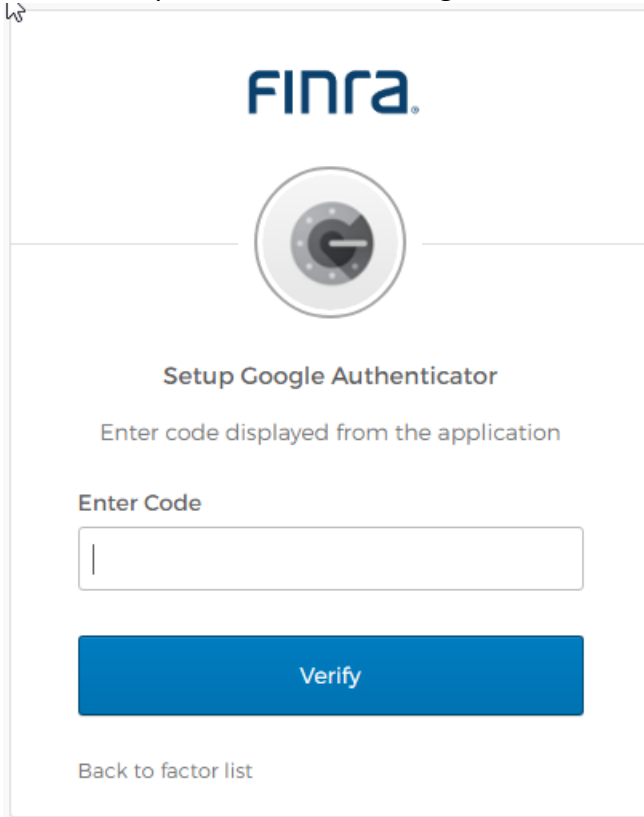
The screenshot shows the FINra mobile application interface for a Blackberry device. It features the same FINra logo and circular icon as the other versions. The text reads "Setup Google Authenticator" and "Select your device type". Three icons are shown: Apple, Android, and BlackBerry. Below this, it says "Install Google Authenticator" and "Download Google Authenticator from the Blackberry World Store onto your mobile device." A blue "Next" button is at the bottom, with a "Back to factor list" link below it.

5. A screen with a **QR Code** will appear on your computer monitor.



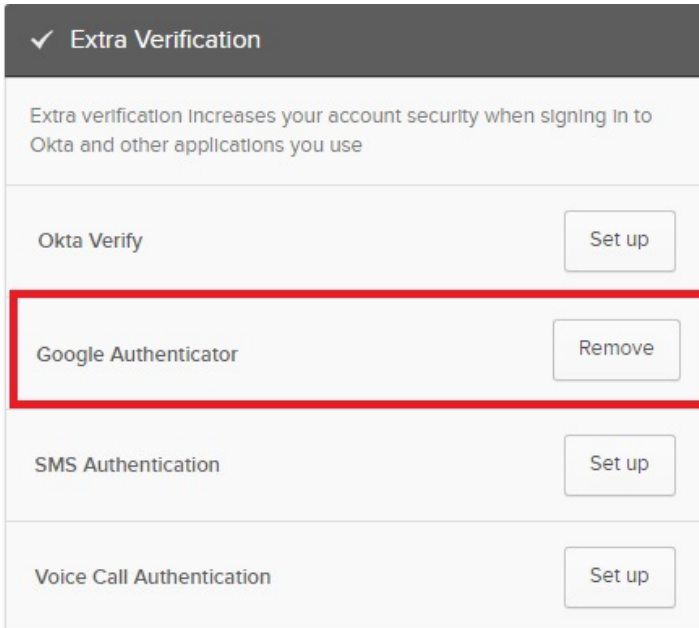
6. **Open the Google Authenticator App** on your mobile device.
7. Follow instructions on your mobile device.

8. **Scan the Barcode** using the Google Authenticator App and click the **Next** button. **Enter the code** from your mobile device without spaces onto the screen and click **Verify**. Please note that the code changes every 30 seconds. If you fail to enter a code within 30 seconds please enter the next generated code.



The screenshot shows the FINRA website's Google Authenticator setup page. At the top is the FINRA logo. Below it is a circular icon representing the Google Authenticator app. The main heading is "Setup Google Authenticator". Underneath, it says "Enter code displayed from the application". There is a text input field labeled "Enter Code" with a vertical cursor. Below the input field is a large blue button labeled "Verify". At the bottom left, there is a link that says "Back to factor list".

9. Once you have completed the set up for a verification, you will be directed back to the profile page and the Google Authentication button will now say "Remove". In some cases, Google Authenticator will have a green check box next to it. Select **Finish** to return to the Account page. Please see [How to Remove My Verifications Devices](#) below for information about removing extra verifications.



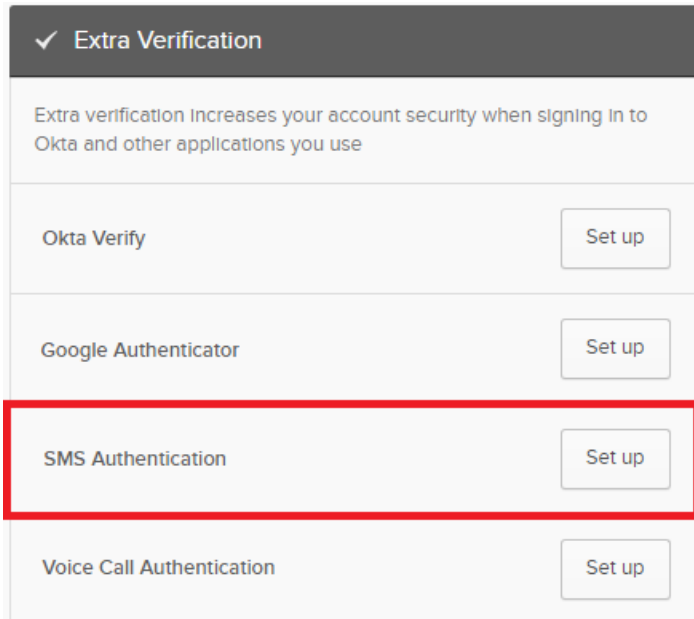
10. Users can choose to add additional factors or proceed directly to the TRAQS website. Please see [Section 3](#) below for instructions on logging into the TRAQS website using MFA.
11. The website will prompt you to use your chosen validation method(s) to login.

SMS Authentication

SMS Authentication uses the text messaging service on your mobile device to generate a 6-digit-code for users to type into the Sign In screen.

Setting up SMS Authentication

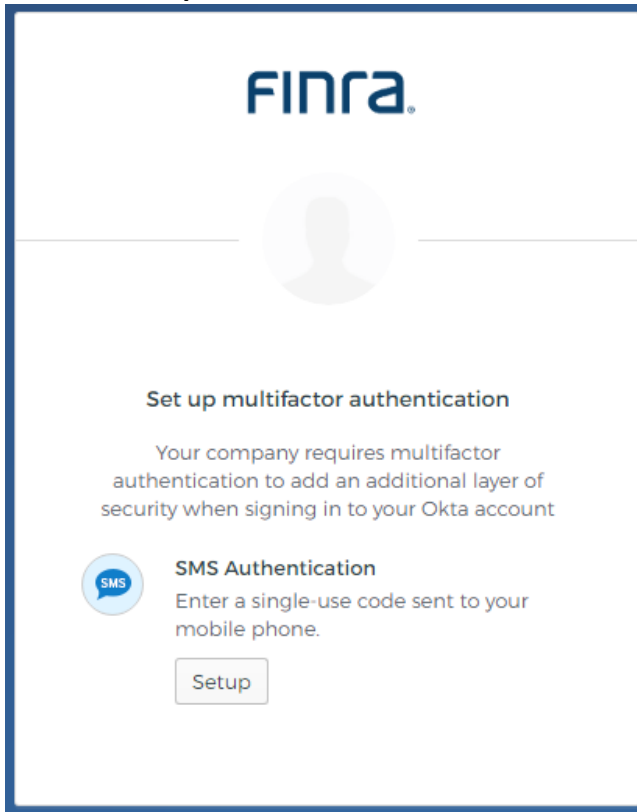
1. Click the **Setup** button next to the SMS Authentication Option



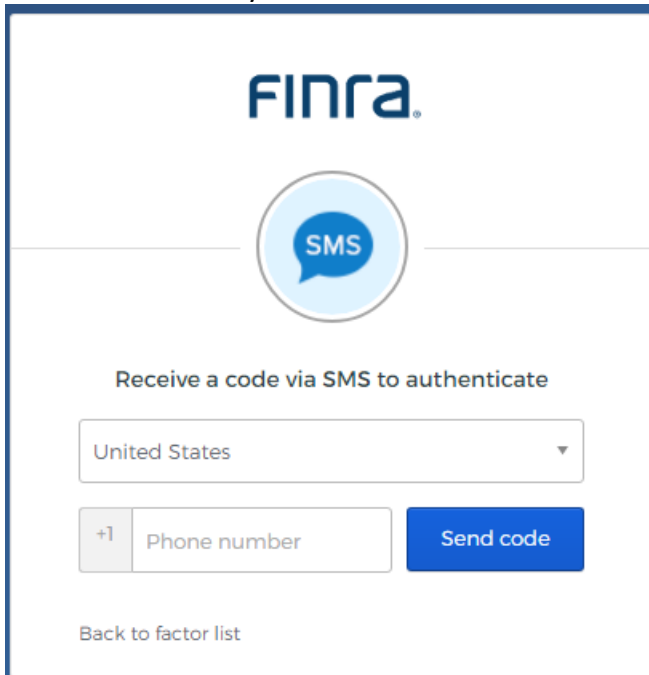
The screenshot shows a settings page for 'Extra Verification'. At the top, there is a dark header with a checkmark and the text 'Extra Verification'. Below this is a descriptive paragraph: 'Extra verification increases your account security when signing in to Okta and other applications you use'. The main content area is a list of authentication options, each with a 'Set up' button to its right. The options are: 'Okta Verify', 'Google Authenticator', 'SMS Authentication', and 'Voice Call Authentication'. The 'SMS Authentication' row is highlighted with a red rectangular border.

✓ Extra Verification	
Extra verification increases your account security when signing in to Okta and other applications you use	
Okta Verify	Set up
Google Authenticator	Set up
SMS Authentication	Set up
Voice Call Authentication	Set up

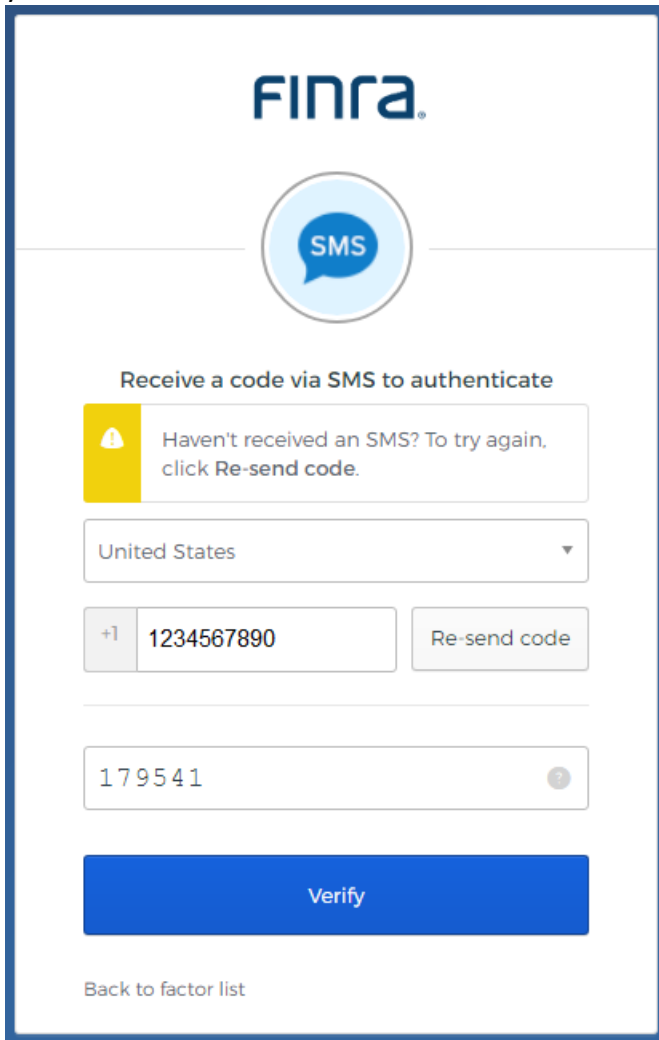
2. Click the **Setup** button below the SMS Authentication.



3. **Choose your country** from the drop-down list and **enter your mobile phone number**. The default country is the United States. Click **Send code**

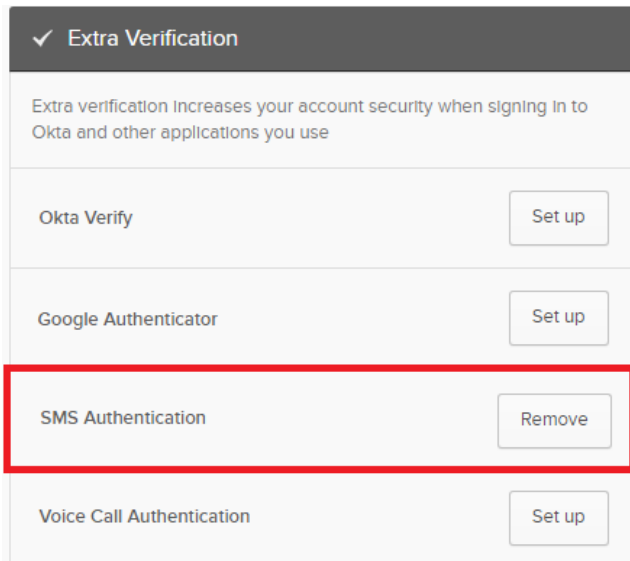


4. **Enter the code** that arrives via text message on your mobile device and click **Verify**. If you don't receive the code via SMS click the **Re-send code** button.



The screenshot shows the FINRA SMS authentication interface. At the top is the FINRA logo. Below it is a circular icon with 'SMS' inside. The main heading reads 'Receive a code via SMS to authenticate'. A yellow warning box contains a triangle icon and the text: 'Haven't received an SMS? To try again, click Re-send code.' Below this is a dropdown menu for the country, currently set to 'United States'. Underneath is a phone number input field with '+1' on the left and '1234567890' in the field, followed by a 'Re-send code' button. A second input field contains the code '179541'. A large blue 'Verify' button is positioned below the code field. At the bottom left, there is a link that says 'Back to factor list'.

5. Once you have completed the set up for a verification, you will be directed back to the profile page and the SMS Authentication button will now say "Remove". Please see [How to Remove My Verifications Devices](#) below for information about removing extra verifications.



6. Users can choose to add additional factors or visit our TRAQS website. Please see [Section 3](#) below for instructions on logging into the website using MFA.
7. The website will prompt you to use your chosen validation method(s) to login.

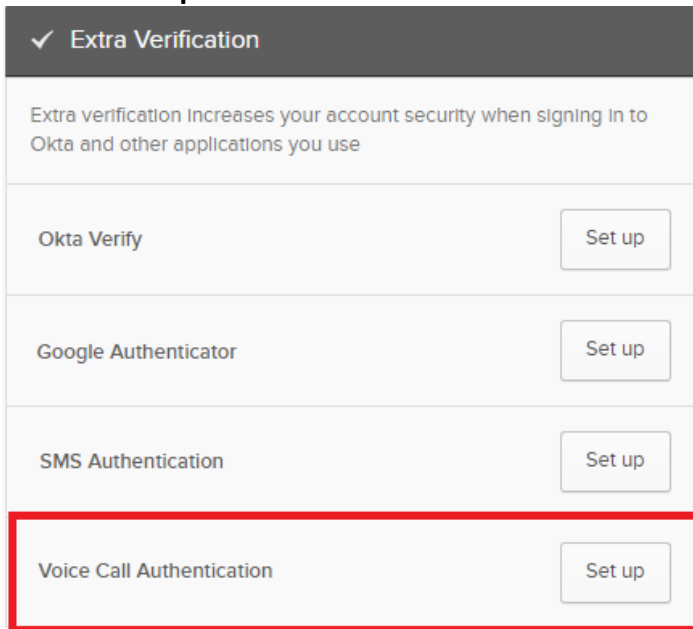
Note: The user must have access to the device associated with the phone number in order to login using this authentication method

Voice Call Authentication

This method of verification will provide a spoken 5-digit-code for users to type into the Sign In screen via mobile device or land line. This method of verification is suitable for users that don't have access to text messaging.

Setting up Voice Call Authentication

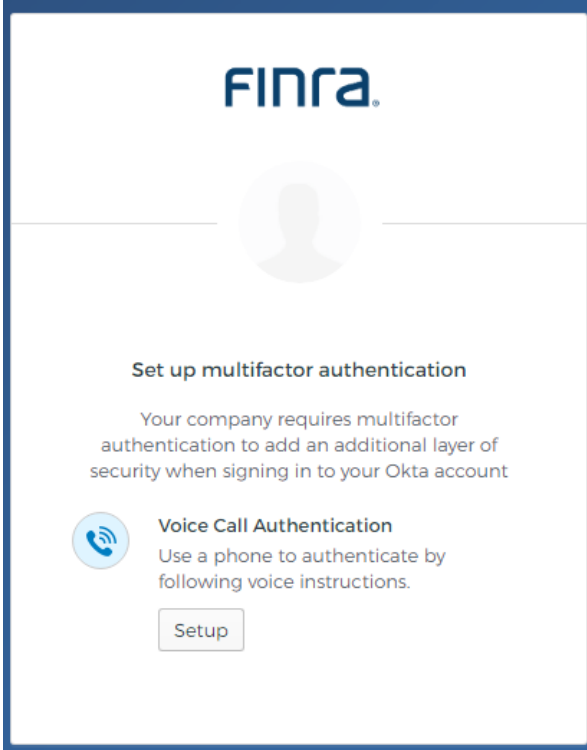
1. Click the **Setup** button next to the Voice Call Authentication option.



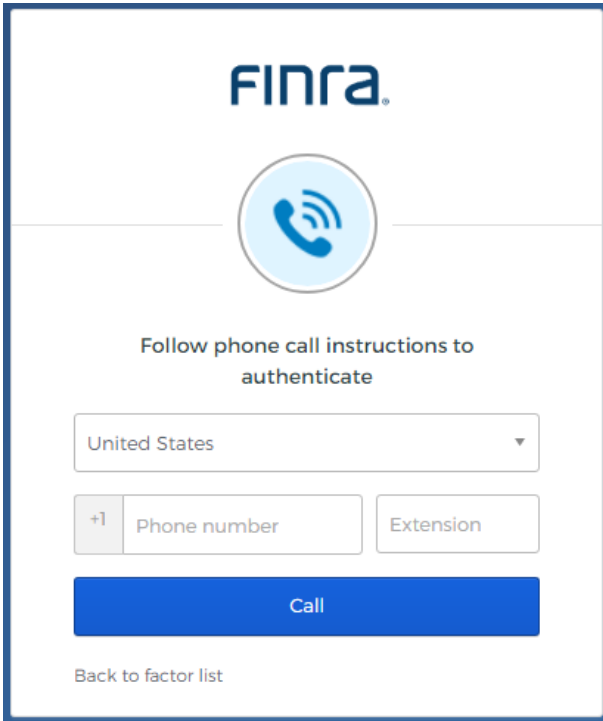
The screenshot shows a settings page for 'Extra Verification'. At the top, there is a dark header with a checkmark and the text 'Extra Verification'. Below this is a descriptive paragraph: 'Extra verification increases your account security when signing in to Okta and other applications you use'. The main content area lists four authentication methods, each with a 'Set up' button to its right. The 'Voice Call Authentication' option is highlighted with a red rectangular border.

✓ Extra Verification	
Extra verification increases your account security when signing in to Okta and other applications you use	
Okta Verify	Set up
Google Authenticator	Set up
SMS Authentication	Set up
Voice Call Authentication	Set up

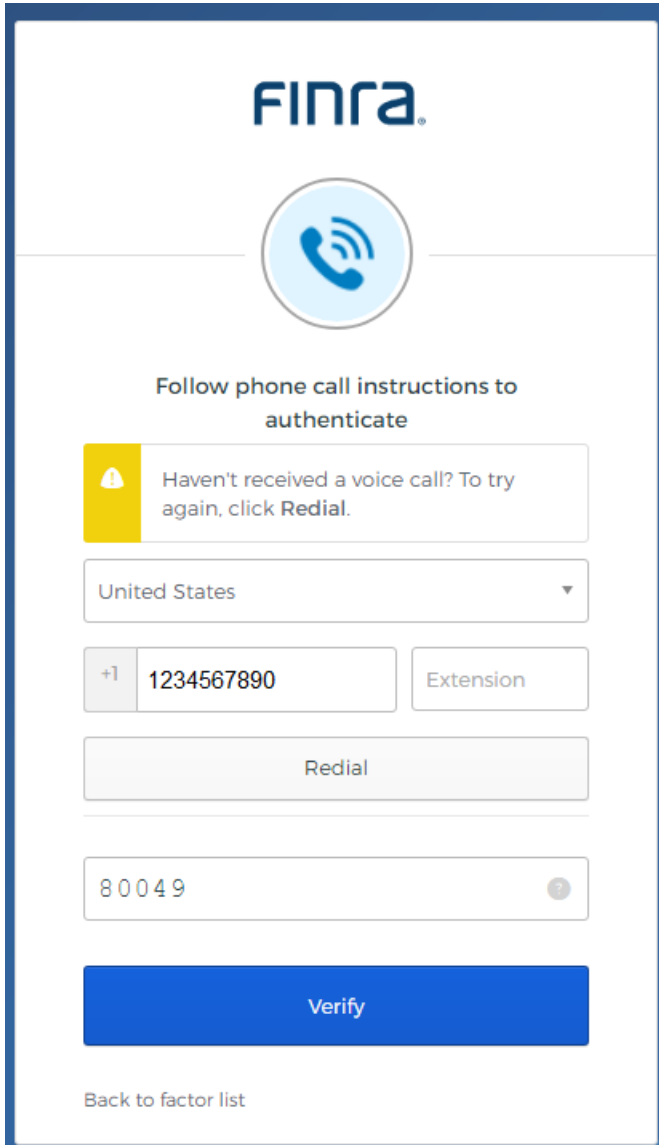
2. Click the **Setup** button below the Voice Call Authentication.



3. **Choose your country** from the drop-down list and **enter your mobile device or landline number** on which you prefer to receive phone calls. The default country is the United states. Click **Call**



4. **Answer the phone** and follow phone call instructions to authenticate.
5. **Enter the provided code** into the Enter code box. Click **Verify**. Note: The call will last about 30 seconds and the code will be repeated twice. If you don't receive the code via a voice call click the **Redial** button.



The screenshot shows the FINRA authentication interface. At the top is the FINRA logo. Below it is a circular icon with a blue telephone handset and signal waves. The text "Follow phone call instructions to authenticate" is centered. A yellow warning box contains a triangle icon and the text: "Haven't received a voice call? To try again, click **Redial**." Below this is a dropdown menu showing "United States". There are two input fields for a phone number: the first contains "+1 1234567890" and the second is labeled "Extension". A "Redial" button is positioned below the phone number fields. A horizontal line separates this section from the code entry section. The code entry section has a text box containing "80049" and a question mark icon. Below the code box is a large blue "Verify" button. At the bottom left, there is a link that says "Back to factor list".

6. Once you have completed the set up for a verification, you will be directed back to the profile page and the Voice Call Authentication button will now say “Remove”. Please see [How to Remove My Verifications Devices](#) below for information about removing extra verifications.

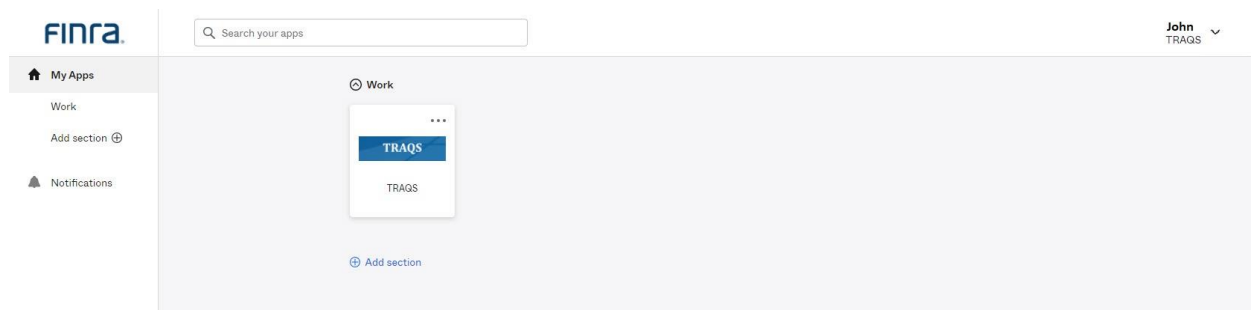
✓ Extra Verification	
Extra verification increases your account security when signing in to Okta and other applications you use	
Okta Verify	Set up
Google Authenticator	Set up
SMS Authentication	Set up
Voice Call Authentication	Remove

7. Users can choose to add additional factors or proceed directly to the TRAQS website. Please see [Section 3](#) below for instructions on logging into the website using MFA.
8. The website will prompt you to use your chosen validation method(s) to login.

Note: The user must have access to the mobile device or land line included in step 2 in order to login using this authentication method.

Section 2: Profile Page

1. Visit the UAT website <https://mpp-test.nasdaq.com> OR Production website <https://mpp.nasdaq.com>
2. Enter your **Username (email address)** and **password**
3. The Main Page (Home page) is where the link to the TRAQS Application resides
4. The Vertical Masthead is always accessible. This is where you can find:
 - **My Apps** – Click to return to the Main Page (Home page)
 - **Notifications** – Click to view any notifications
5. The Horizontal Masthead is always accessible. This is where you can find:
 - **FINRA Logo** – Click to return to the Main Page (Home page)
 - **User Profile** – Settings, Preferences or Sign out selections
 - User can select **Settings** to go to the Account Page
 - User can select **Preferences** to go to the layout page where you can change to Grid View or List View
 - User can select **Sign out** to Sign out of the Profile Page



6. The Account Page is where you can view Personal Information, Change Password, Change Security Image, Change Forgotten Password Question, Setup/Remove Verifications, and Change Display Language. Click on your **Name** and select **Settings**. This will open the Account page.

The screenshot shows the Okta Account page for a user named John TRAGS. The page is divided into several sections:

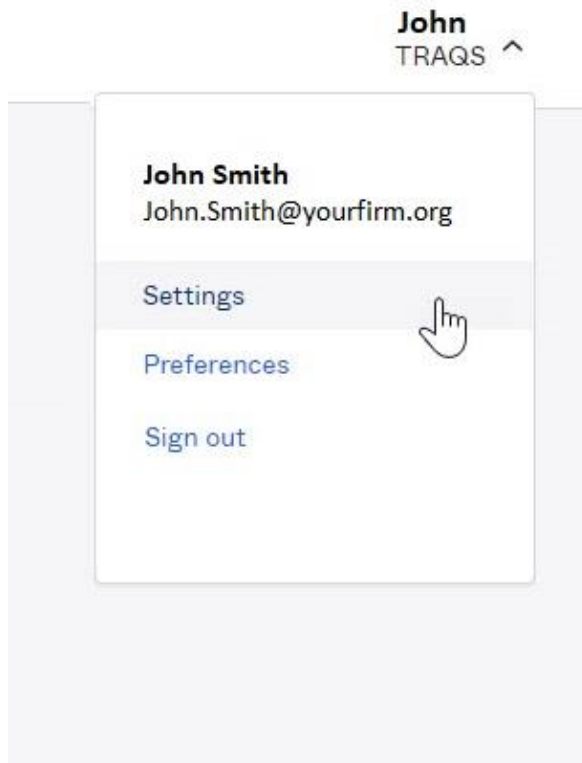
- Personal Information:** Displays fields for First name (John), Last name (Smith), Okta username (John.smith@yourfirm.org), Primary email (John.smith@yourfirm.org), and TRAGS Username (["username1", "username2"]).
- Change Password:** Lists password requirements:
 - At least 12 characters
 - A lowercase letter
 - An uppercase letter
 - A number
 - No parts of your username
 - Does not include your first name
 - Does not include your last name
 - Your password cannot be any of your last 7 passwords
 - At least 1 day(s) must have elapsed since you last changed your password
- Forgotten Password Question:** A section to select a question for password resets.
- Extra Verification:** A table showing the status of various authentication methods:

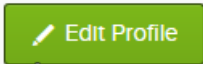
Method	Status
Okta Verify	Enabled
Google Authenticator	Disabled
SMS Authentication	Disabled
Voice Call Authentication	Disabled
- Display Language:** Shows the current language is English, with instructions on how to change it.
- Security Image:** A placeholder for a security image with a description: "Your security image gives you additional assurance that you are logging into Okta, and not a fraudulent website." An image of a shark is shown.
- Recently Used Apps:** A section to enable or disable recently used apps, with an "Enable recently used apps" checkbox.

At the bottom left, it says "Last sign in: a few seconds ago" and "© 2021 Okta, Inc. | Privacy".

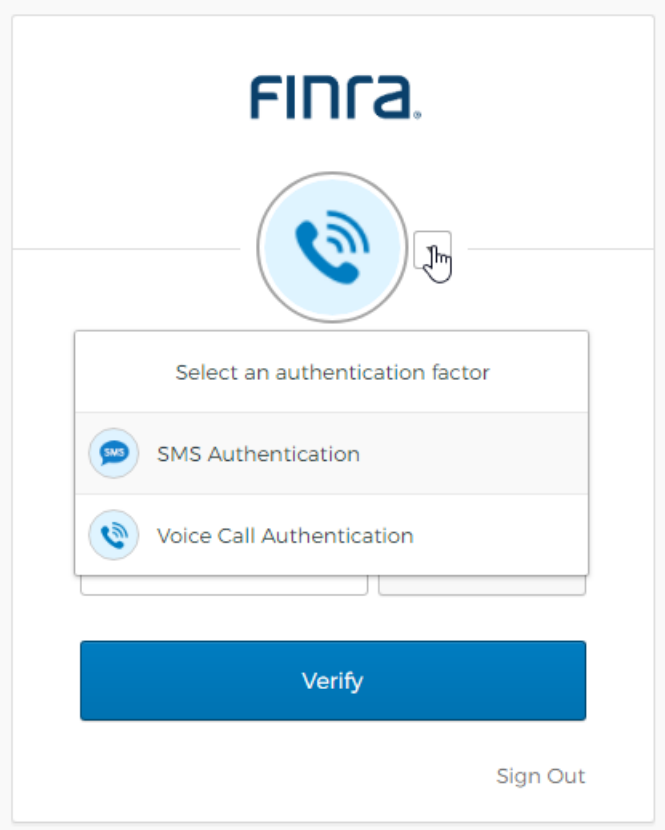
How to Edit the User Profile

1. Visit the UAT website <https://mpp-test.nasdaq.com> OR Production website <https://mpp.nasdaq.com>
2. Enter your **Username (email address)** and **password**
3. Click on your **Name** and select **Settings**. This will open the Account page.



4. Click the **Edit Profile** button , then enter your **Password** if prompted. This will allow you to edit your Account.

5. Authenticate your account using your chosen authentication method(s). Please note, the default authentication method will be the last method you used. Select the method you wish to use from the authentication method drop down. The drop down only contains authentication methods that you have enrolled in.



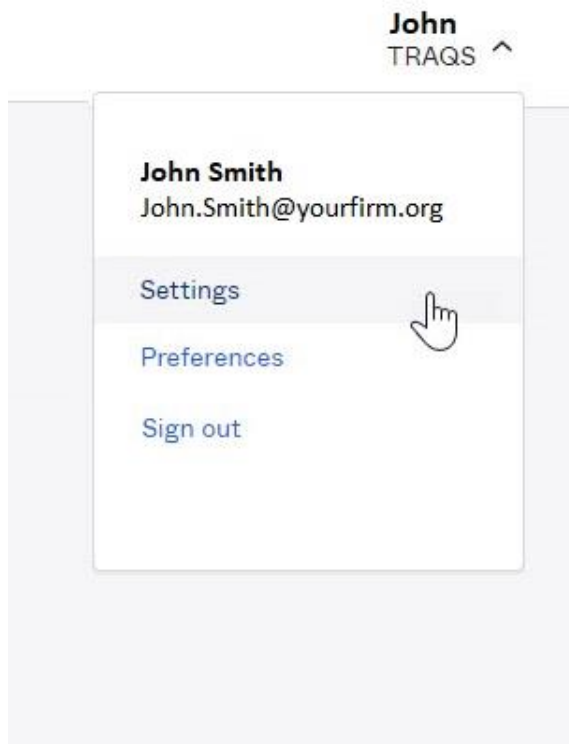
The screenshot displays the FINRA authentication interface. At the top, the FINRA logo is centered. Below it is a circular icon containing a blue telephone handset with signal waves, and a mouse cursor is hovering over it. A dropdown menu is open below this icon, titled "Select an authentication factor". The menu lists two options: "SMS Authentication" with a blue speech bubble icon containing "SMS", and "Voice Call Authentication" with a blue telephone handset icon. Below the dropdown menu is a large blue button labeled "Verify". In the bottom right corner of the interface, there is a "Sign Out" link.

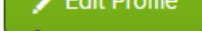
6. Users are able to update the information in the profile screen by clicking the **Edit** button beside the profile item. Note: Change Password and Extra Verification will not have the edit button.
7. Users can not edit the personal information section of this site. If your primary email or phone number need updating please contact **FINRA Market Operations at 1-866-776-0800 option 2** or finraoperations@finra.org.
8. To **Change your Password**: Enter the current password, enter a new password and confirm a new password.
9. To **Change your Security Image**: click the edit button and select a new image.
10. To **Change your Forgotten Password Questions**: click the edit button and select a new question
11. To **Change the Extra Verification(s)**: Click on the Setup or Remove button next to the verification method. Please review the appropriate section of this document for instructions. **Note**: If you see an enabled or disabled button click on the Edit Profile button, then enter your password.
12. To **Change the Display Language** of the profile screen: click on the edit button and select the language you prefer from the drop down.

Note: If you Change the Password, Security Image, Forgotten Password Question, Extra Verification or Display Language, you will receive an email from Okta notifying you of the change.

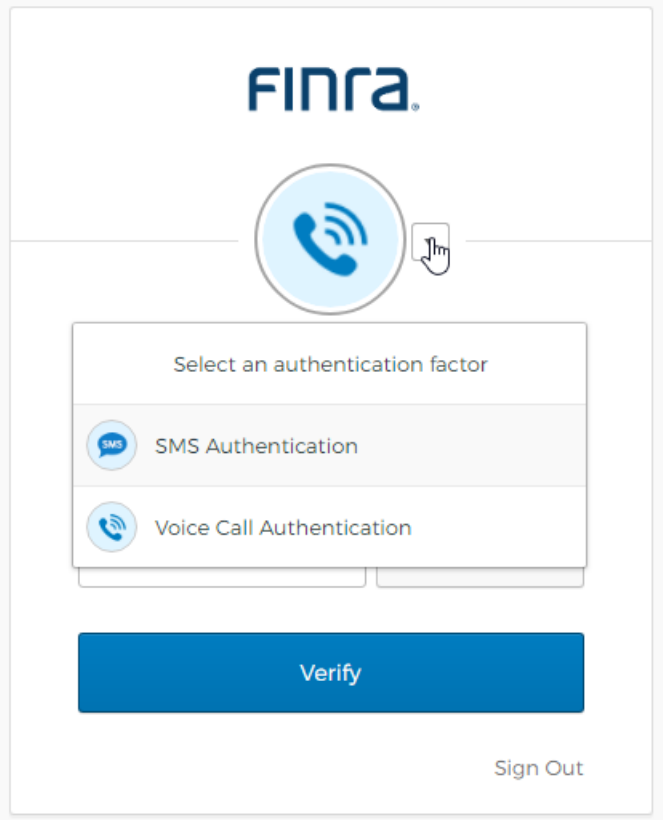
How to Remove My Verification Devices

1. Visit the UAT website <https://mpp-test.nasdaq.com> OR Production website <https://mpp.nasdaq.com>
2. Enter your **Username (email address)** and **password**
3. Click on your **Name** and select **Settings**. This will open the Account page.

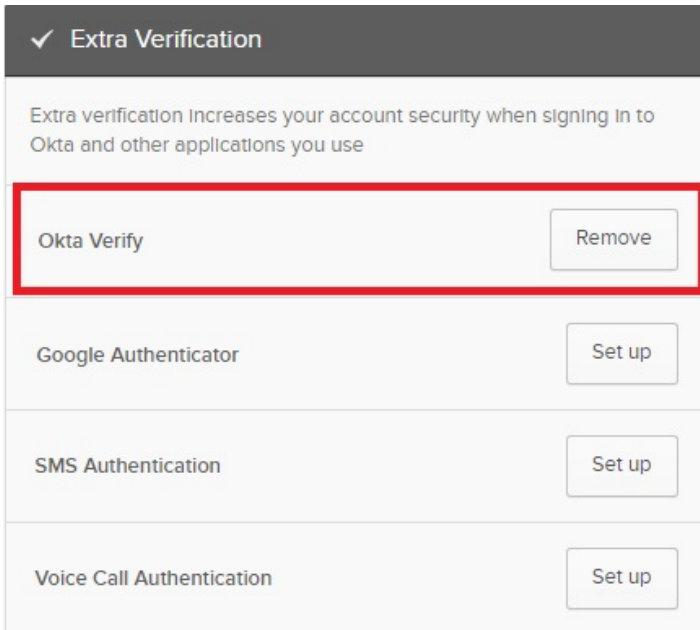


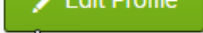
4. Click the **Edit Profile** button , then enter your **Password** if prompted. This will allow you to edit your Account.

5. Authenticate your account using your chosen authentication method(s). Please note, the default authentication method will be the last method you used. Select the method you wish to use from the authentication method drop down. The drop down only contains authentication methods that you have enrolled in. Authenticate your account using your chosen authentication method(s).

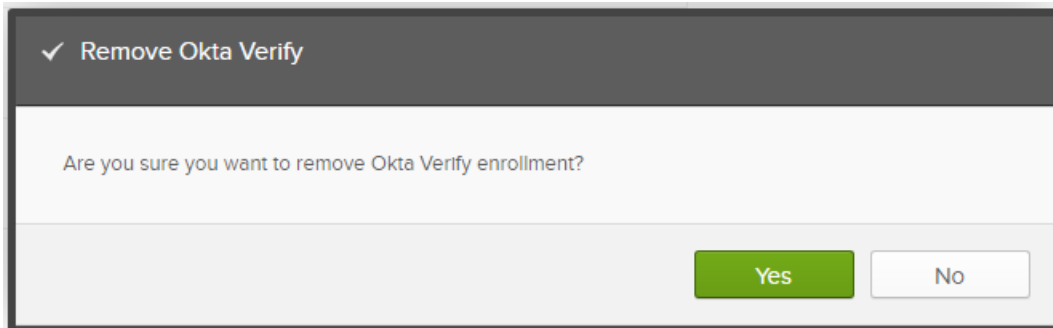


- Under the Extra Verification menu click the **Remove** button beside the authentication method.



Note: If the **Remove** button is inactive click on the Edit Profile button , then enter your **Password**.

- Confirm that you want to remove the authentication method by clicking the **Yes** button



- Once Confirmed you will be directed back to the profile page and the Okta Verify button will now say "Set up".
- If necessary, set up the new device using the steps outlined in [Section 1](#). You will receive an email alerting you that an authentication method has been reset.

This is an automatically generated message from [Okta \[okta.com\]](#). Replies are not monitored or answered.



Hi John,

One or more multi-factor authenticators have been reset for your account
John.smith@yourfirm.org

Details

Okta Verify Push
Wednesday, September 30, 2020 5:57:18 PM UTC
City, State, Country
Performed by: John Smith

Don't recognize this activity?

Your account may have been compromised; we recommend reporting the suspicious activity to your organization.

[Report Suspicious Activity](#)

For further information regarding MFA for TRAQS please click [here](#)

Note: You must have at least one verification method set up in order to access the TRAQS website.

How to Unlock your Account

If you enter your password or authentication credentials inaccurately too many times your account will lock. The account will automatically unlock after 15 minutes.

The user will also receive an **Account Locked** email with instructions for unlocking the account. Please follow the steps below to unlock your account.

1. Click on the **Unlock Account** link in the email

This is an automatically generated message from [Okta \[okta.com\]](mailto:Okta [okta.com]). Replies are not monitored or answered.



TRAQS - Account Locked

Hi John,

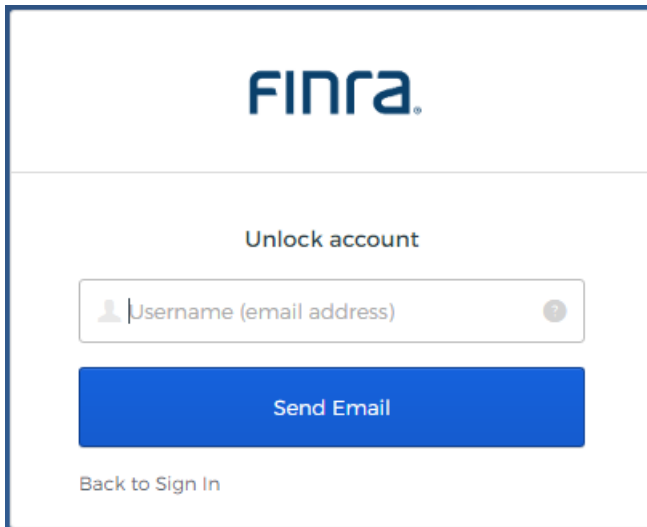
Your Okta account for FINRA TRAQS has been locked due to too many failed login attempts. If you did not make this request please click [here](#). Someone could be trying to access your account.

To reset your Okta account, it may be possible to use the link below:

[Unlock Account](#)

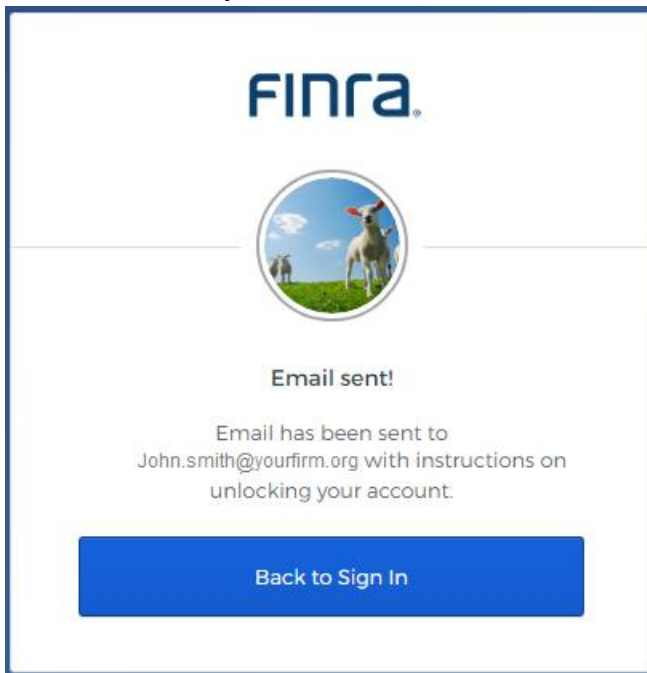
For further information regarding MFA for TRAQS please click [here](#)

2. Enter your **Email Address** and click **Send Email**



The screenshot shows the FINra 'Unlock account' page. At the top is the FINra logo. Below it is the heading 'Unlock account'. There is a text input field with a person icon and the placeholder text 'Username (email address)'. To the right of the input field is a question mark icon. Below the input field is a blue button labeled 'Send Email'. At the bottom left of the page is a link labeled 'Back to Sign In'.

3. An **Unlocked Requested** email will be sent to have you verify your account



4. Click on the **Unlock Account** link in the email

This is an automatically generated message from [Okta \[okta.com\]](mailto:Okta [okta.com]). Replies are not monitored or answered.



FINRA TRAQS - Account Unlock Requested

Hi John,

An account unlock request was made for your Okta account for FINRA TRAQS access. If you did not make this request, please click [here](#). Someone could be trying to access your account.

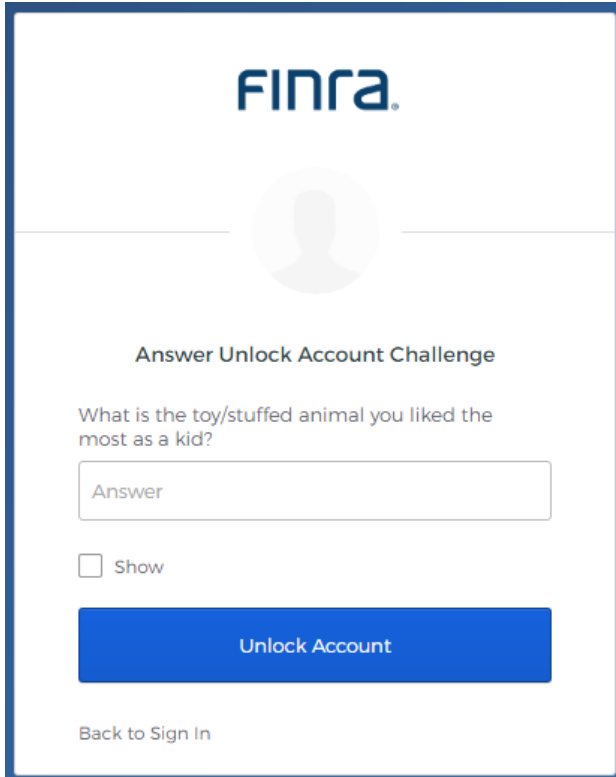
Click the link below to unlock the Account for your Username, John.smith@yourfirm.org



This link expires in 8 hours.

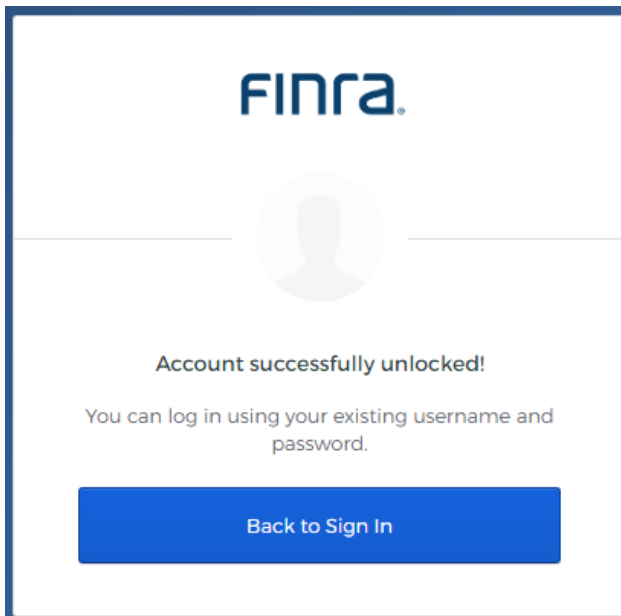
For further information regarding MFA for TRAQS please click [here](#)

5. Answer the **Unlock Account Challenge question** and click the **Unlock Account** button



The screenshot shows the FINRA account unlock challenge interface. At the top is the FINRA logo. Below it is a placeholder for a user profile picture. The main heading is "Answer Unlock Account Challenge". The challenge question is "What is the toy/stuffed animal you liked the most as a kid?". There is a text input field labeled "Answer". Below the input field is a checkbox labeled "Show". At the bottom of the challenge area is a blue button labeled "Unlock Account". At the very bottom of the screen is a link labeled "Back to Sign In".

6. If successful you can click on the **Back to Sign In** button



The screenshot shows the FINRA account successfully unlocked confirmation screen. At the top is the FINRA logo. Below it is a placeholder for a user profile picture. The main heading is "Account successfully unlocked!". Below the heading is the text "You can log in using your existing username and password.". At the bottom of the screen is a blue button labeled "Back to Sign In".

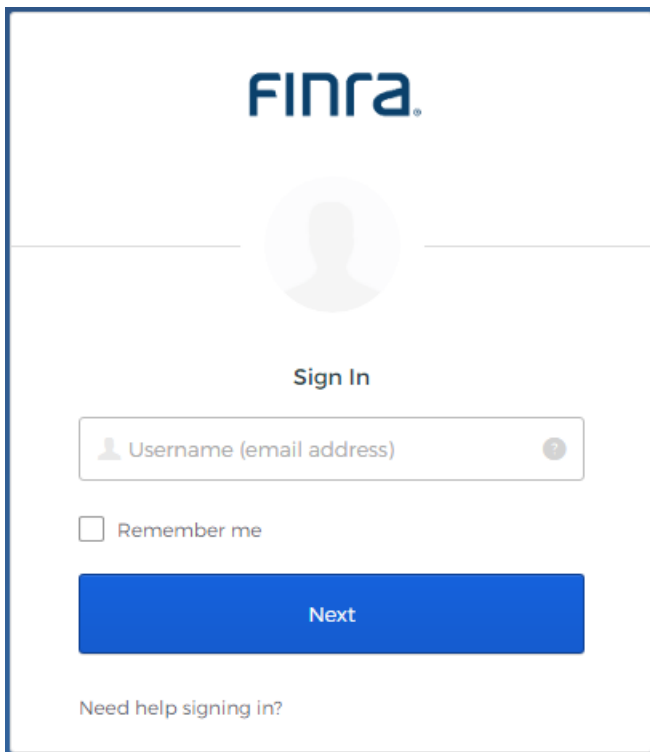
Note: Your account automatically unlocks after 15 minutes. If you don't act on the unlock email within 15 minutes your account will automatically unlock.

Section 3: How to Login to the TRAQS Website Using MFA

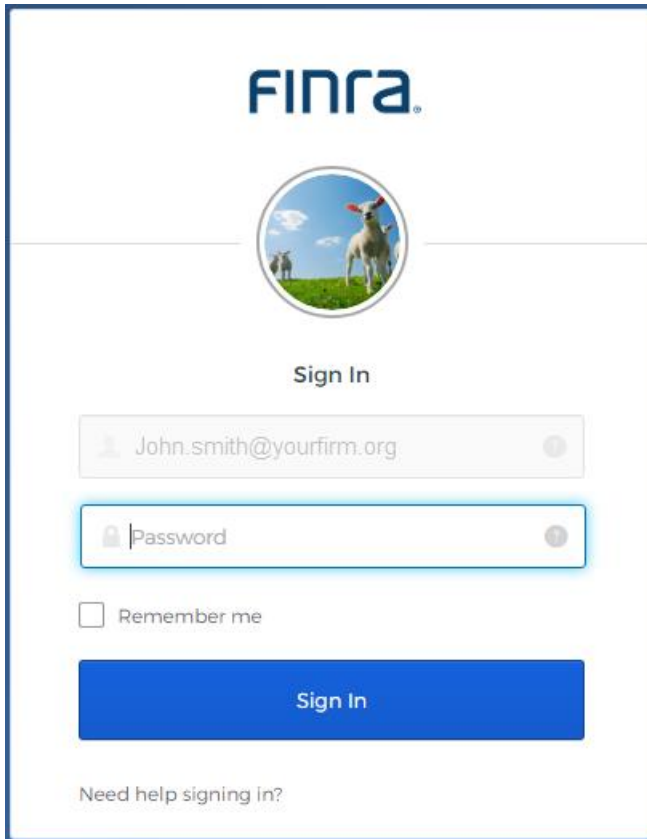
1. Enter the TRAQS URL in your browser **OR** from the Main Page (Home page) click on the TRAQS website icon in your Profile page. **Note:** If you access TRAQS thru the profile page you will not have to enter your factor again.



2. Enter your **Username (email address)** and click **Next**. Click the **Remember me checkbox** to save your Username for the next time you sign in.

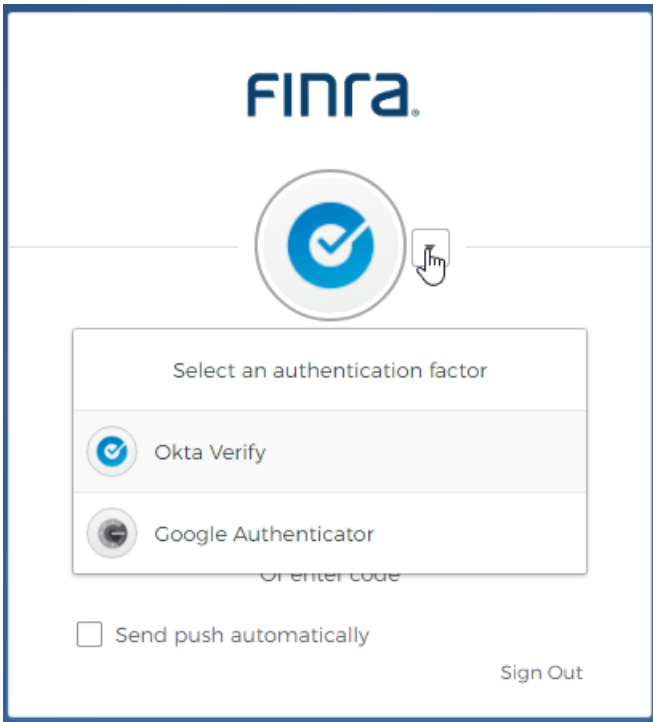
A screenshot of the FINra Sign In page. At the top center is the 'FINra' logo. Below the logo is a circular placeholder for a user profile picture. Underneath the picture is the text 'Sign In'. Below that is a text input field with a person icon on the left and a question mark icon on the right, containing the placeholder text 'Username (email address)'. Below the input field is a checkbox labeled 'Remember me'. Below the checkbox is a large blue button with the text 'Next'. At the bottom left of the page is the text 'Need help signing in?'.

3. Enter your **Password** and click **Sign In**.

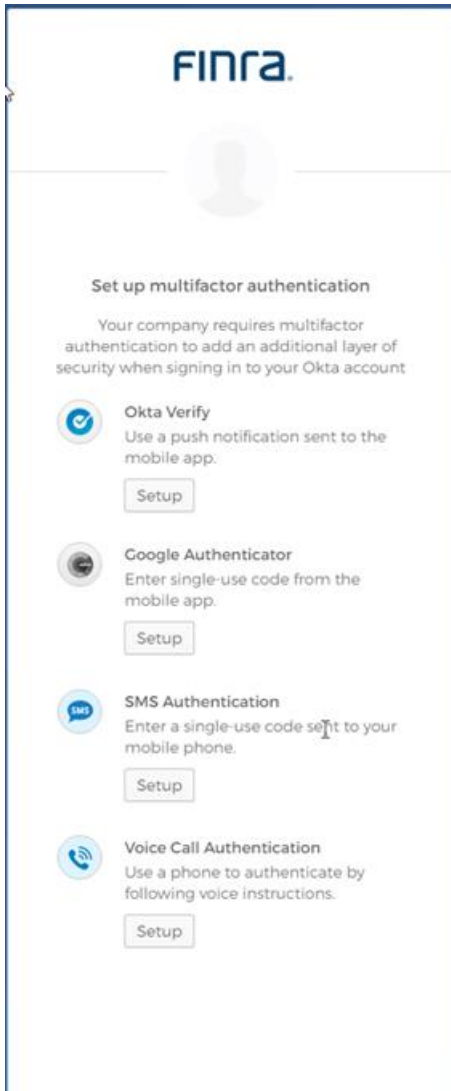


The screenshot shows the FINra sign-in interface. At the top is the FINra logo. Below it is a circular profile picture of a cow. Underneath the picture is the text "Sign In". There are two input fields: the first contains the email "John.smith@yourfirm.org" and the second is labeled "Password". Below the password field is a checkbox labeled "Remember me". A large blue "Sign In" button is positioned below the checkbox. At the bottom left, there is a link that says "Need help signing in?".

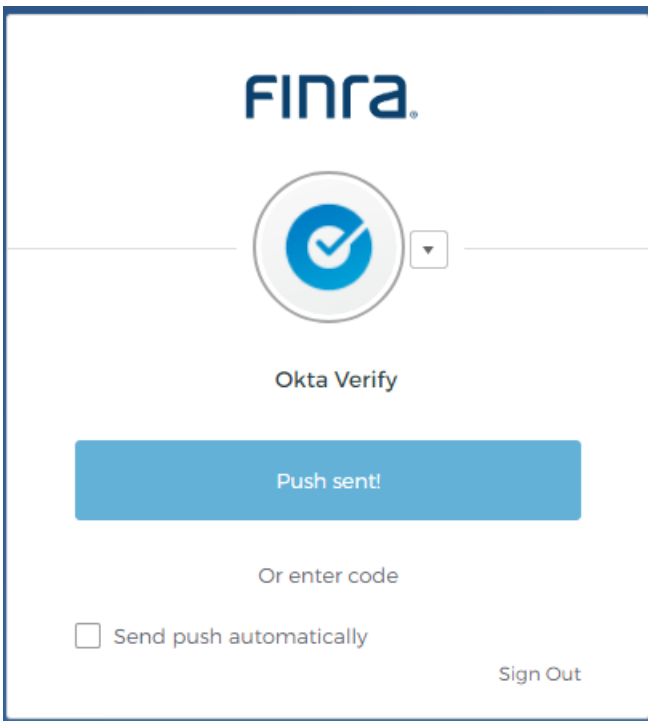
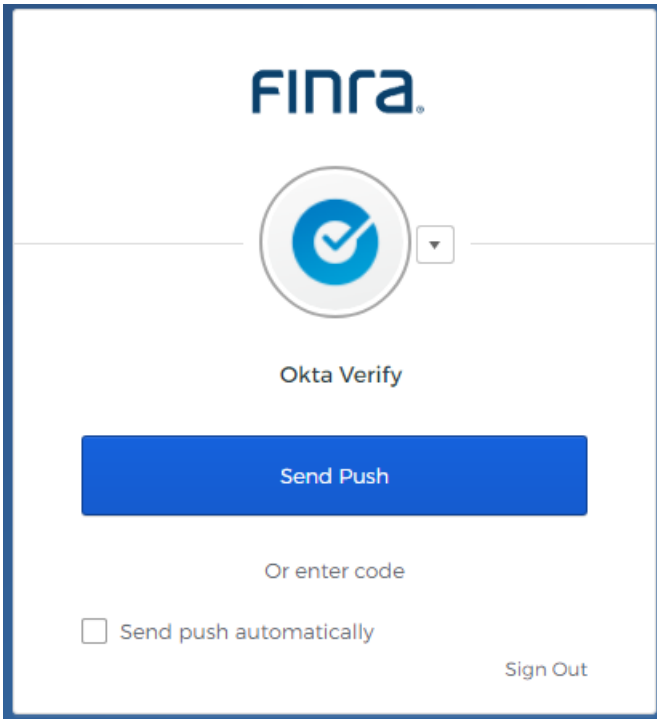
4. Select the desired authentication method by clicking the **Drop-Down Arrow**. The drop down will contain every authentication method you are enrolled in. **Note:** In the following example we are using Okta Verify.



4a. If you did not set up an Authentication Method your screen will look like this. Set up an Authentication. Complete the steps outlined in [Section 1](#) of this document to set up a new authentication method.

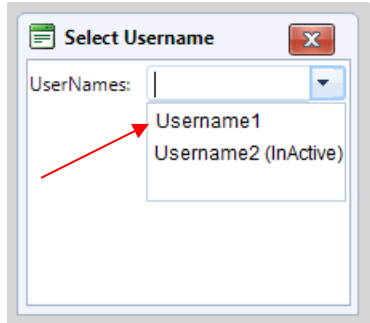


5. Verify the account using the desired Authentication method. The users can click **Send Push** or **Enter Code** button to verify their account. **Note:** If users would like an automatic push notification, please select the **Send Push Automatically** check box.



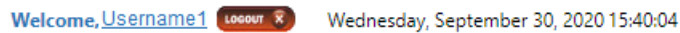
6. Users will next be directed into the TRAQS website, if a user has only one username associated with their Username (email address).

7. If a user has multiple usernames associated with their Login (email address) there will be several available options in the drop-down list of usernames. Choose the **Username** you want to use and click the **Select** button

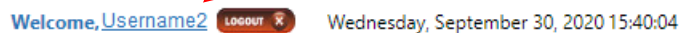
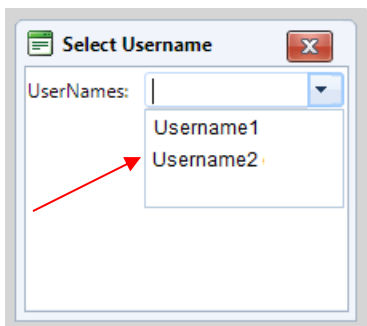


Note: If your username in the drop down above has “InActive” beside it. Please call Market Operations at 1-866-776-0800 option 2 prior to logging in.

8. You will now be using the credentials from the username you selected
9. To switch to different Username. Click the **Username** link found at the top right corner of TRAQS screen.



Popup screen will come up, select a **Different Username**, click the **Select** button and you will see the username change.



Section 4: How to Access the API Download

At this time API is not being transitioned to MFA. Users will continue to access API files using existing NWSF certificates and passwords. Please review the API specification doc for the trade reporting product for directions to access the API.

TRACE Fixed Income - <https://www.finra.org/filing-reporting/trace/documentation>

ADF - <https://www.finra.org/filing-reporting/alternative-display-facility-adf>

ORF - <https://www.finra.org/filing-reporting/orf/orf-forms-and-documentation>

Note: During the NTF Beta and Production Parallel period users are encouraged to use their NWSF certificate and password to access the API via NTF download-ntf2.finratraqs.org OR Production Parallel download2.finratraqs.org. For more guidance please see the API user guide for the product.

Section 5: Common Questions

Why is FINRA implementing Multi Factor Authentication (MFA) for TRAQS?

Passwords are increasingly easy to compromise. Passwords can often be stolen, guessed or hacked; often without the user knowing. MFA adds a second layer of security by helping the account stay secure even if the password is compromised.

Is enrollment in MFA mandatory?

Yes, users are required to enroll in MFA to access the FINRA TRAQS website for trade reporting. Any user that attempts to login to the TRAQS website without enrolling in MFA will be prompted to enroll in MFA.

My SAA ~~requested a new completed an order form to add a~~ TRAQS Username for me, I haven't received an enrollment email. How do I get a new email?

If you need a new enrollment email please contact finraoperations@finra.org or 1-866-776-0800 option 2.

Does the enrollment email expire?

Yes. Users have 30 days from the date the email was sent to take action to set up the Okta account for TRAQS access Username (email address). If your enrollment email expired, please contact FINRA Operations at 1-866-776-0800 option 2 or finraoperations@finra.org.

What do I do if I lost my mobile device?

It is strongly recommended that you remove the lost device from your MFA settings. Enter the Okta profile screen and remove the authentication method associated with the device. Please see [Section 2](#) for instructions.

Why do I have 2 Okta verify or 2 Google Authentication accounts?

The NTF (UAT) and production environment for MPP are separate. The account <https://mpp-test.nasdaq.com> is associated with NTF (UAT) access. The account <https://mpp.nasdaq.com> is associated with production access.

How can I edit my personal profile data?

Your profile data can be edited at any time. Please see [Section 2](#) for instructions. Please note, the personal information section of the user profile cannot be edited. Please have your SAA contact FINRA Operations at 1-866-776-0800 option 2 or finraoperations@finra.org to update this data.

Can I set up a push notification when using Okta Verify?

Yes, users can select the "send push automatically" at any time after enrolling in Okta verify. Be sure to turn on notifications, on your device. Your device will receive a notification asking to approve the login. Once you select approve you will be directed to the TRAQS website as normal.

Why did I receive two MFA enrollment emails from Okta?

You likely received two enrollment emails because you are set up to access TRAQS in both the production and test environment. Although your Username may be the same for both environments they require two separate enrollments. Please follow the [How to Enroll and Choose Authentication Method](#) instructions above for each environment.

I've forgotten my password or entered my authentication method inaccurately a few times and locked my account. How can I unlock it?

Your account will automatically unlock after 15 minutes. There are two ways to unlock your account.

1. You will receive an email notifying you that your account is locked. Follow the instructions in the email to unlock your account.
2. Click the "Need Help signing in" link at the bottom of the TRAQS Sign In screen. Select the "Forgot password" or "Unlock account" option. Enter your email address in the provided box to generate a reset email. Click on the Reset Password or Unlock Account link in the email within the 8-hour expiration and answer your forgotten password questions.

If you do not know the answers to any of your forgotten password options, need assistance with unlocking your account or any other password issues, you may call NASDAQ tech support at 212-231-5180 option 4.

Why am I also receiving an email for a TRAQS certificate if I have enrolled in MFA?

During the transition period from January until April users will receive an email for MFA enrollment and a TRAQS NWSF certificate. Users who have access to API will use the NWSF certificate and password to access API files. Only users with API privileges will be able to access the API files using the TRAQS certificate.

What is the Okta profile link to the test environment?

Users can enroll, edit their profile and log into TRAQS in the test environment using the following link <https://mpp-test.nasdaq.com>

What is the Okta profile link to the production environment?

Users can enroll, edit their profile and log into TRAQS in the production environment using the following link <https://mpp.nasdaq.com>

Report Suspicious Activity

To report unrecognized activity from an account activity email notification. Contact FINRA Operations at 1-866-776-0800 option 2 or finraoperations@finra.org.

Okta Account Token Expiration Error

If your Account Activation Token is no longer valid. Contact FINRA Operations at 1-866-776-0800 option 2 or finraoperations@finra.org.

Need Help?

If you need assistance using Multi Factor Authentication for TRAQS, contact the FINRA Market Operations at 1-866-776-0800 option 2.

Section 6: Revision History

Date	Version	Changes
11/12/2020	1.0	Initial Version
02/16/2021	1.1	Updated document to include information relevant for production release. Updates are as follows: <ul style="list-style-type: none">• Section 2: Profile Page - Included links to the production site• Section 4: How to Access the API Download - Included production parallel• Section 5: Common Questions - Included common questions regarding MFA production migration
<u>01/31/2022</u>	<u>1.2</u>	<u>Updated document with PDM (Participant Data Management System)</u>