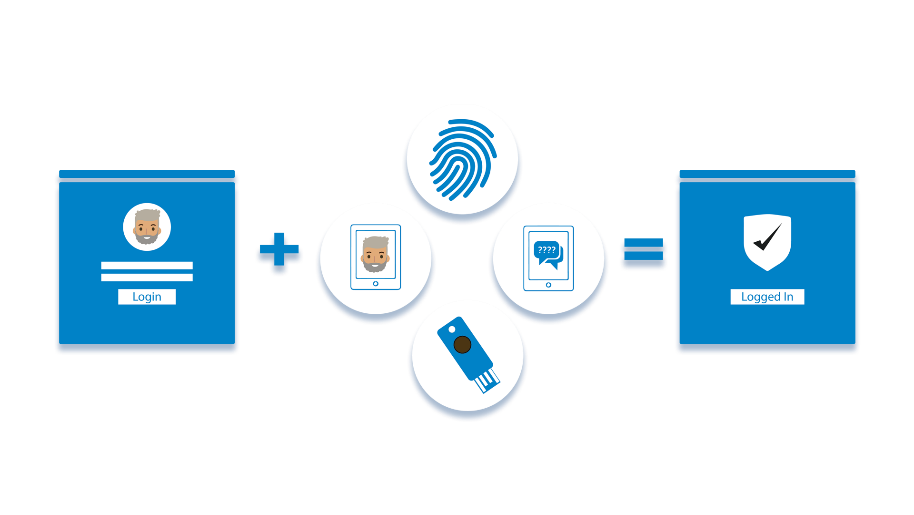
# Introduction to MFA (Multi-Factor Authentication)

As an organization, we’re always striving to stay ahead of the curve with our security and IT practices. Today, I’m excited to announce that we’re going to introduce Okta MFA, short for Multi-Factor Authentication, to strengthen our approach to security.

The key to a secure login is MFA. It adds an extra layer of security by asking for ‘something else’ alongside your username and password—and that ‘something else’ is called a factor.



A factor can be anything from a push notification sent via a smartphone app to a biometric scan of your iris. Hackers might steal your password from halfway around the world, but they can’t get at your fingerprint or your smartphone as easily.

* When IT enables MFA for your account you must select and enroll in at least 1 of the following options, but we recommend at least 2.
  + If you have a company managed phone, #1 and #2 are best, with either #3 or #4 as a backup plan if phone gets lost, stolen, or broken
  + If you don’t have a company phone, #3 and #4 are no cost, and a mobile device isn’t necessary.
  + Personal phone use is OK with all options, too, but not required as it could incur data costs.

**Option 1. Okta Verify** (a free authenticator app for a COMPANY mobile device that allows you to click “**Yes**, I just logged in”, or “**No** this is not me”, **or to generate a unique 6-digit code every 30 seconds** you can use if you can’t receive a network signal). This is the best method for McCarthy partners with a smartphone, works on WIFI or Cellular data and is quick and easy for most situations. *NOTE:* *Only one mobile device is supported for security reasons.*

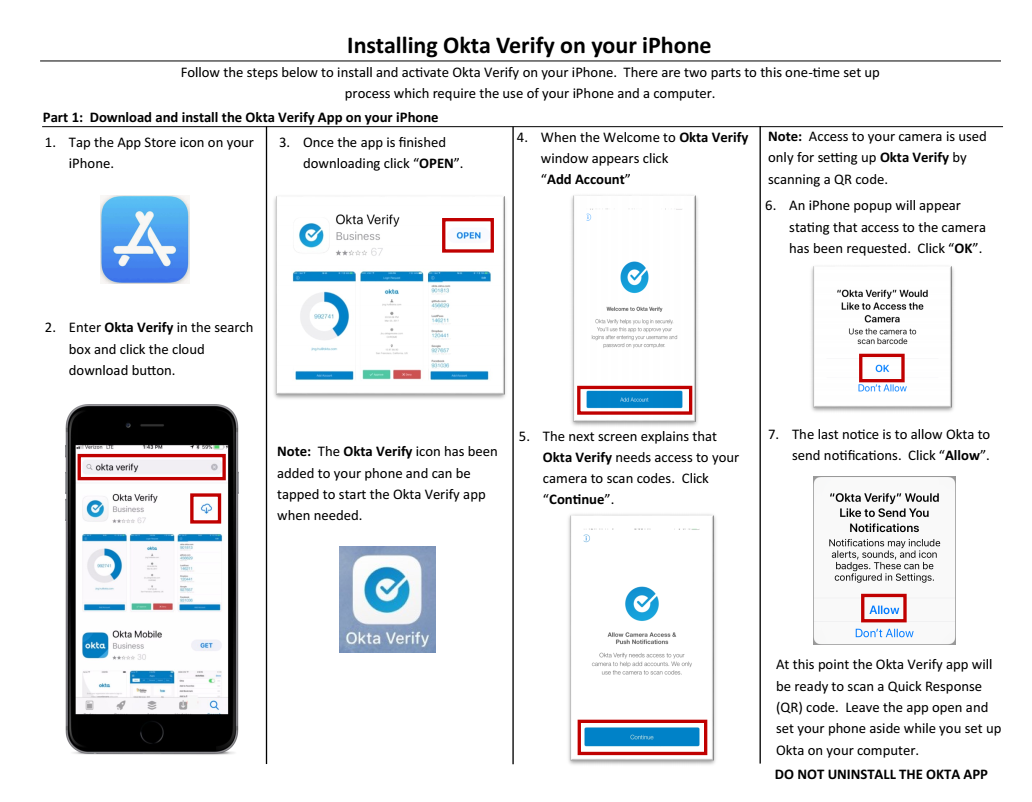
**Option 2. SMS Authentication** is a less secure, but common method that sends a one-time code to your cell as a text message. You enter the code into the PC screen to authenticate. It depends on a good cell signal and carrier service with your phone’s text service.

**Option 3. Voice Call Authentication** is an alternate that we recommend everyone setup in case the first two options are or become unavailable. This will call your designated phone number and speak the one-time code to enter (we recommend using a direct dial phone line like a desk phone if available).

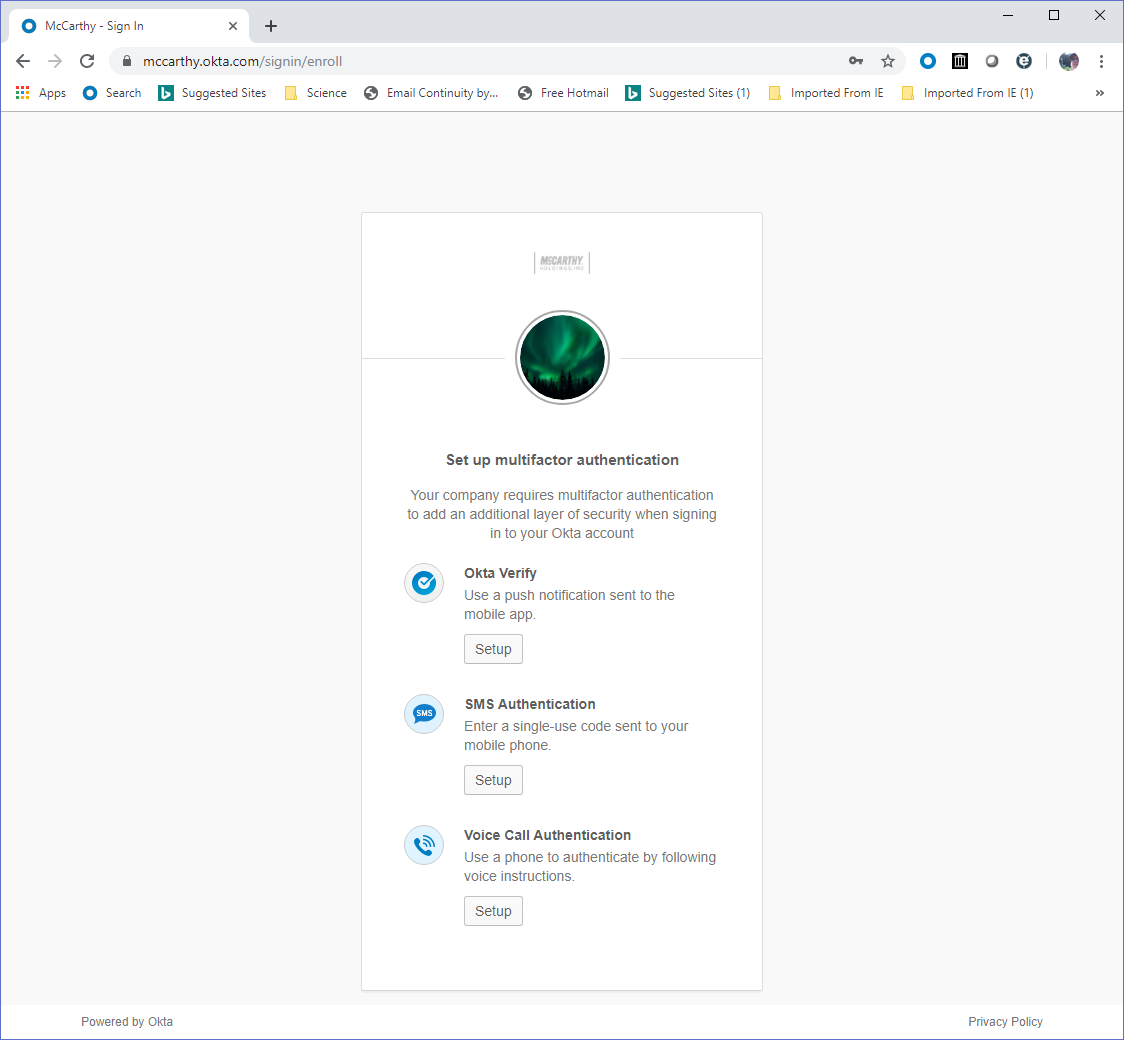
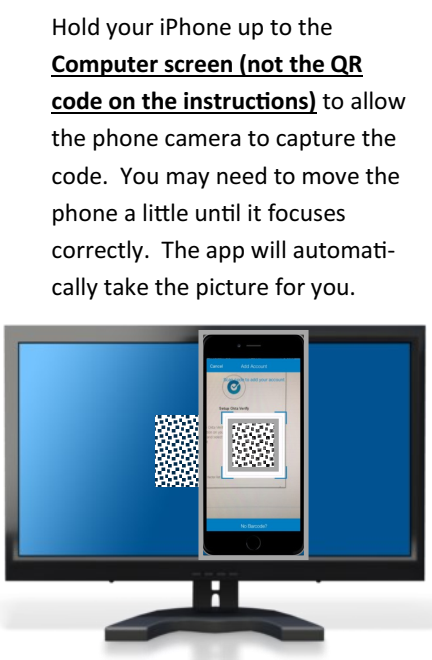
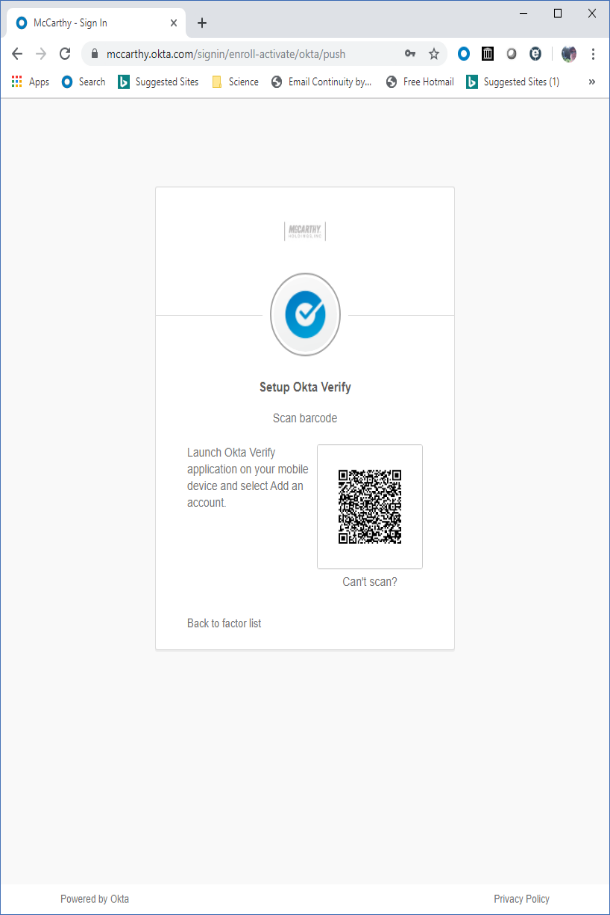
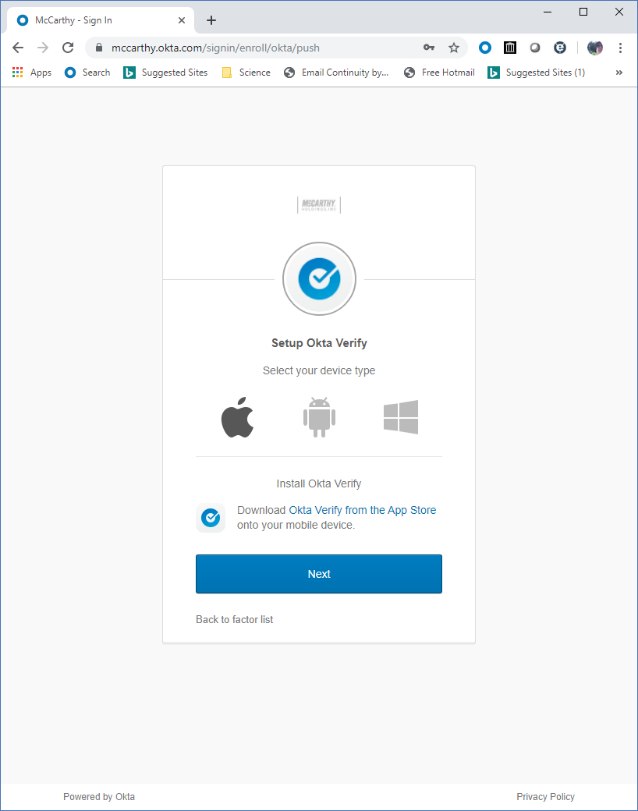
**Option 4. Security Question** is weak, but easy to deploy and no other device required, where users must enter the correct response to a security question that they select from a list.  
  
**McCarthy IT may add or modify available factors in the future to stay on top of best practices and adapt to the security needs of the company.**

**McCarthy Multifactor Authentication Quick Start Guide**

Option 1-1. Install Okta Verify App on your Company Smart phone ahead of time (**BEST METHOD**)



Option 1-2. When IT enables MFA and you are prompted, Use Okta Verify (Must be completed within 5 min.)

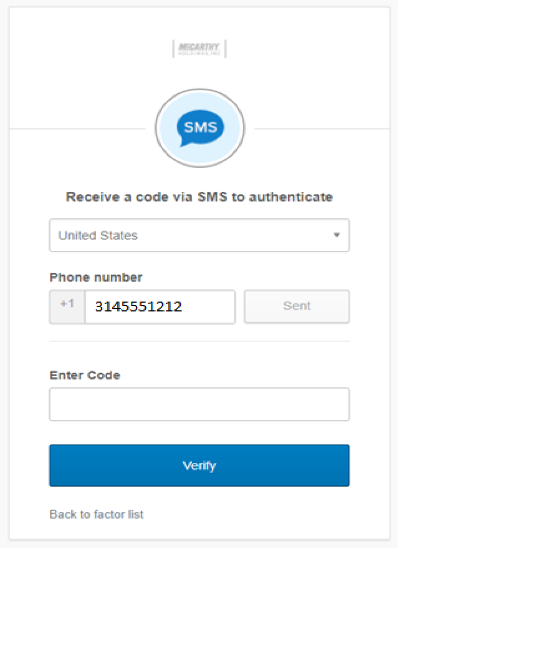
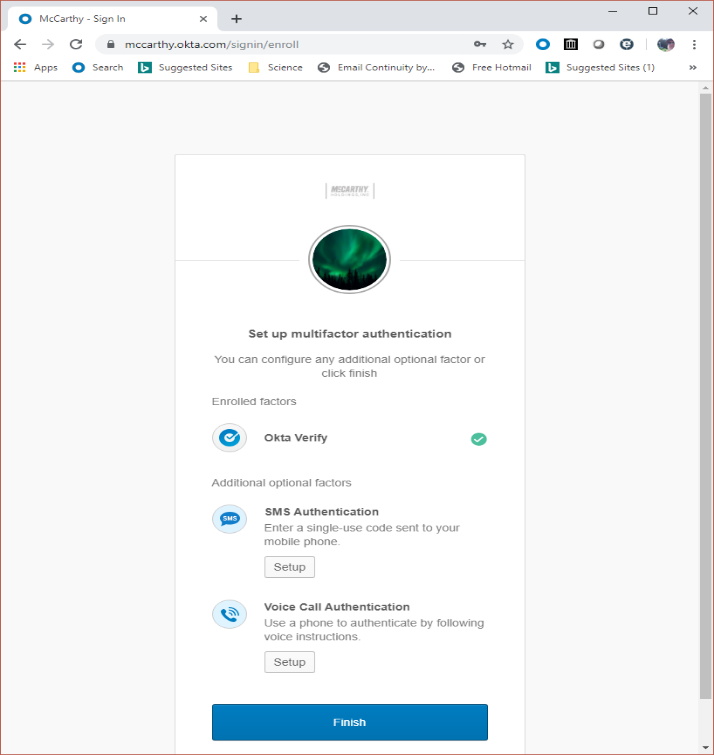
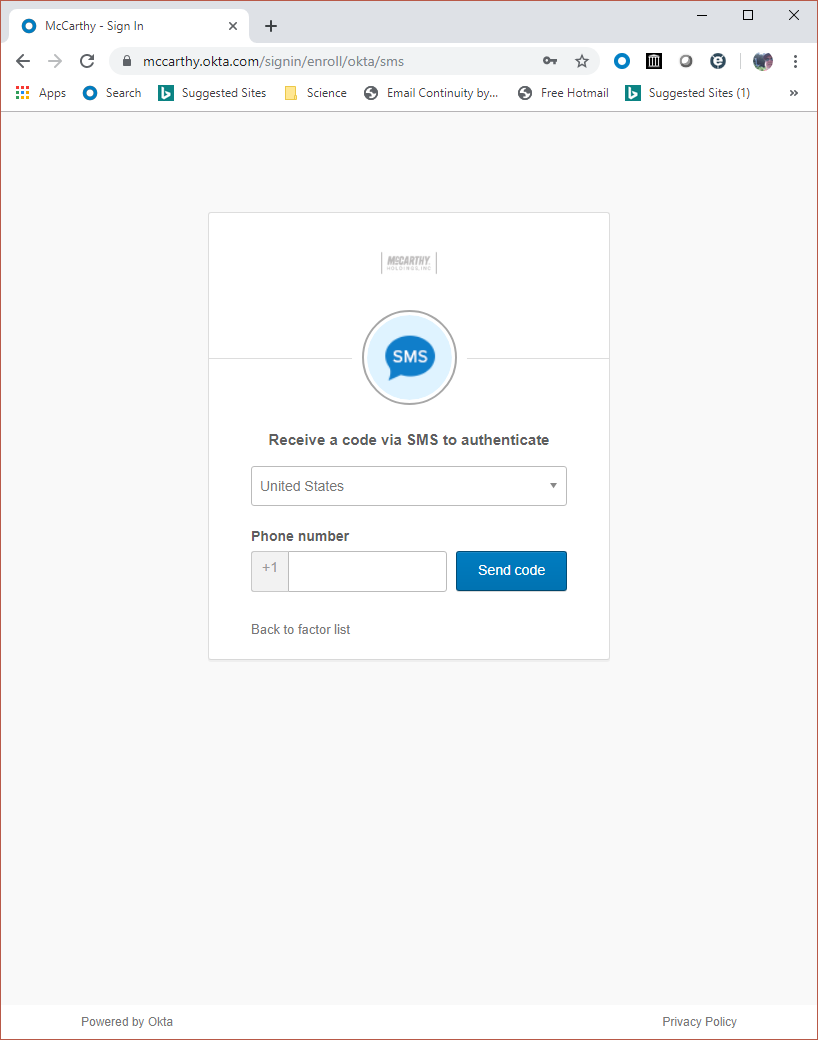
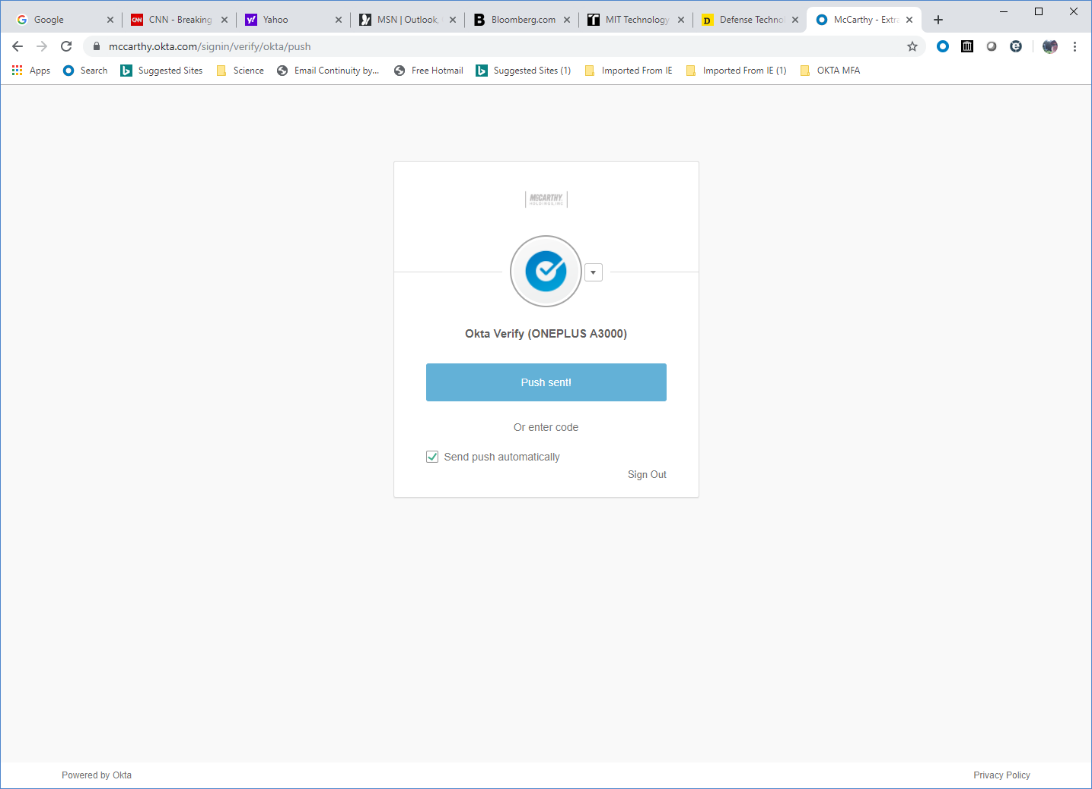
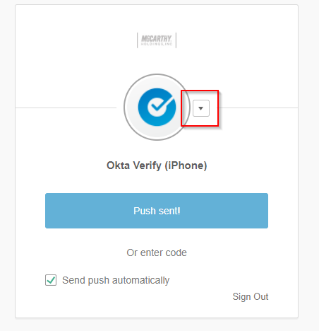
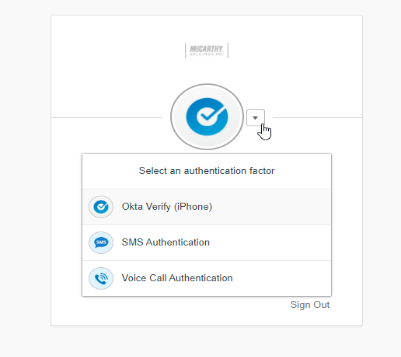


2c. Open OKTA Verify app on your Mobile Device, select Add and scan the unique QR Code that appears on **YOUR SETUP** screen 🡪

2b. Select your mobile device type, **Apple or Android**

**How to use OKTA Verify when prompted for second factor**

2a. Click Setup under Okta Verify

Option 2. Setup SMS Authentication on text capable smart phone.

2. Use Drop-down arrow to change to another factor if OKTA verify isn’t available.

3. Switch to alternate method you’ve setup if needed.

1. If auto push is not selected, then Push manually and answer Yes on your mobile. Or click enter code and use 30 second code shown by OKTA Verify on your mobile.

**3c**. Once the screen shows Sent, you should receive a text message to your mobile. This is valid for about 5 minutes.

Example: Your McCarthy verification code is 123456.

Enter the verification code you just received into the Enter Code box and press Verify.

3b. Type your mobile phone number with area code &

Press Send code

3a. Click Setup under SMS Authentication

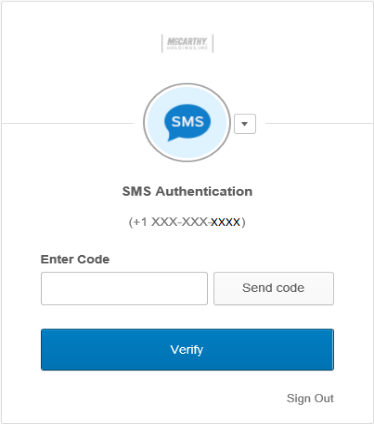
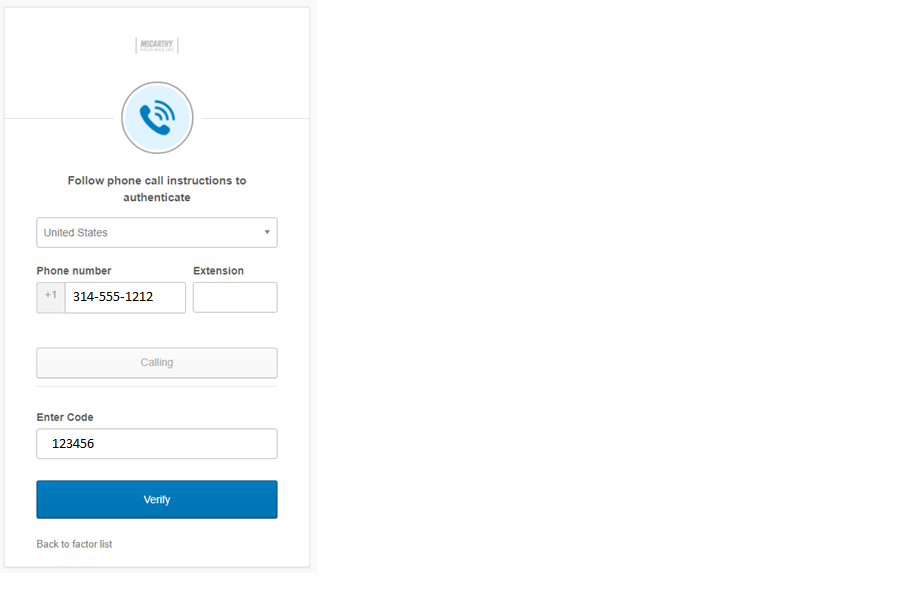
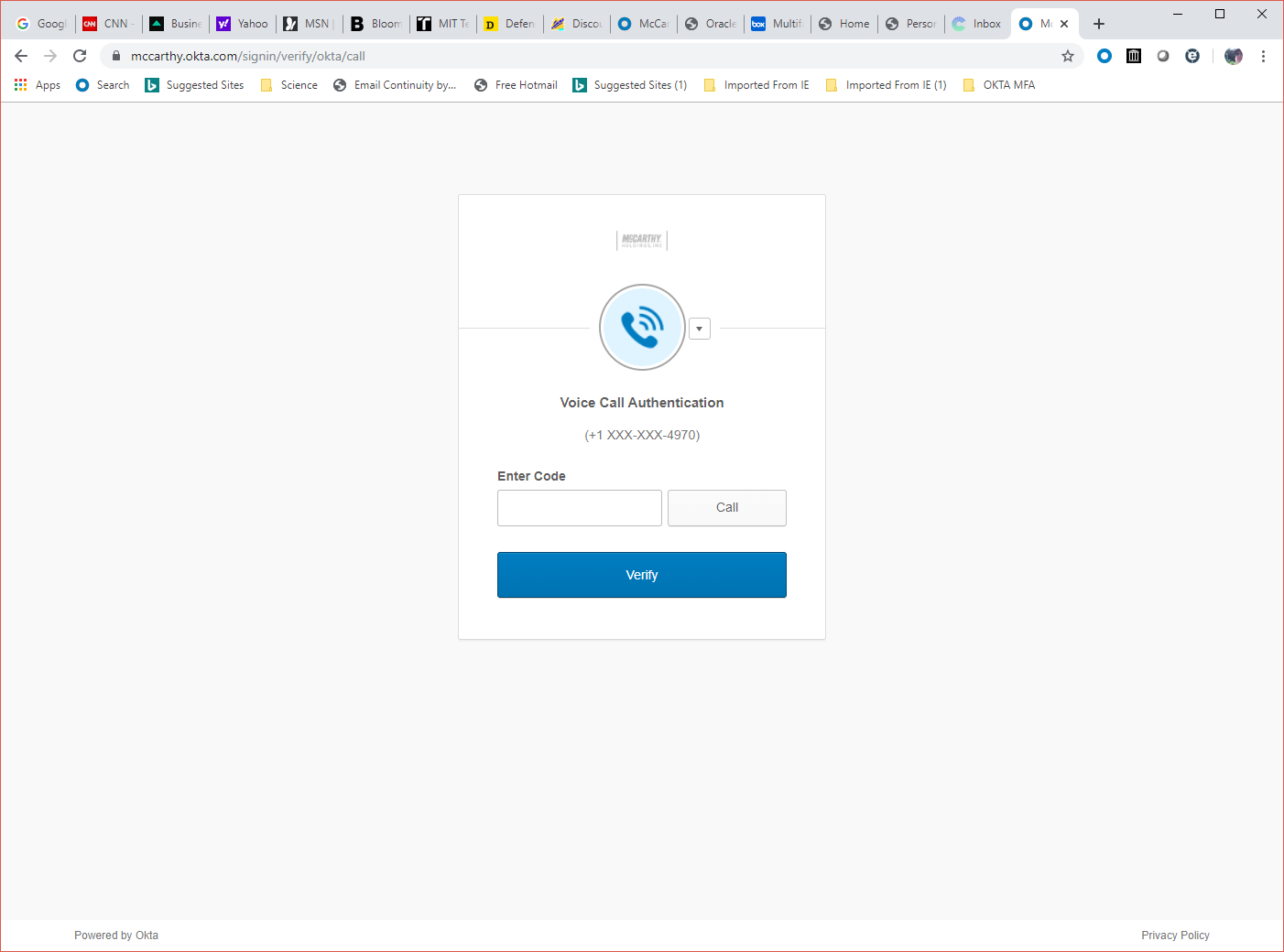
Once the screen shows Sent, you should receive a text message to your mobile. This is valid for about 5 minutes.

Example: Your McCarthy verification code is 123456.

Enter the verification code you just received into the Enter Code box and press Verify.

**How to use SMS Authentication**

**when prompted for second factor**

Option 3. Setup Voice Call Authentication on desk phone or alternate cell if available, else use what you have

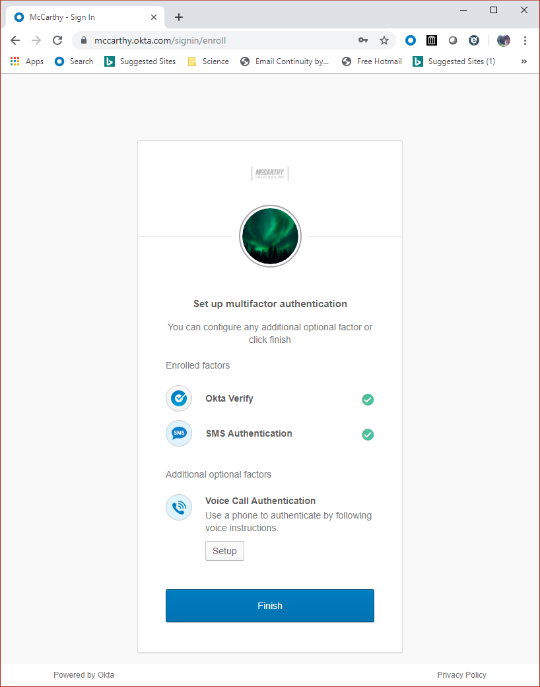
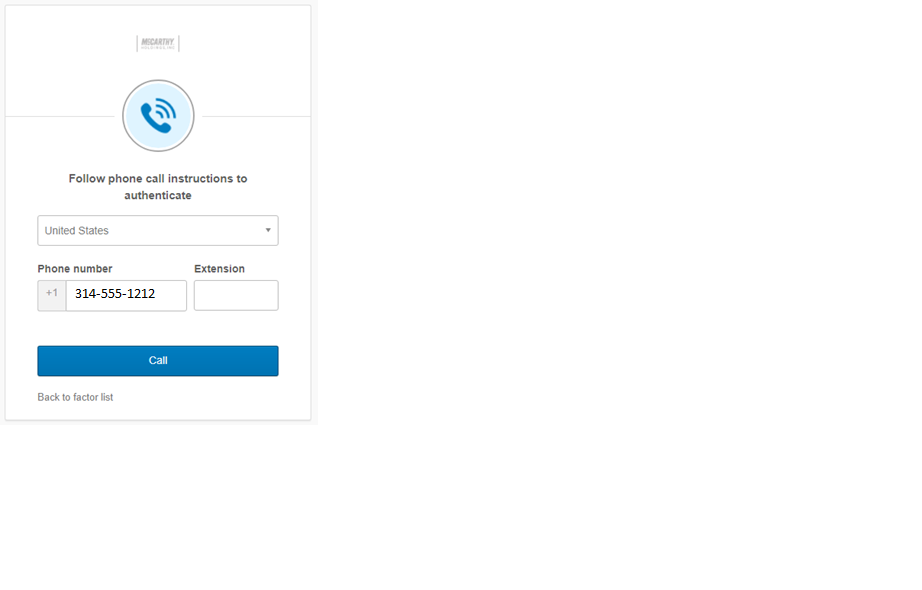
When you get this screen, Press Send Code

Your unique one-time code will be sent to your phone via Text message

Enter the verification code you just received into the Enter Code box and press Verify

**How to use Voice Call Authentication**

**when prompted for second factor (Below)**



4b. Type your DIRECT phone number & Click Call

Press Call

*Calling is displayed in place of Call button, followed by a phone call to the number you have designated for Voice Call Authentication.*

Answer the phone call to hear the code you need.

Enter the provided code into the **Enter Code** box and press Verify.

*NOTE: If you don’t hear the call, you are offered a redial button. Your incoming call may drop into voicemail, and you can retrieve it there if within 5 minutes.*

***4c****. A “Call is in progress…” message appears, followed by a phone call to the number you just entered.*

Answer the phone call to hear the code you need. Enter the provided code into the **Enter Code** box.

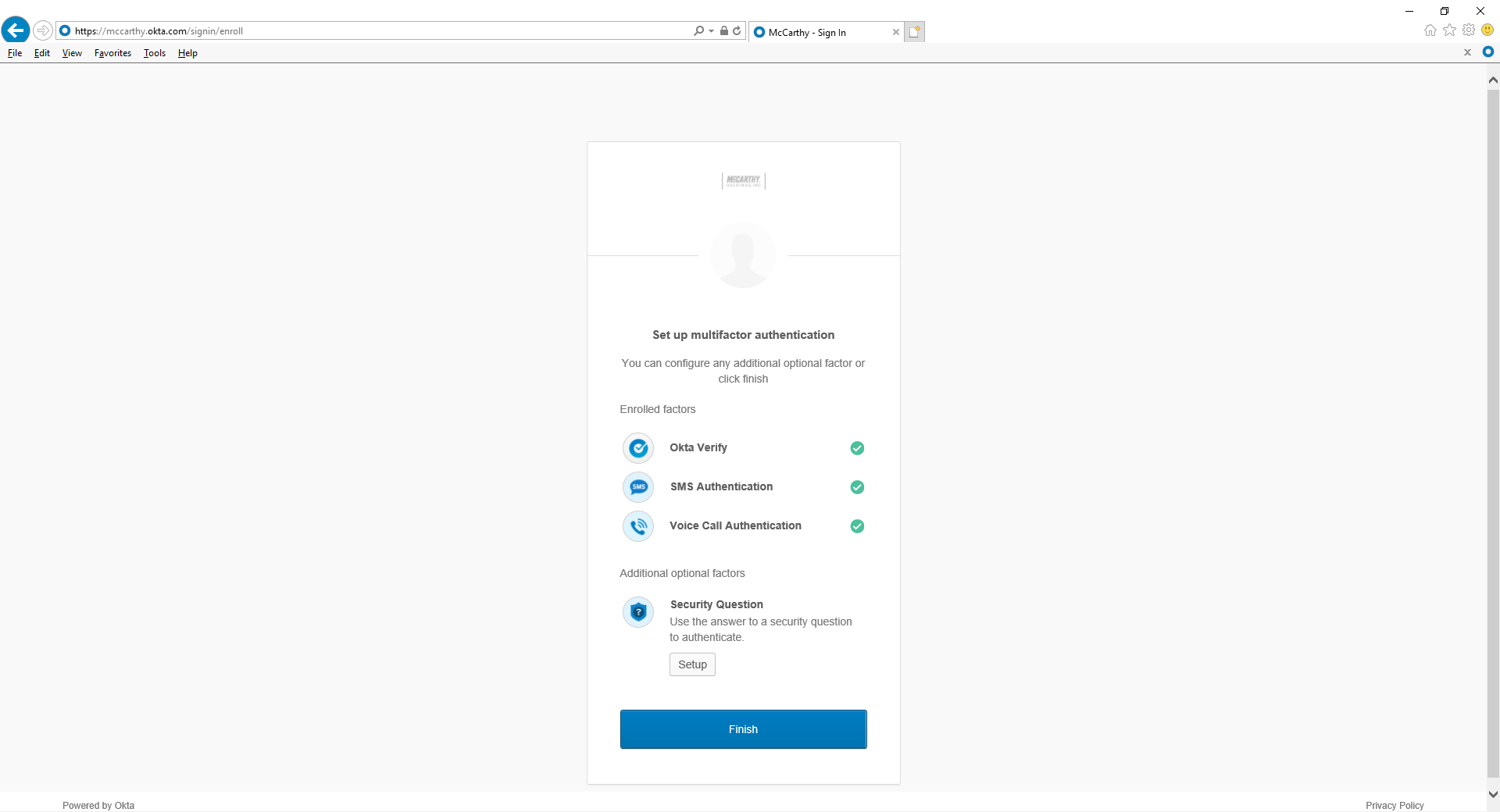
Click the **Verify** button, then **Done to complete setup.**

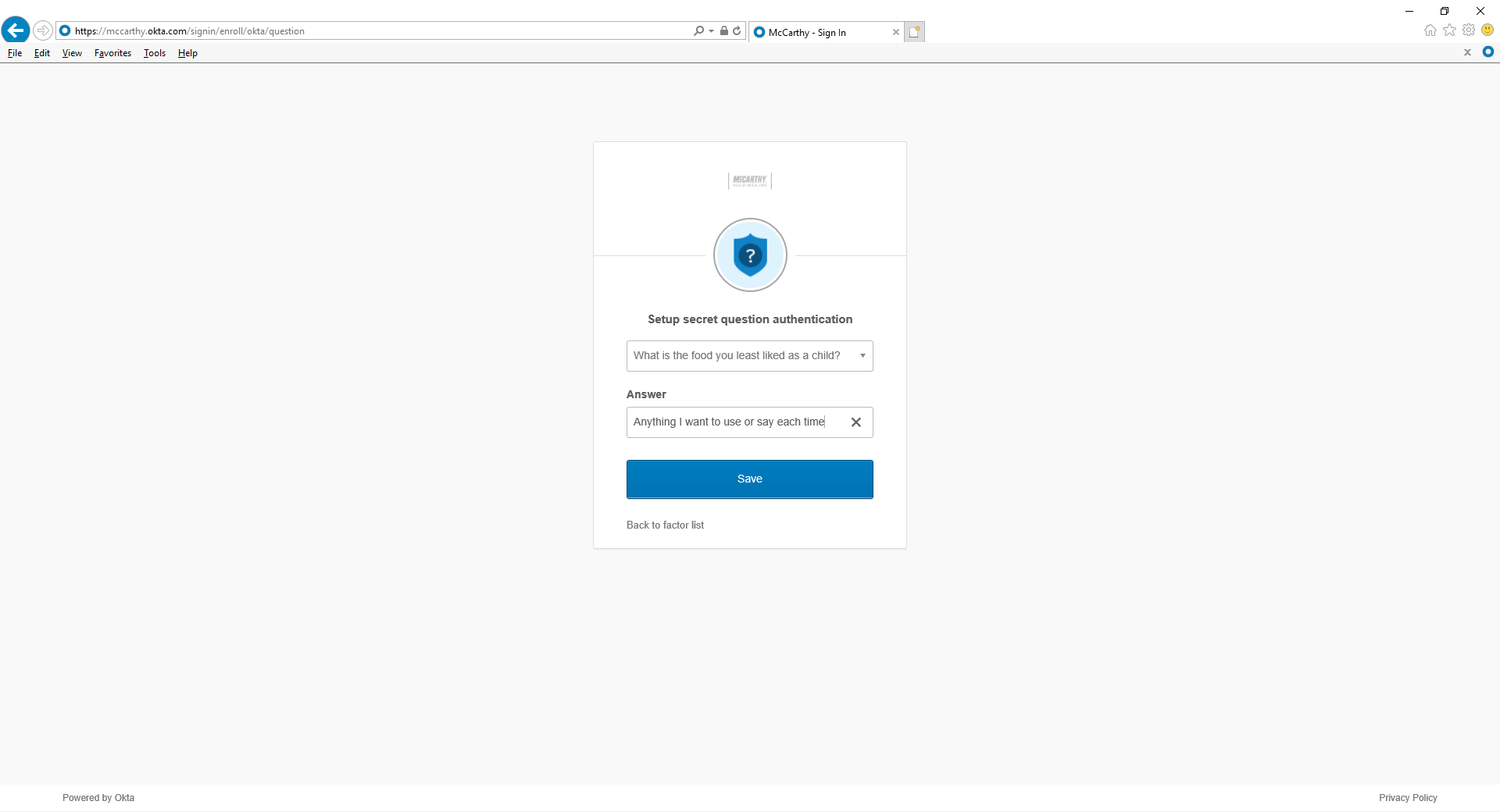
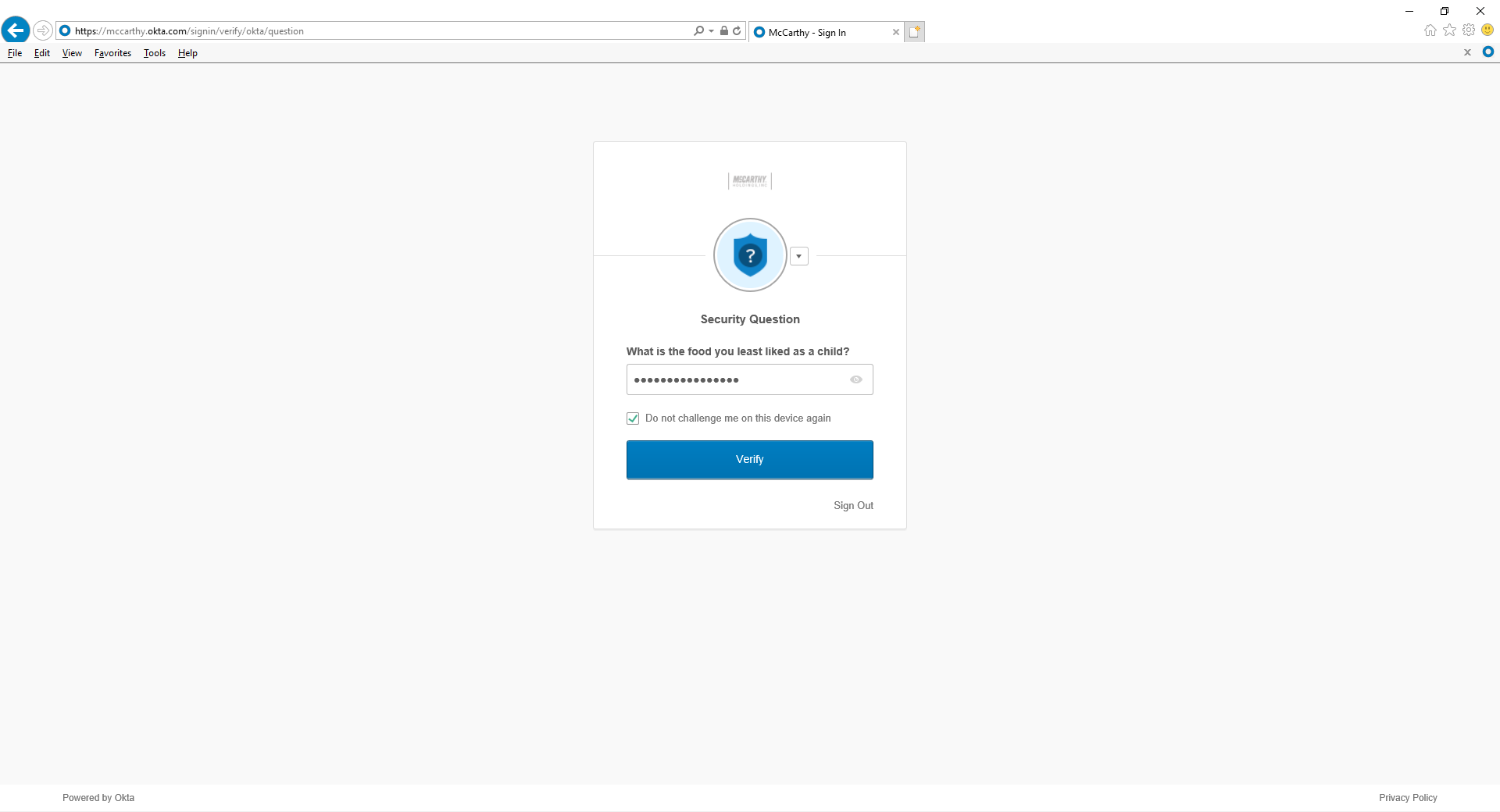
4a. Click Setup under Voice Call Authentication

Option 4. Setup Security Question, useful if you don’t have a company provided mobile device or direct dial desk.

Security questions are often insecure because the answers to questions like “what is your mother’s maiden name” or “what is the first street you grew up on” are often commonly available, either through public record searches or social media.

One way to help make security questions stronger is not to answer them truthfully. After all, your answer just has to match the answer you wrote in when you set the questions; it doesn’t need to be honest.

For example, you may have a favorite PIN, or alternate passcode you might use regardless of the question



When prompted with your stored security question, just type it EXACTLY as you had typed it during the enrollment setup, and press Verify.

**How to use Security Question when prompted (Below)**

5b. Select a secret question from the dropdown and   
Type the answer you will respond with each time it is asked.

5a. Click Setup under Security Questions

**Having Trouble?**

If you’re having trouble setting up or using any of these factors, we recommend contacting the Help Desk at (314) 968-4777 directly.