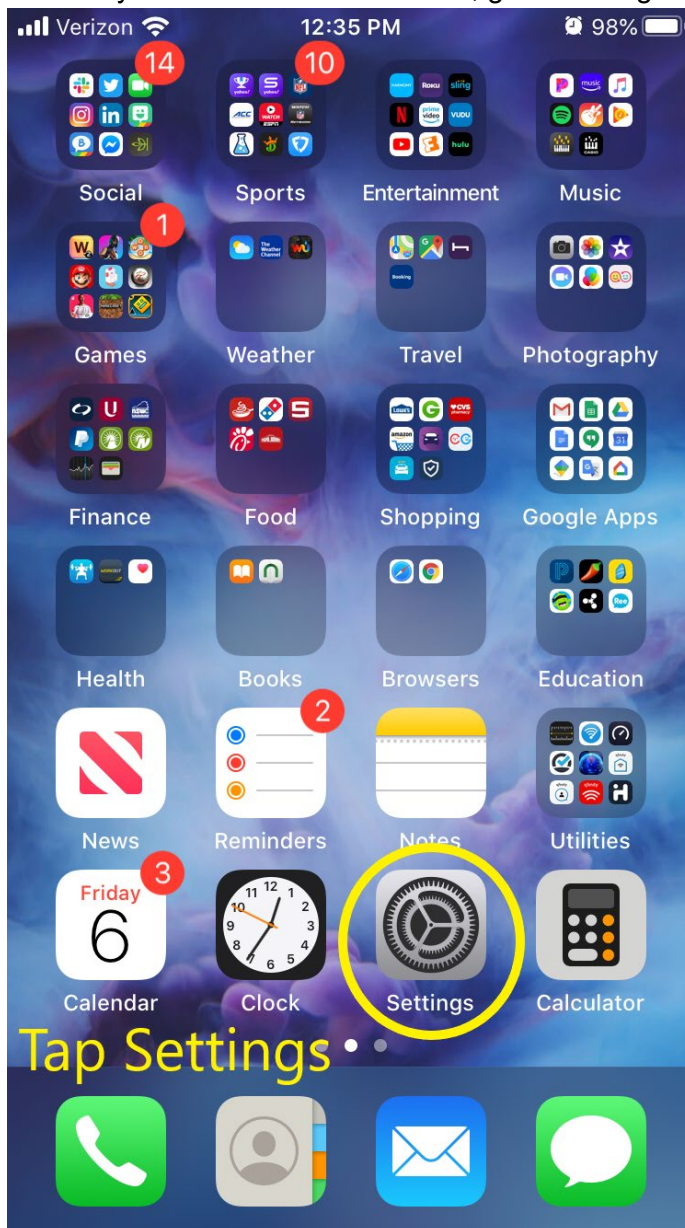


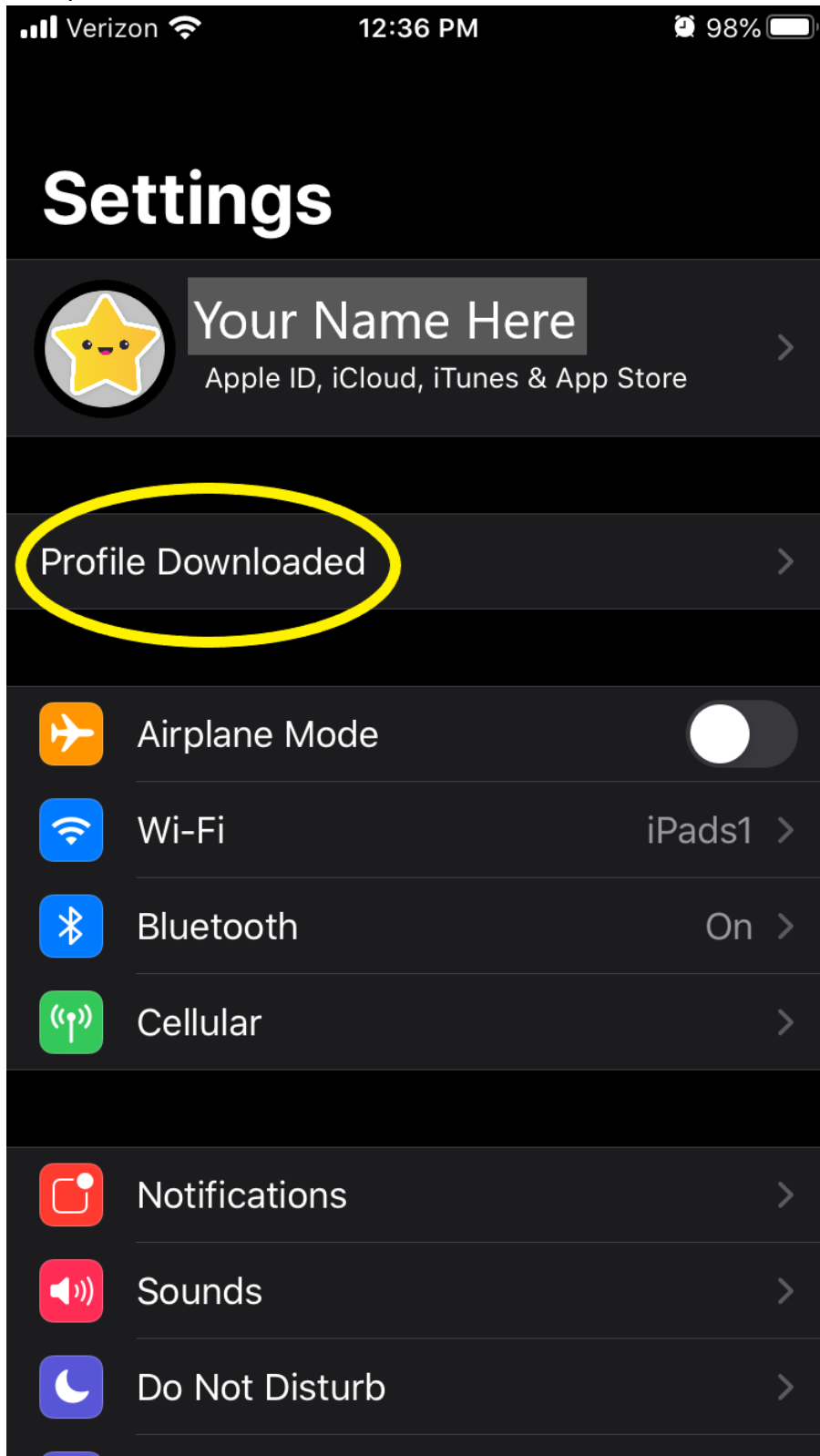
\*\*\* Note: It recommended that you update your iOS version to the latest version before installing this certificate. The following example is on iOS version 13.2.3. Your screens may be slightly different depending on what version is running.\*\*\*

#### SSL Certificate Installation Instructions for Apple iOS:

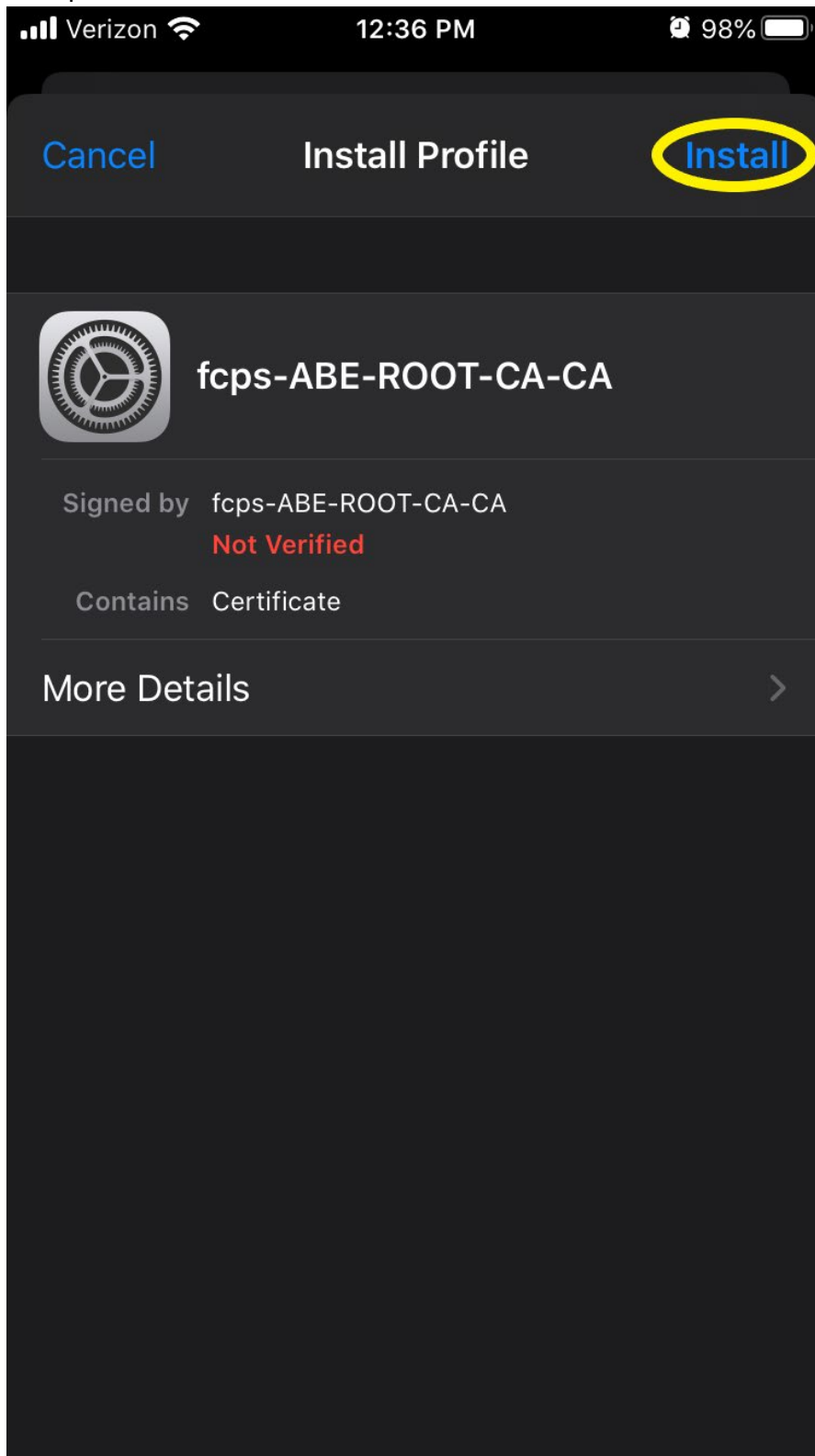
1. If you do not have a passcode configured on your phone, you will need to configure one. If you already have a passcode configured on your phone skip to Step 2. If you need to configure a passcode go to Settings > Touch ID & Passcode. Configure a code of your choice.
2. Navigate to <http://fluco.org/tech/downloads/ABE-ROOT-CA.cer> to download the certificate. The certificate will download as soon as you click on the link.
3. From your iPhone's home screen, go to Settings:



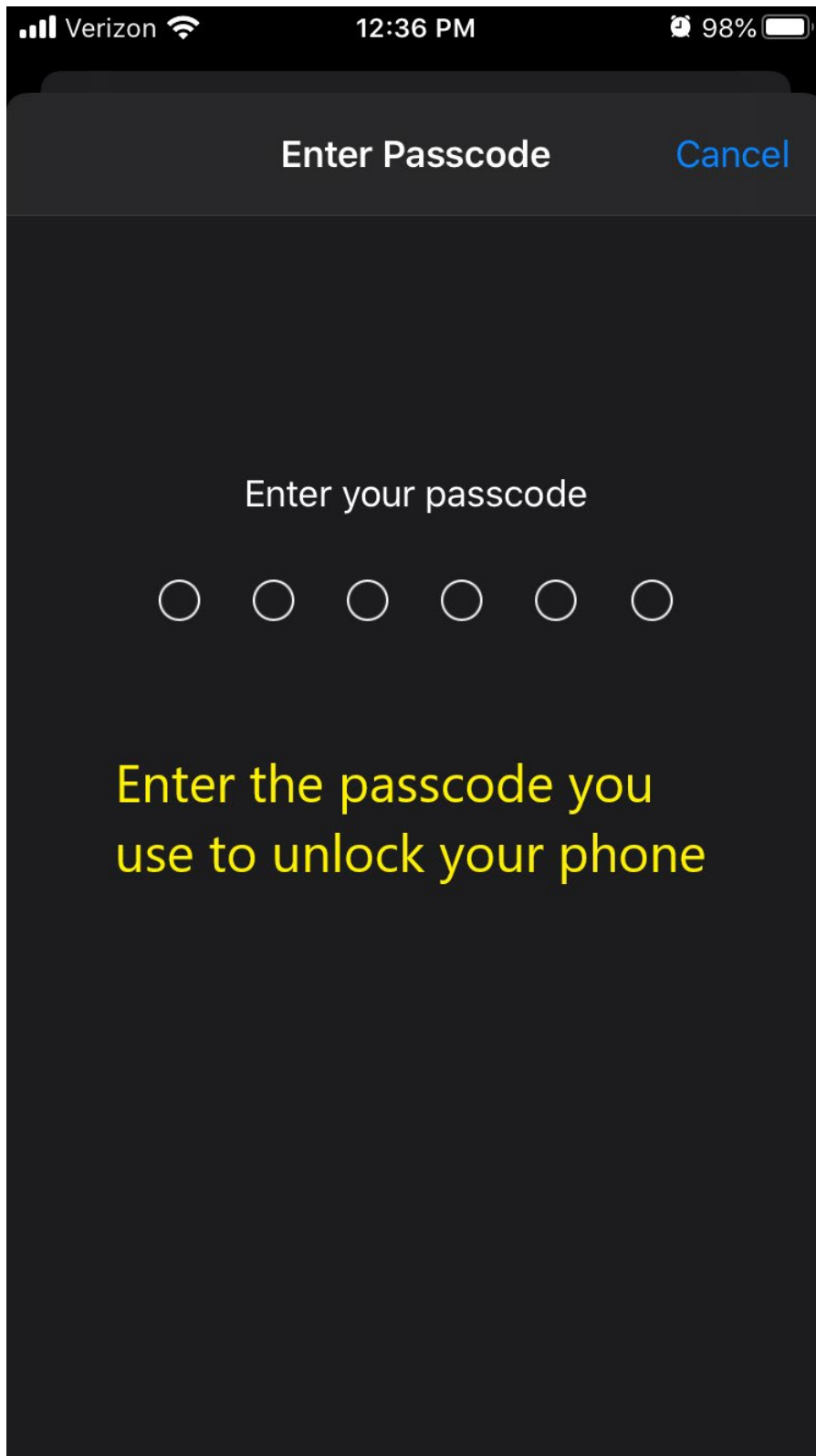
4. Tap "Profile Downloaded":



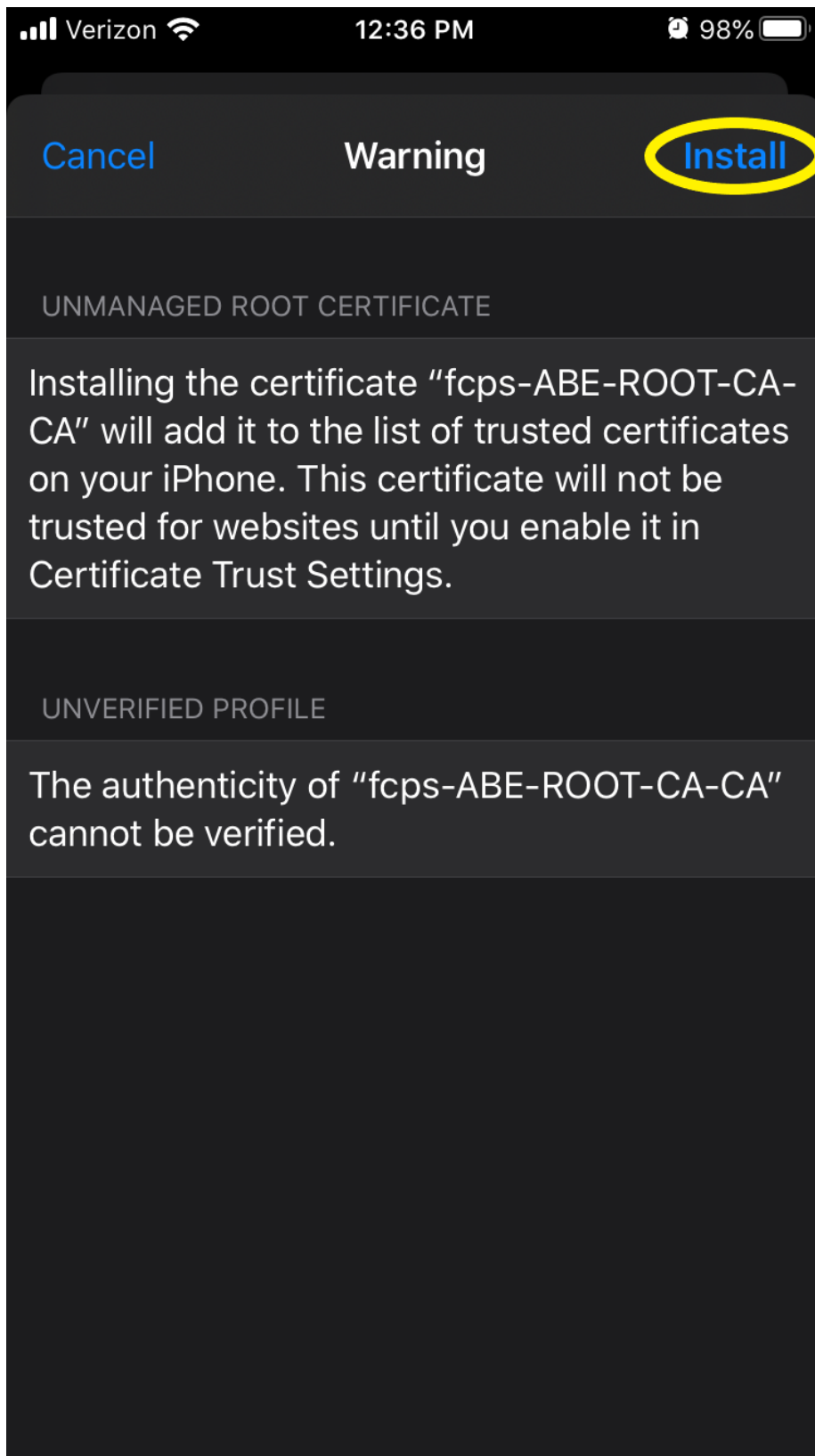
5. Tap "Install":



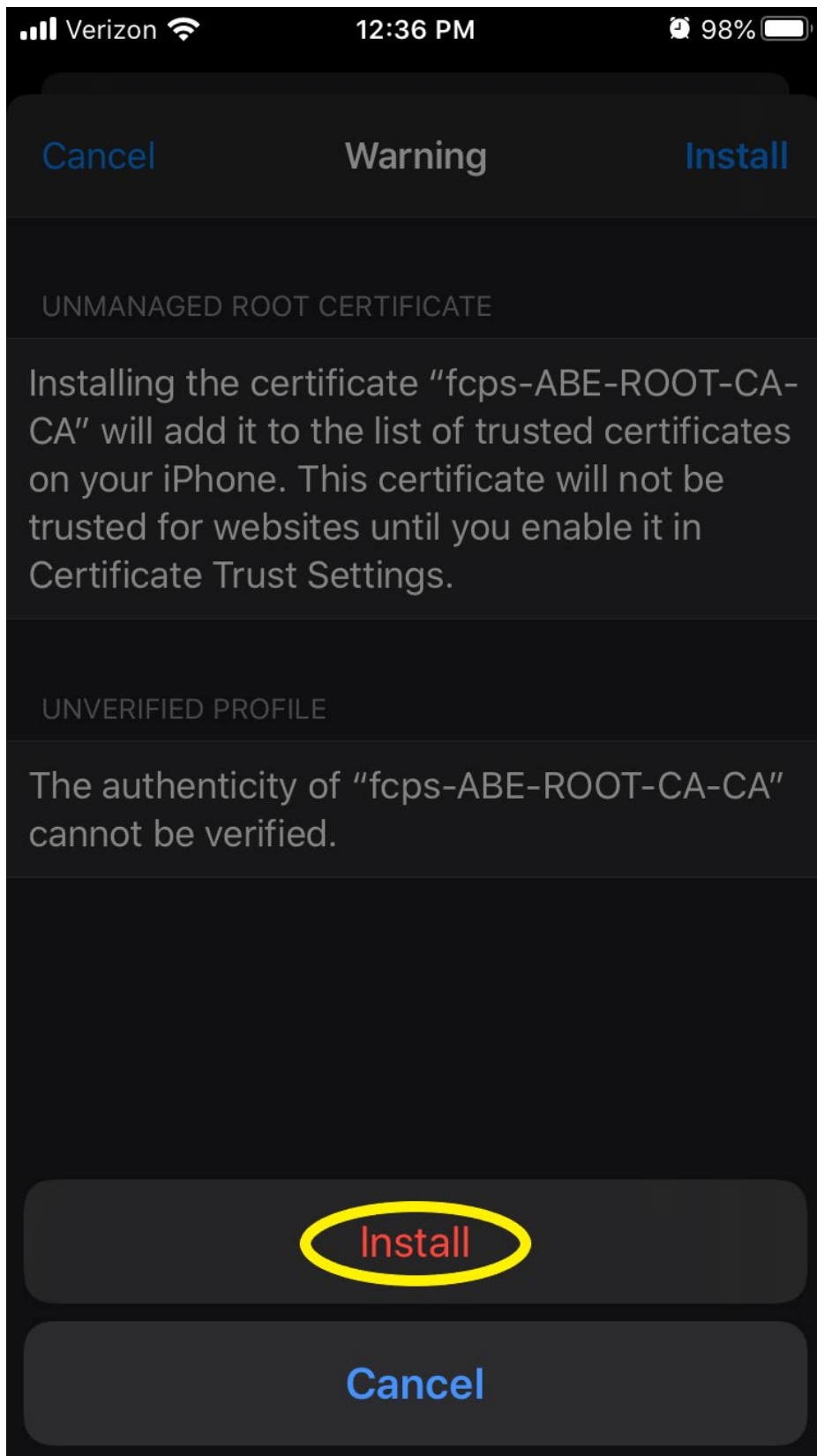
6. Enter the passcode you use to unlock your iPhone (the one you created in Step 1):



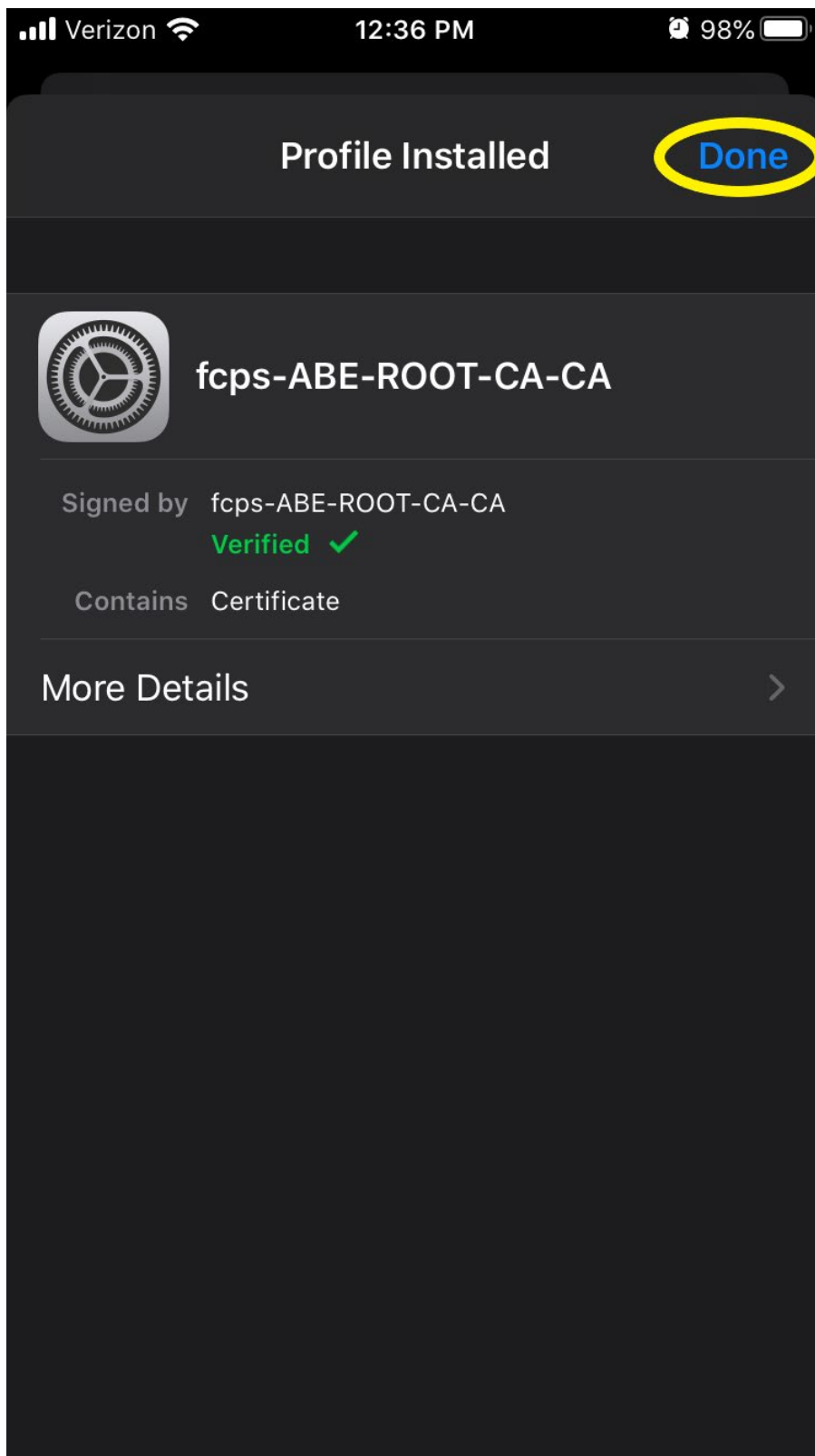
7. You will see a warning about the authenticity of the unmanaged root certificate. Tap "Install" to proceed:



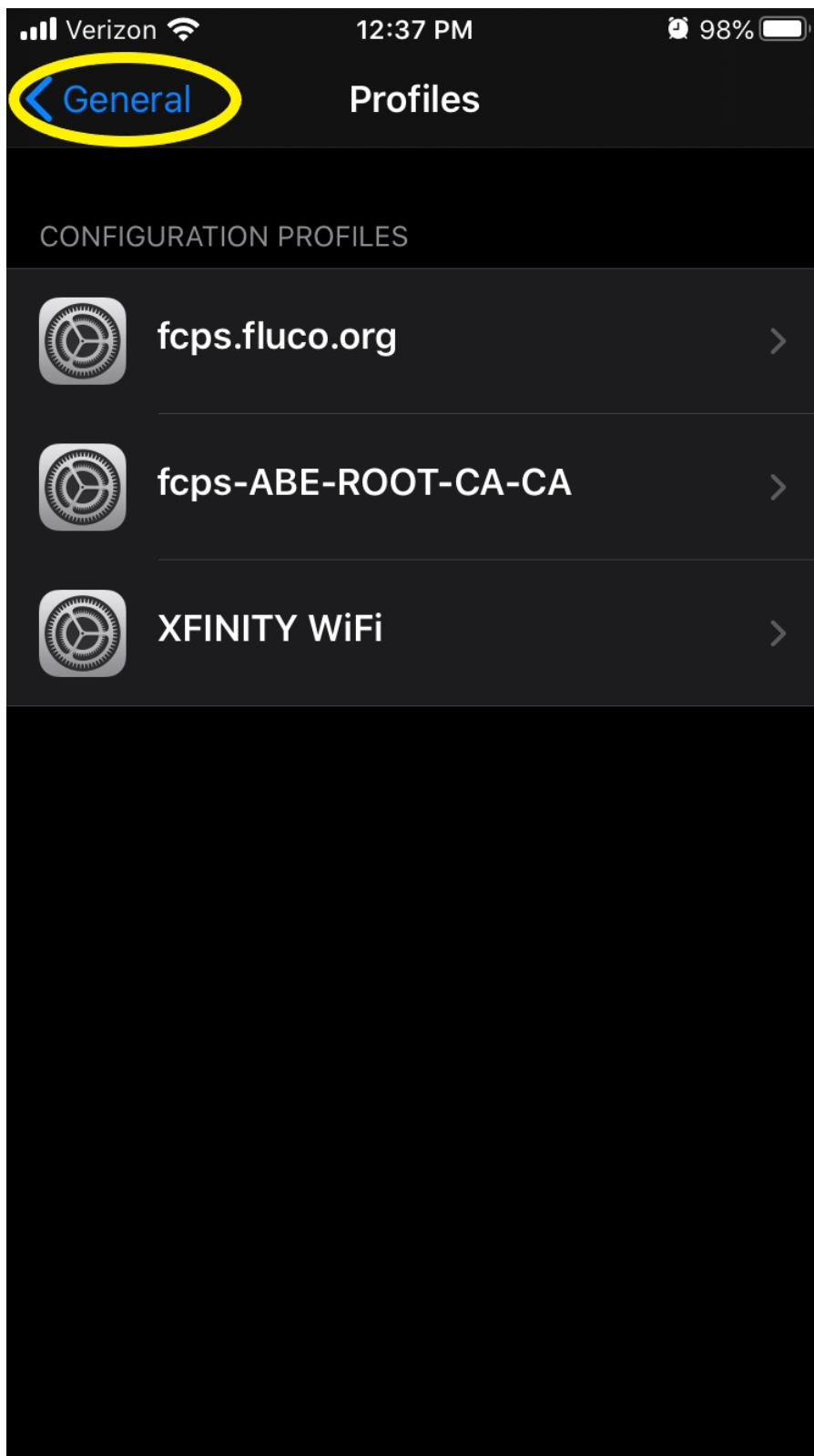
8. Tap "Install" again:



9. The next screen will show the profile is installed. Tap "Done":

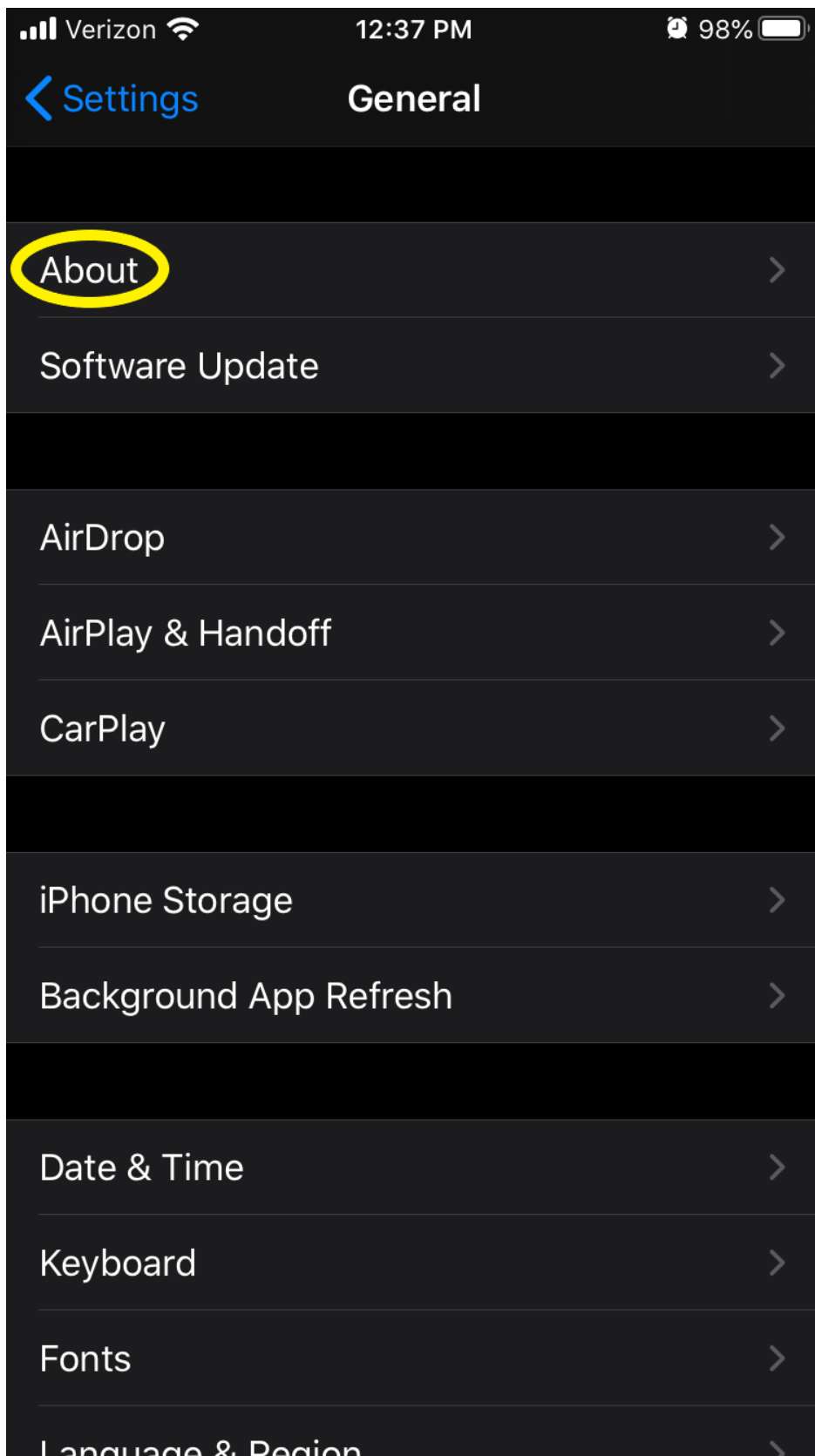


10. The next screen shows the new profile along with any other profiles already installed on the phone. Tap “General”:

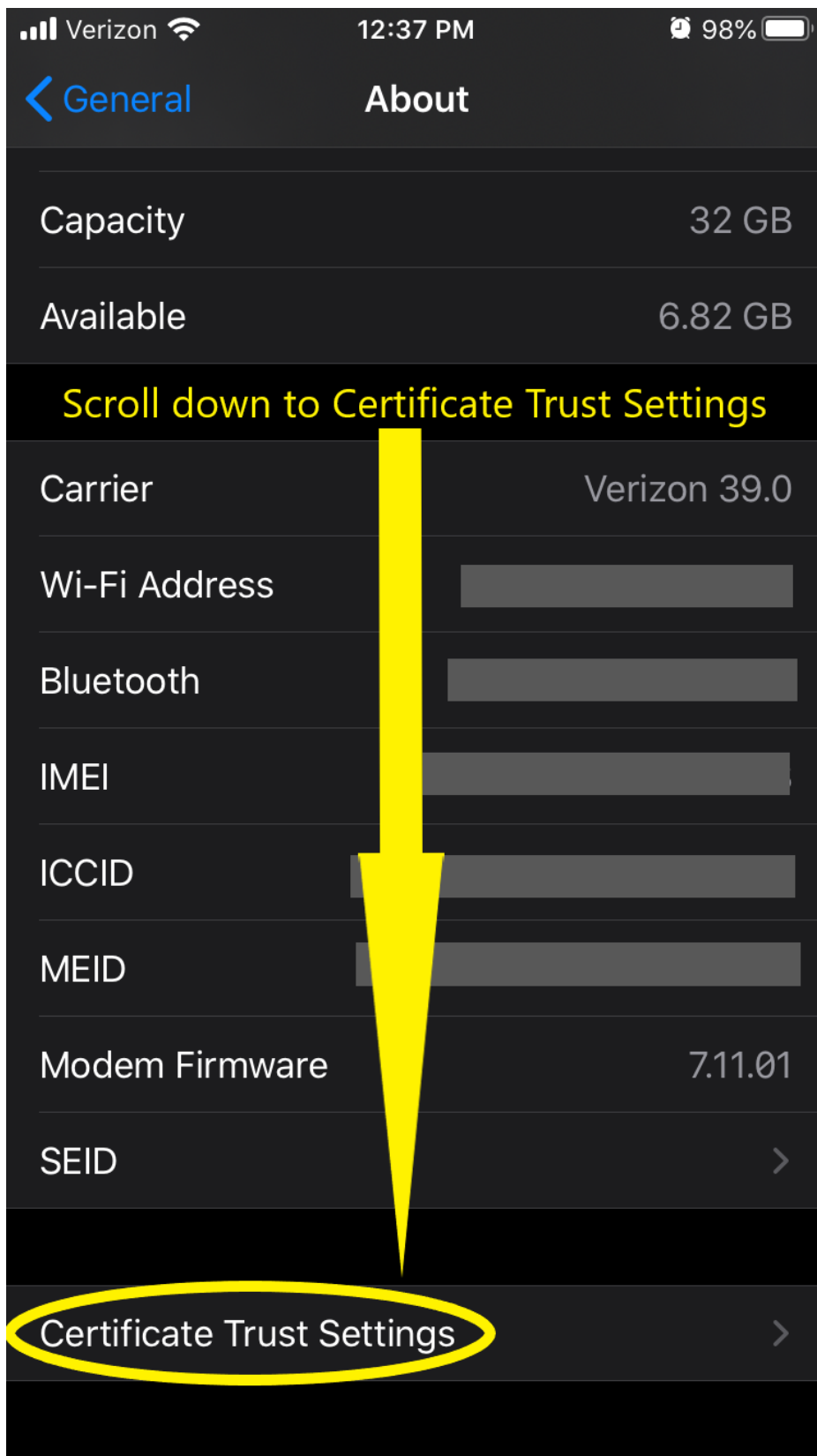


11. Tap "About":

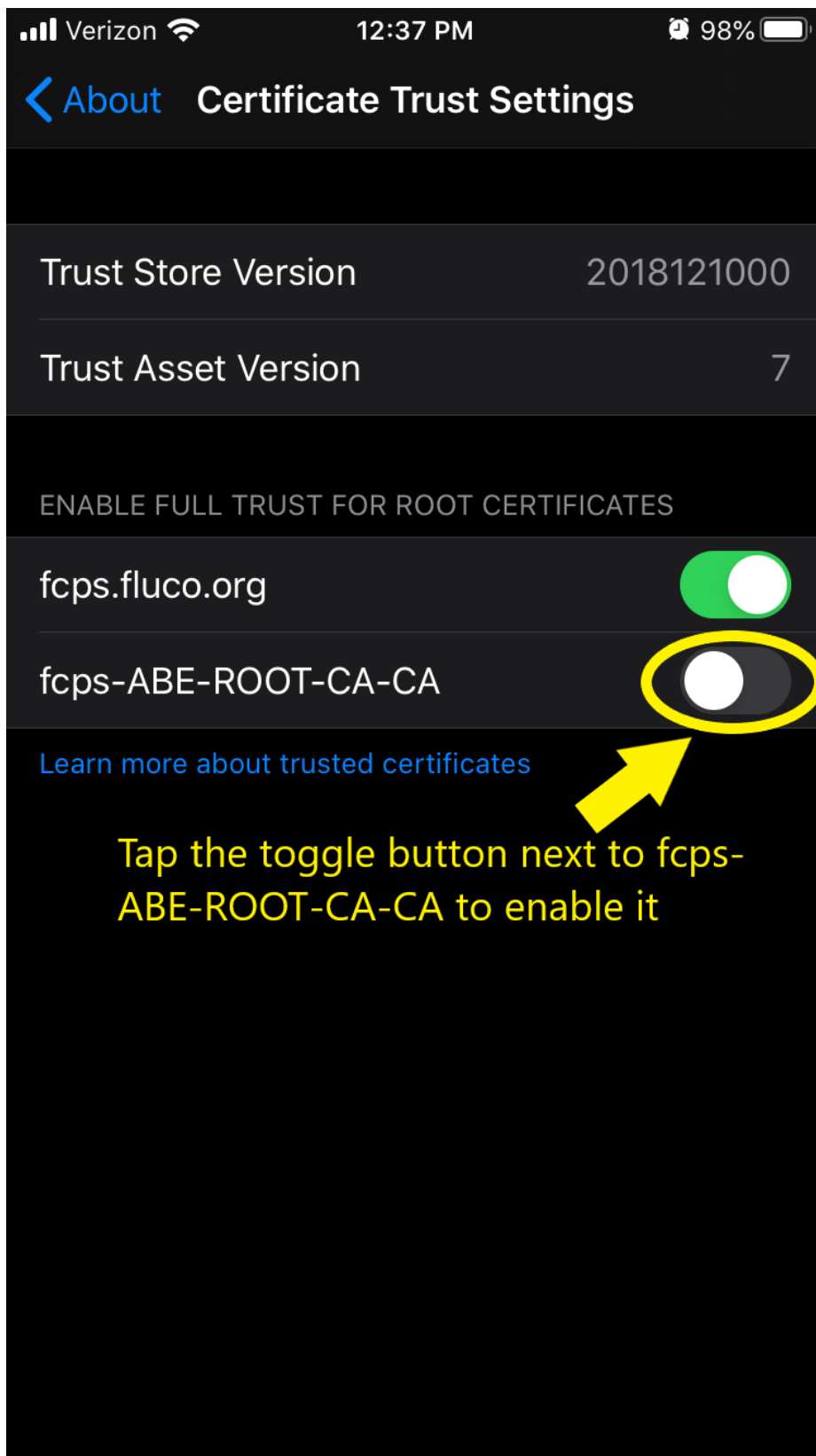




12. Scroll to the bottom of the “About” screen and tap on “Certificate Trust Settings”:



13. Tap the toggle button next to fcps-ABE-ROOT-CA-CA to enable it:



14. You'll see a warning about enabling certificates for websites. Tap "Continue":

## Certificate Trust Settings

Trust Store Version 2018121000

Trust Asset Version 7

ENABLE FULL TRUST FOR ROOT CERTIFICATES

fcps.fluco.org



fcps-



[Learn](#)

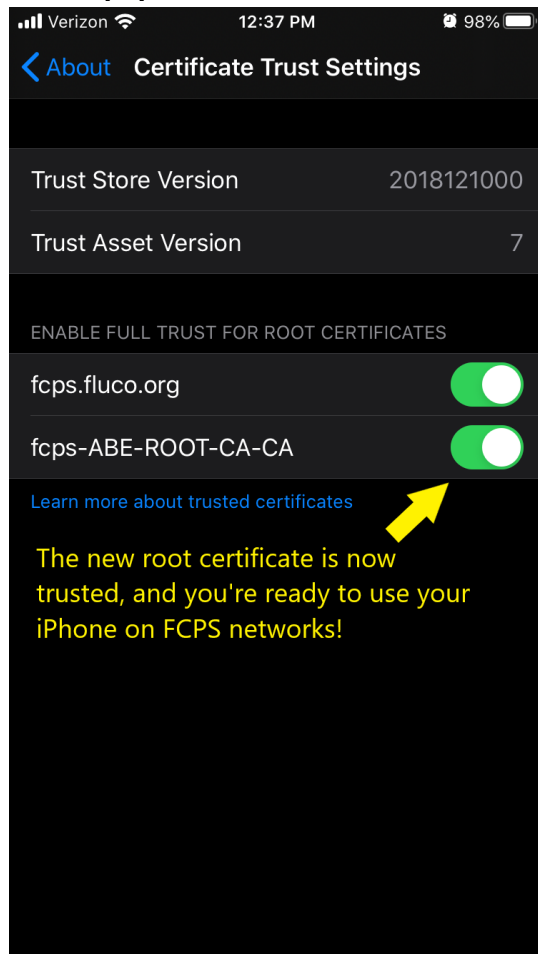
### Root Certificate

Warning: enabling this certificate for websites will allow third parties to view any private data sent to websites.

Cancel

Continue

15. The toggle button will turn green, indicating the new certificate is trusted and enabled. You're now ready to use your iPhone on FCPS networks. **If you use an Apple laptop or desktop, please read further for additional instructions.**



**ADDITIONAL STEPS for Apple laptops and desktops:** On Apple desktops and laptops, you may or may not get an installation wizard, depending on the MacOS version you are running:

- If you get a wizard pop-up, you will see that the certificate that you just installed is not trusted. To “trust” the certificate, double click on the error message text, and a pop-up window will open. There will be a drop down at the top of this window that will allow you to select “always trust this certificate”.
- If you do not get a wizard, you will receive a notification from your Apple “Keychain” service after you download the certificate. You will need your “Keychain” password to “unlock” this service. In the upper right corner of the “Keychain” window you will see “File”. Click on “File” and select “Import Files”. Select the certificate that you downloaded in the earlier step. Before you hit “Import” make sure the dropdown says to place it in “System” folder, and not the “Microsoft Intermediate Certificate Folder”. Once you install the certificate in the “System Folder” you will see that the certificate that you just installed is not trusted. To “trust” the certificate, double click on the error message text, and a pop-up window will open. There will be a drop down at the top of this window that will allow you to select “always trust this certificate”.