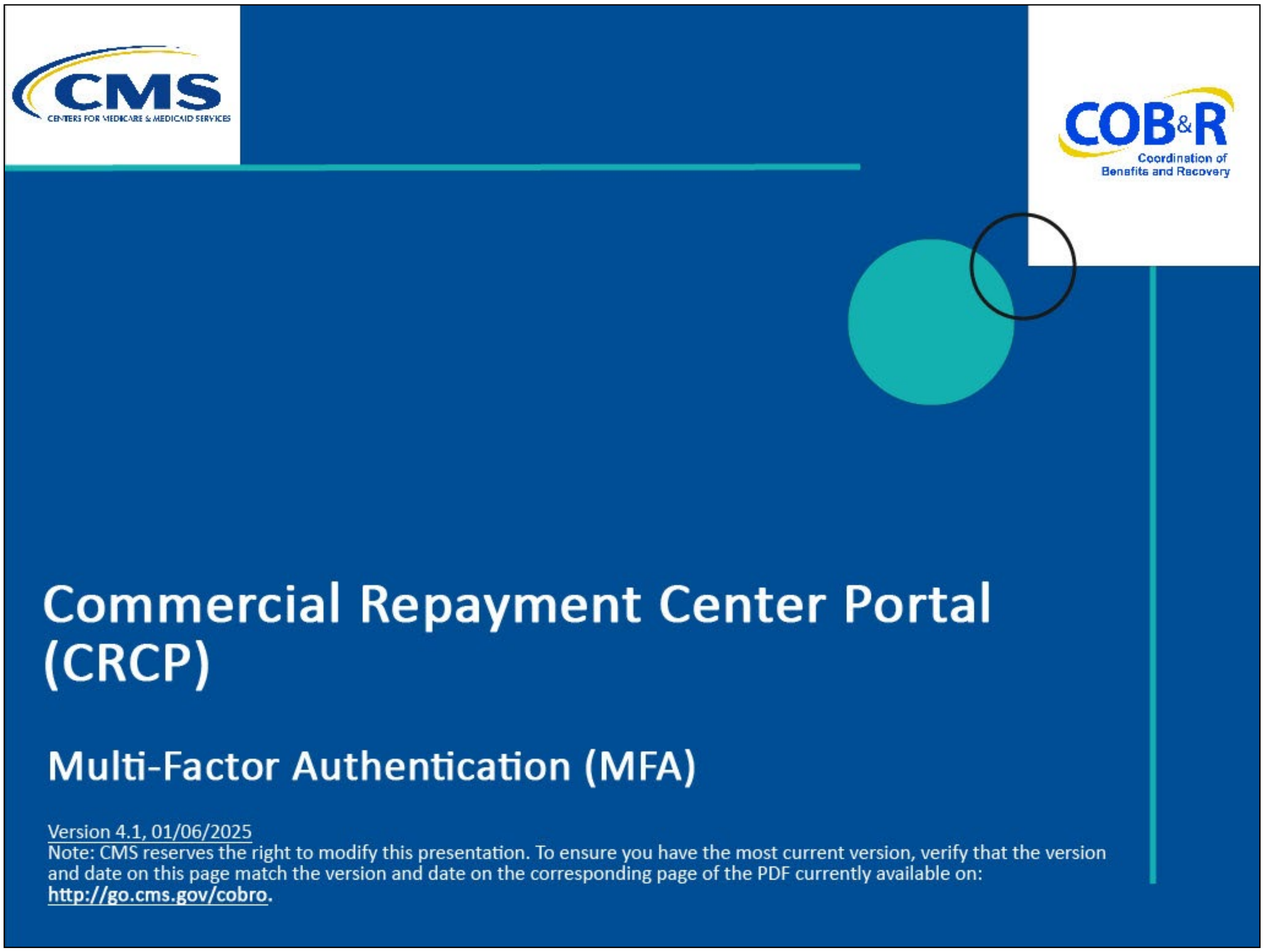
Multi-Factor Authentication Process

Slide 1 of 40 - Multi-Factor Authentication Process



CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
COB&R
Coordination of Benefits and Recovery

Commercial Repayment Center Portal (CRCP)

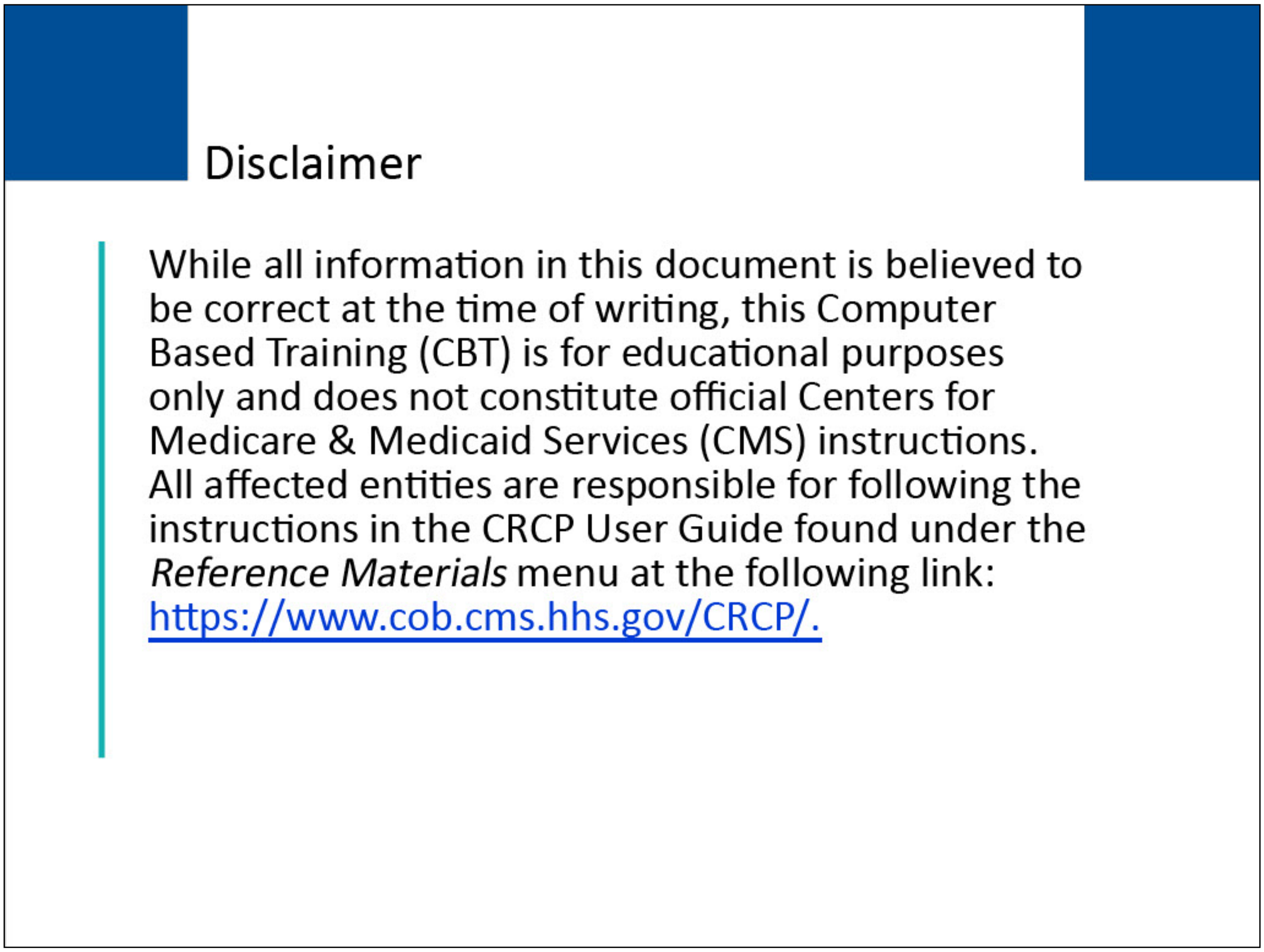
Multi-Factor Authentication (MFA)

Version 4.1, 01/06/2025
Note: CMS reserves the right to modify this presentation. To ensure you have the most current version, verify that the version and date on this page match the version and date on the corresponding page of the PDF currently available on: **http://go.cms.gov/cobro**.

Slide notes

Welcome to the CRCP Multi-Factor Authentication (MFA) Process course.

Process **Slide 2 of 40 - Disclaimer**



Disclaimer

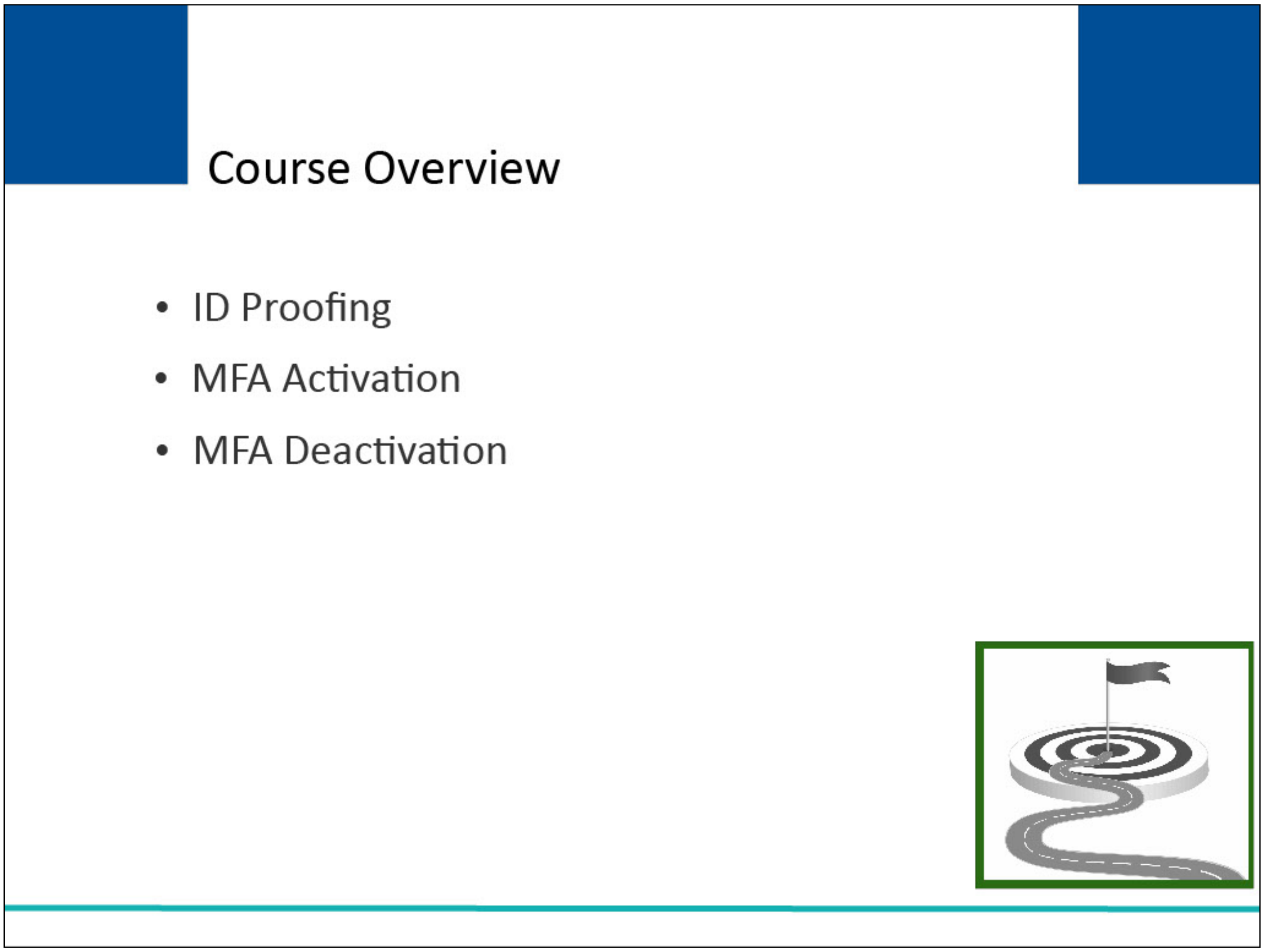
While all information in this document is believed to be correct at the time of writing, this Computer Based Training (CBT) is for educational purposes only and does not constitute official Centers for Medicare & Medicaid Services (CMS) instructions. All affected entities are responsible for following the instructions in the CRCP User Guide found under the *Reference Materials* menu at the following link: https://www.cob.cms.hhs.gov/CRCP/.

Slide notes

While all information in this document is believed to be correct at the time of writing, this Computer Based Training (CBT) is for educational purposes only and does not constitute official Centers for Medicare & Medicaid Services (CMS) instructions.

All affected entities are responsible for following the instructions in the CRCP User Guide found under the Reference Materials menu at the following link: https://www.cob.cms.hhs.gov/CRCP/.

Slide 3 of 40 - Course Overview



Course Overview

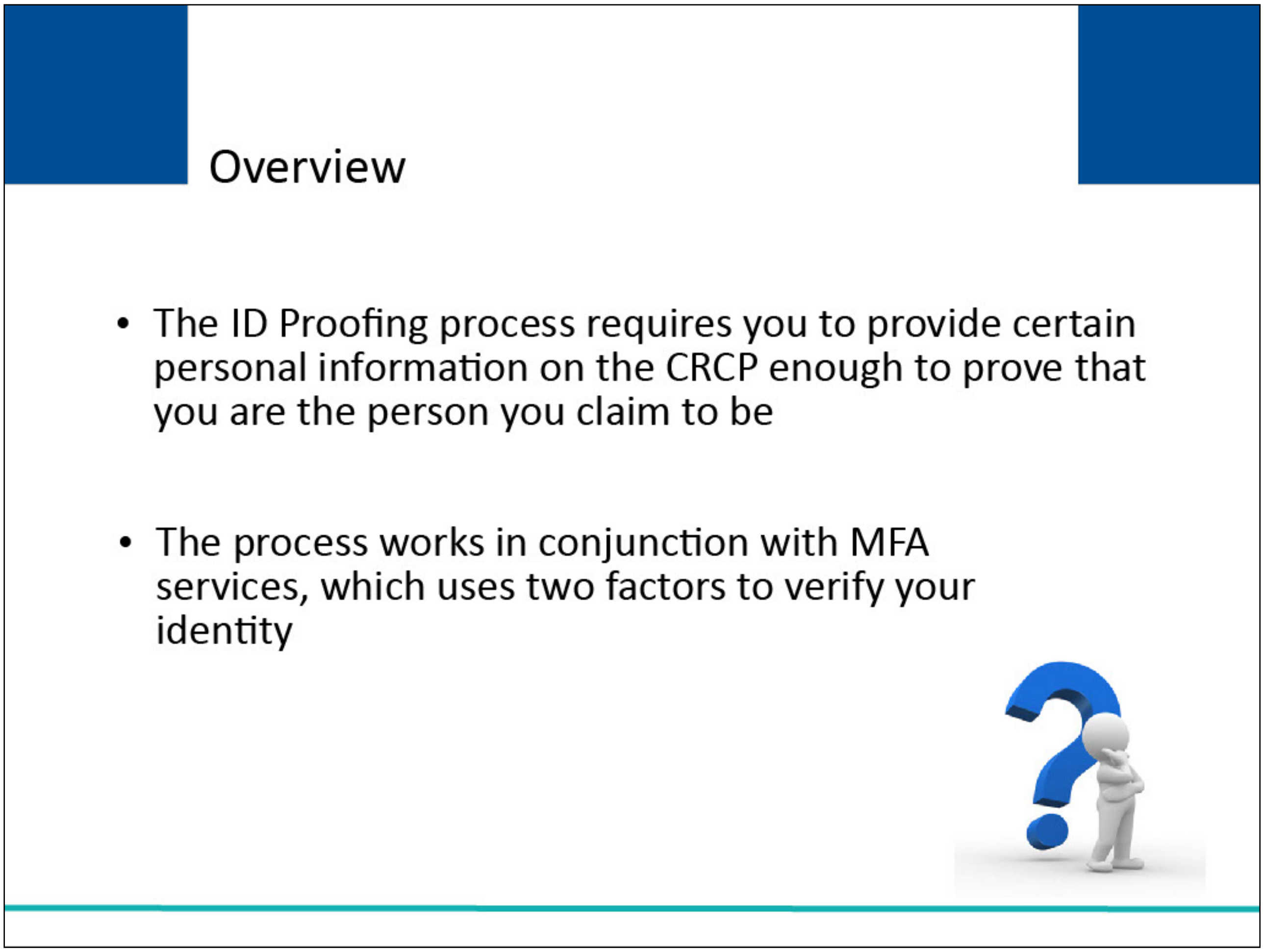
- ID Proofing
- MFA Activation
- MFA Deactivation

Slide notes

This module explains the steps a non-beneficiary user must take to be able to view unmasked case information in the CRCP.

It explains how a user can become identity proofed using the CRCP and how Multi-Factor Authentication (MFA) is activated and deactivated (if needed).

Process **Slide 4 of 40 - Overview**



Overview

- The ID Proofing process requires you to provide certain personal information on the CRCP enough to prove that you are the person you claim to be
- The process works in conjunction with MFA services, which uses two factors to verify your identity

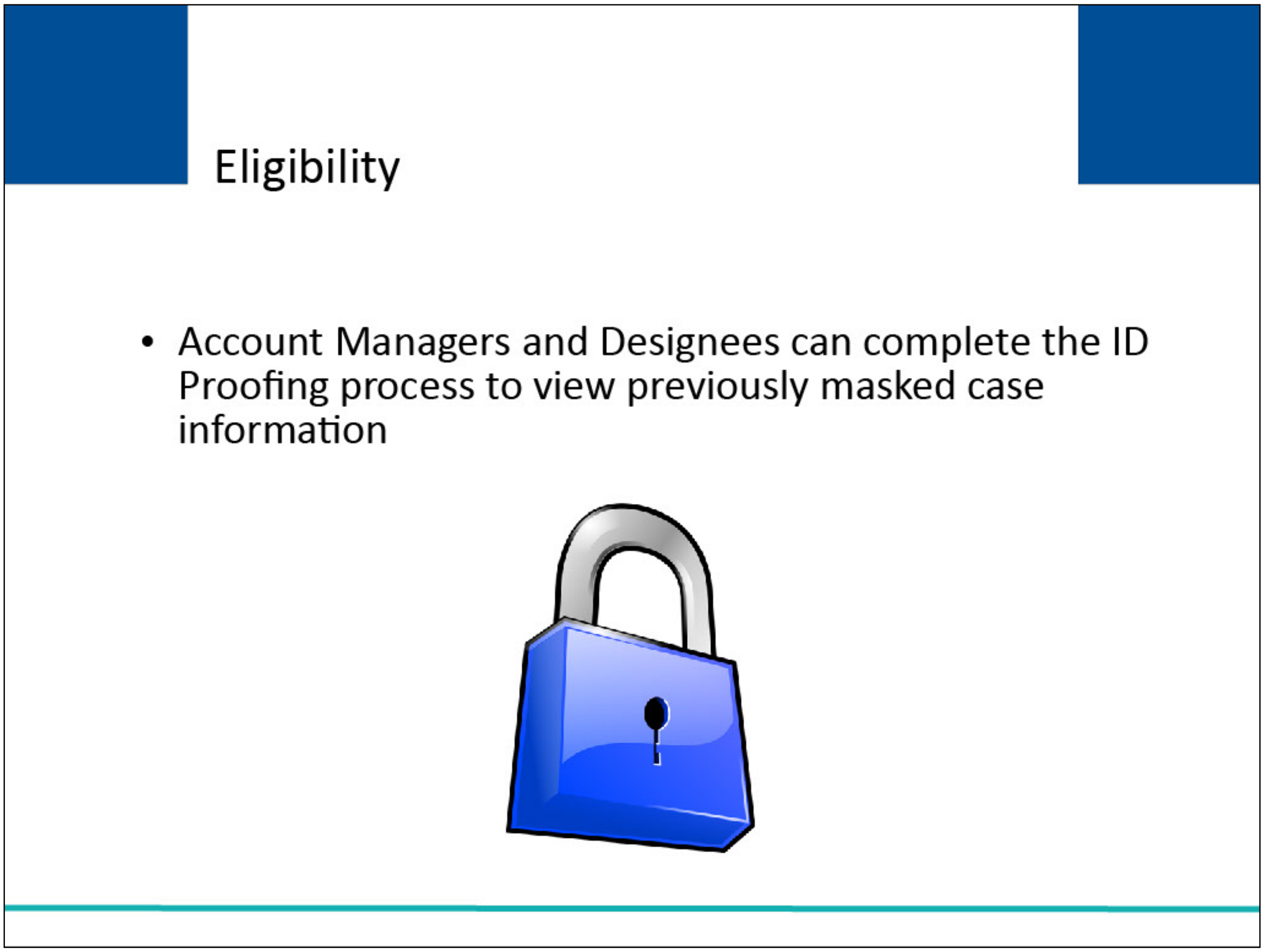
Slide notes

CMS has adopted Multi-Factor Authentication (MFA) to provide certain users with the ability to view unmasked case information.

The ID Proofing process requires you to provide certain personal information on the CRCP sufficient enough to prove that you are the person you claim to be.

This process works in conjunction with MFA services, which uses two different factors to verify your identity.

Process **Slide 5 of 40- Eligibility**



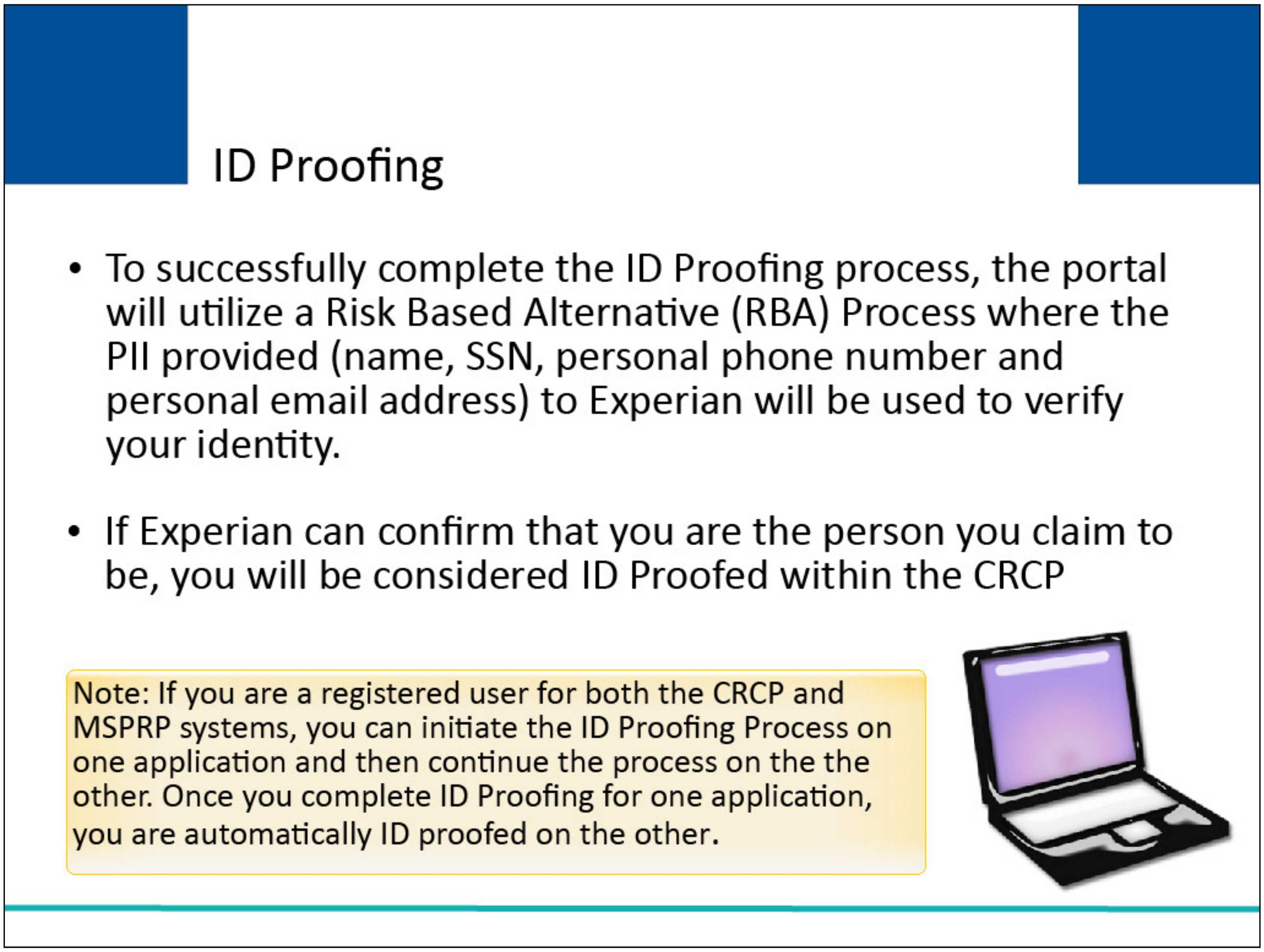
Eligibility

- Account Managers and Designees can complete the ID Proofing process to view previously masked case information

Slide notes

Account Managers and Account Designees can complete the ID Proofing process.

Process **Slide 6 of 40 - ID Proofing**



ID Proofing

- To successfully complete the ID Proofing process, the portal will utilize a Risk Based Alternative (RBA) Process where the PII provided (name, SSN, personal phone number and personal email address) to Experian will be used to verify your identity.
- If Experian can confirm that you are the person you claim to be, you will be considered ID Proofed within the CRCP

Note: If you are a registered user for both the CRCP and MSPRP systems, you can initiate the ID Proofing Process on one application and then continue the process on the the other. Once you complete ID Proofing for one application, you are automatically ID proofed on the other.

Slide notes

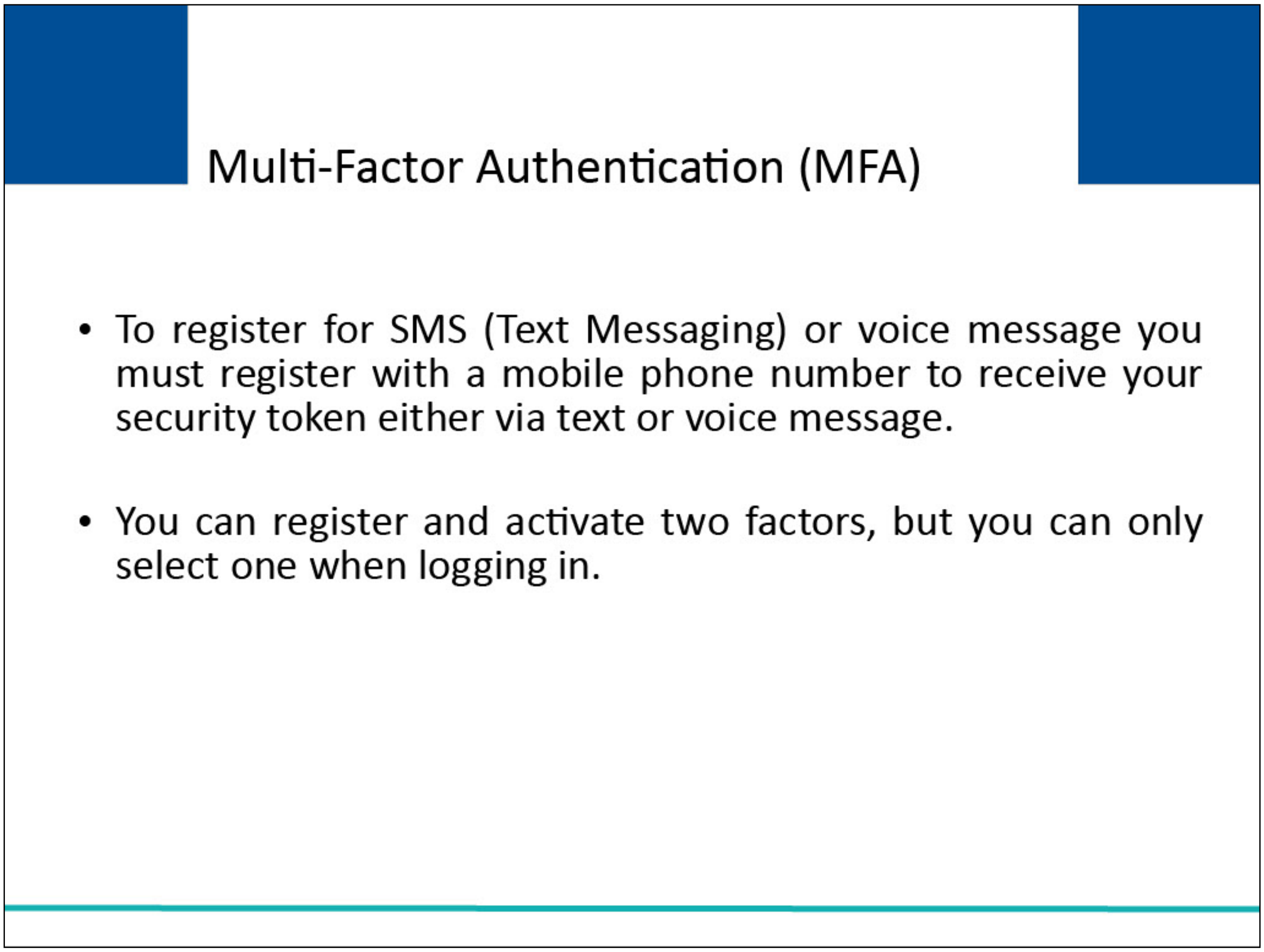
To successfully complete the ID Proofing process, the portal will utilize a Risk Based Alternative (RBA) Process where the PII provided (name, SSN, personal phone number, and personal email address) to Experian will be used to verify your identity.

If Experian is able to confirm that you are the person you claim to be, you will be considered ID Proofed within the CRCP.

Note: If you are a registered user for both the CRCP and MSPRP systems, you can initiate the ID Proofing process on one application and then continue the process on the other. Once you complete ID proofing for one application, you are automatically ID proofed on the other.

Also, users who have not completed the ID Proofing process can continue to access the CRCP as they currently do with limited views of case information.

Slide 7 of 40- Multi-Factor Authentication (MFA)



Multi-Factor Authentication (MFA)

- To register for SMS (Text Messaging) or voice message you must register with a mobile phone number to receive your security token either via text or voice message.
- You can register and activate two factors, but you can only select one when logging in.

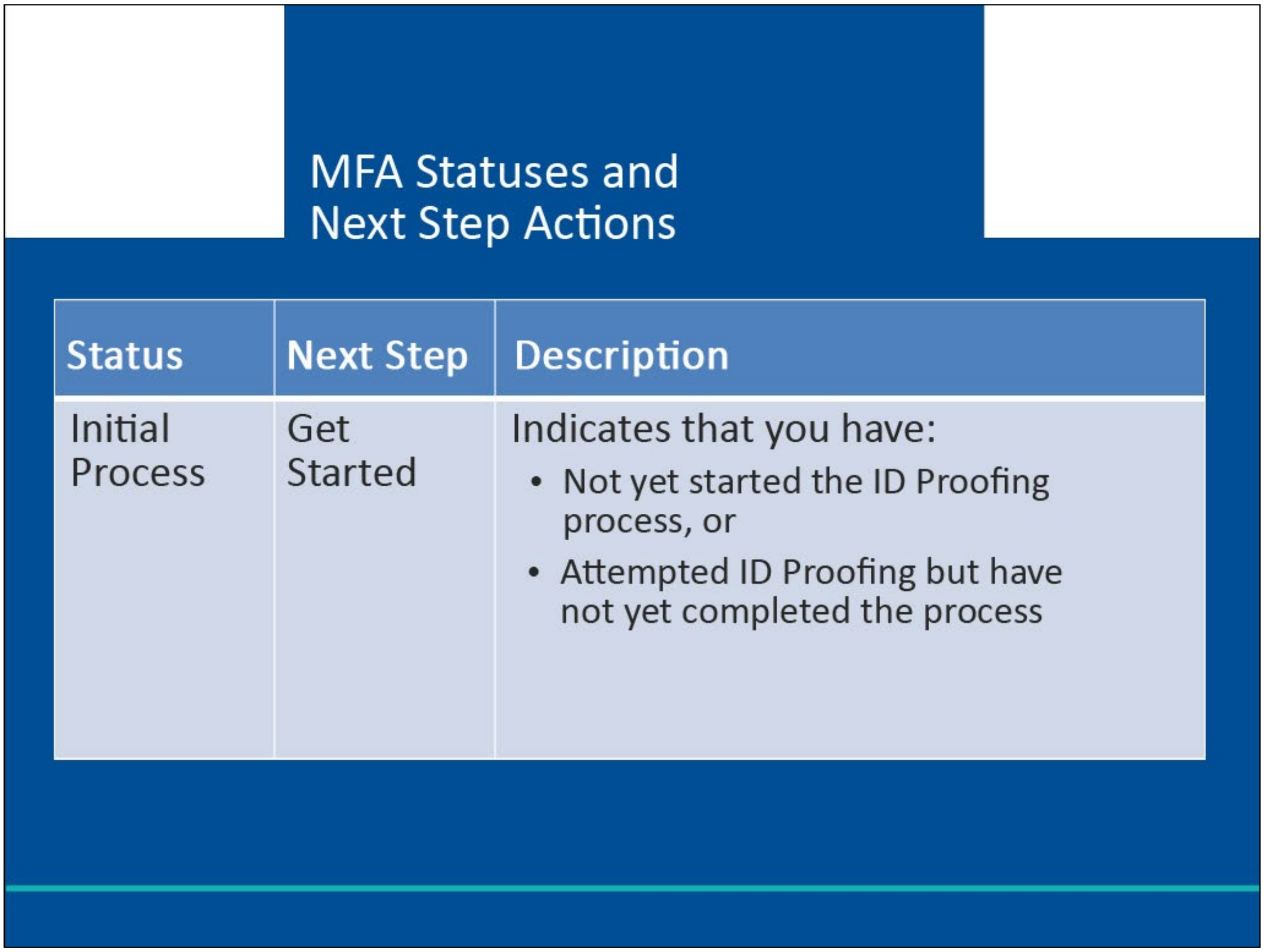
Slide notes

To begin the Multi-factor Authentication process, you must register and activate one or both, the SMS (Text Messaging) or voice message. You must register with a mobile phone number to receive your security token either via text or voice message.

You can register and activate two factors, but you can only select one when logging in.

Note: Starting March 2025 the Multi-Factor Authentication process will be updated. The SMS and Voice Message will be deactivated and replaced with the Okta Verify and/or Google Authenticator.

Slide 8 of 40- MFA Statuses and Next Step Actions



MFA Statuses and Next Step Actions

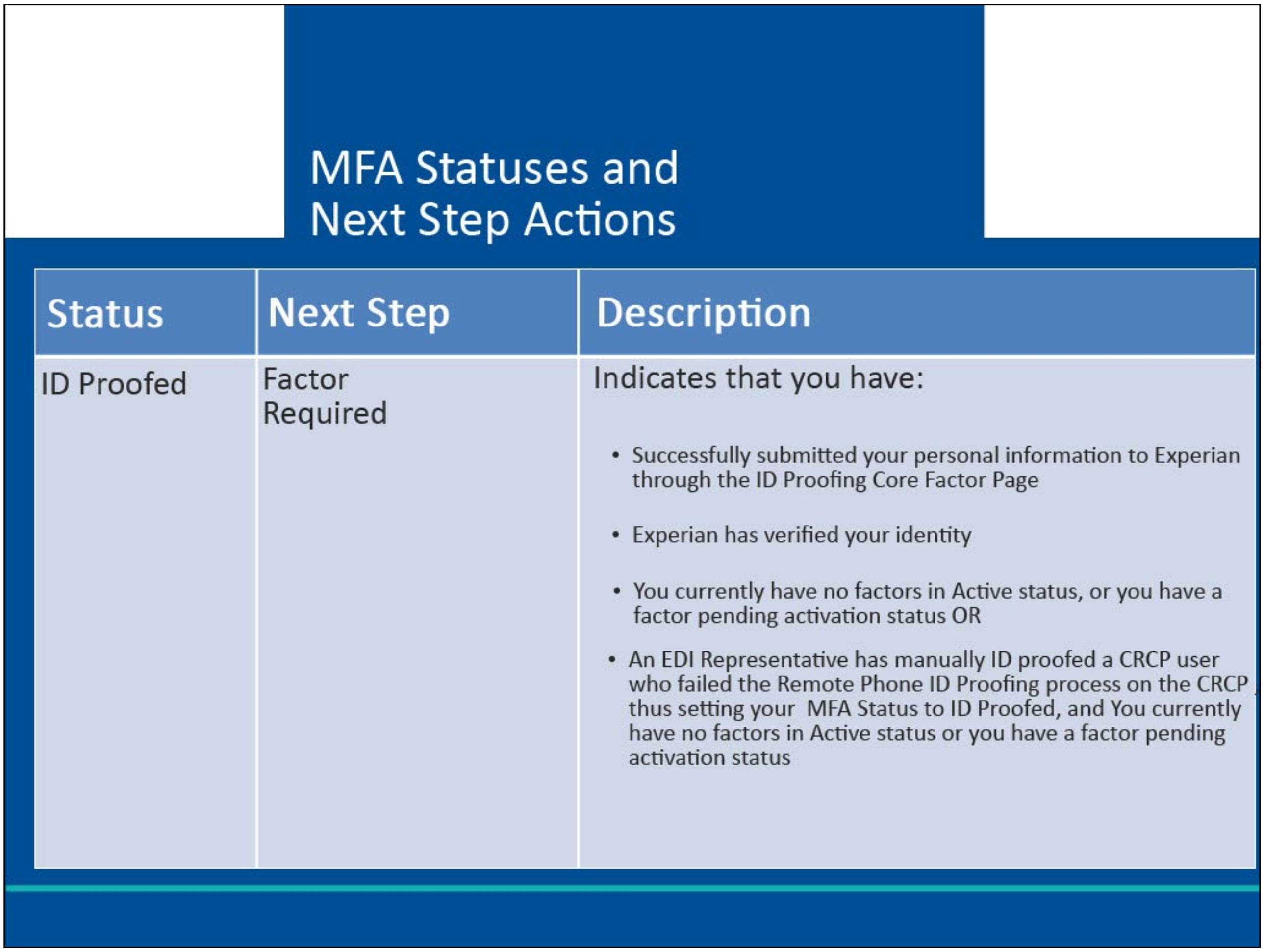
Status	Next Step	Description
Initial Process	Get Started	Indicates that you have: • Not yet started the ID Proofing process, or • Attempted ID Proofing but have not yet completed the process

Slide notes

When the MFA status for a CRCP user is set to Initial Process, the next step will be set to Get Started.

This indicates that you have not yet started the ID Proofing process or that you have attempted ID proofing but have not yet completed the process.

Slide 9 of 40 MFA Statuses and Next Step Actions



MFA Statuses and Next Step Actions

Status	Next Step	Description
ID Proofed	Factor Required	Indicates that you have: • Successfully submitted your personal information to Experian through the ID Proofing Core Factor Page • Experian has verified your identity • You currently have no factors in Active status, or you have a factor pending activation status OR • An EDI Representative has manually ID proofed a CRCP user who failed the Remote Phone ID Proofing process on the CRCP , thus setting your MFA Status to ID Proofed, and You currently have no factors in Active status or you have a factor pending activation status

Slide notes

When the MFA Status for a CRCP user is set to ID Proofed, the next step will be Factor Required. This indicates that you have:

Successfully submitted your personal information to Experian through the ID Proofing Core Factor Page;

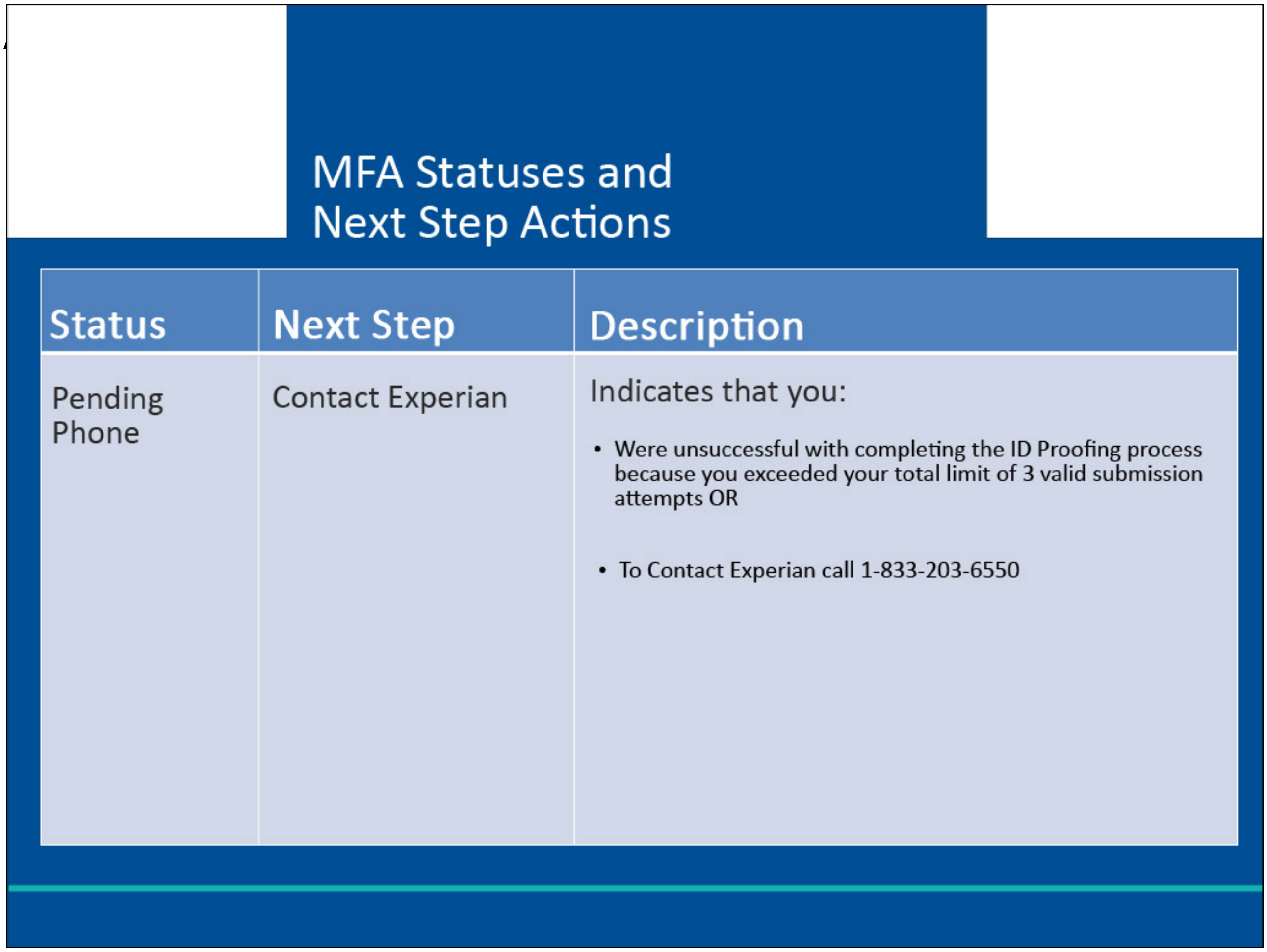
Experian has verified your identity;

You currently have no factors in Active status, or you have a factor pending activation status;

OR

An EDI Representative has manually ID proofed a CRCP user who failed the Remote Phone ID Proofing process on the CRCP, thus setting your MFA Status to ID Proofed and you currently have no factors in Active status, or you have a factor pending activation status.

Slide 10 of 40 - MFA Statuses and Next Step



MFA Statuses and Next Step Actions

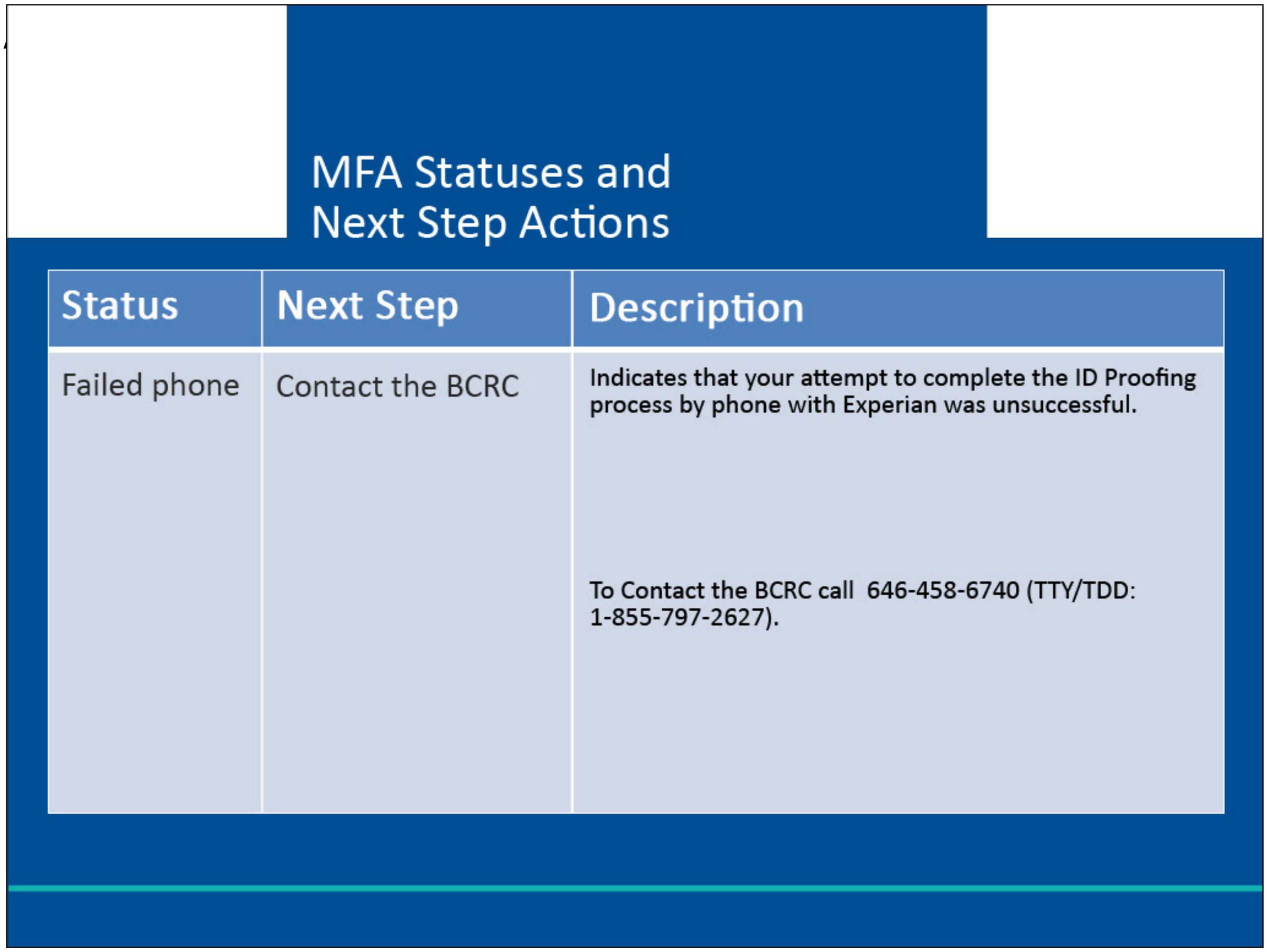
Status	Next Step	Description
Pending Phone	Contact Experian	Indicates that you: • Were unsuccessful with completing the ID Proofing process because you exceeded your total limit of 3 valid submission attempts OR • To Contact Experian call 1-833-203-6550

Slide notes

When the MFA Status is set to Pending Phone, the next step will be to Contact Experian. The status indicates that you were unsuccessful with completing the ID Proofing process because you exceeded your total limit of four valid submission attempts (i.e., you clicked the Continue button without receiving validation errors the maximum three times allowed on the ID Proofing and Core Factor page) or you clicked the Contact Experian button on the ID Proofing Core Factors page.

To Contact the BCRC call 646-458-6740 (TTY/TDD). Experian call 1-833-203-6550.

Slide 11 of 40 - MFA Statuses and Next Step



MFA Statuses and Next Step Actions

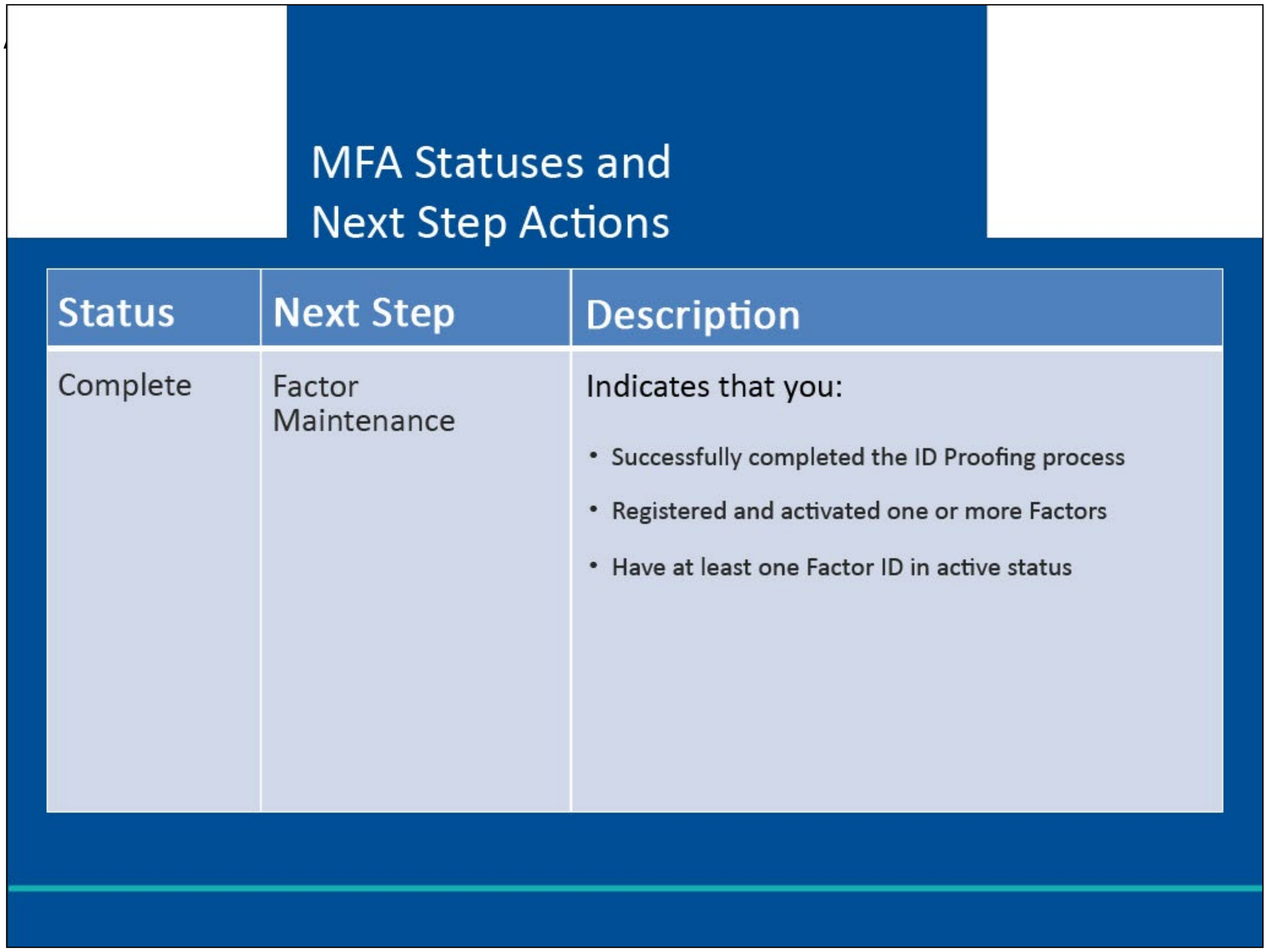
Status	Next Step	Description
Failed phone	Contact the BCRC	Indicates that your attempt to complete the ID Proofing process by phone with Experian was unsuccessful. To Contact the BCRC call 646-458-6740 (TTY/TDD: 1-855-797-2627).

Slide notes

When the MFA Status for a CRCP user is set to Failed Phone, the next step will be to Contact the BCRC. This indicates that your attempt to complete the ID Proofing process by phone with Experian was unsuccessful.

To Contact the BCRC call 646-458-6740 (TTY/TDD: 1-855-797-2627).

Slide 12 of 40 - MFA Statuses and Next Step



MFA Statuses and Next Step Actions

Status	Next Step	Description
Complete	Factor Maintenance	Indicates that you: • Successfully completed the ID Proofing process • Registered and activated one or more Factors • Have at least one Factor ID in active status

Slide notes

When the MFA Status for a CRCP user is set to Complete, the next step will be Factor Maintenance. This indicates that you:

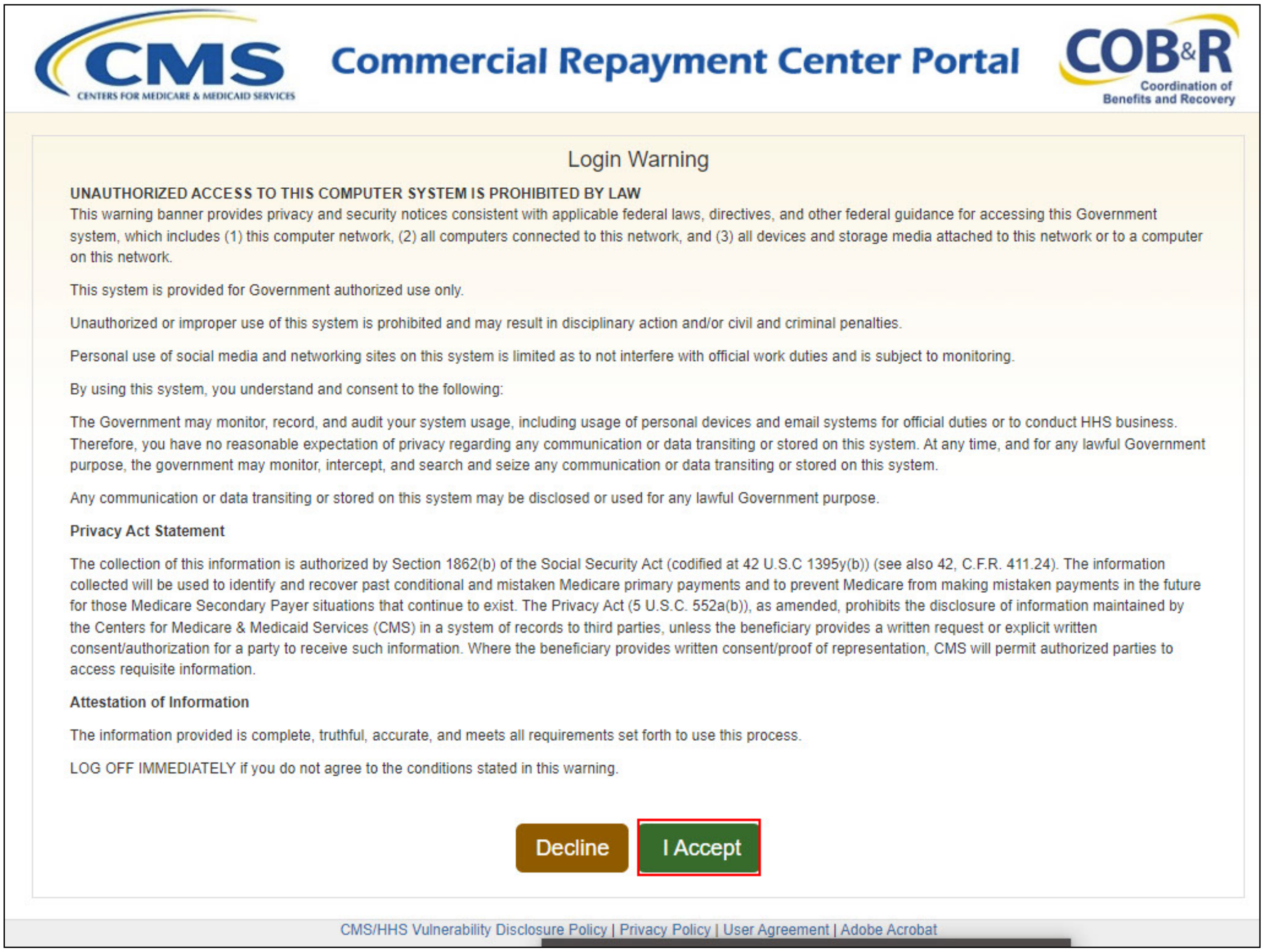
Successfully completed the ID Proofing process,

Registered and activated one or more Factors, and

Have at least one Factor ID in active status.

Note: In this case, the Next Step is replaced with the Factor Maintenance link. Click this link to activate or deactivate Factors.

Slide 13 of 40 - Login Warning Page



CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery

Login Warning

UNAUTHORIZED ACCESS TO THIS COMPUTER SYSTEM IS PROHIBITED BY LAW

This warning banner provides privacy and security notices consistent with applicable federal laws, directives, and other federal guidance for accessing this Government system, which includes (1) this computer network, (2) all computers connected to this network, and (3) all devices and storage media attached to this network or to a computer on this network.

This system is provided for Government authorized use only.

Unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties.

Personal use of social media and networking sites on this system is limited as to not interfere with official work duties and is subject to monitoring.

By using this system, you understand and consent to the following:

The Government may monitor, record, and audit your system usage, including usage of personal devices and email systems for official duties or to conduct HHS business. Therefore, you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this system. At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this system.

Any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose.

Privacy Act Statement

The collection of this information is authorized by Section 1862(b) of the Social Security Act (codified at 42 U.S.C 1395y(b)) (see also 42, C.F.R. 411.24). The information collected will be used to identify and recover past conditional and mistaken Medicare primary payments and to prevent Medicare from making mistaken payments in the future for those Medicare Secondary Payer situations that continue to exist. The Privacy Act (5 U.S.C. 552a(b)), as amended, prohibits the disclosure of information maintained by the Centers for Medicare & Medicaid Services (CMS) in a system of records to third parties, unless the beneficiary provides a written request or explicit written consent/authorization for a party to receive such information. Where the beneficiary provides written consent/proof of representation, CMS will permit authorized parties to access requisite information.

Attestation of Information

The information provided is complete, truthful, accurate, and meets all requirements set forth to use this process.

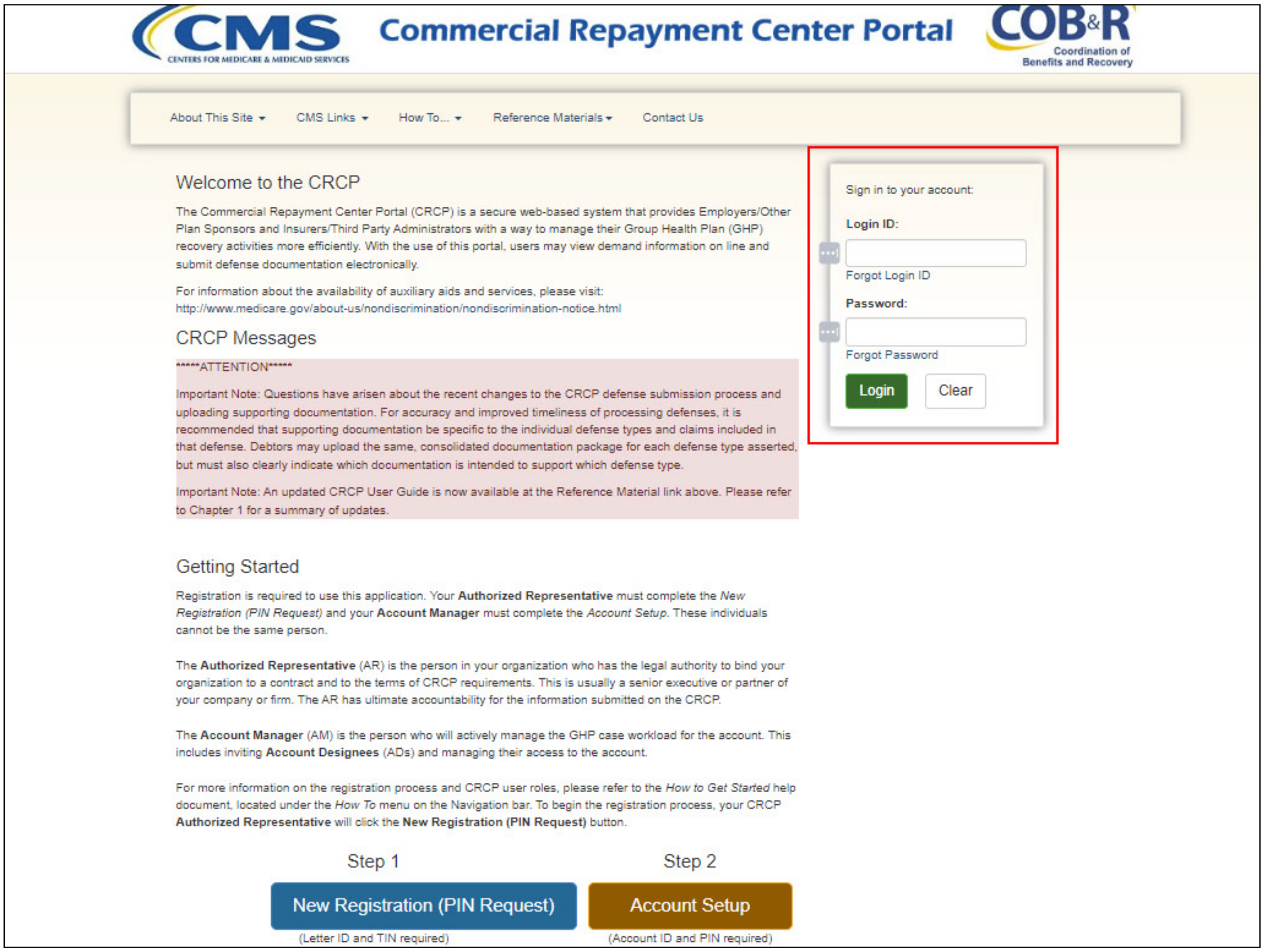
LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

Decline
I Accept
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Slide notes

Access the CRCP at the following link: https://www.cob.cms.hhs.gov/CRCP/. The Login Warning page will appear. After reviewing the User Agreement, click “I Accept” to continue.

Slide 14 of 40 - Welcome to the CRCP


CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Login
Clear
Step 1
New Registration (PIN Request)
Step 2
Account Setup

Sign in to your account:

Login ID:

Forgot Login ID

Password:

Forgot Password

Welcome to the CRCP

The Commercial Repayment Center Portal (CRCP) is a secure web-based system that provides Employers/Other Plan Sponsors and Insurers/Third Party Administrators with a way to manage their Group Health Plan (GHP) recovery activities more efficiently. With the use of this portal, users may view demand information on line and submit defense documentation electronically.

For information about the availability of auxiliary aids and services, please visit: http://www.medicare.gov/about-us/nondiscrimination/nondiscrimination-notice.html

CRCP Messages

*****ATTENTION*****

Important Note: Questions have arisen about the recent changes to the CRCP defense submission process and uploading supporting documentation. For accuracy and improved timeliness of processing defenses, it is recommended that supporting documentation be specific to the individual defense types and claims included in that defense. Debtors may upload the same, consolidated documentation package for each defense type asserted, but must also clearly indicate which documentation is intended to support which defense type.

Important Note: An updated CRCP User Guide is now available at the Reference Material link above. Please refer to Chapter 1 for a summary of updates.

Getting Started

Registration is required to use this application. Your **Authorized Representative** must complete the *New Registration (PIN Request)* and your **Account Manager** must complete the *Account Setup*. These individuals cannot be the same person.

The **Authorized Representative** (AR) is the person in your organization who has the legal authority to bind your organization to a contract and to the terms of CRCP requirements. This is usually a senior executive or partner of your company or firm. The AR has ultimate accountability for the information submitted on the CRCP.

The **Account Manager** (AM) is the person who will actively manage the GHP case workload for the account. This includes inviting **Account Designees** (ADs) and managing their access to the account.

For more information on the registration process and CRCP user roles, please refer to the *How to Get Started* help document, located under the *How To* menu on the Navigation bar. To begin the registration process, your CRCP **Authorized Representative** will click the **New Registration (PIN Request)** button.

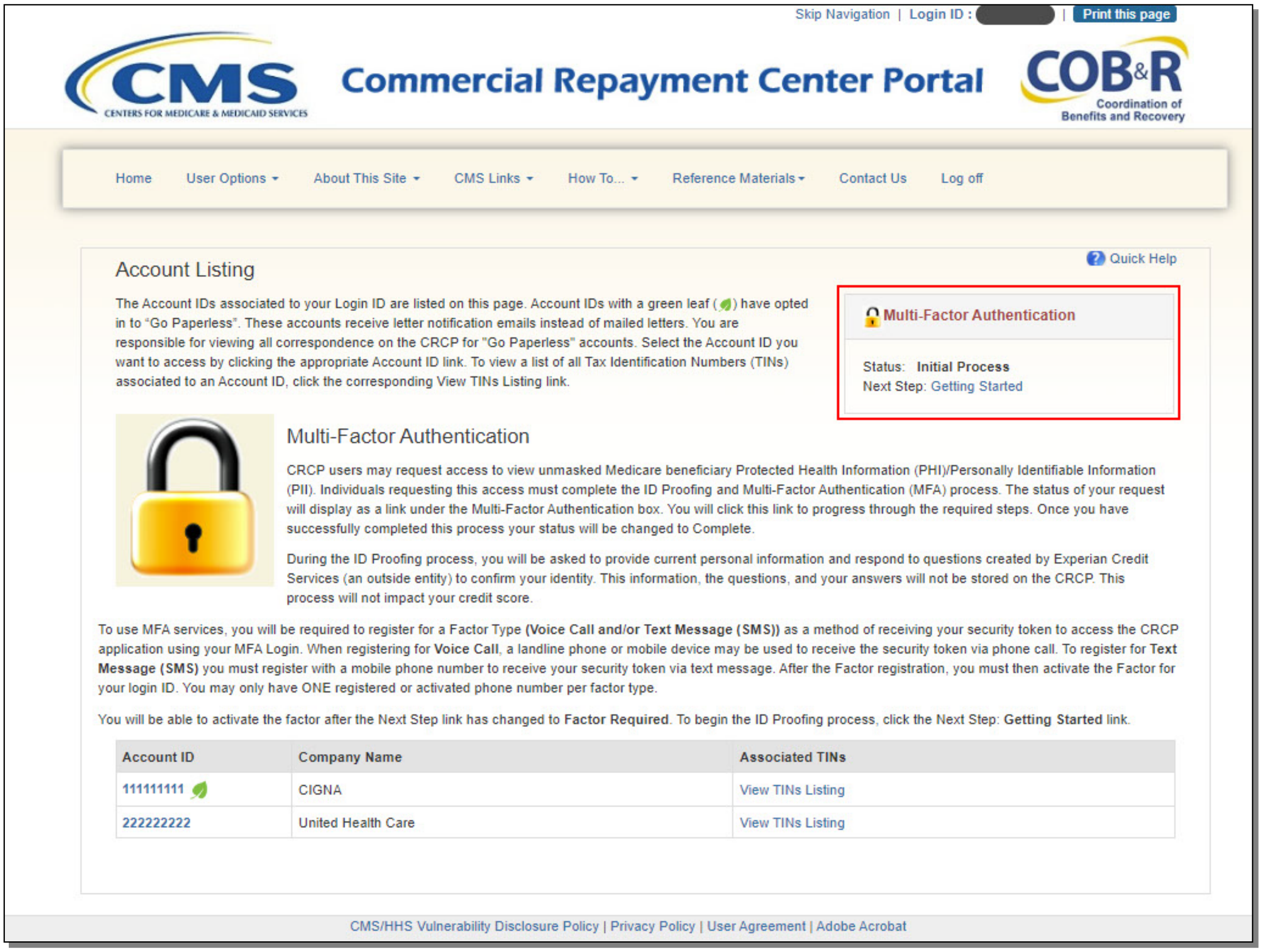
(Letter ID and TIN required)

(Account ID and PIN required)

Slide notes

The Welcome to the CRCP page will display along with a section to sign into your account.

Slide 15 of 40 - Account Listing Page



Skip Navigation | Login ID : [redacted] | Print this page
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
Home
User Options
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Log off
Quick Help

Account Listing

The Account IDs associated to your Login ID are listed on this page. Account IDs with a green leaf (🍃) have opted in to "Go Paperless". These accounts receive letter notification emails instead of mailed letters. You are responsible for viewing all correspondence on the CRCP for "Go Paperless" accounts. Select the Account ID you want to access by clicking the appropriate Account ID link. To view a list of all Tax Identification Numbers (TINs) associated to an Account ID, click the corresponding View TINs Listing link.

Multi-Factor Authentication

Status: **Initial Process**
Next Step: Getting Started

Multi-Factor Authentication

CRCP users may request access to view unmasked Medicare beneficiary Protected Health Information (PHI)/Personally Identifiable Information (PII). Individuals requesting this access must complete the ID Proofing and Multi-Factor Authentication (MFA) process. The status of your request will display as a link under the Multi-Factor Authentication box. You will click this link to progress through the required steps. Once you have successfully completed this process your status will be changed to Complete.

During the ID Proofing process, you will be asked to provide current personal information and respond to questions created by Experian Credit Services (an outside entity) to confirm your identity. This information, the questions, and your answers will not be stored on the CRCP. This process will not impact your credit score.

To use MFA services, you will be required to register for a Factor Type **(Voice Call and/or Text Message (SMS))** as a method of receiving your security token to access the CRCP application using your MFA Login. When registering for **Voice Call**, a landline phone or mobile device may be used to receive the security token via phone call. To register for **Text Message (SMS)** you must register with a mobile phone number to receive your security token via text message. After the Factor registration, you must then activate the Factor for your login ID. You may only have ONE registered or activated phone number per factor type.

You will be able to activate the factor after the Next Step link has changed to **Factor Required**. To begin the ID Proofing process, click the Next Step: **Getting Started** link.

Account ID	Company Name	Associated TINs
111111111 🍃	CIGNA	View TINs Listing
222222222	United Health Care	View TINs Listing

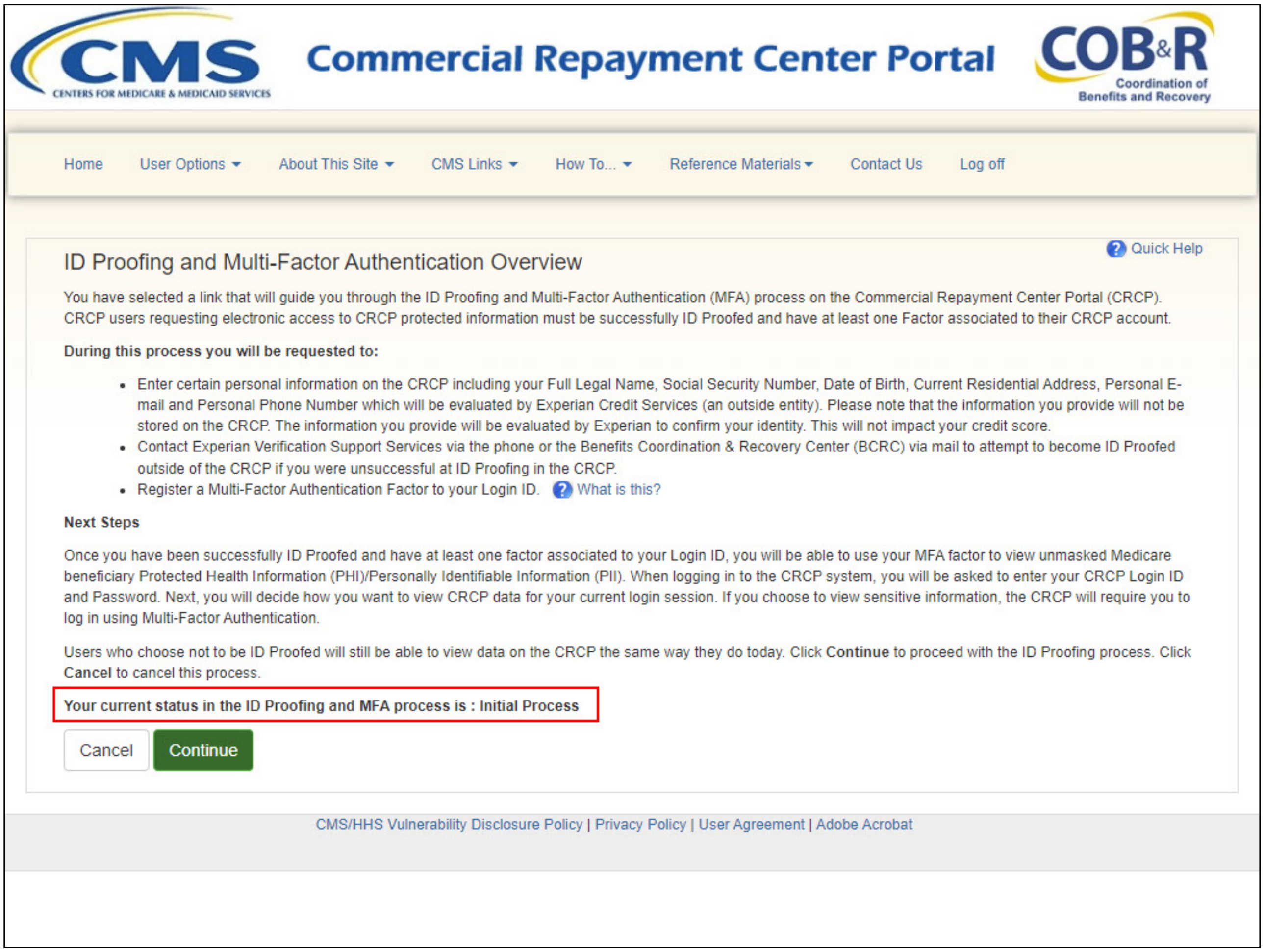
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Slide notes

The Multi-Factor Authentication section of the home page is used for the ID Proofing and MFA process.

To begin the ID Proofing process, click the Getting Started link on your home page.

Slide 16 of 40 - ID Proofing and Multi-Factor Authentication Overview Page


CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
Home
User Options
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Log off
Quick Help

ID Proofing and Multi-Factor Authentication Overview

You have selected a link that will guide you through the ID Proofing and Multi-Factor Authentication (MFA) process on the Commercial Repayment Center Portal (CRCP). CRCP users requesting electronic access to CRCP protected information must be successfully ID Proofed and have at least one Factor associated to their CRCP account.

During this process you will be requested to:

- Enter certain personal information on the CRCP including your Full Legal Name, Social Security Number, Date of Birth, Current Residential Address, Personal E-mail and Personal Phone Number which will be evaluated by Experian Credit Services (an outside entity). Please note that the information you provide will not be stored on the CRCP. The information you provide will be evaluated by Experian to confirm your identity. This will not impact your credit score.
- Contact Experian Verification Support Services via the phone or the Benefits Coordination & Recovery Center (BCRC) via mail to attempt to become ID Proofed outside of the CRCP if you were unsuccessful at ID Proofing in the CRCP.
- Register a Multi-Factor Authentication Factor to your Login ID. What is this?

Next Steps

Once you have been successfully ID Proofed and have at least one factor associated to your Login ID, you will be able to use your MFA factor to view unmasked Medicare beneficiary Protected Health Information (PHI)/Personally Identifiable Information (PII). When logging in to the CRCP system, you will be asked to enter your CRCP Login ID and Password. Next, you will decide how you want to view CRCP data for your current login session. If you choose to view sensitive information, the CRCP will require you to log in using Multi-Factor Authentication.

Users who choose not to be ID Proofed will still be able to view data on the CRCP the same way they do today. Click **Continue** to proceed with the ID Proofing process. Click **Cancel** to cancel this process.

Your current status in the ID Proofing and MFA process is : Initial Process

Cancel
Continue
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

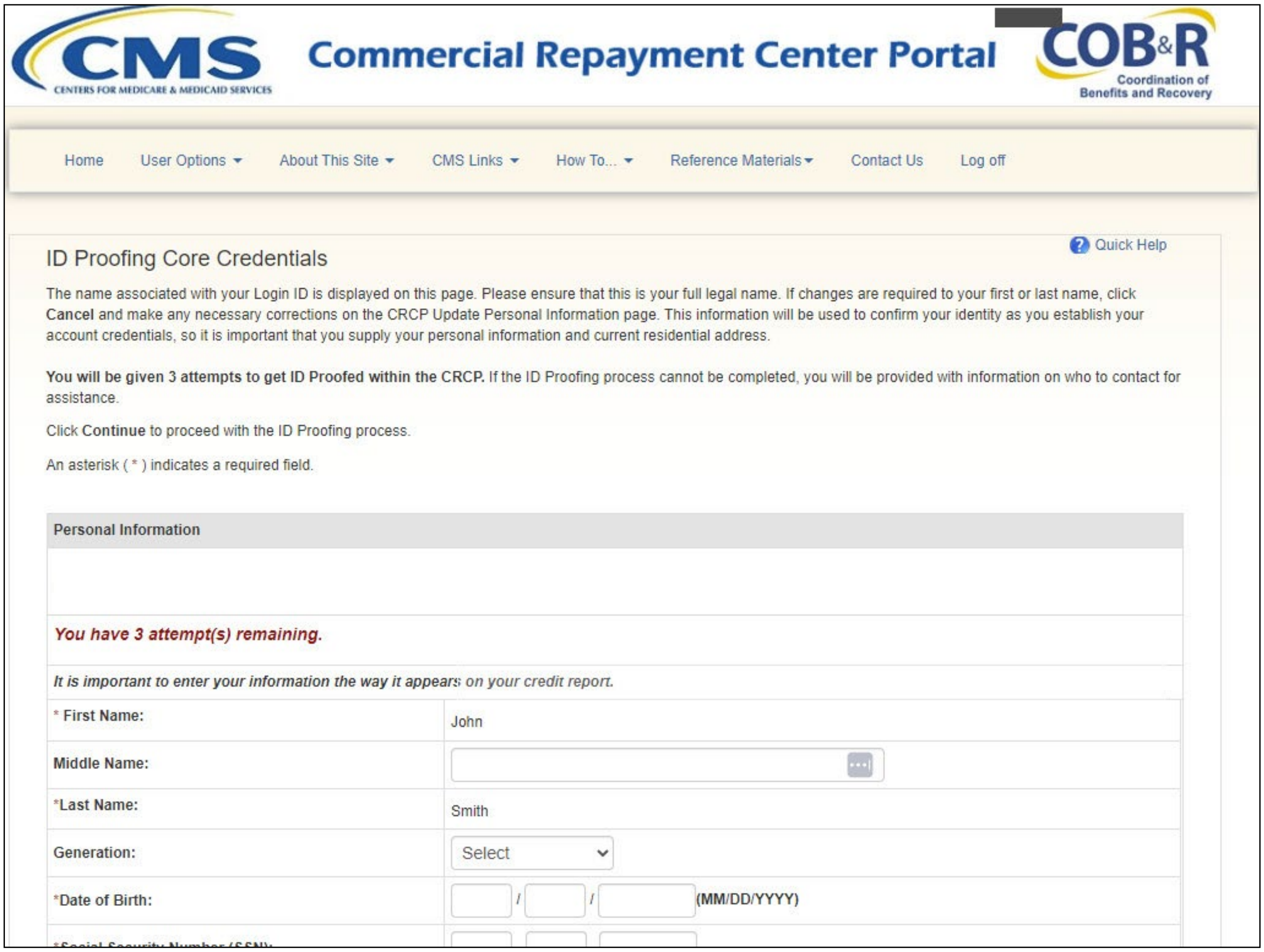
Slide notes

The ID Proofing and Multi-Factor Authentication Overview page appears.

This page provides general information about the process and its purpose. It also displays your current MFA status.

Click Continue to proceed.

Slide 17 of 40- ID Proofing Core Credentials Page


CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
Home
User Options
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Log off
Quick Help

ID Proofing Core Credentials

The name associated with your Login ID is displayed on this page. Please ensure that this is your full legal name. If changes are required to your first or last name, click **Cancel** and make any necessary corrections on the CRCP Update Personal Information page. This information will be used to confirm your identity as you establish your account credentials, so it is important that you supply your personal information and current residential address.

You will be given 3 attempts to get ID Proofed within the CRCP. If the ID Proofing process cannot be completed, you will be provided with information on who to contact for assistance.

Click **Continue** to proceed with the ID Proofing process.

An asterisk (*) indicates a required field.

Personal Information

You have 3 attempt(s) remaining.

It is important to enter your information the way it appears on your credit report.

* First Name:	John
Middle Name:	
*Last Name:	Smith
Generation:	Select
*Date of Birth:	/ / (MM/DD/YYYY)
*Social Security Number (SSN):	

Slide notes

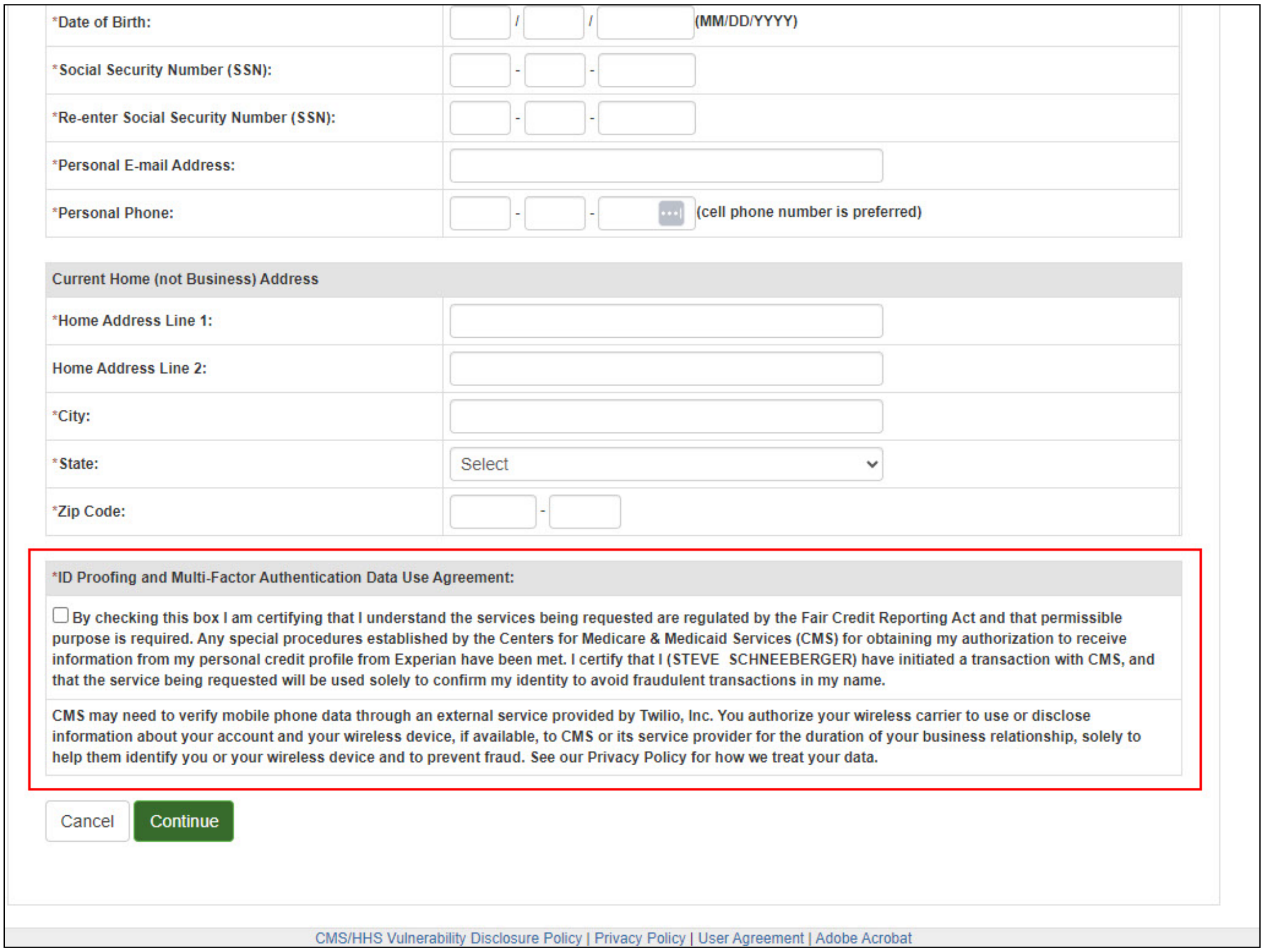
The ID Proofing Core Credentials page appears.

This page requires you to enter personal information.

The First and Last Name fields are pre-filled by the system and are the ones associated to your Login ID. If corrections are required, click Cancel on this page and make any necessary changes on the CRCP Update Personal Information page.

See the User Maintenance CBT for more information.

Slide 18 of 40 - ID Proofing and Multi-Factor Authentication Data Use Agreement



*Date of Birth:	/ / (MM/DD/YYYY)
*Social Security Number (SSN):	- -
*Re-enter Social Security Number (SSN):	- -
*Personal E-mail Address:	
*Personal Phone:	- - (cell phone number is preferred)

Current Home (not Business) Address

*Home Address Line 1:	
Home Address Line 2:	
*City:	
*State:	Select
*Zip Code:	-

*ID Proofing and Multi-Factor Authentication Data Use Agreement:

☐ By checking this box I am certifying that I understand the services being requested are regulated by the Fair Credit Reporting Act and that permissible purpose is required. Any special procedures established by the Centers for Medicare & Medicaid Services (CMS) for obtaining my authorization to receive information from my personal credit profile from Experian have been met. I certify that I (STEVE SCHNEEBERGER) have initiated a transaction with CMS, and that the service being requested will be used solely to confirm my identity to avoid fraudulent transactions in my name.

CMS may need to verify mobile phone data through an external service provided by Twilio, Inc. You authorize your wireless carrier to use or disclose information about your account and your wireless device, if available, to CMS or its service provider for the duration of your business relationship, solely to help them identify you or your wireless device and to prevent fraud. See our Privacy Policy for how we treat your data.

Cancel
Continue
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

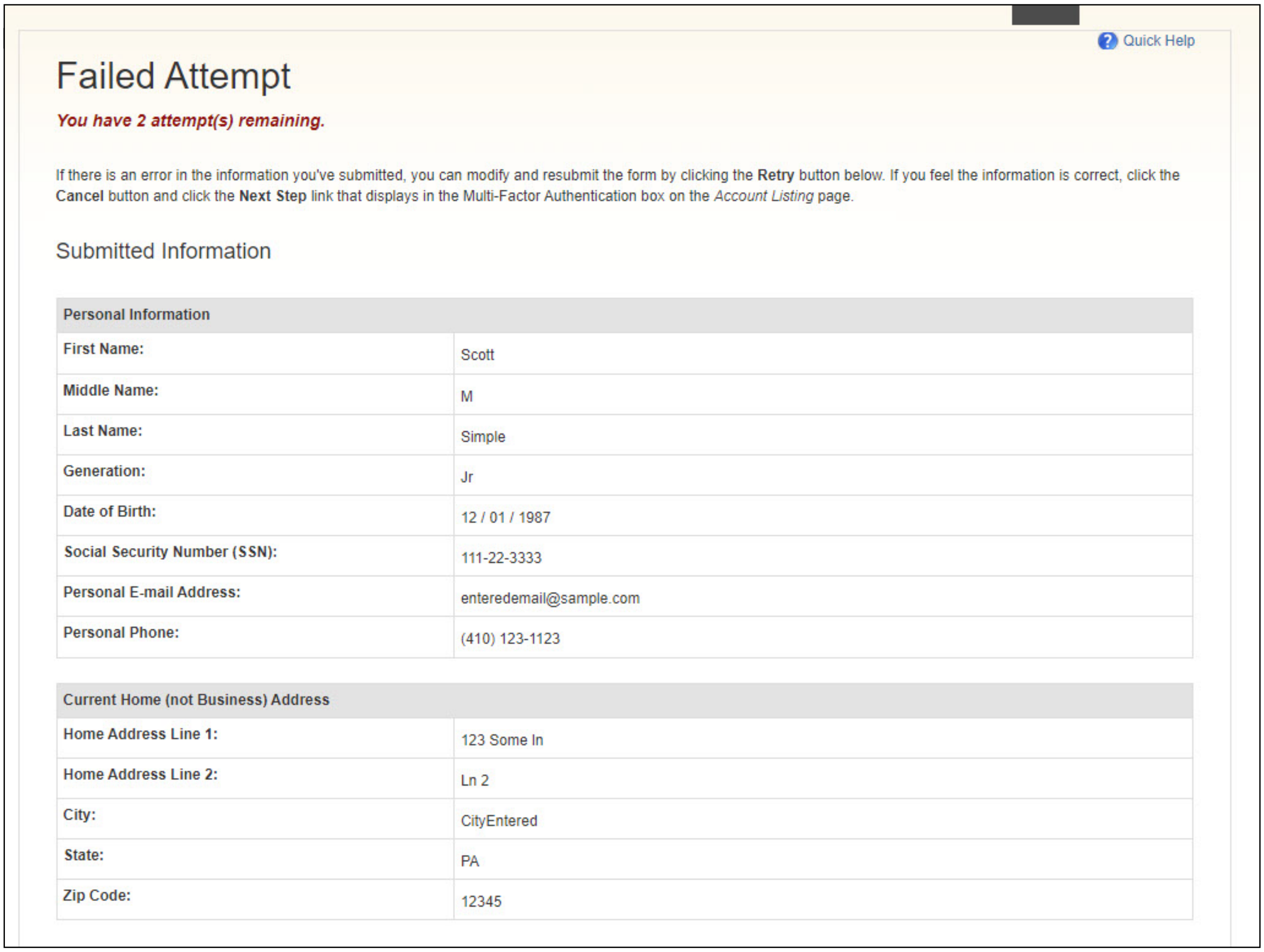
Slide notes

The address information entered on this page should match your current residential address so Experian can verify your identity.

Successful ID proofing hinges upon Experian being able to use the address you provide to match to the address they have on file for you. Once all required information has been entered, check the Data Use Agreement box, and click Continue to submit your information to Experian Credit Services to be validated.

Note: Before you click Continue, ensure that your First and Last Names are correct and that they match your full legal name. If there is an error in the information you've submitted the Failed Attempt page will appear.

Slide 19 of 40 - Contact Experian



Failed Attempt

You have 2 attempt(s) remaining.

If there is an error in the information you've submitted, you can modify and resubmit the form by clicking the **Retry** button below. If you feel the information is correct, click the **Cancel** button and click the **Next Step** link that displays in the Multi-Factor Authentication box on the *Account Listing* page.

Submitted Information

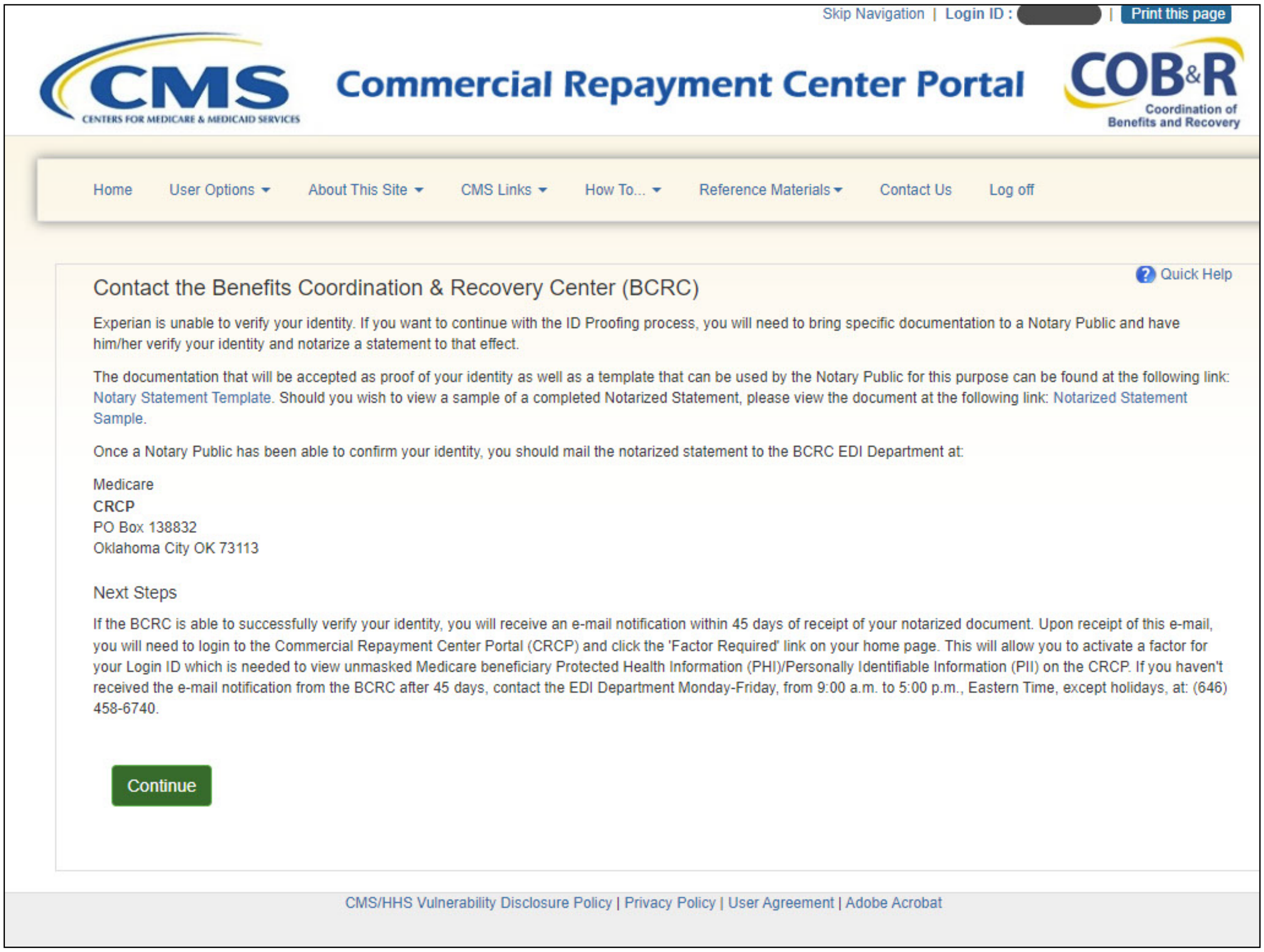
Personal Information	
First Name:	Scott
Middle Name:	M
Last Name:	Simple
Generation:	Jr
Date of Birth:	12 / 01 / 1987
Social Security Number (SSN):	111-22-3333
Personal E-mail Address:	enteredemail@sample.com
Personal Phone:	(410) 123-1123

Current Home (not Business) Address	
Home Address Line 1:	123 Some ln
Home Address Line 2:	Ln 2
City:	CityEntered
State:	PA
Zip Code:	12345

Slide notes

The Failed Attempt page will allow you to modify and submit the form.

Slide 20 of 40 - Contact the Benefits Coordination & Recovery Center Page


Skip Navigation | Login ID : [redacted] | Print this page
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
Home
User Options
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Log off
Quick Help
Continue
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Contact the Benefits Coordination & Recovery Center (BCRC)

Experian is unable to verify your identity. If you want to continue with the ID Proofing process, you will need to bring specific documentation to a Notary Public and have him/her verify your identity and notarize a statement to that effect.

The documentation that will be accepted as proof of your identity as well as a template that can be used by the Notary Public for this purpose can be found at the following link: Notary Statement Template. Should you wish to view a sample of a completed Notarized Statement, please view the document at the following link: Notarized Statement Sample.

Once a Notary Public has been able to confirm your identity, you should mail the notarized statement to the BCRC EDI Department at:

Medicare
CRCP
PO Box 138832
Oklahoma City OK 73113

Next Steps

If the BCRC is able to successfully verify your identity, you will receive an e-mail notification within 45 days of receipt of your notarized document. Upon receipt of this e-mail, you will need to login to the Commercial Repayment Center Portal (CRCP) and click the 'Factor Required' link on your home page. This will allow you to activate a factor for your Login ID which is needed to view unmasked Medicare beneficiary Protected Health Information (PHI)/Personally Identifiable Information (PII) on the CRCP. If you haven't received the e-mail notification from the BCRC after 45 days, contact the EDI Department Monday-Friday, from 9:00 a.m. to 5:00 p.m., Eastern Time, except holidays, at: (646) 458-6740.

Slide notes

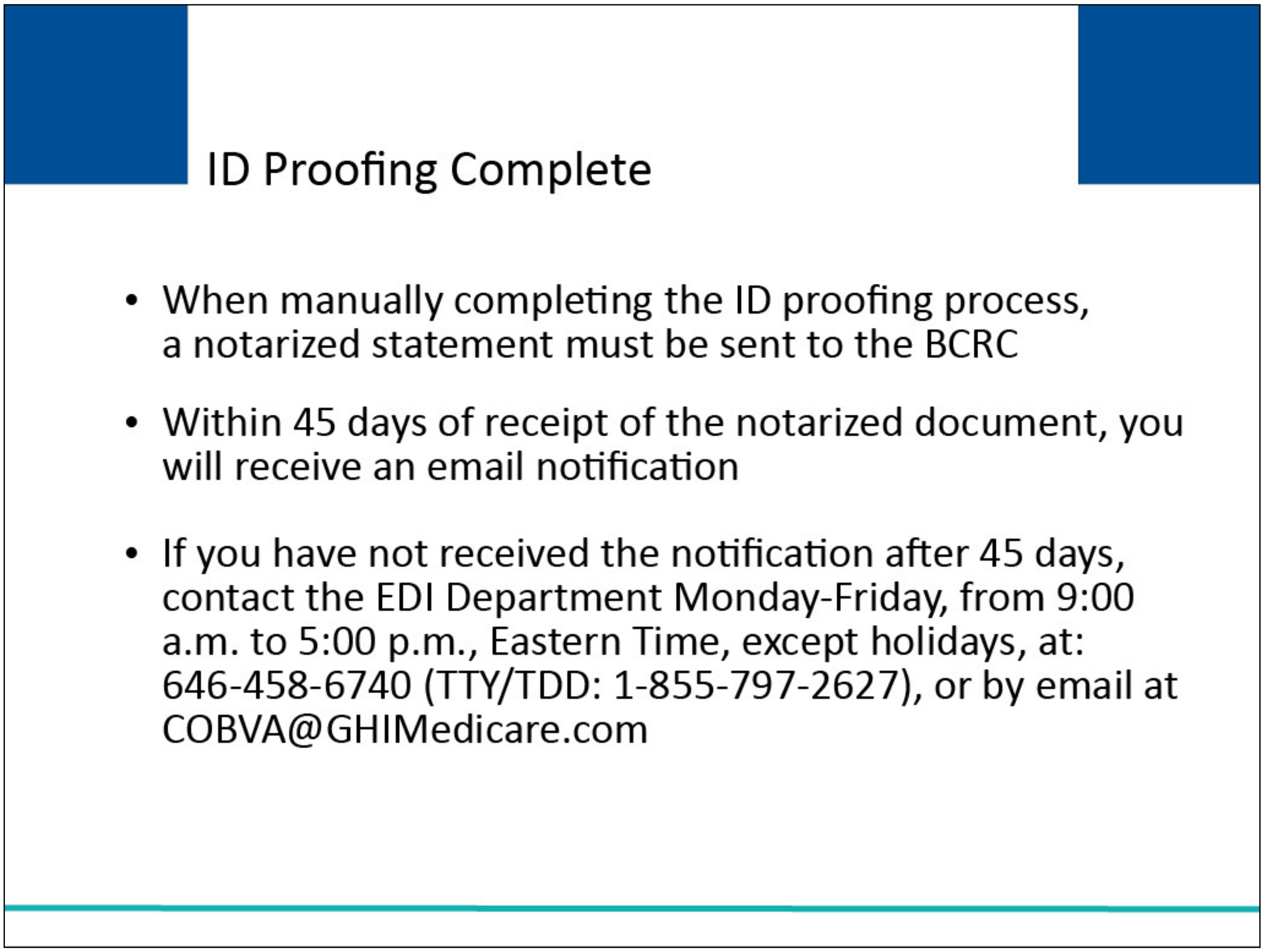
If you still want to continue with the ID Proofing process, you will need to bring specific documentation to a Notary Public and have that individual verify your identity and notarize a statement to that effect.

You will then need to send your documentation to the BCRC and have an EDI representative manually complete ID Proofing for you.

When you click the Contact BCRC link, the Contact the Benefits Coordination & Recovery Center (BCRC) page appears.

This page provides information for contacting the BCRC so you can complete the ID Proofing process through a manual process external to the CRCP.

Slide 21 of 40 - ID Proofing Complete



ID Proofing Complete

- When manually completing the ID proofing process, a notarized statement must be sent to the BCRC
- Within 45 days of receipt of the notarized document, you will receive an email notification
- If you have not received the notification after 45 days, contact the EDI Department Monday-Friday, from 9:00 a.m. to 5:00 p.m., Eastern Time, except holidays, at: 646-458-6740 (TTY/TDD: 1-855-797-2627), or by email at COBVA@GHIMedicare.com

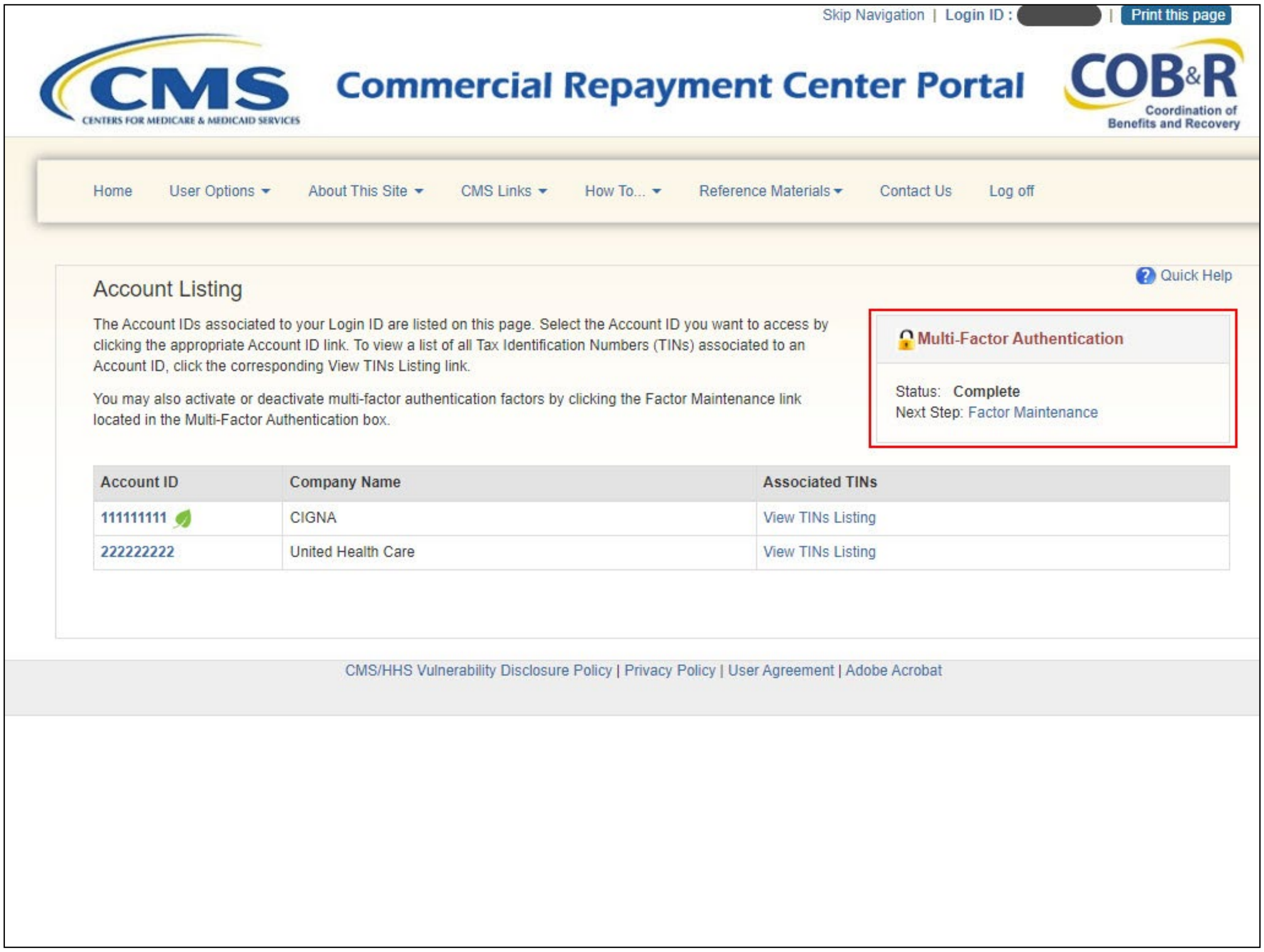
Slide notes

When manually completing the ID proofing process, a notarized statement must be sent to the BCRC.

Within 45 days of receipt of the notarized document, you will receive an email notification.

If you have not received the notification after 45 days, contact the EDI Department Monday-Friday, from 9:00 a.m. to 5:00 p.m., Eastern Time, except holidays, at: 646-458-6740 (TTY/TDD: 1-855-797-2627), or by email at COBVA@GHIMedicare.com.

Slide 22 of 40 - Account Listing Page


Skip Navigation | Login ID : [redacted] | Print this page
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
Home
User Options
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Log off
Quick Help

Account Listing

The Account IDs associated to your Login ID are listed on this page. Select the Account ID you want to access by clicking the appropriate Account ID link. To view a list of all Tax Identification Numbers (TINs) associated to an Account ID, click the corresponding View TINs Listing link.

You may also activate or deactivate multi-factor authentication factors by clicking the Factor Maintenance link located in the Multi-Factor Authentication box.

Multi-Factor Authentication

Status: **Complete**
Next Step: Factor Maintenance

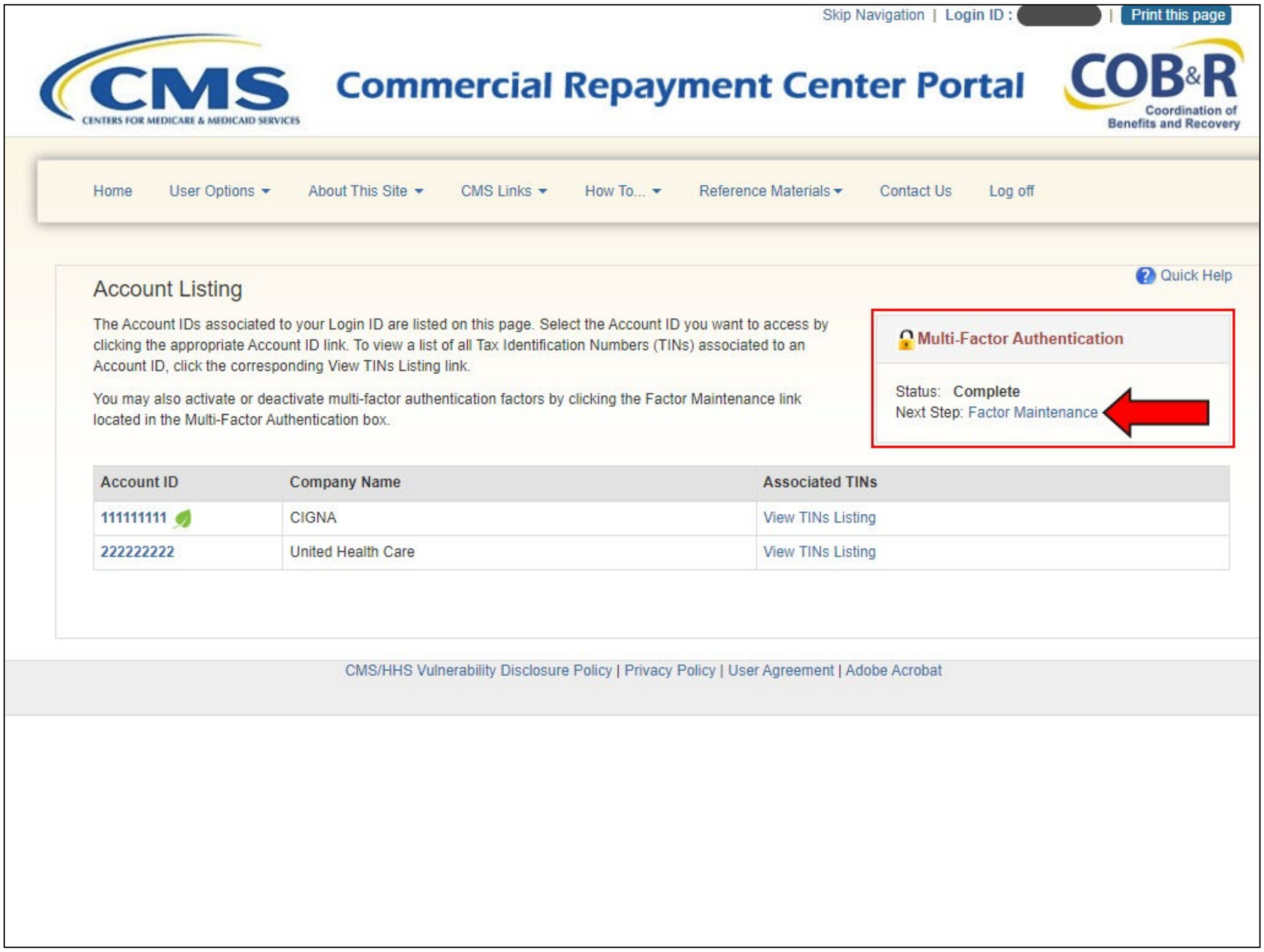
Account ID	Company Name	Associated TINs
111111111	CIGNA	View TINs Listing
222222222	United Health Care	View TINs Listing

CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Slide notes

Once you have been ID proofed, the status of your request will display as a link under the Multi-Factor Authentication box.

Slide 23 of 40 - Account Listing Page



Skip Navigation | Login ID : [redacted] | Print this page
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
Home
User Options
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Log off
Quick Help

Account Listing

The Account IDs associated to your Login ID are listed on this page. Select the Account ID you want to access by clicking the appropriate Account ID link. To view a list of all Tax Identification Numbers (TINs) associated to an Account ID, click the corresponding View TINs Listing link.

You may also activate or deactivate multi-factor authentication factors by clicking the Factor Maintenance link located in the Multi-Factor Authentication box.

Multi-Factor Authentication

Status: Complete
Next Step: Factor Maintenance

Account ID	Company Name	Associated TINs
111111111	CIGNA	View TINs Listing
222222222	United Health Care	View TINs Listing

CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Slide notes

To use MFA services, you will be required to register for a Factor Type (Voice Call and/or SMS (Text Messaging)) as a method of receiving your security token to access the CRCP application using your MFA Login.

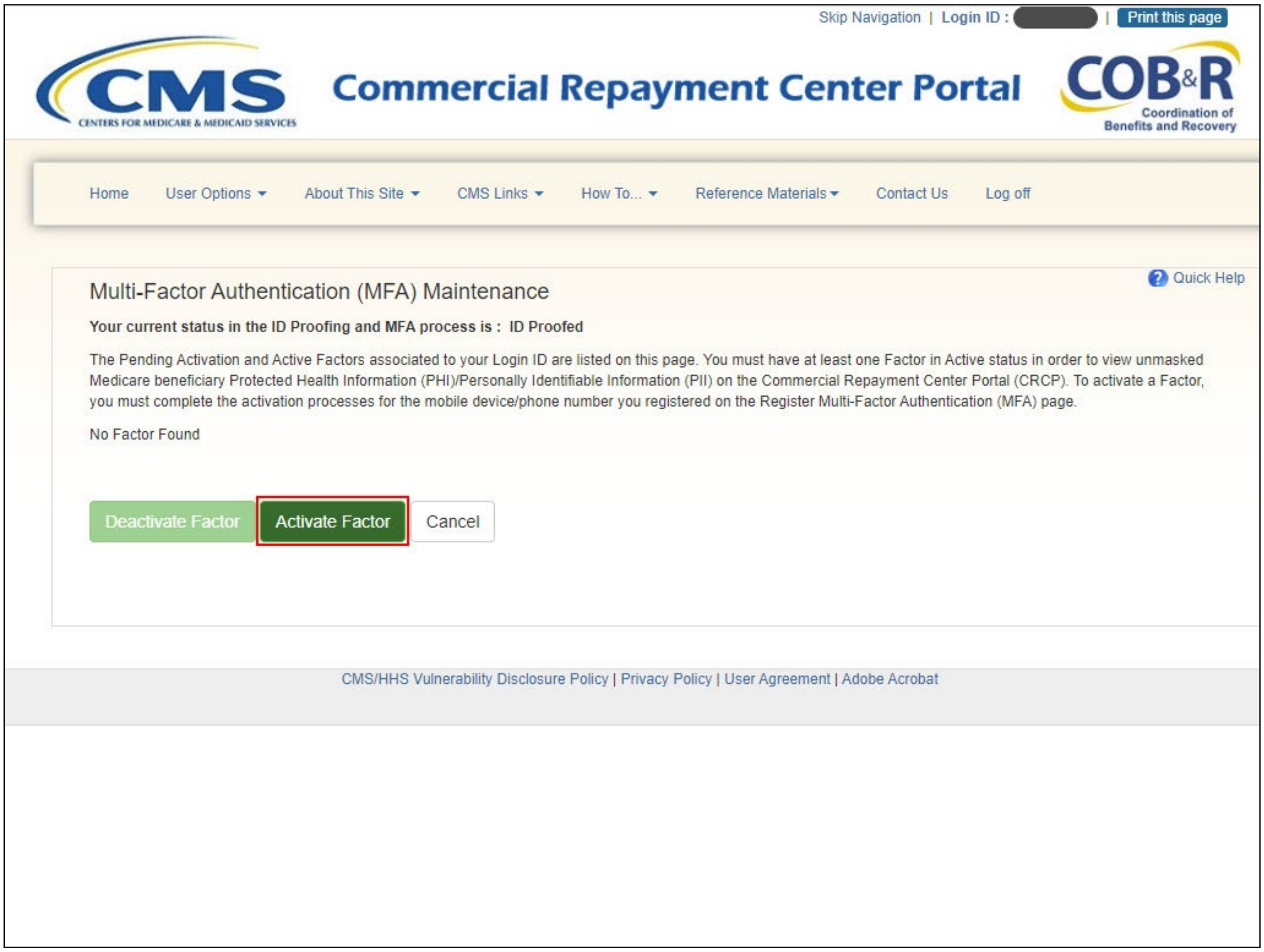
When registering for Voice Call, a landline phone or mobile device may be used to receive the security token via phone call. To register for SMS (Text Messaging) you must register with a mobile phone number in order to receive your security token via text message.

After the Factor registration, you then must activate the Factor for your login ID. You may only have ONE registered or activated phone number per factor type.

Click the Factor Required link to progress through the required steps.

Once you have successfully completed the process your status will be changed to Complete.

Slide 24 of 40- Multi-Factor Authentication Maintenance Page


Skip Navigation | Login ID : [redacted] | Print this page
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
Home
User Options
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Log off
Quick Help

Multi-Factor Authentication (MFA) Maintenance

Your current status in the ID Proofing and MFA process is : ID Proofed

The Pending Activation and Active Factors associated to your Login ID are listed on this page. You must have at least one Factor in Active status in order to view unmasked Medicare beneficiary Protected Health Information (PHI)/Personally Identifiable Information (PII) on the Commercial Repayment Center Portal (CRCP). To activate a Factor, you must complete the activation processes for the mobile device/phone number you registered on the Register Multi-Factor Authentication (MFA) page.

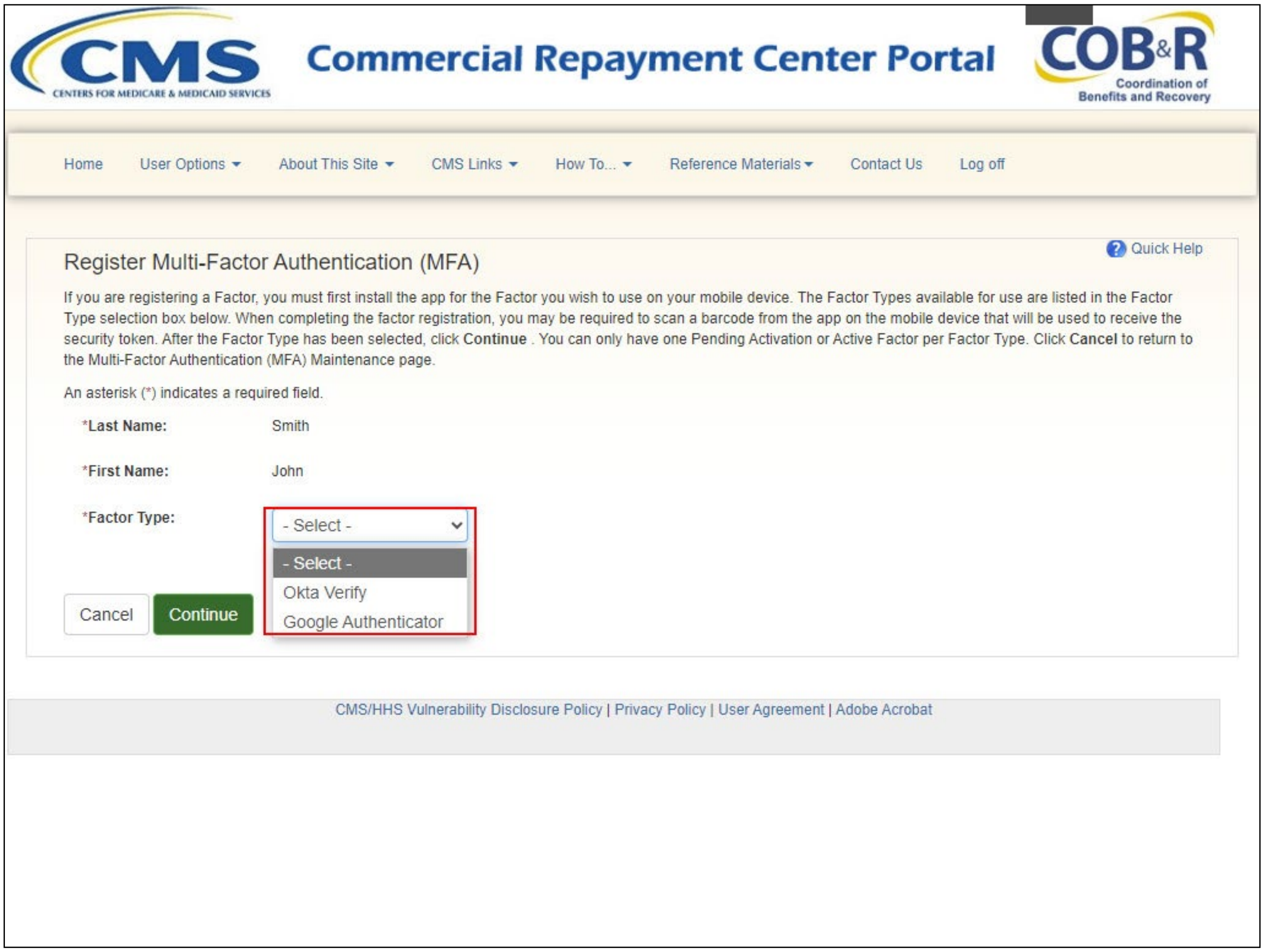
No Factor Found

Deactivate Factor
Activate Factor
Cancel
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Slide notes

Click Activate Factor.

Slide 25 of 40 - Register Multi-Factor Authentication Page



Register Multi-Factor Authentication (MFA)

If you are registering a Factor, you must first install the app for the Factor you wish to use on your mobile device. The Factor Types available for use are listed in the Factor Type selection box below. When completing the factor registration, you may be required to scan a barcode from the app on the mobile device that will be used to receive the security token. After the Factor Type has been selected, click **Continue** . You can only have one Pending Activation or Active Factor per Factor Type. Click **Cancel** to return to the Multi-Factor Authentication (MFA) Maintenance page.

An asterisk (*) indicates a required field.

***Last Name:**	Smith
***First Name:**	John
***Factor Type:**	- Select -

- Select -
Okta Verify
Google Authenticator
Cancel
Continue
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

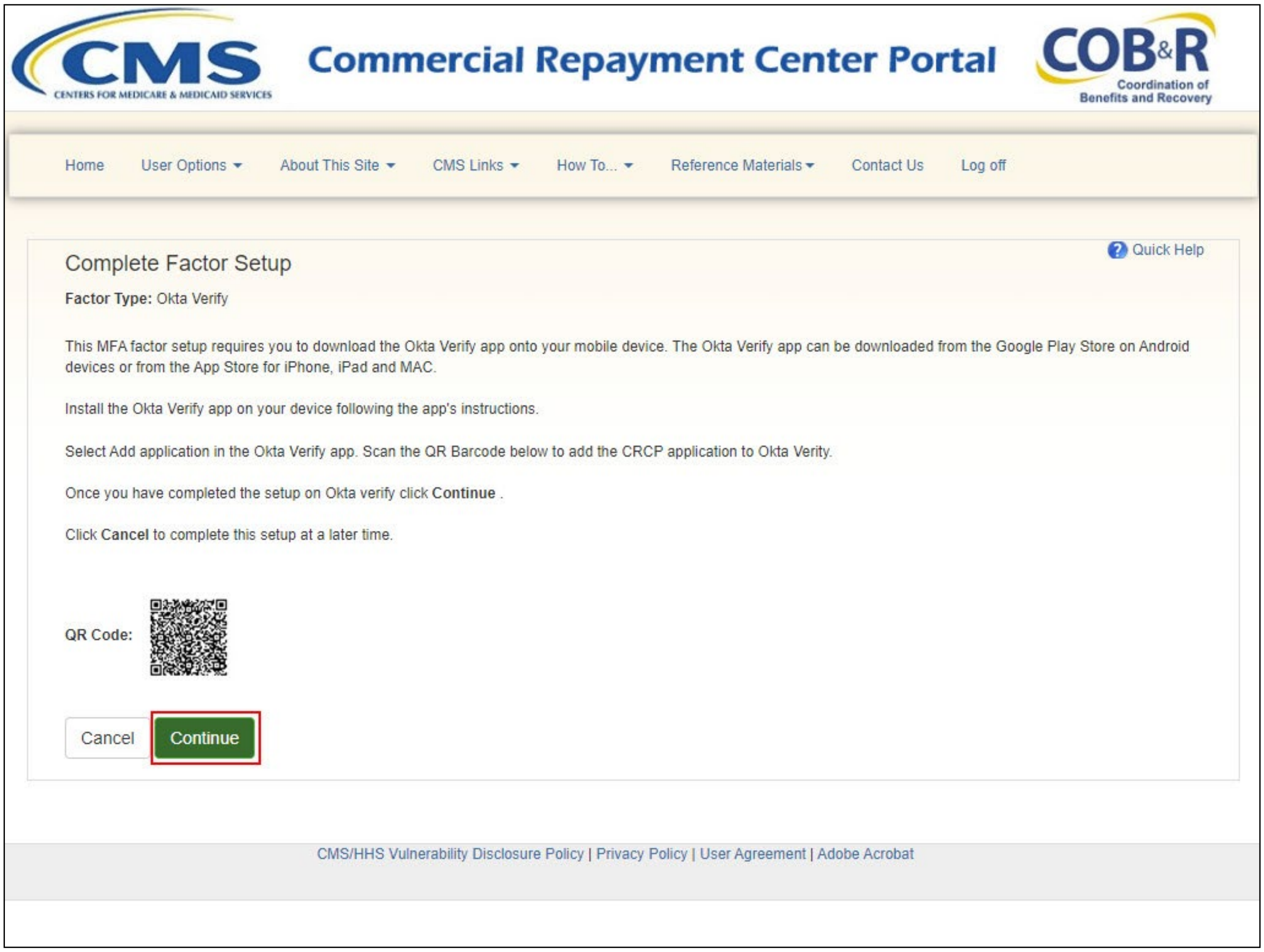
Slide notes

Select Factor Type.

You can select Okta Verify or Google Authenticator.

Then click Continue.

Slide 26 of 40 - Activate Factor Page



CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
Home
User Options
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Log off
Quick Help

Complete Factor Setup

Factor Type: Okta Verify

This MFA factor setup requires you to download the Okta Verify app onto your mobile device. The Okta Verify app can be downloaded from the Google Play Store on Android devices or from the App Store for iPhone, iPad and MAC.

Install the Okta Verify app on your device following the app's instructions.

Select Add application in the Okta Verify app. Scan the QR Barcode below to add the CRCP application to Okta Verity.

Once you have completed the setup on Okta verify click **Continue** .

Click **Cancel** to complete this setup at a later time.

QR Code:

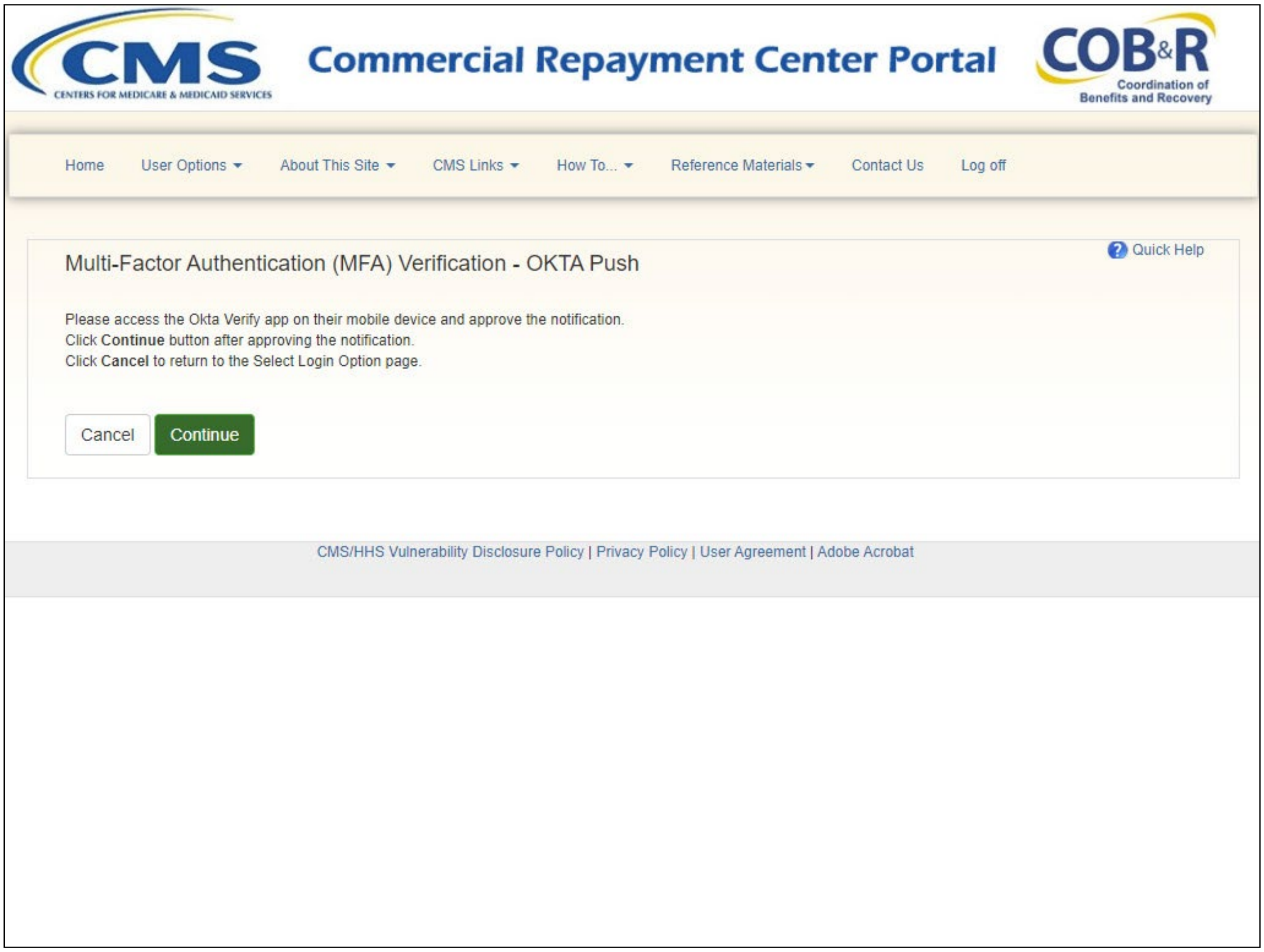
Cancel
Continue
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Slide notes

The Complete Factor Setup page will appear.

Follow the instructions for the MFA factor you chose. Then click Continue.

Slide 27 of 40 - Multi-Factor Authentication (MFA) Verification – OKTA Push Page


CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
Home
User Options
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Log off
Quick Help
Cancel
Continue
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

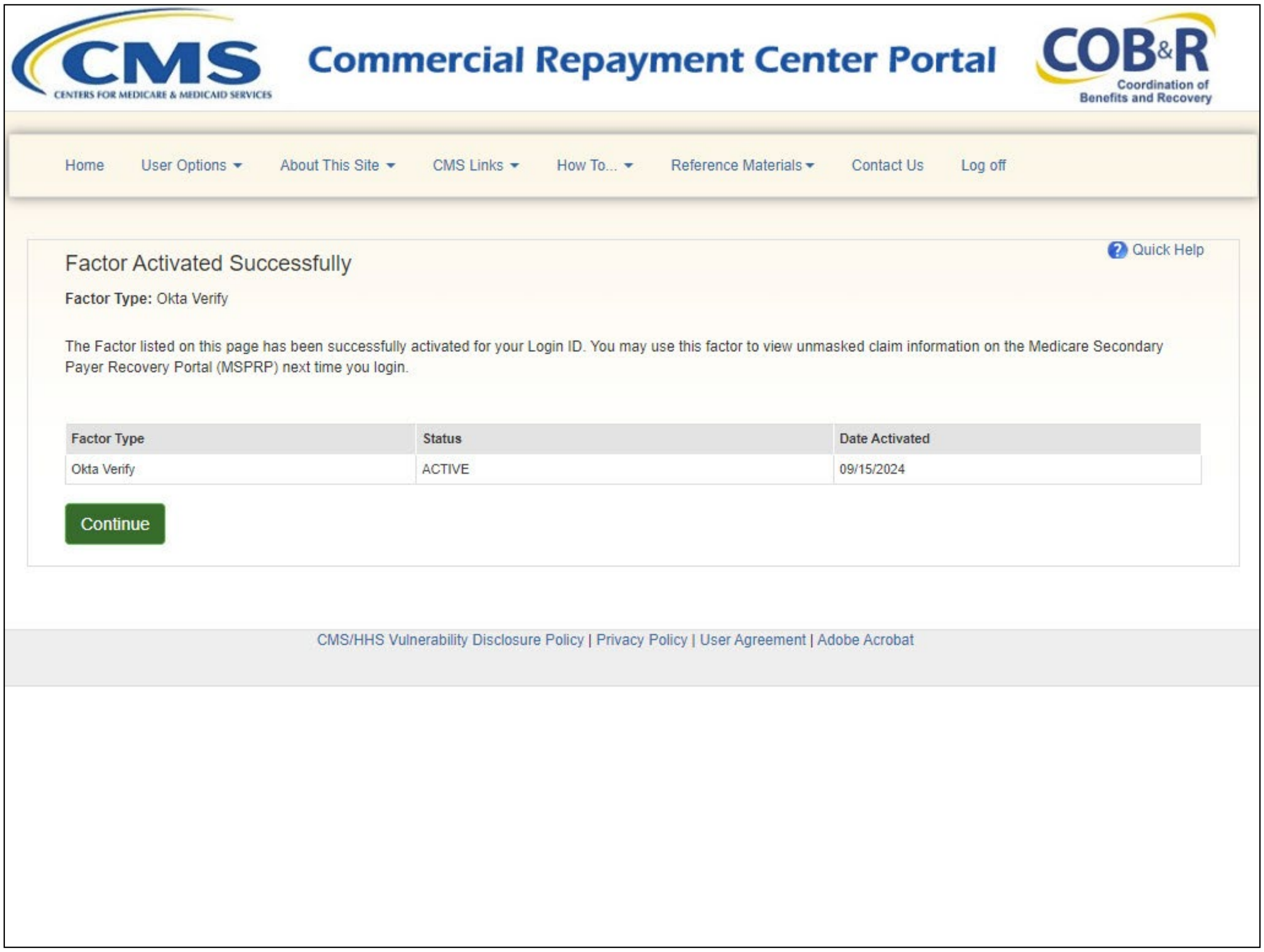
Multi-Factor Authentication (MFA) Verification - OKTA Push

Please access the Okta Verify app on their mobile device and approve the notification.
Click **Continue** button after approving the notification.
Click **Cancel** to return to the Select Login Option page.

Slide notes

Select Continue after approving the notification.

Slide 28 of 40 – Factor Activated Successfully Page


Commercial Repayment Center Portal
Home
User Options
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Log off
Quick Help
Continue
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Factor Activated Successfully

Factor Type: Okta Verify

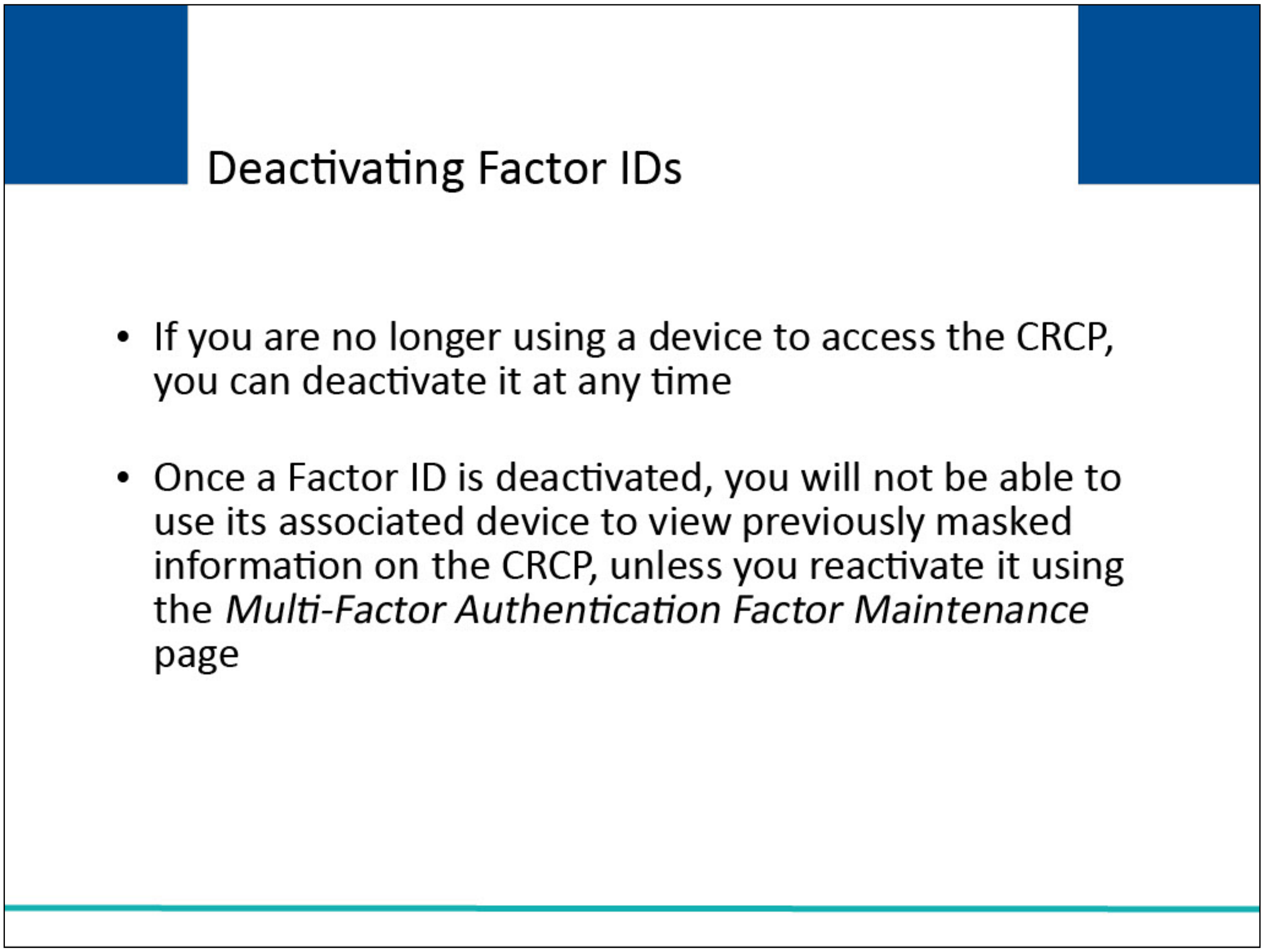
The Factor listed on this page has been successfully activated for your Login ID. You may use this factor to view unmasked claim information on the Medicare Secondary Payer Recovery Portal (MSPRP) next time you login.

Factor Type	Status	Date Activated
Okta Verify	ACTIVE	09/15/2024

Slide notes

The Factor Activated Successfully page will appear showing the Factor Type, Status, and Date Activated.

Slide 29 of 40 - Deactivating Factor IDs



Deactivating Factor IDs

- If you are no longer using a device to access the CRCP, you can deactivate it at any time
- Once a Factor ID is deactivated, you will not be able to use its associated device to view previously masked information on the CRCP, unless you reactivate it using the *Multi-Factor Authentication Factor Maintenance* page

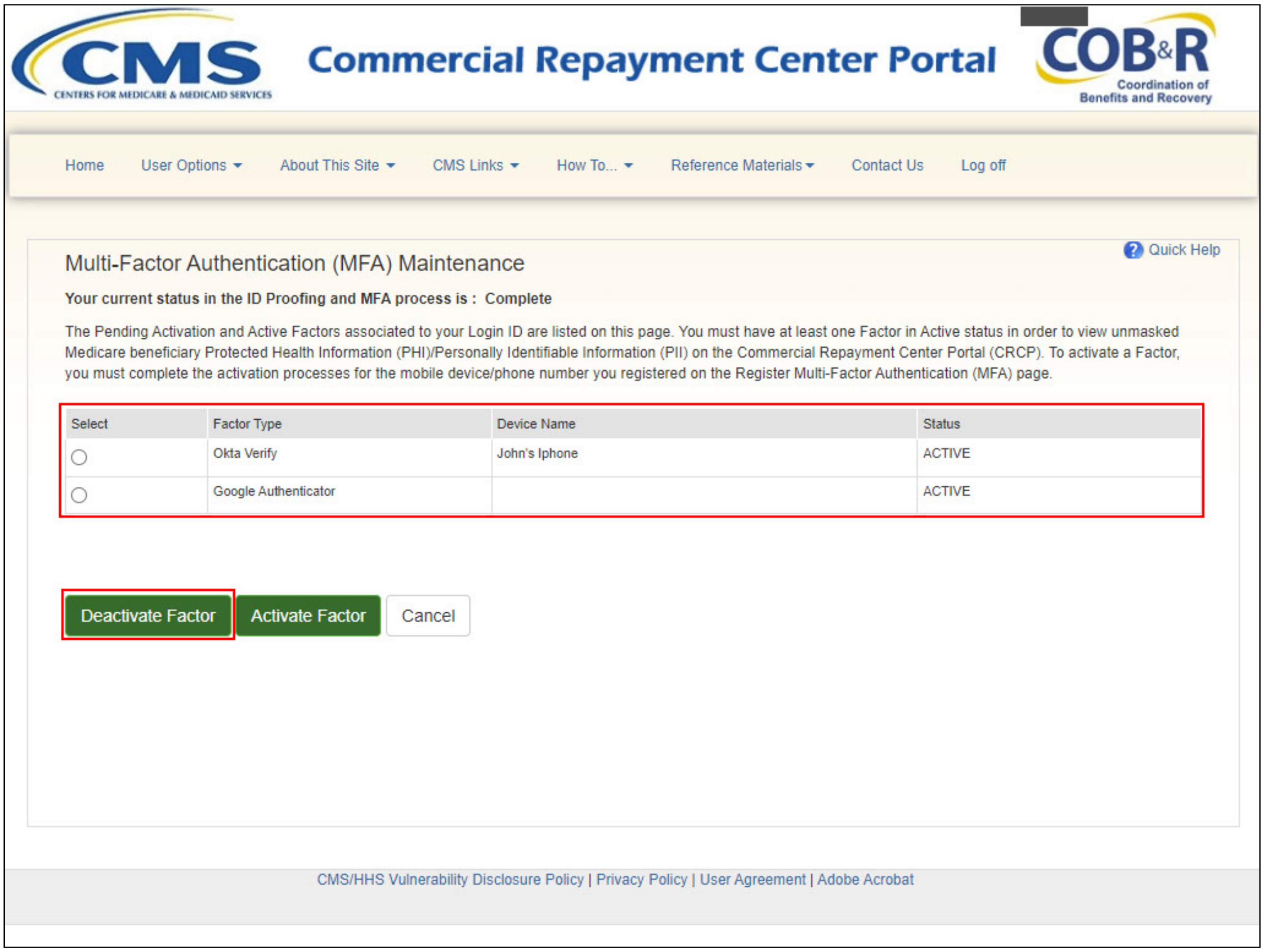
Slide notes

If you are no longer using a device to access the CRCP, you can deactivate it at any time.

For example, if you switch phones or computers, you should deactivate the Factor ID associated to the old device and activate a Factor ID for the new one.

Once a Factor ID is deactivated, you will not be able to use its associated device to view previously masked information on the CRCP, unless you reactivate it using the Multi-Factor Authentication Maintenance page.

Slide 30 of 40 - Multi-Factor Authentication Maintenance Page


CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
Home
User Options
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Log off
Quick Help

Multi-Factor Authentication (MFA) Maintenance

Your current status in the ID Proofing and MFA process is : Complete

The Pending Activation and Active Factors associated to your Login ID are listed on this page. You must have at least one Factor in Active status in order to view unmasked Medicare beneficiary Protected Health Information (PHI)/Personally Identifiable Information (PII) on the Commercial Repayment Center Portal (CRCP). To activate a Factor, you must complete the activation processes for the mobile device/phone number you registered on the Register Multi-Factor Authentication (MFA) page.

Select	Factor Type	Device Name	Status
○	Okta Verify	John's Iphone	ACTIVE
○	Google Authenticator		ACTIVE

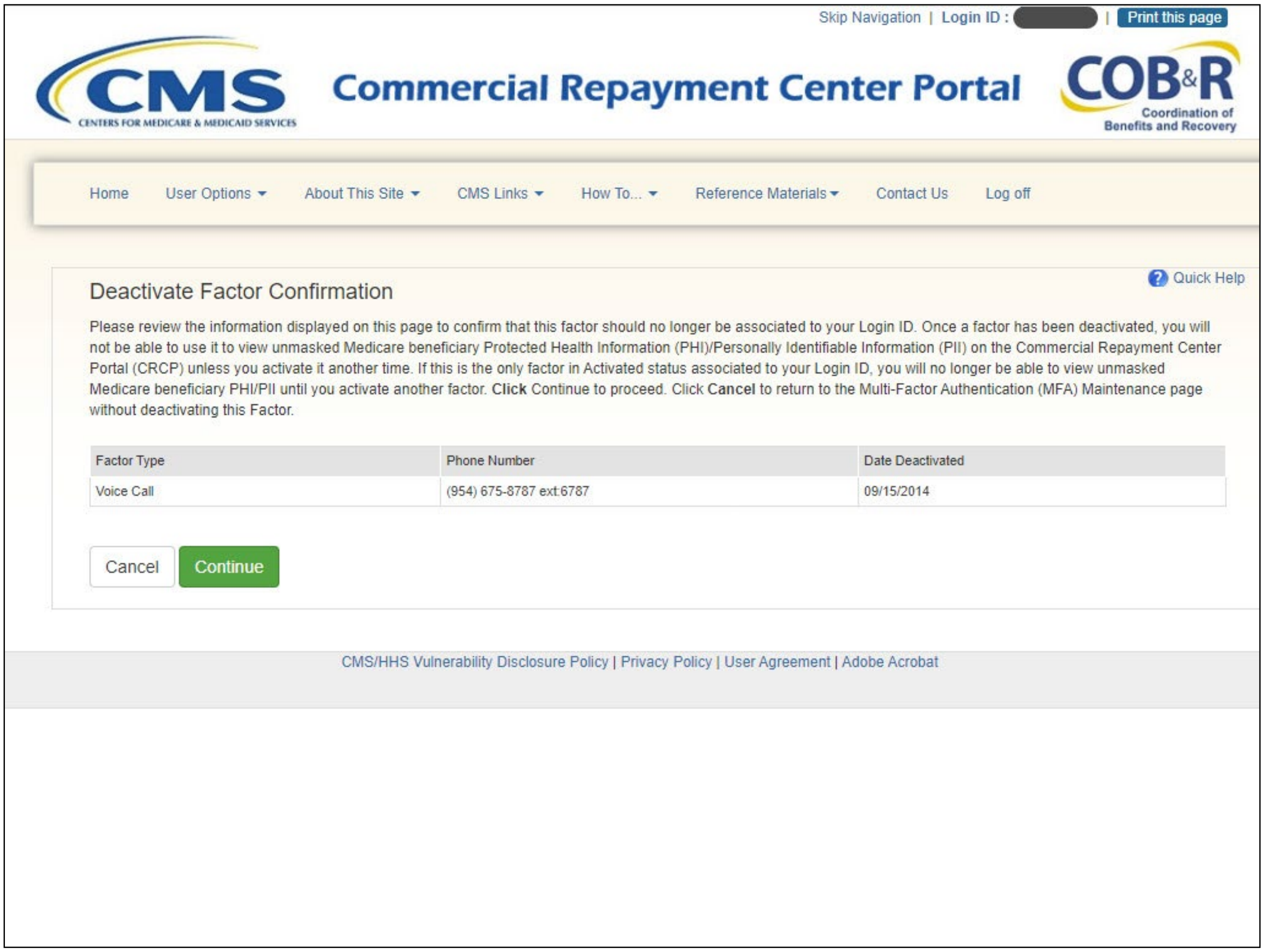
Deactivate Factor
Activate Factor
Cancel
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Slide notes

To Deactivate a Factor, click the Factor Maintenance link on your home page.

The Multi-Factor Authentication (MFA) Maintenance page shown here appears. Next, click the radio button corresponding to the Factor you want to deactivate and then click the Deactivate Factor button.

Slide 31 of 40 - Deactivate Factor Confirmation Page


Skip Navigation | Login ID : [redacted] | Print this page
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
Home
User Options
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Log off
Quick Help
Cancel
Continue
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Deactivate Factor Confirmation

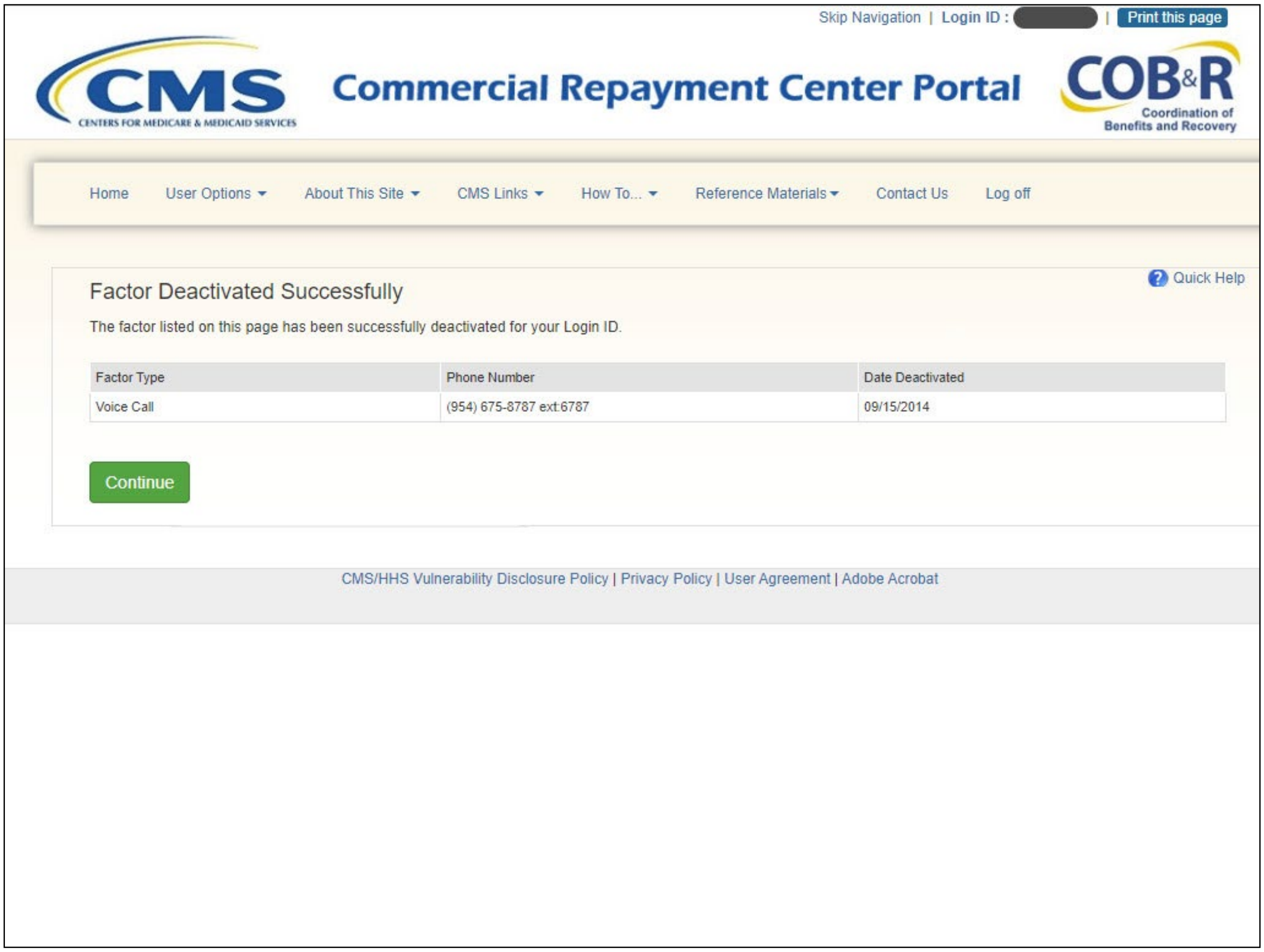
Please review the information displayed on this page to confirm that this factor should no longer be associated to your Login ID. Once a factor has been deactivated, you will not be able to use it to view unmasked Medicare beneficiary Protected Health Information (PHI)/Personally Identifiable Information (PII) on the Commercial Repayment Center Portal (CRCP) unless you activate it another time. If this is the only factor in Activated status associated to your Login ID, you will no longer be able to view unmasked Medicare beneficiary PHI/PII until you activate another factor. **Click** Continue to proceed. Click **Cancel** to return to the Multi-Factor Authentication (MFA) Maintenance page without deactivating this Factor.

Factor Type	Phone Number	Date Deactivated
Voice Call	(954) 675-8787 ext:6787	09/15/2014

Slide notes

The Deactivate Factor Confirmation page will appear. When this page displays, click Continue to confirm the deactivation, or click Cancel to cancel the deactivation process.

Slide 32 of 40 - Factor Deactivated Successfully Page


Skip Navigation | Login ID : [redacted] | Print this page
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
Home
User Options
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Log off
Quick Help
Continue
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Factor Deactivated Successfully

The factor listed on this page has been successfully deactivated for your Login ID.

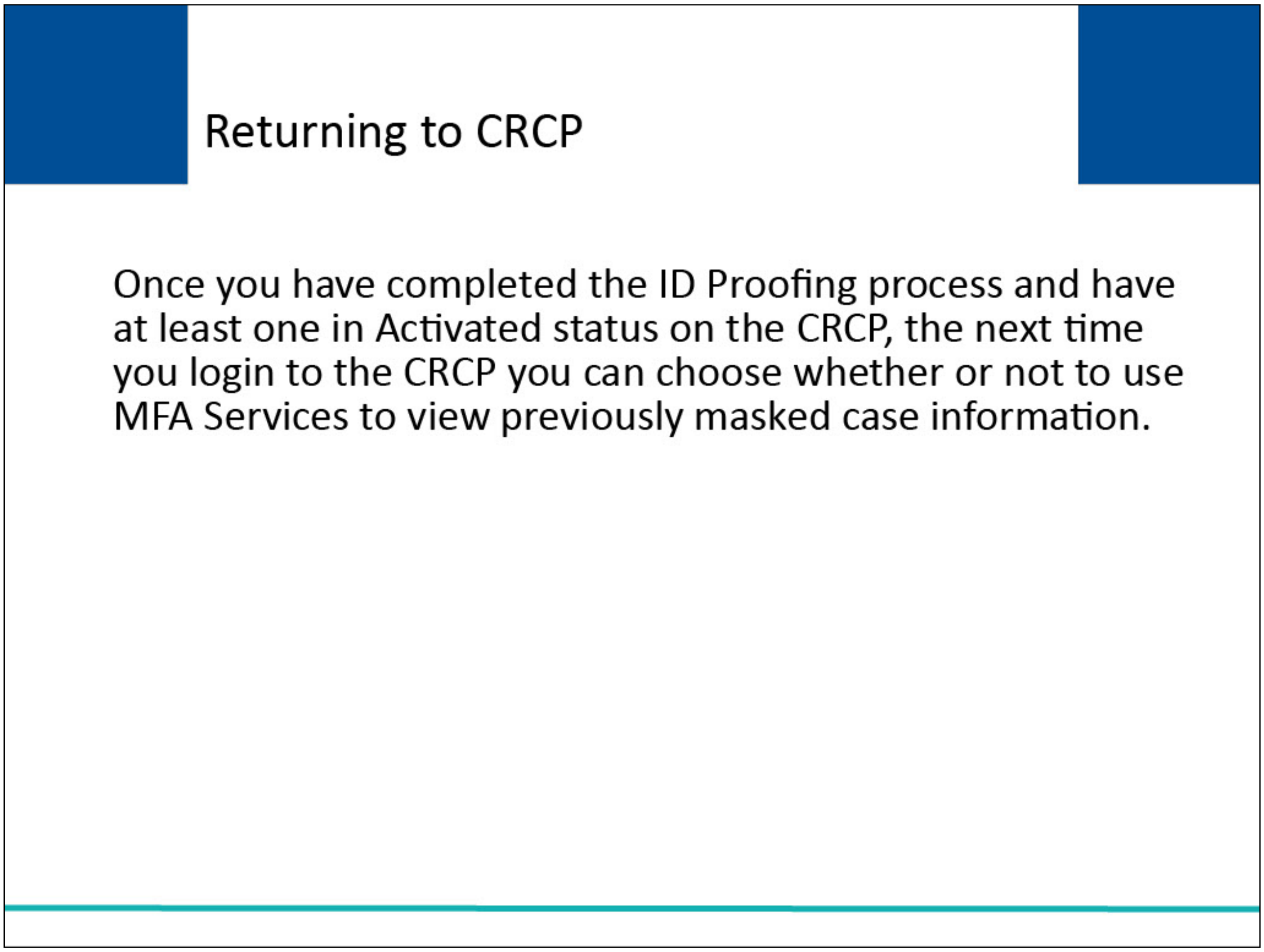
Factor Type	Phone Number	Date Deactivated
Voice Call	(954) 675-8787 ext:6787	09/15/2014

Slide notes

The Factor Deactivated Successfully page will appear.

Click Continue to confirm deactivation and return to the Multi-Factor Authentication Factor Maintenance page.

Slide 33 of 40 - Returning to CRCP



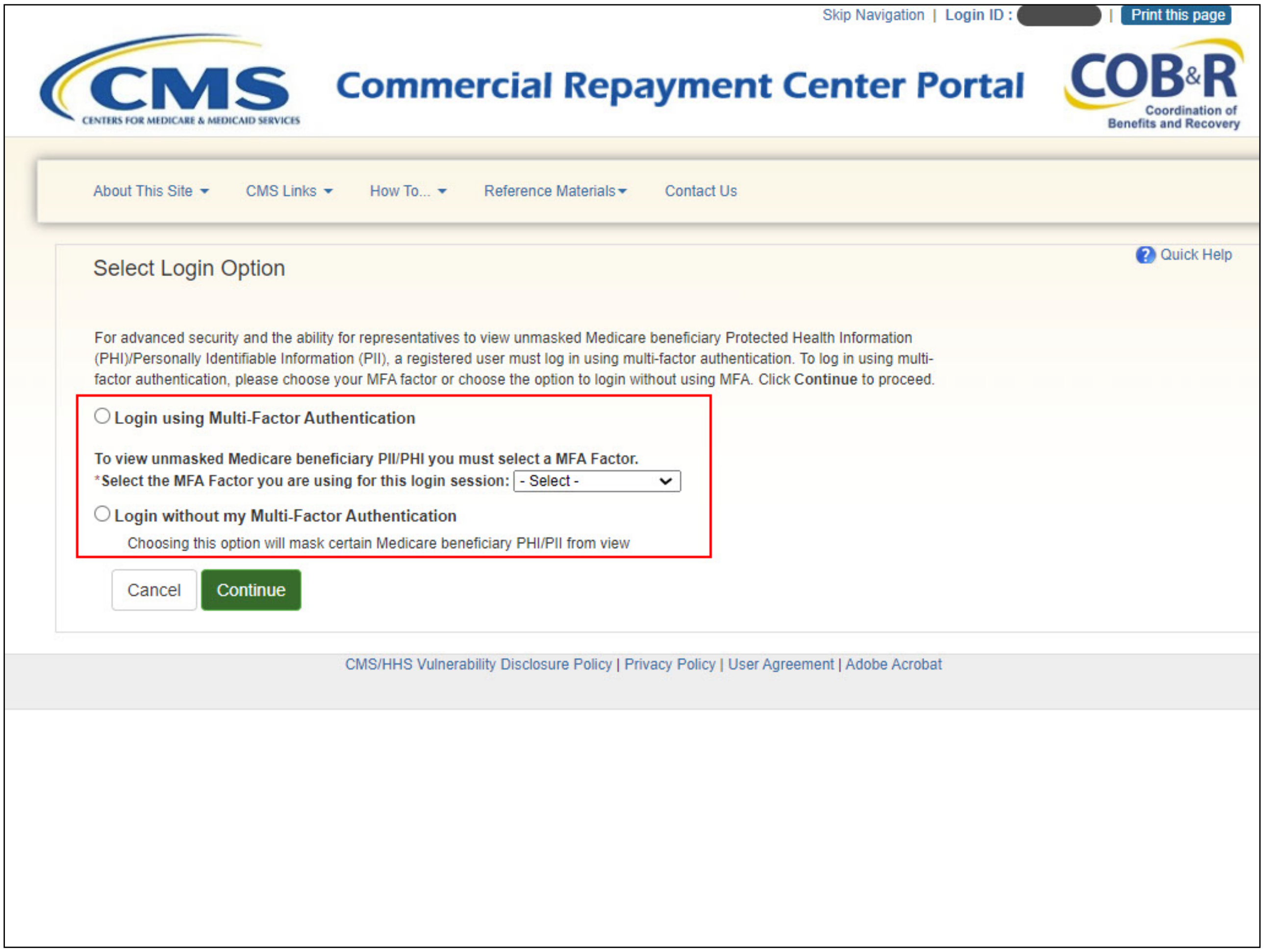
Returning to CRCP

Once you have completed the ID Proofing process and have at least one in Activated status on the CRCP, the next time you login to the CRCP you can choose whether or not to use MFA Services to view previously masked case information.

Slide notes

Once you have completed the ID Proofing process and have at least one in Activated status on the CRCP, the next time you login to the CRCP you can choose whether or not to use MFA Services to view previously masked case information.

Slide 34 of 40 - Select Login Option Page


Skip Navigation | Login ID : [redacted] | Print this page
CMS CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R Coordination of Benefits and Recovery
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Quick Help
Cancel
Continue
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Select Login Option

For advanced security and the ability for representatives to view unmasked Medicare beneficiary Protected Health Information (PHI)/Personally Identifiable Information (PII), a registered user must log in using multi-factor authentication. To log in using multi-factor authentication, please choose your MFA factor or choose the option to login without using MFA. Click **Continue** to proceed.

○ **Login using Multi-Factor Authentication**

To view unmasked Medicare beneficiary PII/PHI you must select a MFA Factor.

***Select the MFA Factor you are using for this login session:** - Select -

○ **Login without my Multi-Factor Authentication**

Choosing this option will mask certain Medicare beneficiary PHI/PII from view

Slide notes

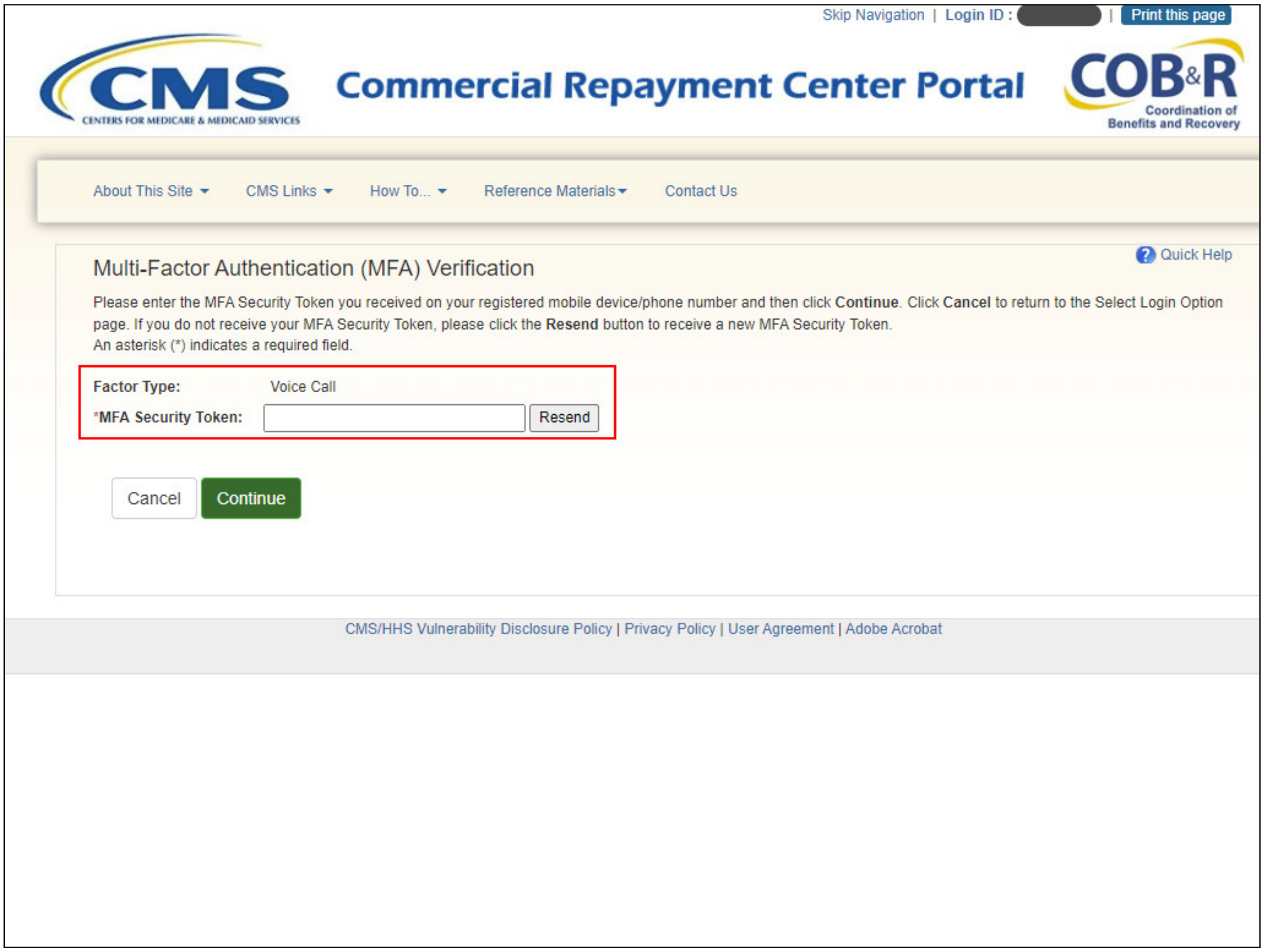
When you log in, the CRCP displays the Select Login Option page automatically.

Click to select either the Login using Multi-Factor Authentication or Login without my Factor ID radio button.

If logging in using MFA Services, select a device from the drop-down menu.

Note: If you do not choose MFA services you will not be able to see any cases unmasked. Once you have selected the appropriate radio button, select continue.

Slide 35 of 40 - Multi-Factor Authentication Verification Page


Skip Navigation | Login ID : [redacted] | Print this page
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Quick Help

Multi-Factor Authentication (MFA) Verification

Please enter the MFA Security Token you received on your registered mobile device/phone number and then click **Continue**. Click **Cancel** to return to the Select Login Option page. If you do not receive your MFA Security Token, please click the **Resend** button to receive a new MFA Security Token.
An asterisk (*) indicates a required field.

Factor Type: Voice Call

***MFA Security Token:**

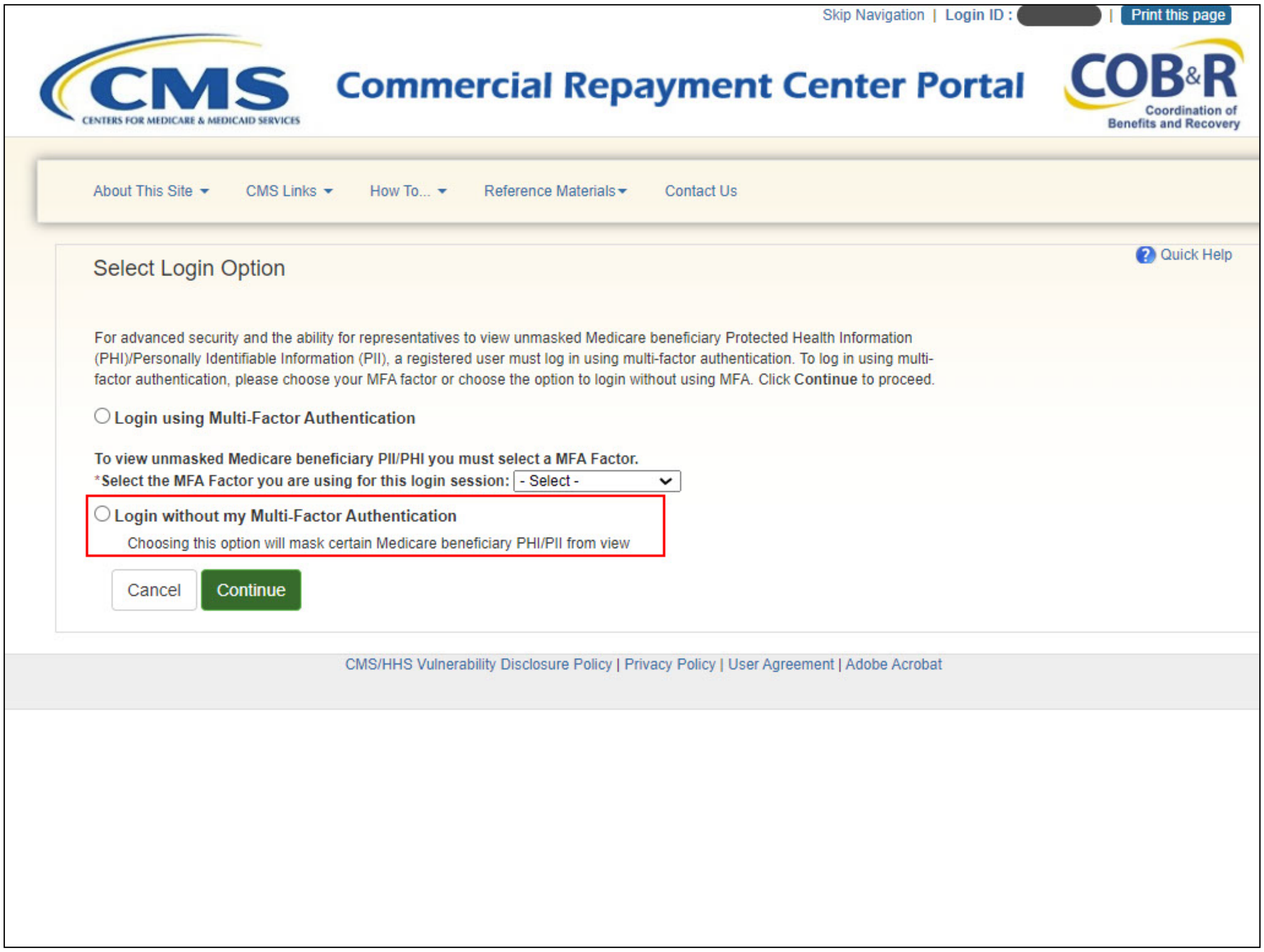
Resend
Cancel
Continue
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Slide notes

Enter the MFA Security Token and click Continue to continue logging in. The Account page will appear with all the unmasked cases.

If you select Cancel you will return to the Select Login Option page.

Slide 36 of 40 - Select Login Option Page



Skip Navigation | Login ID : [redacted] | Print this page
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Quick Help

Select Login Option

For advanced security and the ability for representatives to view unmasked Medicare beneficiary Protected Health Information (PHI)/Personally Identifiable Information (PII), a registered user must log in using multi-factor authentication. To log in using multi-factor authentication, please choose your MFA factor or choose the option to login without using MFA. Click **Continue** to proceed.

○ **Login using Multi-Factor Authentication**

To view unmasked Medicare beneficiary PII/PHI you must select a MFA Factor.

***Select the MFA Factor you are using for this login session:** - Select -

○ **Login without my Multi-Factor Authentication**

Choosing this option will mask certain Medicare beneficiary PHI/PII from view

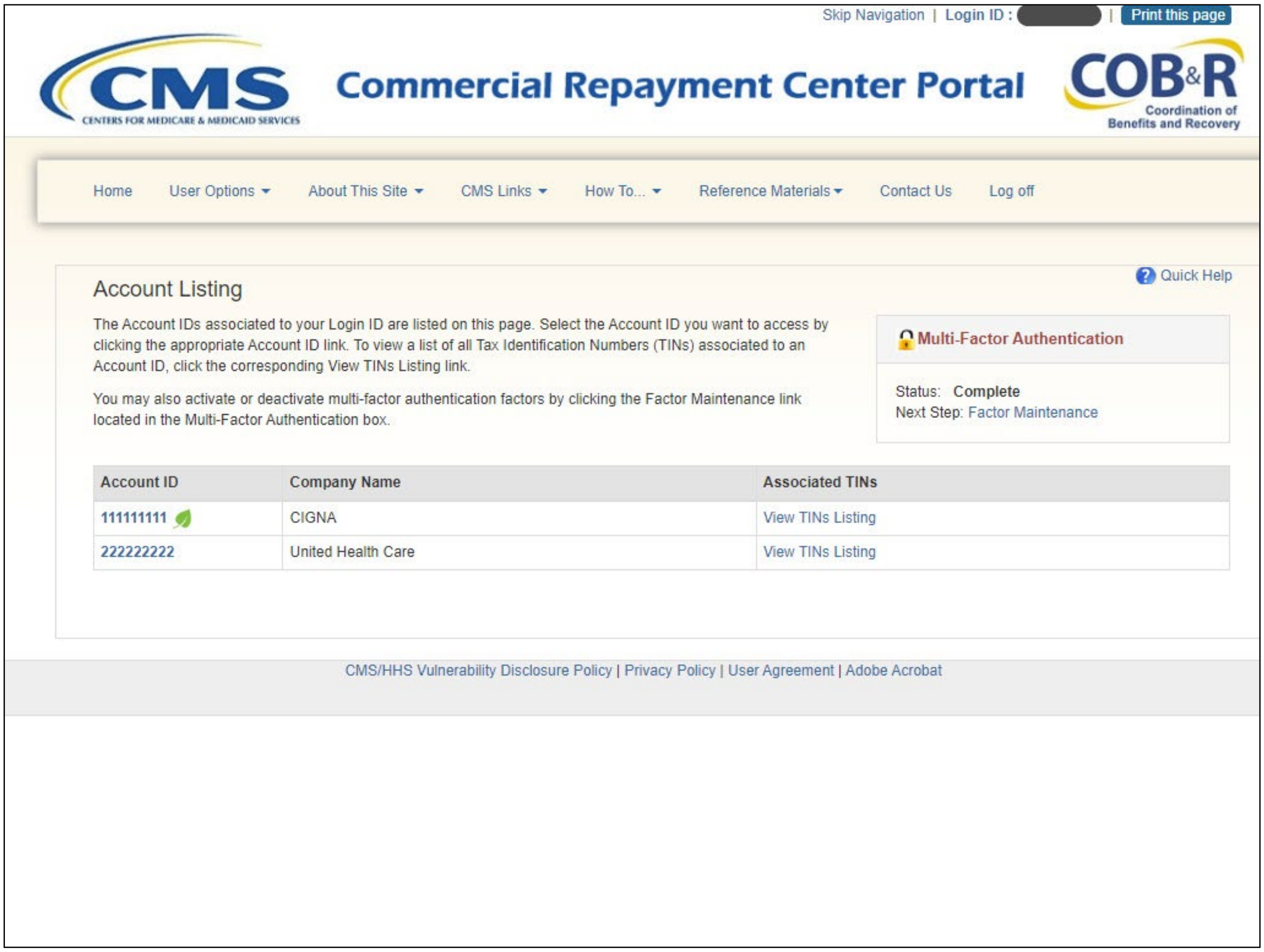
Cancel
Continue
CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Slide notes

When logging in without MFA services you will not be able to see any cases unmasked.

Once you select continue, the Account Listing page will appear.

Slide 37 of 40 - Account Listing


Skip Navigation | Login ID : [redacted] | Print this page
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
Commercial Repayment Center Portal
COB&R
Coordination of Benefits and Recovery
Home
User Options
About This Site
CMS Links
How To...
Reference Materials
Contact Us
Log off
Quick Help

Account Listing

The Account IDs associated to your Login ID are listed on this page. Select the Account ID you want to access by clicking the appropriate Account ID link. To view a list of all Tax Identification Numbers (TINs) associated to an Account ID, click the corresponding View TINs Listing link.

You may also activate or deactivate multi-factor authentication factors by clicking the Factor Maintenance link located in the Multi-Factor Authentication box.

Multi-Factor Authentication

Status: Complete
Next Step: Factor Maintenance

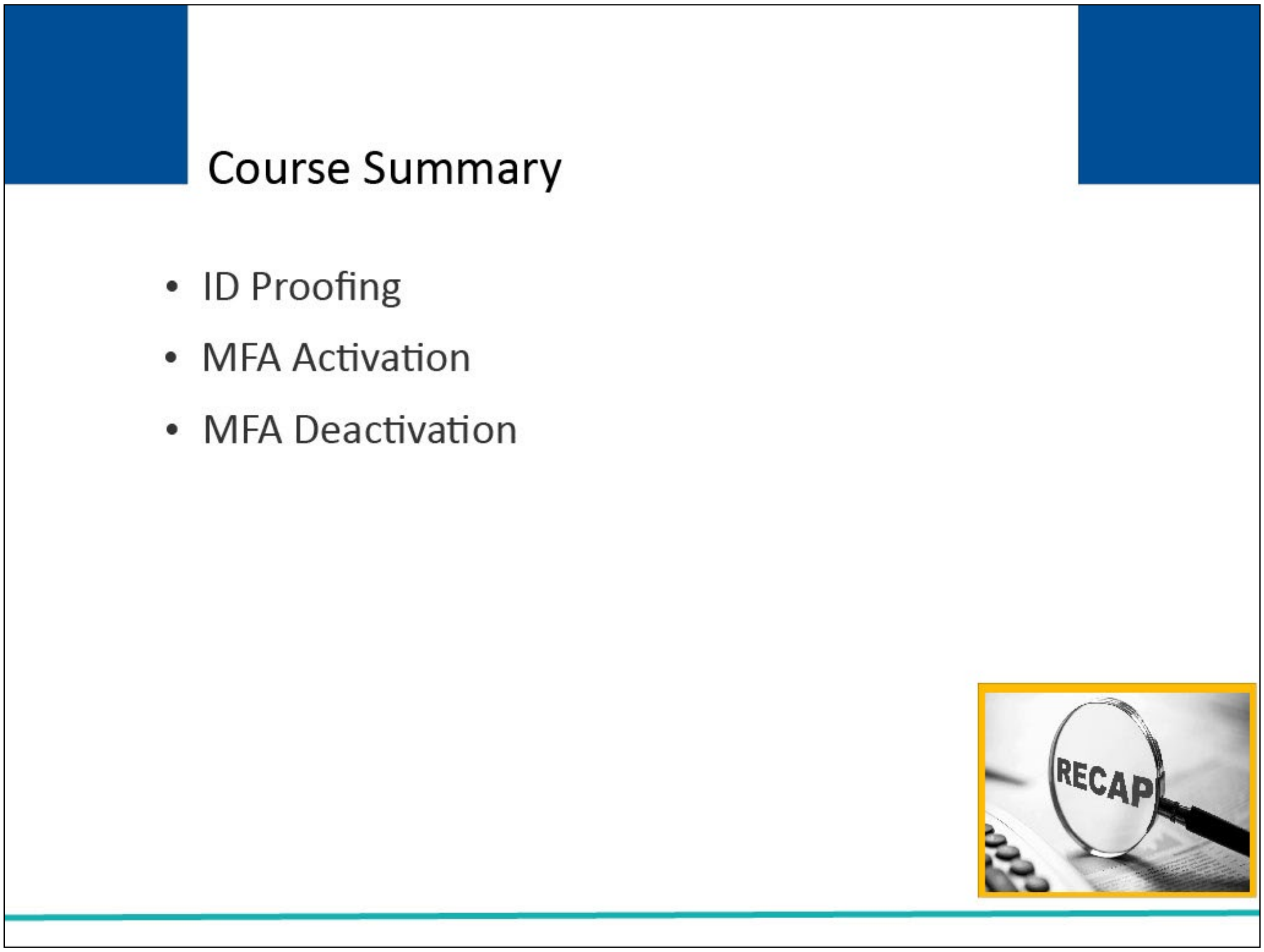
Account ID	Company Name	Associated TINs
111111111	CIGNA	View TINs Listing
222222222	United Health Care	View TINs Listing

CMS/HHS Vulnerability Disclosure Policy | Privacy Policy | User Agreement | Adobe Acrobat

Slide notes

You will not be able to see any cases unmasked since you opted to login without MFA.

Slide 38 of 40 - Course Summary



Course Summary

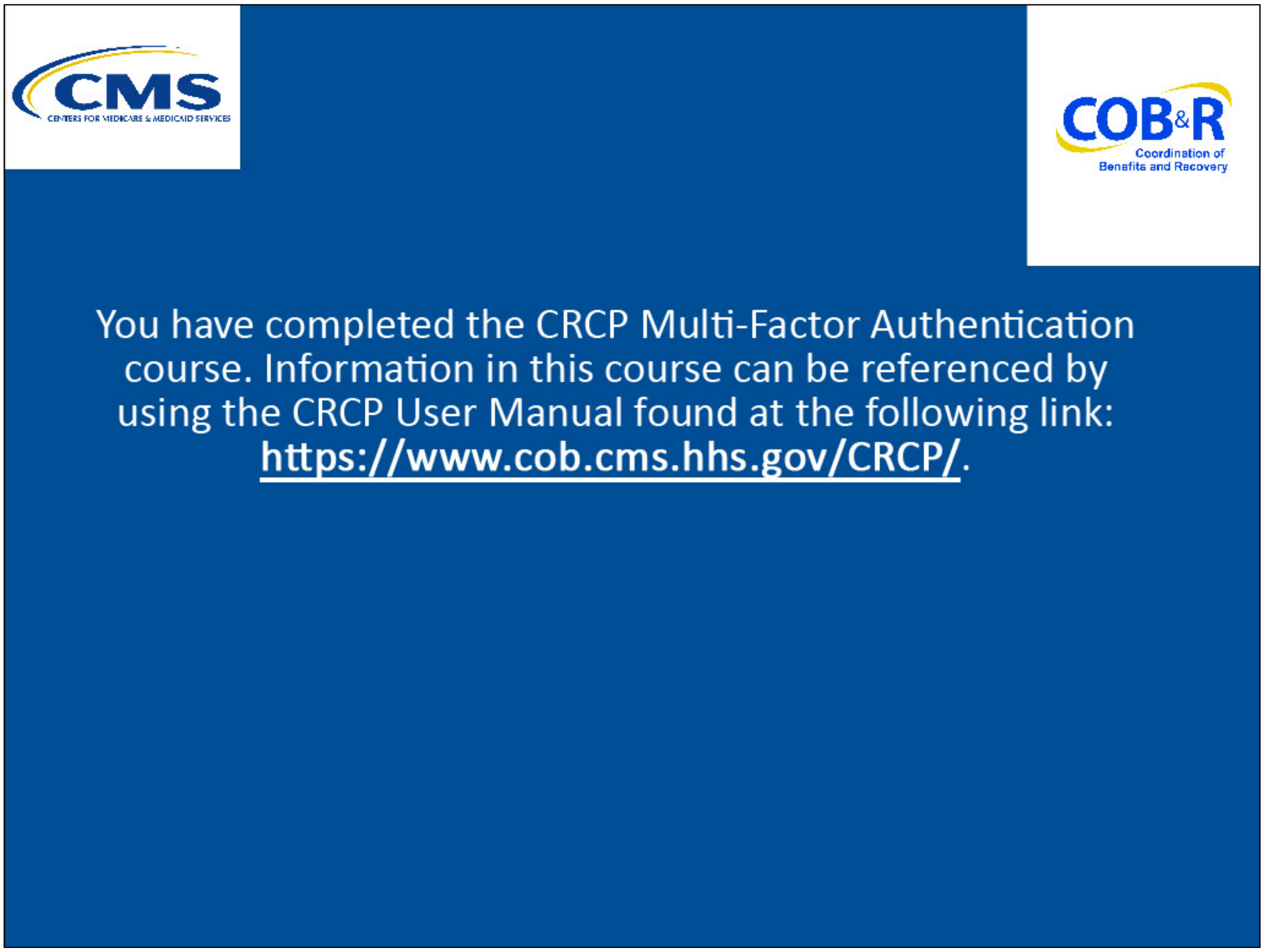
- ID Proofing
- MFA Activation
- MFA Deactivation

Slide notes

This module explained the steps a non-beneficiary user must take to be able to view unmasked case information in the CRCP.

It explained how a user can become identity proofed using the CRCP and how Multi-Factor Authentication (MFA) is activated and deactivated (if needed).

Slide 39 of 40 - Multi-Factor Authentication Conclusion

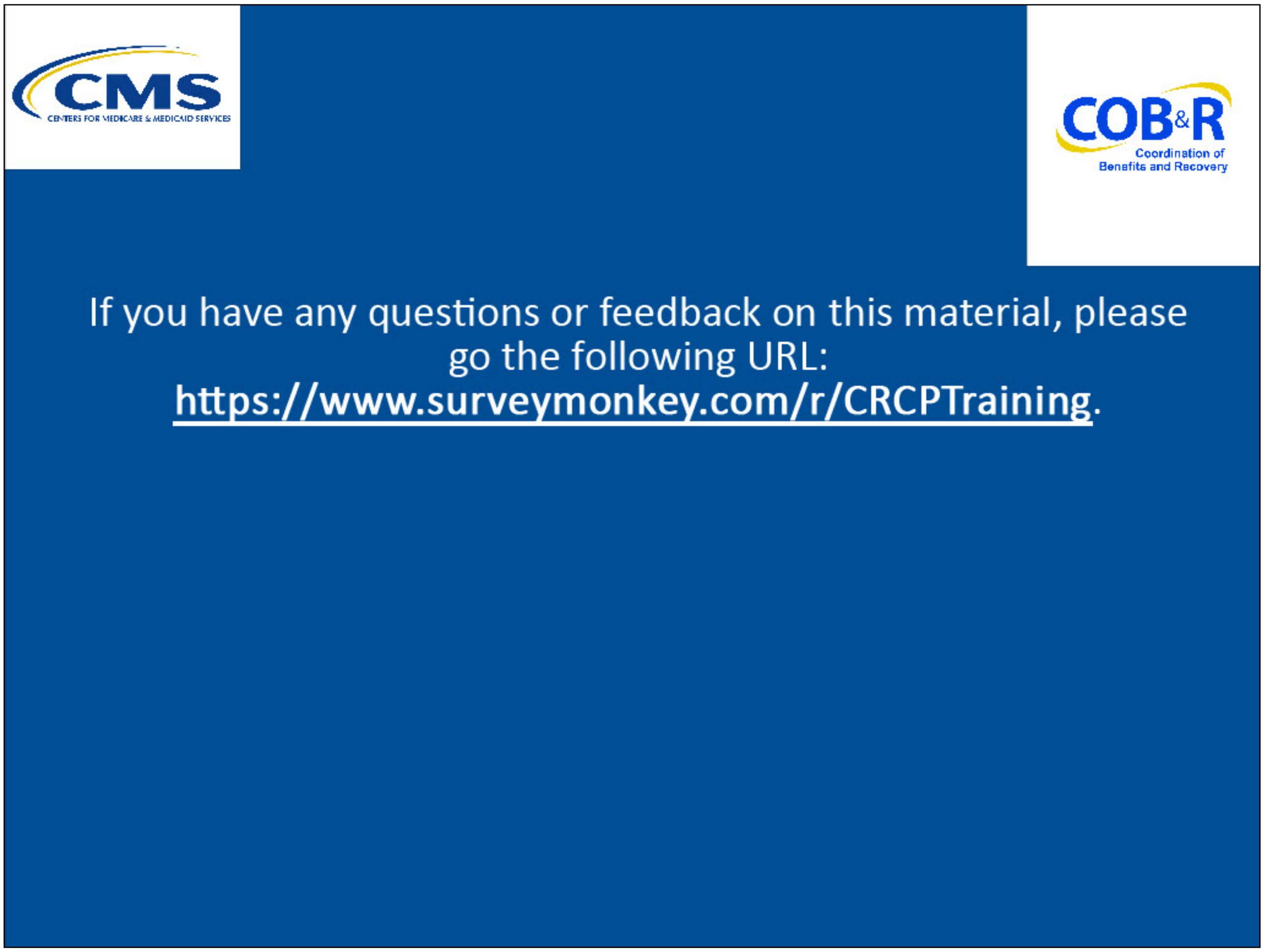

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
COB&R
Coordination of Benefits and Recovery

You have completed the CRCP Multi-Factor Authentication course. Information in this course can be referenced by using the CRCP User Manual found at the following link: https://www.cob.cms.hhs.gov/CRCP/.

Slide notes

You have completed the CRCP Multi-Factor Authentication course. Information in this course can be referenced by using the CRCP User Manual found at the following link: CMS CRCP Website.

Slide 40 of 40 - CRCP Training Survey


CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
COB&R
Coordination of Benefits and Recovery

If you have any questions or feedback on this material, please go the following URL: https://www.surveymonkey.com/r/CRCPTraining.

Slide notes

If you have any questions or feedback on this material, please go the following URL: CRCP Training Survey.