Remote Identity Proofing (RIDP)—Multi-Factor Authentication (MFA)

The Medicare Secondary Recovery Portal (MSPRP) and Commercial Recovery Center Portal (CRCP) use an identity management solution provided by the Centers for Medicare & Medicaid Services (CMS). Remote Identity Proofing (RIDP) and Multi-Factor Authentication (MFA) services are intended to reduce fraud and ensure system security. If you complete the RIDP process and use MFA services, you will be able to view beneficiary information on the MSPRP and CRCP. The purpose of this document is to provide you with background on both services.

What is Remote Identity Proofing?

RIDP is the process of validating sufficient information that uniquely identifies you. You must be identity proofed to gain electronic access to protected CMS information or systems. You may already have encountered RIDP through interactions with banking systems, credit reporting agencies, and shipping companies.

CMS uses the Experian identity verification system (Experian) to remotely perform identity proofing. CMS uses Experian's risk-based alternative (RBA) solution, which requires users to submit personally identifiable information (PII) instead of answering knowledge-based or out-of-wallet questions.

When you log in to the MSPRP or CRCP, you will have the option to complete RIDP. You will be asked to provide a set of core credentials, which include:

- Full Legal Name
- Social Security Number (may be optional)
- Date of Birth
- Current Residential Address
- Personal Telephone Number (mobile preferred)
- Personal E-mail Address

Experian will use your core credentials to attempt to verify your identity to the appropriate level of assurance with the information you provided. Most users are able to complete the ID proofing process in less than five minutes. If you encounter problems with RIDP, you will be asked to contact the Experian Call Center via telephone to resolve any issues or to complete the manual proofing process with the COB&R's EDI Department. Please see the "Remote Identity Proofing Tips for Success" section in this document for some tips on navigating the ID proofing process successfully.

What happens to the data submitted for identity proofing?

You will enter your personal information into the MSPRP or CRCP. Your personal information is described as data that is unique to you, such as name, address, social security number, and date of birth. Neither the MSPRP nor CRCP store your personal information; they only pass it to Experian to confirm your identity. Your social security number will be validated with Experian only for the purpose of verifying your identity. Experian verifies the information you provided against their records. For more information on how CMS uses the information you provide, please read the CMS Privacy Act Statement.

Will RIDP affect my credit?

No, this type of inquiry does not affect your credit score and there is no cost related to this credit score inquiry. When you complete the identity proofing process, Experian creates something called a soft inquiry. Soft inquiries are visible only to you, the consumer, and no one else. Soft inquiries have no impact on your credit report, history, or score other than being recorded and maintained for 23 months.

What happens if my identity cannot be verified during the online RIDP process?

If Experian cannot identity proof you online, you may be asked to contact the Experian Call Center. The system will provide you with a reference number to track your case. For security purposes, the Experian Call Center cannot assist you if you do not have the reference number. Some users may be directed to complete manual identity proofing following the COB&R EDI Department process.

What happens if my identity cannot be verified by the Experian Call Center?

If you contact the Experian Call Center and your identity cannot be verified, you will be referred to the Coordination of Benefits & Recovery (COB&R) Electronic Data Interchange (EDI) Department to complete the manual identity proofing process. Directions on the manual proofing process are provided on the MSPRP and CRCP if the Experian RIDP process is unsuccessful.

How do I contact the COB&R EDI Department?

The COB&R EDI Department is open Monday through Friday from 9:00 a.m. to 5:00 p.m., Eastern Time except holidays.

You can contact the EDI Department using either of the following methods:

Email address: COBVA@bcrcgdit.com
Telephone Number: (646) 458-6740

How do I contact the Experian Help Desk?

The Experian Call Center is open Monday through Friday from 8:30 a.m. to midnight, Saturday from 10:00 a.m. to 8:00 p.m., and Sunday from 11:00 a.m. to 7:00 p.m., Eastern Standard Time.

Contact the Experian Call Center at (833) 203-6550, or via the website at www.experian.com.

Remote Identity Proofing Tips for Success

Name:

- You must use your full legal name. Refer to your Driver's License or financial account information.
- Your surname **HAS** to match the surname Experian has for you on file.
- Do not use nicknames.
- If you have a two-part name, enter the second part in the middle name field (i.e., Mary Jo would have Mary in the first name field and Jo in the middle name field).

Address:

- Enter your current **residential** address:
  - Address where you receive financial statements including credit cards and/or utilities
  - Address you most consistently use for billing purposes
  - Address associated with your credit report
- If you have a recent change in address, you can try to ID proof with a prior address.
- Do not enter any extraneous symbols in the address field. If you want to confirm the correct format, visit USPS Look Up a Zip Code.

Telephone:

- Enter a personal mobile number, which is preferred.
- A personal landline telephone can be used (if you have one).

E-mail:

- Enter a personal email address.

Consent:

- You will be asked for consent to verify your identity information from your credit report.
- The information is used only for purposes of IDENTITY PROOFING—"you are who you say you are." The consent to use the information does post as a soft inquiry on your credit report. The soft inquiry is visible only to you.
- The consent/inquiry **does not** affect your credit score.

Exclusions:

- If you have a Victim's Statement or a blocked or frozen file, you will NOT be able to complete the identity proofing process online. After attempting online, you will be directed to call Experian's Consumer Services at 1-833-985-0709 to have the alert temporarily lifted so that you can attempt the ID proofing process.
- If you are listed as deceased on the Social Security Administration's (SSA) Death Master File, you will NOT be able to complete the identity proofing process online.

You may contact the SSA at **1-800-269-0271**. They will be able to make sure that your information is being reported correctly.

Other:

- To download a free copy of your credit report, go to www.annualcreditreport.com.

What is Multi-Factor Authentication (MFA)?

MFA is an approach to security authentication that requires you to provide more than one form of a credential in order to prove your identity. CMS policy specifies that all users who request access to a CMS application that has an Identity Assurance Level 2 (IAL2) security rating, must be identity proofed to the corresponding IAL2 standards. This includes the requirement that users be authenticated using MFA. As of January 2019, CMS uses Okta Verify or Google Authenticator services to add a layer of protection for your online identity. These services use government-certified technology and techniques to provide this multi-factor authentication.

How do we use MFA?

CMS uses MFA to grant access to a protected CMS application designated by the Information Systems Security Officer (ISSO) to be an IAL2 Application. You will be asked to enter your username and password and an MFA security token that is generated by Okta Verify or Google Authenticator software to gain access to the CMS application. You will be required to register for a Factor Type (Okta Verify or Google Authenticator) as the method of receiving the MFA security token.

How do I get an MFA factor?

The MSPRP or CRCP will prompt you to register an MFA factor when you request access to protected information that requires IAL2, and you have not already registered an MFA factor in the MSPRP or CRCP. You will be given a choice of Okta Verify or Google Authenticator. You must download the Okta Verify or Google Authenticator app to your device and follow the steps to complete setup. No other apps can be used to complete this task. You may have up to two MFA factors, one for Okta Verify and one for Google Authenticator.

If I am no longer using a factor, can I deactivate it?

You can activate and deactivate a factor type at any time using the Multi-Factor Authentication Maintenance page. You are limited to having only one type of each factor active at a time.

How do I use Multi-Factor Authentication?

When you access the MSPRP or CRCP, you will log in as you do today. If you have an MFA factor activated the system will display the Select Login Option screen. You will be required to select the MFA factor you are using and hit continue. You will then enter the code generated by your Okta Verify or Google Authenticator app to complete login.