Remote Identity Proofing (RIDP) – Multi-Factor Authentication (MFA) on the Medicare Secondary Payer Recovery Portal (MSPRP)

The MSPRP has implemented an identity management solution provided by the Centers for Medicare & Medicaid Services (CMS). The adoption of Remote Identity Proofing (RIDP) and Multi-Factor Authentication (MFA) services will help improve CMS' ability 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. 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 (e.g., credit history, personal demographic information, and other indicators). If you are requesting electronic access to protected CMS information or systems, you must be identity proofed to gain access.

CMS uses the Experian identity verification system (Experian) to remotely perform identity proofing.

You may have already encountered RIDP through various interactions with banking systems, credit reporting agencies, and shipping companies. Experian is used by CMS to confirm your identity when you need to access a protected CMS Application. When you log in to the MSPRP, you will have the option to 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

Experian will use your core credentials to locate your personal information in Experian and generate a set of questions. Experian will 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 Experian Support Services via telephone to resolve any issues. 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. Your personal information is described as data that is unique to you as an individual, such as name, address, telephone number, Social Security Number, and date of birth. The MSPRP does not store your personal information; only passes it to Experian, an external identity verification system, to help 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 and may present you with questions based on your credit profile, called out-of-wallet questions. The out-of-wallet questions and answers, including financial history, are strictly between you and the RIDP service Experian; neither the MSPRP nor the CMS will store them. Experian is required by law to securely maintain this data for seven years. For more information regarding 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 you will not incur any charges related to this credit score inquiry. When you identity proof, 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 identify cannot be verified during the online RIDP process?

If Experian cannot identity proof you online, you will be asked to contact the Experian Verification Support Services Help Desk. The system will provide you with a reference number to track your case. For security purposes, the Experian Help Desk cannot assist you if you do not have the reference number.

What happens if my identify cannot be verified during the Experian phone proofing RIDP process?

If you contact the Experian Verification Support Services Help Desk 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 if you cannot complete the Experian telephone proofing RIDP process successfully.

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@GHIMedicare.com
Telephone Number: (646) 458-6740

How do I contact the Experian Help Desk?

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

You can contact the Experian Help Desk at (866) 578-5409.
The Experian website can be accessed 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., Billy Bob would have Billy in the first name field and Bob 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 landline telephone number (if you have one).
- A cell phone can be used, but a residential landline is preferred.

Out-of-Wallet Questions:

- You will be asked a series of questions regarding your personal financial transactions/information.
- Try to collect all of your information together before attempting the session.
- Download a free copy of your credit report at www.annualcreditreport.com.

Consent:

- You will be asked to give consent to verify your identity information from your credit report.
- The information is utilized only for purposes of IDENTITY PROOFING – "you are who you say you are." The consent of utilizing 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 **1-866-578-5409** 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.

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 a level of assurance (LOA) 3 security rating, must be identity proofed to the corresponding LOA 3 standards. This includes the requirement that users be authenticated using MFA. Effective January 2019 CMS will use OKTA Verify service to add a layer of protection for your online identity. OKTA Verify utilizes 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 LOA 3 Application. You will be asked to enter your username and password and an MFA security token that is generated by OKTA Verify software to gain access to the CMS Application. You will be required to register for a Factor Type (Voice Call and/or SMS (Text Message)) as the method of receiving the MFA security token.

How do I get an MFA factor?

The MSPRP will prompt you to register an MFA factor when you request access to protected information that requires LOA 3, and you have not already registered an MFA factor in the MSPRP. You will be given a choice of voice call or SMS text message.

If I am no longer using a factor (cell or landline number) 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 have only one type of each factor active at a time.

How do I use Multi-Factor Authentication?

When you access the MSPRP, 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 received to complete login.

Will I be charged cell phone time each time I receive a factor call or text on my mobile device?

While there is no cost associated with setting up MFA, costs associated with receiving a voice call or SMS text message will be dependent on your individual carrier.