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

The MSPRP has implemented a new identity management solution provided by the Centers for Medicare & Medicaid Services (CMS). Part of this transition is the adoption of Remote Identity Proofing (RIDP) and Multi-Factor Authentication (MFA) services. This transition 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 of these 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 identity 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 identity 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 @ **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. CMS uses Symantec's Validation and Identity Protection (VIP) service to add a layer of protection for your online identity. Symantec's VIP 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 a One Time Password (OTP) that is generated by Symantec VIP software to gain access to the CMS Application. The OTP can be generated by a free Symantec application that can be downloaded to your desktop or smartphone once you have registered your smartphone in the MSPRP. The "Where can we get the MFA software?" section below provides the necessary information to install the Symantec application on your desktop or smartphone.

How do I get an MFA credential?

The MSPRP will prompt you to register an MFA credential when you request access to protected information that requires LOA 3, and you have not already registered an MFA credential in the MSPRP. You will be given a choice of MFA token delivery methods. The primary MFA token delivery method is to download software and install it on your computer or a mobile device. Where to get the MFA software is discussed below.

Where can I get the MFA software?

You will need MFA software if you choose to receive your MFA credential on a computer, laptop or a mobile device. You will be required to download the MFA software from Symantec and install it in your device of choice.

To download the desktop software for Windows or Mac, navigate to https://idprotect.vip.symantec.com/desktop/home.v and follow the instructions.

If using an iPhone, Android, Blackberry, or other mobile device, use your device to navigate to https://m.vip.symantec.com/home.v and follow the instructions.

How do I register for MFA if I receive an error when installing the software on my computer?

If you are having trouble downloading and installing the MFA software on your desktop or laptop, it is possibly due to your company's IT policy that disables users from installing any software on their company-provided machines. Check with your company's IT department for assistance. If your company does not allow you to install MFA software, one alternative is to use a mobile device that you control.

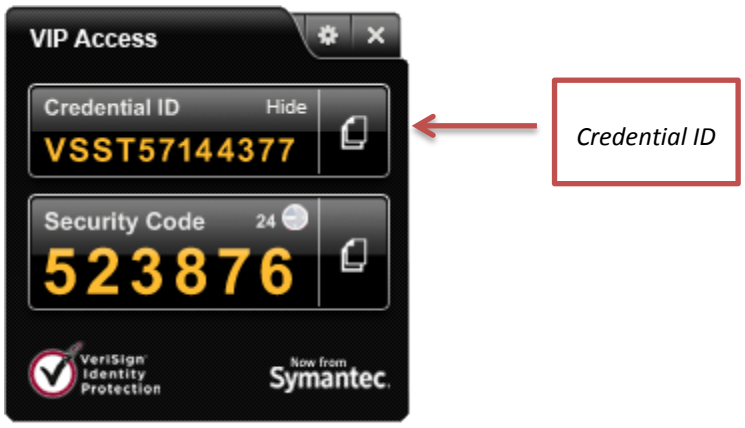
I cannot download Symantec VIP on my BlackBerry.

If your BlackBerry is a company-provided BlackBerry, your IT department may have locked down your device and disallowed users from loading applications. Check with your IT department to see if you have the required permissions to download an application on your BlackBerry. Some companies have also allowed the download of applications on their

Blackberries but only over Wi-Fi networks. If this is the case, connect your BlackBerry to a Wi-Fi network to download Symantec VIP by typing https://m.vip.symantec.com/home.v in the BlackBerry browser.

I am being asked to type a Credential ID. Where do I find the Credential ID?

The Credential ID is the 12-digit alpha-numeric number on the top of the soft token that was downloaded to your device from Symantec. The Credential ID begins with four letters and ends with eight numbers. In the example below, the token displays the credential ID as VSST57144377.



How do I register additional devices to my user account?

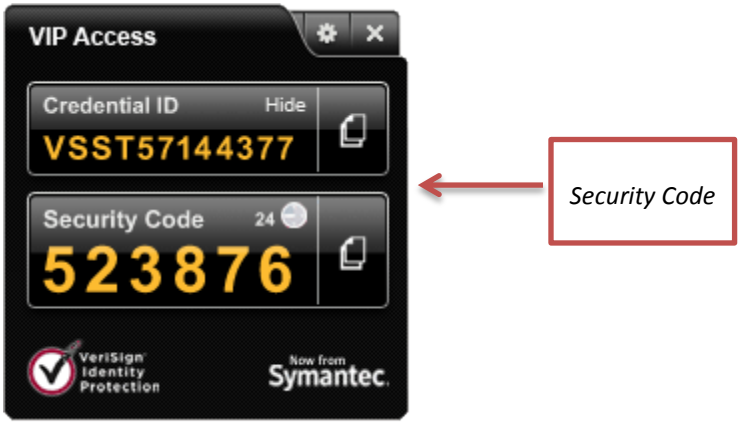
You can register up to five MFA credentials in my user account. Additional MFA credentials can be added to your account after you have set up the first MFA credential on the MSPRP. The "Credential Maintenance" hyperlink on your home page will appear once you have successfully set up your first MFA credential. You can click on the link and add additional MFA devices to your user account.

I lost all of the MFA devices linked to my user account. How do I deactivate the linked devices and link new devices to my user account?

The COB&R EDI Department should be able to assist you in removing/deactivating the registered devices and registering new devices to your user account.

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 token device activated the system will display the Choose Credential ID and Enter Security Code screen. You will be required to select the Credential you are using and enter the VIP security code that is displayed on your MFA token device.



For your protection, an MFA device automatically generates a new security code each time it counts down from a 30-second timer.

I already have a Symantec VIP token. Do I need another one?

The Symantec VIP tokens are used by many organizations. The tokens are interchangeable so you may re-use an existing Symantec token you may have assigned to a different system. However you must register this token with the MSPRP to enable its use on the system.

Will I be charged cell phone time each time I use Symantec VIP MFA on my mobile device?

It depends on what delivery method you use. The Symantec VIP MFA software is free. Once the Symantec VIP MFA application is downloaded and installed on the smartphone it does not utilize any cell time to generate the six-digit security code. Cell or network traffic is used to download the application to one's mobile device. There are no recurring charges associated the use of either software option.