Remote Identity Proofing (RIDP) – Multi-Factor Authentication (MFA) Communications Letter

In the near future CJR Support Team will be adding Remote Identity Proofing (RIDP) and Multi-Factor Authentication (MFA) to the services provided by the CMS.gov | Enterprise Portal (https://portal.cms.gov). This transition will help improve CMS' ability to ensure system security and reduce fraud. The purpose of this letter is to provide you with some background to prepare you for the transition.

What is Remote Identity Proofing?

Before you can be granted electronic access to protected CMS information or systems, you must be uniquely identified. RIDP is the process of validating enough information to establish your identity. You may have already encountered RIDP through various interactions with banking systems, credit reporting agencies, and shipping companies. CMS uses the Experian RIDP service to confirm your identity.

When you log into the CMS.gov | Enterprise Portal (https://portal.cms.gov) and request access to CJR Support Team, you may be prompted to go through RIDP. Be prepared to supply some or all of the following information and to answer a few other questions generated by Experian:

- *Full Legal Name*
- *Social Security Number (may be optional)*
- *Date of Birth*
- *Current Residential Address*
- *Personal Phone Number*

Most users are able to complete the ID proofing process in under five minutes. If you encounter problems with RIDP, you will be asked to contact the Experian Verification Support Services Help Desk via phone to resolve any issues. Please see the "Remote Identity Proofing Tips for Success" section in this letter for some tips on navigating the ID proofing process successfully.

What happens to the data submitted for identity proofing?

CJR Support Team collects some personal information that is unique to you as an individual, such as name, address, telephone number, Social Security Number, and date of birth. CJR Support Team collects personal information only to verify your identity. Your information will be sent to Experian, an external identity verification provider, to help us confirm your identity. Experian verifies the information you give us against their records and may present you with additional questions based on your credit profile. The questions and the answers, including financial history, are strictly between you and the Experian RIDP service. Neither CJR Support Team nor CMS will store the questions or the answers to 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 Terms & Conditions Statement (https://portal.cms.gov/wps/portal/unauthportal/registration).***

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 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. The Experian Verification Support Services Help Desk cannot assist you if you do not have the reference number. If the Experian Verification Support Services Help Desk cannot successfully identity proof you by phone, you will be advised to call the CJR Support Team Help Desk and request that they perform their manual identity proofing process with you.

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 CJR Support Team Help Desk to complete the manual identity proofing process.

How do I contact the CJR Support Team Help Desk?

The CJR Support Team Help Desk is open Monday through Friday from 8:30 a.m. to 6:00 p.m., Eastern Standard Time.

You can contact CJR Support Team *Help Desk using any of the following methods:*

Email address: cjrsupport@cms.hhs.gov

Phone Number: 1-844-711-CMMI (2664) Option 1

What are the Experian Verification Support Services Help Desk hours of operation?

The Experian Verification Support Services 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.

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 **must** 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.*

Phone:

- *Enter a personal landline phone 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.*
- *You may want to have such information readily accessible before attempting the session.*
- *You can 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/soft 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 a type of login (authentication) that, in addition to a User ID and Password, requires another "factor" such as a PIN. To comply with CMS policy, most users will need to establish a second login "factor" commensurate with the level of access requested. CMS uses Symantec's Validation and Identity Protection (VIP) service to add a second layer of protection for your online identity.

How do we use MFA?

You will be asked to enter your username and password and an additional One Time Password (OTP) that is generated by Symantec VIP software to gain access to CJR Support Team. The OTP can be generated by a free Symantec application that can be downloaded to your desktop or smartphone; or alternatively, you can receive an OTP via a Short Message Service (SMS) or voice phone call once you have registered your phone in CJR Support Team; or by Email. The "Where can I 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?

CJR Support Team will prompt you to register an MFA credential when you request access to protected information and you have not already registered an MFA credential in CJR Support Team. 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. Alternatively, if you require special support, you can set up SMS or voice token to deliver your MFA credential. 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 or 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.

SMS OTP, Voice OTP and Email options do not require a software download.

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, or you can also use a voice call to obtain the OTP. You can refer to other instructions in this FAQ document for information on cell phone installation and voice token usage.

I cannot use the desktop MFA software or the mobile phone MFA software.

CJR Support Team allows you to set up a voice or SMS delivery method for your OTP that does not require an MFA software download. You can register a phone number and select SMS or Voice OTP, and then CJR Support Team can register your phone number and delivery method with Symantec. After your MFA is activated, when you request access to CJR Support Team you will receive either a phone call or text message that contains your OTP, depending on the delivery method that you select.

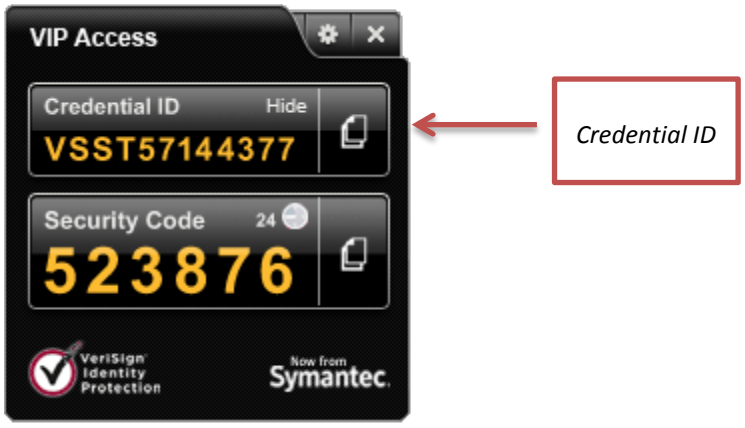
The SMS and Voice OTP expire within 10 minutes of when they are sent, so please make sure you provide a phone number that will be accessible to you during your typical work hours. As an example, do not use a residential phone number if you will normally log in from your place of employment.

I cannot download Symantec VIP on my mobile phone.

If your mobile phone is company-provided, 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 to your mobile phone. Some companies have also allowed the download of applications on their mobile phones but only over Wi-Fi networks. If this is the case, connect your mobile phone to a Wi-Fi network to download Symantec VIP by typing https://m.vip.symantec.com/home.v in the mobile phone 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 your user account. Additional MFA credentials can be added to your account after you have been prompted by CJR Support Team to set up the first MFA credential. The "Register your Smartphone or Computer" hyperlink on the "My Profile" 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 CJR Support Team Help Desk 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 CJR Support Team, the system will display the MFA login screen. You will be required to enter your user ID, password, and the VIP security code. If you have registered an MFA token device, enter your user ID and password and the 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.

If you have registered an MFA SMS token or MFA Voice token, when you access Application Name, the system will send you a security code via text message or voice call to the number you registered in EIDM .

For your protection a security code sent via SMS or Voice counts down from a 10-minute timer.

Can I access multiple Applications if I'm multi-factor authenticated?

Once you have been multi-factor authenticated (i.e. "logged in") into CJR Support Team , if you do not log out of the system, you can access other protected CMS Applications that require MFA without having to be authenticated again with an MFA credential. If you log out of the system, when you log in, you will be asked to present your MFA credential when accessing a protected CMS Application.

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 phone 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. If you choose not to use the software option and select SMS or Voice OTP, carrier charges may apply.