Centers for Medicare & Medicaid Services
CMS eXpedited Life Cycle (XLC)

Identity Management (IDM) System

Quick Start Remote Identity Proofing (RIDP) User Guide

Version 0.06

11/14/2023

Document Number: Quick Start Remote Identity Proofing (RIDP) User Guide

Contract Number: HHSM-500-2017-00015I TO HHSM-500-T0001

Last Reviewed: 11/14/2023

Table of Contents

List of Figures

List of Tables

1. Introduction

The Centers for Medicare & Medicaid Services (CMS) is a federal agency that ensures health care coverage for more than 100 million Americans. CMS administers Medicare and Medicaid and provides funds and guidance for all of the 50 states in the nation, for their Medicaid programs, and Children's Health Insurance Program (CHIP). CMS works together with the CMS community and organizations in delivering improved and better coordinated care.

1.1 Identity Management (IDM) System Overview

CMS created the IDM system to provide Business Partners with a means to request and obtain a single User ID which they can use to access one or more CMS applications. The IDM system uses a cloud-based distributed architecture that supports the needs of both legacy and new applications while providing an improved user experience on desktop and laptop computers as well as tablet and smartphone mobile devices.

1.2 Purpose of the Quick Start Remote Identity Proofing (RIDP) User Guide

This quick start user guide provides the user with basic step-by-step instructions on how to use the following core functions of the IDM user interface:

- **RIDP:** An automated web-enabled process that verifies a user's identity quickly and securely.

2. Remote Identity Proofing

2.1 Overview of Remote Identity Proofing

RIDP is an important component of the CMS IDM system. It provides application owners with a basis to establish a high Identity Assurance Level (IAL) that a user is, in fact, who they claim to be.

RIDP makes use of a web service and data provided by Experian, a consumer credit reporting company. Experian uses information from a user's credit history to remotely confirm the user's identity.

2.2 Description of the RIDP Process

Remote Identity Proofing is a process that permits a user to verify their identity quickly and reliably by providing evidence to support their claim using a highly reliable computer-based automated service.

Remote identity proofing is a simple process that consists of the following stages:

1. Review and accept the RIDP Terms and Conditions.
2. Verify personally identifiable information (PII).
3. Recover from a failed RIDP session (only necessary if a previous attempt failed).

3. RIDP Calling Options and User Authentication Procedure

This section provides information and procedures for calling RIDP and the RIDP authentication process.

3.1 Options for Calling RIDP

The RIDP process can be called by clicking or entering the following URLs for the respective environments as listed in **Table 1: RIDP Standalone Mode URLs.**

Table 1: RIDP Standalone Mode URLs

Environment	URL
Test	https://test.home.idm.cms.gov/ridp/?ial=IAL2?success-url=<url>&failed-url=<url>
Impl	https://impl.home.idm.cms.gov/ridp/?ial=IAL2?success-url=<url>&failed-url=<url>
Prod	https://home.idm.cms.gov/ridp/?ial=IAL2?success-url=<url>&failed-url=<url>

Each URL contains parameters that will vary based on the calling application **Table 2: Standalone URL Parameters** summarizes those parameters.

Table 2: Standalone URL Parameters

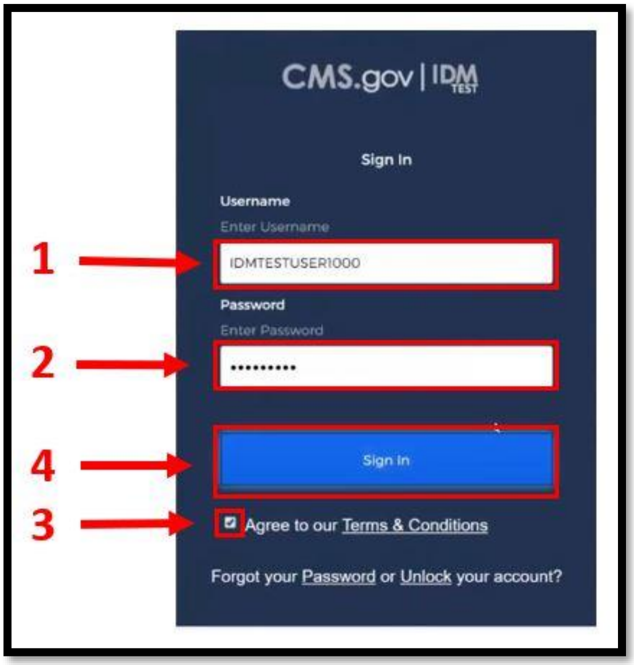
Parameter	Value(s)	Meaning
ial	IAL2	The requested Identity Assurance Level
success-url	<url>	The URL to which the user should be redirected after completing the RIDP process successfully.
failed-url	<url>	The URL to which the user should be redirected in case of any failure.

3.2 The RIDP User Authentication Procedure

This section provides the procedure for how to authenticate to the CMS IDM system. The IDM system authenticates the user and permits the user to access the RIDP application with the proper IAL.

Note(s):

1. If the user has previously authenticated to the IDM system **AND** their session **HAS NOT** expired, the user will be taken directly to the RIDP user interface.
2. If the user has previously authenticated to the IDM system **BUT** their session **HAS** expired, the user will be taken to the IDM login screen.



CMS.gov | IDM TEST

Sign In

Username

Enter Username

IDMTESTUSER1000

Password

Enter Password

•••••••••

Sign In

☑ Agree to our Terms & Conditions

Forgot your Password or Unlock your account?

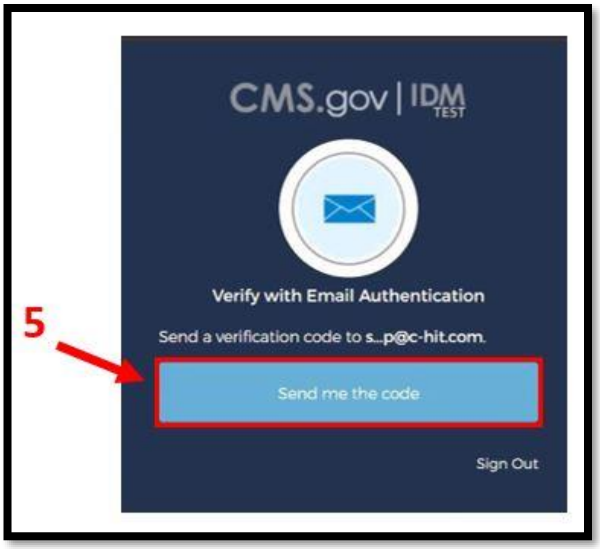
Figure 1: IDM Login Screen (Username, Password, and Terms Agreement)

Step 1: ***Type*** the **Username** into the **Username** dialog box.

Step 2: ***Type*** the **Password** into the **Password** dialog box.

Step 3: ***Click*** the checkbox to acknowledge agreement with the **Terms & Conditions.**

Step 4: ***Click*** the green **Sign In** button.



CMS.gov | IDM TEST

Verify with Email Authentication

Send a verification code to s...p@c-hit.com.

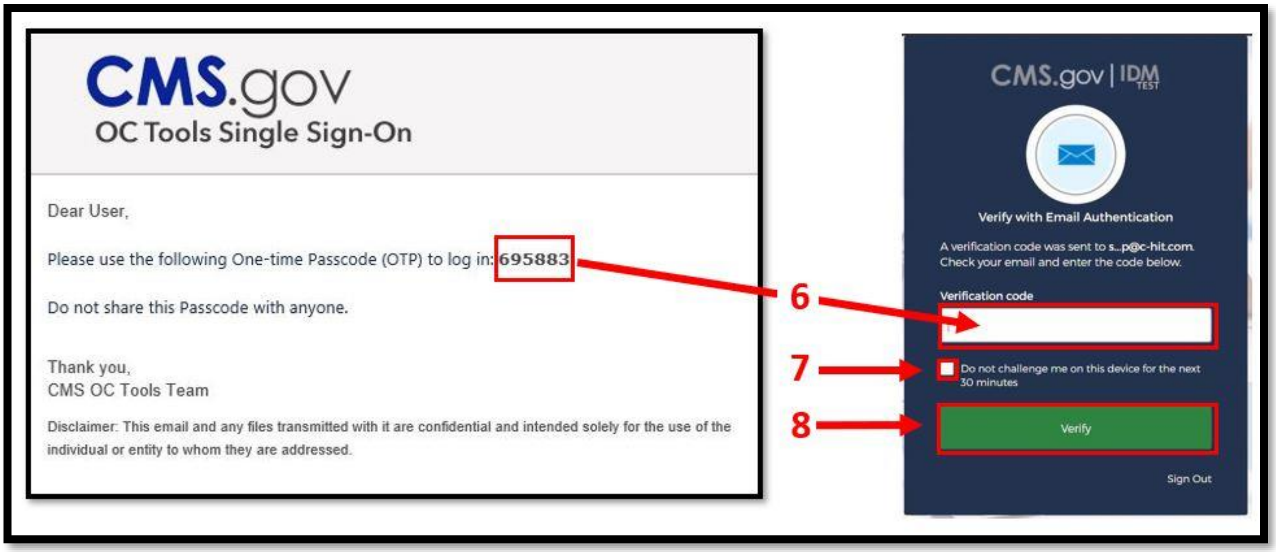
Figure 2: MFA OTP Request Window

Step 5: When the Multi-factor Authentication (MFA) One-time Password (OTP) Request window appears, ***Click*** the **Send me the code** button to request an OTP.

- The OTP delivery method can be an email, a voice message, a text message, or a push notification based on the user's MFA device choice.

Note(s):

1. The IDM system uses Email MFA by default, but it allows the user to use other MFA devices. If an alternate MFA device is used, then Step 5, Step 6, and Step 7 will vary slightly in the way a user requests and receives the OTP. In addition to Email MFA, IDM currently supports the following MFA devices:
    a. Interactive Voice Response (IVR)
    b. Google Authenticator
    c. Okta Verify
    d. Short Message Service (SMS) Text Message
    e. YubiKey
2. In some cases, users may not be required to use MFA verification. If MFA is not required, Step 5, Step 6, and Step 7 will be skipped, and the system will proceed to the LOA check phase.



CMS.gov
OC Tools Single Sign-On

Dear User,

Please use the following One-time Passcode (OTP) to log in: 695883

Do not share this Passcode with anyone.

Thank you,
CMS OC Tools Team

Disclaimer: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed.

CMS.gov | IDM TEST

Verify with Email Authentication

A verification code was sent to s...p@c-hit.com. Check your email and enter the code below.

Verification code

□ Do not challenge me on this device for the next 30 minutes

Figure 3: MFA OTP Email and MFA Verification Window

Step 6: The MFA device will return a six-digit OTP. ***Type*** the **OTP** into the **Verification Code** dialog box. If the MFA device uses push notifications, a code will not be required.

Step 7: ***(Optional) Click*** the checkbox to select the option "**Do not challenge me on this device for the next 30 minutes**".

- If this step is performed, users will bypass the MFA verification phase of the authentication process if they logoff and log back onto the system again within 30 minutes of completing this MFA verification event.

Step 8: ***Click*** the **Verify** button.

Identity Assurance Level (IAL) Checks

A user's identity assurance level is used to indicate the level of confidence that a given user is who they say they are based on the information they provide to the system during the initial account creation process and during subsequent logins and system use.

There are two IALs: IAL 1 and IAL 2; where IAL 1 represents the lowest Identity Assurance Level and IAL 2 represents the highest Identity Assurance Level. The following general guidelines pertain to a user's IAL:

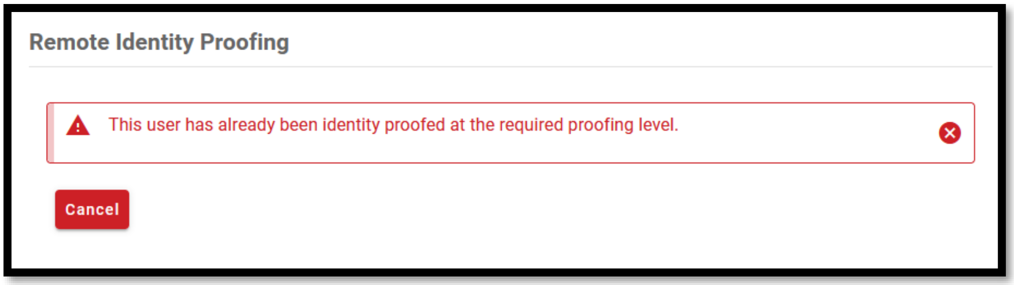
- A user is IAL 1 by default as soon as they register.
- Once IAL 2 is reached, no changes can be made to the IAL.

Once the user authenticates to the system, the requested IAL will be checked against the user's existing IAL if one exists. The RIDP process will not initiate if the following condition exists:

- The requested IAL is equal to the existing IAL.

Requested IAL is Equal to Existing IAL: The RIDP process will not initiate if the user possesses an IAL that is equal to the requested IAL. The following will occur instead:

- The system will display a message that states, "**This user has already been identity proofed at the required proofing level.**"
- ***Click*** the red **Cancel** button.



Remote Identity Proofing

This user has already been identity proofed at the required proofing level.

Figure 4: IAL Check Response Message for Requested IAL Equal to Existing IAL

4. Procedure to Complete the RIDP Process

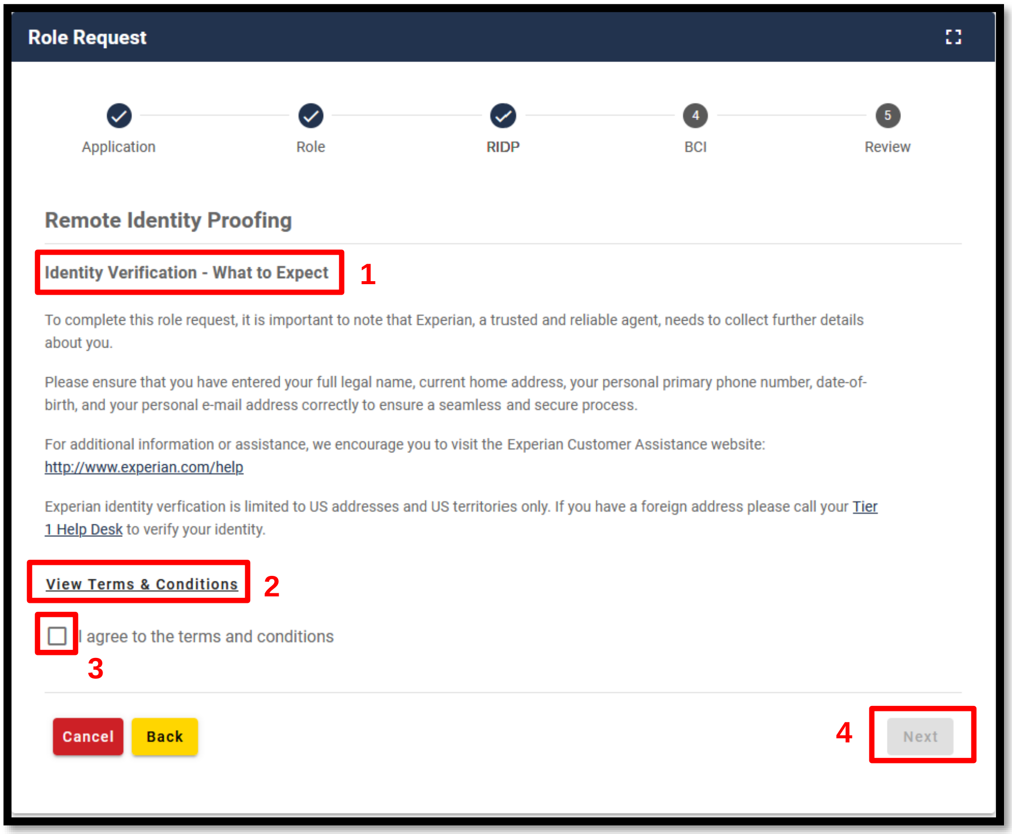
This section provides the procedure for how to use the RIDP application.

4.1 Review and Accept the RIDP Terms and Conditions

The initial page provides an overview of the RIDP process and provides users with an opportunity to review the RIDP terms and conditions. The procedure in this section provides the steps to review and accept the RIDP terms and conditions.

Note(s):

1. The **Next** button will not turn green nor will it become selectable until agreement with the terms and conditions have been acknowledged.



Remote Identity Proofing

Identity Verification - What to Expect

To complete this role request, it is important to note that Experian, a trusted and reliable agent, needs to collect further details about you.

Please ensure that you have entered your full legal name, current home address, your personal primary phone number, date-of-birth, and your personal e-mail address correctly to ensure a seamless and secure process.

For additional information or assistance, we encourage you to visit the Experian Customer Assistance website: http://www.experian.com/help

Experian identity verfication is limited to US addresses and US territories only. If you have a foreign address please call your Tier 1 Help Desk to verify your identity.

View Terms & Conditions

□ I agree to the terms and conditions

Figure 5: RIDP Overview Page with Link to Terms and Conditions

Step 1: ***Review*** the **IDENTITY VERIFICATION** description statement.

Step 2: ***Click*** the "**View Terms & Conditions**" link to review the RIDP terms and conditions.

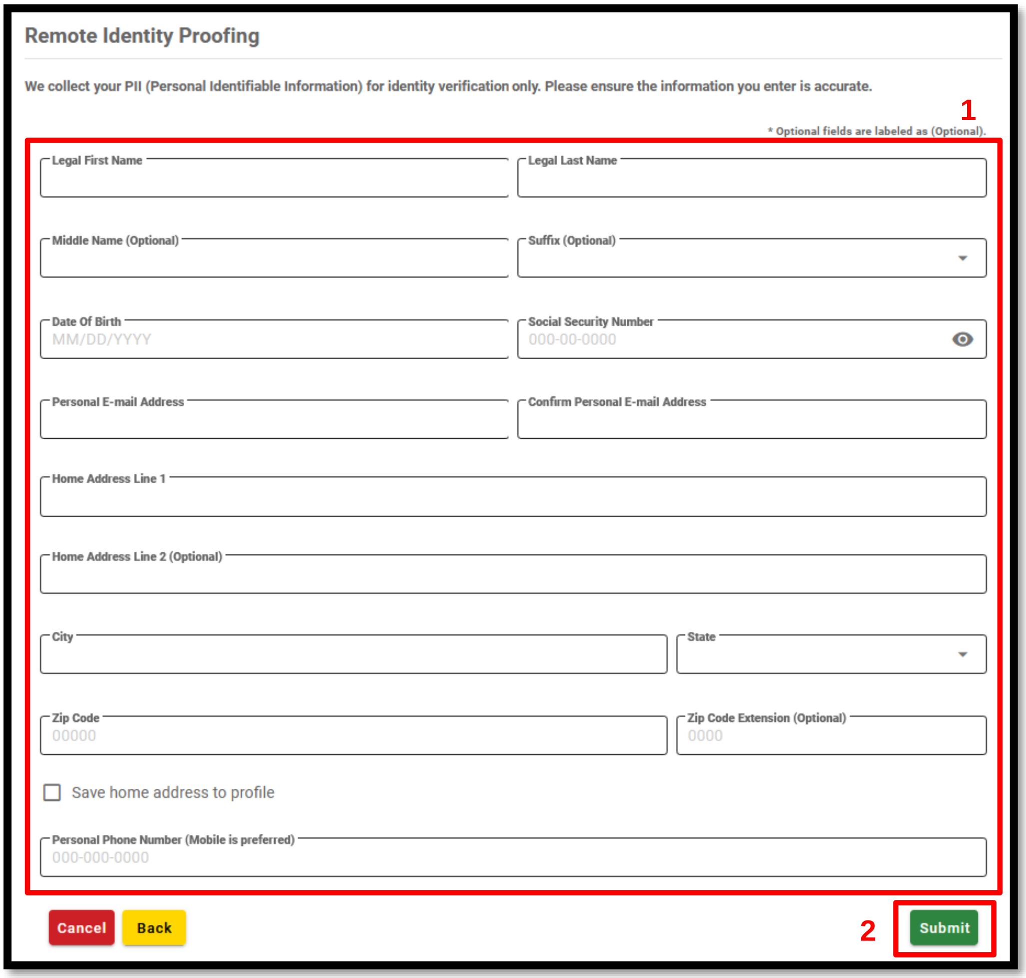
Step 3: ***Click*** the "**I agree to the terms and conditions**" checkbox.

Step 4: ***Click*** the green **Next** button.

4.2 Verify Personally Identifiable Information (PII)

This stage of the RIDP process verifies the user's identity based on the personally identifiable information (PII) that they provide using this form. The procedure in this section provides the steps users must follow to fill out the PII verification form.

The PII entered into this form will directly impact the decision to grant a higher IAL if the role being requested requires a higher IAL than what the user currently has for a given application.



Remote Identity Proofing

We collect your PII (Personal Identifiable Information) for identity verification only. Please ensure the information you enter is accurate.

* Optional fields are labeled as (Optional).

Figure 6: RIDP PII Verification Form

Step 1: ***Type*** the legal name, date of birth, social security number, personal email address, home address information, and personal mobile phone number into the respective fields.

Step 2: ***Click*** the green **Submit** button.

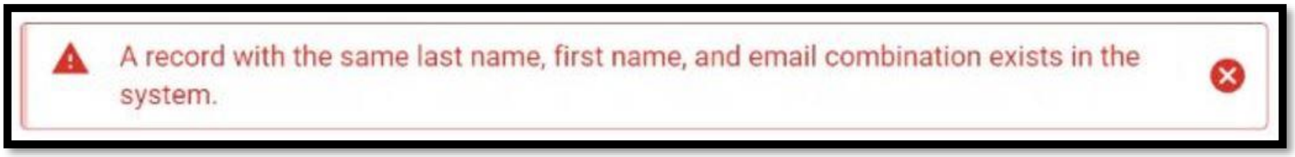
PII Data Validation

When a user submits PII data, that data is subject to local PII validation checks. The purpose of these checks is to maintain the integrity of the user information that is used by the IDM system for user authentication. The following three validation checks are performed:

- The combination of the user's first name, last name, and email address must be unique in IDM.
- The SSN must be unique in IDM.
- The same PII must not be submitted again after a failed RIDP attempt.

The combination of last name, first name, and email address is not unique in IDM: This condition will cause a message to be displayed which states, "**A record with the same last name, first name, and email combination exists in the system.**" as shown in **Figure 7**: .

- If this message appears, review the information that was entered into the form. If it was entered correctly, contact the Application Helpdesk.

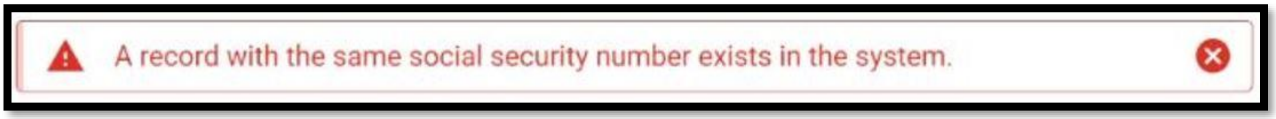


A record with the same last name, first name, and email combination exists in the system.

Figure 7: Data Validation Error Message for Name and Email

The social security number is not unique in IDM: This condition will cause a message to be displayed which states, "**A record with the same social security number exists in the system.**" as shown in **Figure 8**: Same Social Security Number Exists in System**.**

- If this message appears, review the information that was entered into the form. If it was entered correctly, contact the Application Helpdesk.

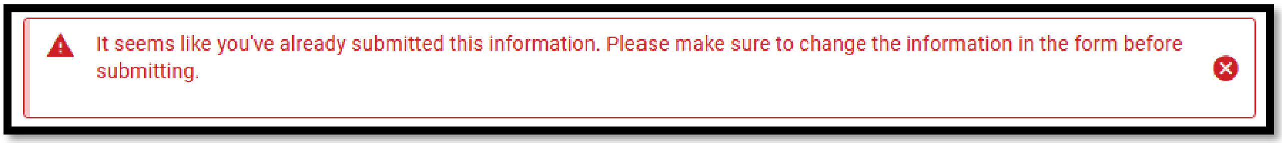


A record with the same social security number exists in the system.

Figure 8: Same Social Security Number Exists in System

The same PII is submitted after a failed RIDP attempt: This condition will cause a message to be displayed which states, "It seems like you've already submitted this information. Please make sure to change the information in the form before submitting." as shown in **Figure 9: Previously Submitted Information.**

- If this message appears, review the information that was entered into the form and update any information that may be inaccurate or entered incorrectly before resubmitting.



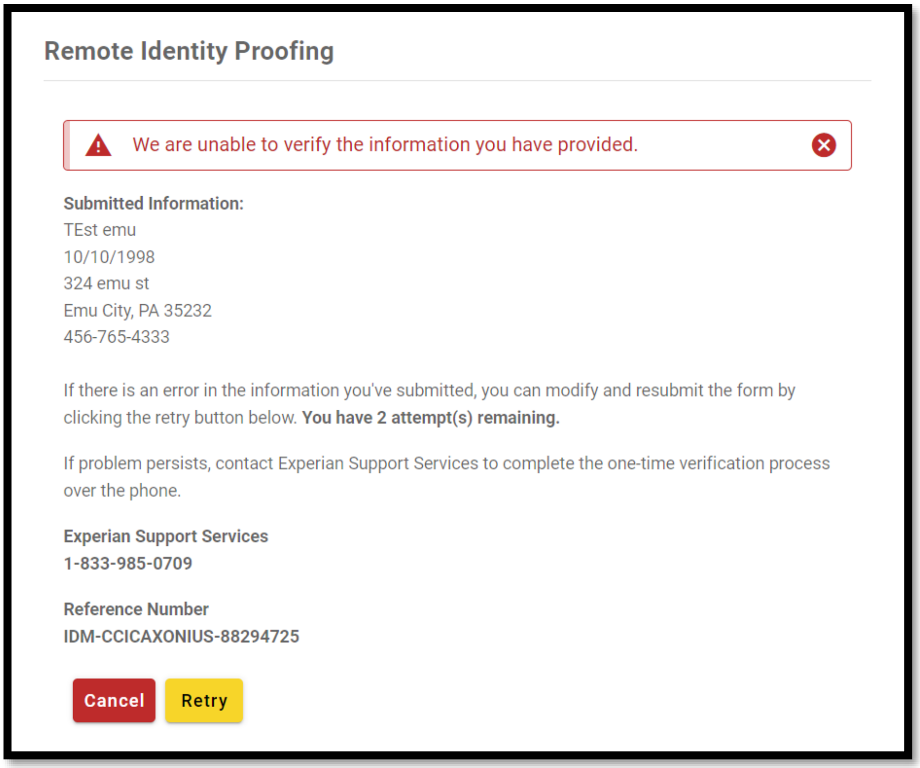
It seems like you've already submitted this information. Please make sure to change the information in the form before submitting.

Figure 9: Previously Submitted Information

Experian PII Data Validation

If Experian is unable to verify the PII information that was submitted using the PII data validation form, the error message illustrated in Error! Reference source not found. will be displayed with the number of attempts remaining**.** If the user has attempted the form more than 3 times without successful verification of the information, **Figure 11** will be displayed.

- Write down the **error message** and the **Reference Number** that is displayed, then contact the Application Helpdesk. The Application Helpdesk will most likely provide instructions to contact Experian and they may instruct the user to follow the procedure in **Section 4.3.**



Remote Identity Proofing

We are unable to verify the information you have provided.

Submitted Information:
TEst emu
10/10/1998
324 emu st
Emu City, PA 35232
456-765-4333

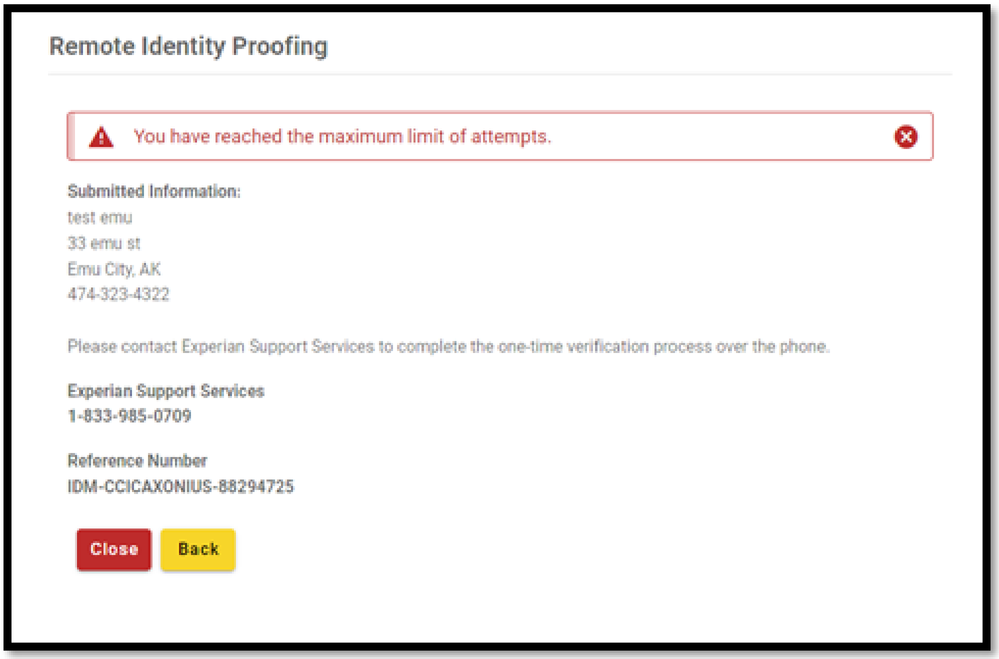
If there is an error in the information you've submitted, you can modify and resubmit the form by clicking the retry button below. **You have 2 attempt(s) remaining.**

If problem persists, contact Experian Support Services to complete the one-time verification process over the phone.

Experian Support Services
1-833-985-0709

Reference Number
IDM-CCICAXONIUS-88294725

Figure 10: Experian PII Verification Error Message and Attempts Remaining



Remote Identity Proofing

You have reached the maximum limit of attempts.

Submitted Information:
test emu
33 emu st
Emu City, AK
474-323-4322

Please contact Experian Support Services to complete the one-time verification process over the phone.

Experian Support Services
1-833-985-0709

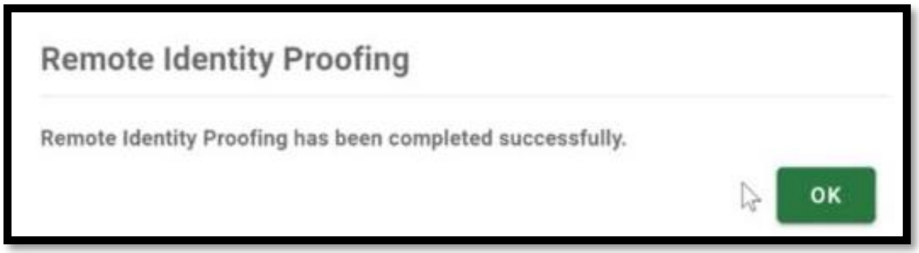
Reference Number
IDM-CCICAXONIUS-88294725

Figure 11: Experian PII Max Retries Error Message

Step 3: **Users that reside at a foreign address will not be able to complete the identity verification process online using this form**. Users with a foreign address must:

- Contact the respective Application Helpdesk.
- Contact Experian as directed by a warning message that will appear.

Step 4: If a successful response is returned from Experian, a window will display a message indicating that “**Remote Identity Proofing has been completed successfully**”.



Remote Identity Proofing

Remote Identity Proofing has been completed successfully.

Figure 10: RIDP Success Message

Step 5: ***Click*** the green **OK** button.

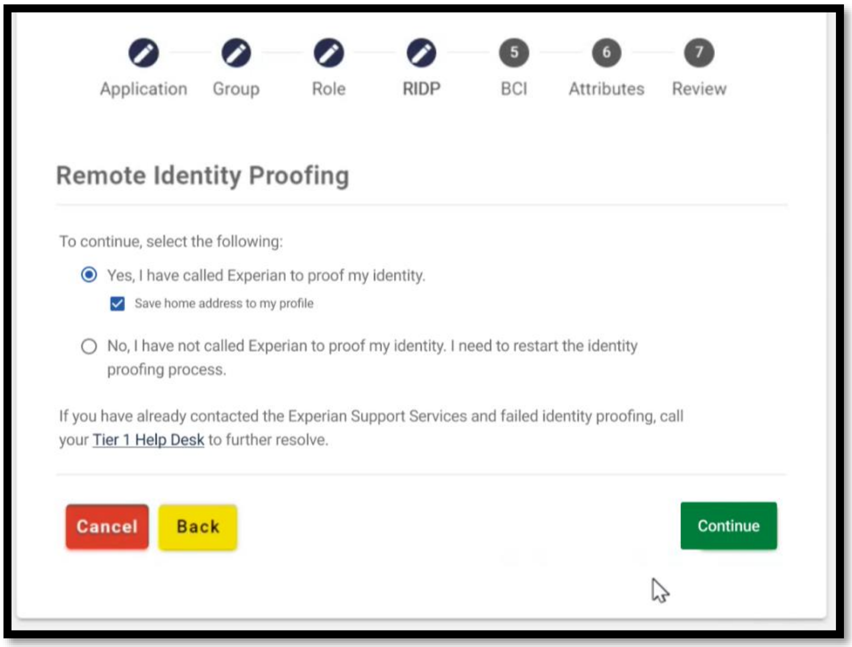
- After the OK button is clicked, the user will be returned to the original process or application that triggered the RIDP procedure. This path will be identified by the **success-url** parameter that was provided by the application that called the RIDP process.

4.3 Failed RIDP Recovery Procedure

This section provides instructions that must be followed if Experian is unable to verify the PII. The procedure in this section provides the steps that must be followed to recover from a failed attempt to remotely verify the user's identity.

Note(s):

1. The user must logout of the IDM system and contact the Application Helpdesk before trying to recover from a failed RIDP attempt. The Application Helpdesk will provide instructions based on the "Reference Number" that was displayed in the web browser.
2. If the Application Helpdesk advises the user to contact Experian, they **must** do so. If they attempt to proceed without contacting Experian, all attempts to use the RIDP procedure will fail. ***Click*** the red **Cancel** button if Experian has not been contacted.



Remote Identity Proofing

To continue, select the following:

● Yes, I have called Experian to proof my identity.

☑ Save home address to my profile

○ No, I have not called Experian to proof my identity. I need to restart the identity proofing process.

If you have already contacted the Experian Support Services and failed identity proofing, call your Tier 1 Help Desk to further resolve.

Figure 11: Experian Identity Verification Confirmation

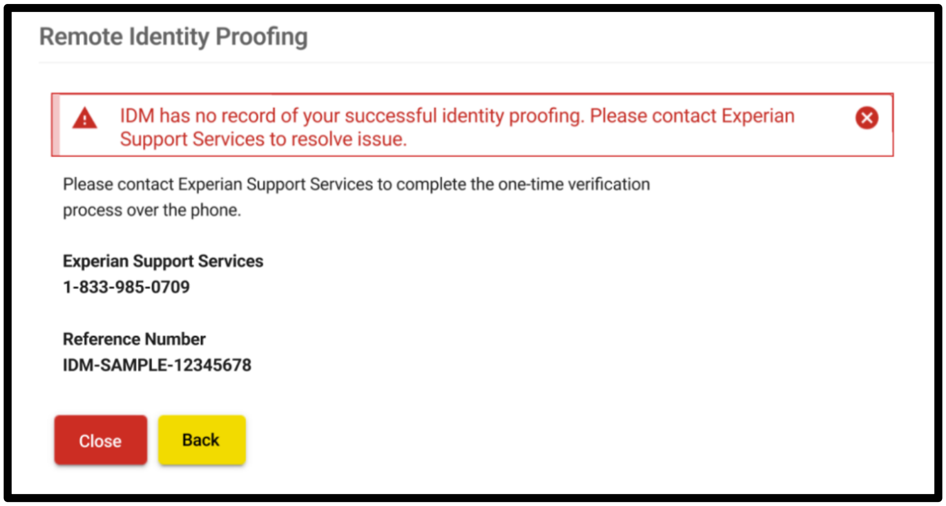
Step 1: ***Login*** to the CMS IDM system. The RIDP application will be aware of the previous failed attempt and will display a window with a message which asks if Experian has been contacted.

Step 2: Click the "*Yes, I have called Experian to proof my identity*" radio button if Experian has been contacted. Then, click the "Save home address to my profile" radio button to overwrite the existing home address in your profile with the address used to identity proof.

Step 3: ***Click*** the green **Next** button.

RIDP Phone Verification Failure

If IDM is unable to find a record of successful phone proofing, a window will display the error message illustrated in **Figure 12**: RIDP Phone Verification Failure.



Remote Identity Proofing

IDM has no record of your successful identity proofing. Please contact Experian Support Services to resolve issue.

Please contact Experian Support Services to complete the one-time verification process over the phone.

Experian Support Services
1-833-985-0709

Reference Number
IDM-SAMPLE-12345678

Figure 12: RIDP Phone Verification Failure

Step 5: ***Click*** the red **Close** button or the yellow **Back** button.

- The **Close** button returns the user to the dashboard.
- The **Back** button returns a user to the beginning of the RIDP process.

Appendix A: Record of Changes

Table 3 Record of Changes

Version Number	Date	Author/Owner	Description of Change	Approval(s)
0.01	07/13/2020	C-HIT	Initial draft: • Assign document title: Quick Start RIDP User Guide.	
0.02	07/20/2020	C-HIT	• Revised document style to reflect 3rd person point view. • Updated Figure 1 and Figure 12.	
0.03	06/13/2023	Omni/Bana	Removed references to KBA and added references to RBA	
0.04	08/15/2023	Omni/Bana	• Updated Figure 11 and Figure 14 • Updated sections 4.2 and 4.3 to remove references to proofing questions.	
0.05	10/02/2023	Omni/Bana	• At the top of section 4.3, “Response Code” has been changed to “Reference Number” in the notes to be consistent with email notifications	
0.06	11/14/2023	Omni/Bana	• Replaced Figures 10 and 11 in section 4.2 in accordance with new UI updates (max retries/number of attempts remaining features). Updated description directly above these two figures.	

Appendix B: Acronyms

Table 4: Acronyms

Acronym	Literal Translation
C-HIT	Chags Health Information Technology
CMS	Centers for Medicare & Medicaid Services
EIDM	Enterprise Identity Management
IDM	Identity Management
IVR	Interactive Voice Response
LOA	Level of Assurance
MFA	Multi-factor Authentication
OTP	One-time Password
PII	Personally Identifiable Information
RIDP	Remote Identity Proofing
SMS	Short Message Service
SSN	Social Security Number