All claimants must verify their identities in ECOMP. There are three identity verification options a user can qualify for: text message code, phone call code, and credit bureau questions. On a user’s first login, they will get two initial identity verification attempts. If either attempt is successful, they are considered a verified user with complete account permissions. If a user does not successfully complete verify their identity, they are considered an unverified user with limited account permissions. Each time an unverified user logs on, they will be prompted to retry verification. If a user fails verification nine times within 30 days, they will not see the retry options for 30 days to avoid setting a fraud alert with the credit bureaus.

The following is a step by step walkthrough of the identity verification process for claimants.

For a New User:

Once a user has successfully registered and upon their first login, they will see an identity verification screen. The user will need to review their information. If they need to change any information they can click “No” to access editable fields where their information can be updated. If their information is correct they can click “Yes” to proceed to the next step.

For an Existing User:

On a claimant’s first login after this enhancement is added to ECOMP, they will see an identity verification screen requesting additional personal information, which needs to be provided to proceed.

Once they have confirmed their information, they are presented with the identity verification options for which they qualify. Users who qualify for text message or phone call verification will see those options as well as the option to verify via credit bureau generated questions. Users who don’t qualify for text or phone call verification will automatically go to the credit bureau generated questions.

Users who selected the code verification option will proceed to enter the code they receive via text message or phone call in the field provided. If the user has any issue with the code, there is a link below the button for them to attempt the credit bureau generated questions.

If a user fails identity verification the first time, they will receive a pushdown notifying them they have failed and need to try again. Users will be asked to review their identity information again to ensure accuracy before proceeding. Most identity verification failures are a result of user information input error.

If the user does wish to update their information at this step, they may click the “No” button in response to, “Is this information correct?” When the user selects “No,” the information becomes editable where they may input any updates and click next to proceed.
Upon their second attempt, users who qualify for the text message or phone call verification option will now see those options along with credit bureau generated questions. Once again, if a user does not qualify for the text message or phone call verification options, they will be directed to the credit bureau generated questions.

All users will then be directed to their dashboard whether they pass or fail the verification attempt. Verified users will see a blue successful verification pushdown and unverified users will see a red unsuccessful verification pushdown with a retry text link.

Once a user is verified, if they attempt to change their name, date of birth, or social security number in their account information, they will need to re-verify their identity by going through the identification process once again. Before updating this information, they will see a modal to confirm that they would like to update and re-verify or cancel.

Each time unverified users' login into their account, they will see the red pushdown notification with a retry link as long as they have remaining attempts.

Users are allotted 9 identity verification attempts every 30 days. The reason for this restriction is that 10 failed attempts would set a fraud alert with the major credit bureaus, which could affect personal finances.

If a user has no remaining attempts, they will see a red pushdown notification informing them that they can try again in 30 days.

Unverified users will also see a button to verify their identity on their account settings page.

Please note that after a user fails identity verification three times, an email will be sent to the user about the suspicious activity. The email will include details of the user’s most recent login. There will also be a text link for the user to select if this activity was not performed by them and to report their account as compromised. If the user does not respond to the email by clicking the link, no further action is taken by the system nor the security team.

If the user clicks the text link from the email to indicate their account has been compromised, they are redirected to a popup. The user will need to confirm that they have reviewed the details from the email and that it was not them who made the identity verification attempts and alerting them that if they confirm they must reset their password to access ECOMP.

If the user clicks the “CONFIRM” button on the popup, they will see a Reset Password screen and a pushdown notification informing them that the Security Team has been notified of the issue. The user will then be offered a password reset flow to re-secure their account and sustain ECOMP access.
The user will get a confirmation email that the Security Team has been notified. Included in the email will be a link for the user to reset their password in the event they did not reset their password after clicking “Confirm” on the popup.

The Security Team will receive an email with information about the user and details of the failed verification attempts.