

What to do if you are victim of Identity Theft?

If you were victim of an Identity (ID) theft or your UC claim was hijacked, you need to contact the UC Service Center (UCSC) in order for, the UCSC staff, to create a work item for UC Fraud Unit.

Please dial 888-313-7284 from Monday to Friday from 8:00 am to 4:30 pm to contact the UC Service Center (UCSC) staff and get a ticket number.

Once you contact the UCSC staff they will do the following actions depending on what category the caller is under. The UCSC staff is not allowed to share claim information and do not make any changes to the claim, such as address, phone number, email, etc. They will make changes **only** on specific circumstances

1. Call from SSN owner/Victim

The UCSC staff should complete an ID theft fraud report with the caller over the phone.

If payments were issued. If payments were received by the victim, the UCSC staff will instruct the victim to follow the guidance posted on the UC website (www.uc.pa.gov). If payments were issued, but the victim did not receive them, the UCSC staff will conduct further investigation.

The UCSC staff will take an official statement from the caller, and it will be sent to the Adjudication department. The Examiner will mail a letter to the victims of the ID theft letting them know that additional information is needed. Please complete the form upon received.

If payments were not issued. No additional information is needed from the victims of the ID theft.

Note: In situations where a victim of ID theft needs to file a claim of their own but cannot because a claim has already been opened by a fraudster, UCSC staff should follow the steps listed above. The Fraud Unit will contact the victim and it will take care of fraudulent claim. Once the process is complete, the victim will be notified that they can open a claim of their own.

2. Hijacked Claims

A Hijacked claim is when the fraudster has taken control of the UC claim, changing method of payments, addresses, phone numbers, email addresses. Sometimes the claimant can log in on the UC Benefits system using the same credentials (Keystone ID and password), but notices some weeks claimed, method of payments has changed, and some personal information changed as well.

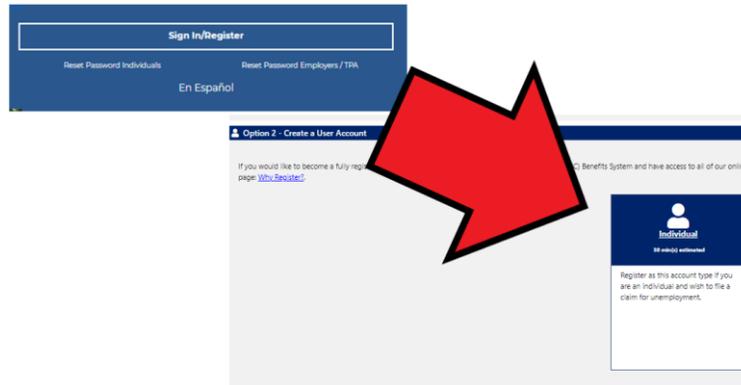
Note: If you notice that only the Method of Payment has changed, and you cannot change it back, please do not call the Department of Treasury. Your UC claim has been Hijacked, and you need to contact the UCSC.

Sometimes the claimant cannot log in at all to the UC Benefits system meaning the fraudster changed the logging information.

If you can log in or not, but your claim has been hijacked you need to contact the UCSC. When the claimant contacts the UCSC staff, they will complete the fraud report with the victim. While the claimant is on the phone, staff review the claim to determine what was changed by the fraudster/hijacker. UCSC Staff will pay particular attention to email, address, zip code, and DOB.

UCSC Staff should make the necessary changes back to what the claimant had originally put in the system when they opened their claim. Once this is complete, staff should remain on the phone with the claimant and inform them to register for a new Keystone ID.

- The claimant should select Sign In/Register at www.benefits.uc.pa.gov, then select Individual.



- The claimant will need to create a new Keystone ID (username) and Password, enter the First Name, Last Name, and Date of Birth in the way that appears on the UC claim. If the UCSC Staff does not take care of changing the information back, the claimant will not be able to change the Keystone ID, and the claimant will be in a loop. That is the reason that you need to talk with the UCSC Representative. Also, all three security questions must change, and then click submit.

Your Information

* **User Name:** Enter User Name (3 - 20 characters, and must include characters, letters or numbers. Allowable characters are - + @ . _)

* **Password:** Enter Password (8 - 18 characters, and must include at least one uppercase letter, one lowercase letter, one number and one special character. Allowable characters are # @ \$ % ^ . ! * _ +)

* **Password Confirm:**

* **First Name:**

* **Last Name:**

* **Date of Birth:** (mm/dd/yyyy)

Security Question Responses must not be duplicated across multiple questions.
Also, Security Question Responses can not contain any part of the question corresponding to the Response.

* **Security Question 1:**

* **Security Question Response 1:**

* **Security Question 2:**

* **Security Question Response 2:**

* **Security Question 3:**

* **Security Question Response 3:**

- Then you will be presented with the following screen. Click “No” when asked if they are attempting to file a UC claim.

Unemployment Insurance Compensation

This system allows you to file an Unemployment Insurance compensation claim. Please confirm your actions below.

* **Are you attempting to file an Unemployment Insurance claim at this time?** Yes No

[Next >>](#)

- After selecting next, the Verify ID.me is now prompted. The change here is that the original Keystone ID will no longer be linked to the Verify ID.me and this UC account. The one that the claimant just created will be linked as soon as the verification from the ID.me site goes through. The claimant can use their previously created ID.me credentials to verify or they will have to go through the ID.me process if they haven't already.



- If payments were issued while the claim was hijacked, staff should report the hijacked claim to the Fraud Unit, and all the weeks paid to the fraudster will be included. If no payments were issued staff do not need to notify the fraud unit.

Once all the information is being taken/processed by UCSC Staff, the hijacked claim is on hands of the UC Fraud Unit. They will contact you to verify that you are the right person, and they will tell you when you can resume with your UC claim. At this moment there is not a time frame for the UC Fraud unit to resolve all the fraudulent activities.