TRAINING AND EMPLOYMENT NOTICE	NO. 14-22
	DATE January 4, 2023

TO: STATE WORKFORCE AGENCIES

FROM: BRENT PARTON /s/
Acting Assistant Secretary

SUBJECT: Updated Unemployment Insurance (UI) Identity (ID) Fraud Reporting Website Content

1. **Purpose.** To announce the release of updated content published on the UI ID fraud reporting website at www.dol.gov/fraud and to encourage states to align their public messaging with the new content and reporting instructions on this website.

2. **Action Requested.** The U.S. Department of Labor's (Department) Employment and Training Administration (ETA) requests that State Administrators provide the information in this Training and Employment Notice (TEN) to appropriate program and other staff in state workforce agencies.

3. **Summary and Background.**

   a. Summary – This TEN announces the release of updated content published on the unemployment ID fraud reporting website at www.dol.gov/fraud and encourages states to align their public messaging with the content and reporting instructions on this website. This TEN also reminds states about the importance of protecting the rights of those individuals experiencing unemployment ID fraud.

   b. Background – On March 22, 2021, the Department launched www.dol.gov/fraud, a website created to help people understand unemployment ID fraud, how to report it, and to provide resources to help individuals experiencing unemployment ID fraud. The Department worked collaboratively with other federal government agencies, federal law enforcement partners, and state UI agencies to consolidate the necessary steps to report unemployment ID fraud, validate state contact information and fraud reporting resources, and conduct user testing to confirm the website's instructions were clear and easy to understand.

   At the time of the initial website launch, the Department referred to unemployment ID fraud as unemployment "ID theft" and the website content reflected this same language. On August 11, 2021, ETA issued two Unemployment Insurance Program Letters (UIPL) introducing and defining the two different types of UI fraud (eligibility fraud and ID fraud) occurring within the unemployment compensation (UC) programs. *See* UIPL Nos. 28-20, Change 2, and 22-21. ETA further defined the two types of UI fraud in UIPL No. 20-21, Change 1, issued on February 7, 2022, and reminded states about the requirement

to protect individuals who suspect their ID was stolen and used by others to apply for UI benefits by providing easily accessible options to report fraudulent activity.

UI ID fraud occurs when one person or group of persons use(s) the identifying information of another person to illegally receive benefits. UI ID fraud also occurs when an individual's UI account is hacked or taken over by a person or group and the benefit payments are re-directed to another account by changing key user data after the claim has been established (*e.g.*, banking information). In addition to using stolen identities or misusing an individual's identity, synthetic ID fraud occurs when real and/or fake information is combined to create false IDs.

4. **Website Updates.** On December 1, 2022, the Department published updated website content on the unemployment ID fraud reporting website at www.dol.gov/fraud. The new content replaces the term "ID theft" with ID fraud" to make clear that, in most circumstances, an individual is not becoming a victim of ID theft when they file for unemployment. In most unemployment ID fraud cases, the victim's personally identifiable information (PII) was already stolen through a past data breach, sold or purchased on the dark web, obtained through an email phishing or text message smishing scheme, or attained through some other means of fraudulent activity. These already stolen identities are then being used to file for and receive UI benefits. For UI purposes, it is important for ETA and state UI agencies to clarify the difference between the terms "ID theft" and "ID fraud", so people are not fearful that their identity will be stolen when they file a UI claim.

   In addition, the updated website content consolidates prior information and adds increased readability by ensuring the usage of plain language. The new content also introduces terminology on "Claim Hijacking" or "Claim/Account Takeover" and strengthens the public message about protecting PII by encouraging individuals to **never** send PII or documents to unverified sites and to **never** click on links from unknown senders or in response to requests from social media, email, or text messages.

   Reminder to States to Protect Victims of UI ID Fraud. As described in Section 5 of UIPL No. 16-21, states must provide individuals who suspect that their ID has been stolen and used to file UI claims with easily accessible options to report such theft or fraudulent activity. This may include dedicated phone options, email addresses, or an online portal by which individuals can notify the state agency. States may also provide links to other agencies that specialize in protecting individuals and their PII, such as the Federal Trade Commission's Consumer website at https://consumer.ftc.gov/identity-theft-and-online-security/identity-theft.

   ETA encourages states to ensure the state's UI fraud reporting requirements are clearly communicated on their state website(s) and have in place established processes and procedures for removing barriers for individuals who have experienced unemployment ID fraud. To reduce confusion and anxiety for a victim of unemployment ID fraud, states should provide updates throughout the process once a report of unemployment ID fraud has been received. This may include, but is not limited to:

- Providing confirmation that the fraud report was received;
- Clearly defining expectations and outlining next steps;
- Providing ongoing updates throughout the investigation; and
- Notifying the individual once the investigation is complete.

When a state determines that UI ID fraud has occurred the state must take actions to protect the rights of the ID fraud victim. As discussed in UIPL No. 20-21, Change 1, once the state issues a fraud determination, one option states can use to mitigate negative impacts on the ID fraud victim is to establish a pseudo claim record and transfer all claim information regarding the fraudulent activity to the pseudo claim. This removes the fraudulent activity from the victim's SSN and/or UI account, should the victim need to file for UI in the future. This also applies to "claim hijacking" or "claims or account takeover". On hijacked claims, any weeks that were fraudulently redirected must be removed from the legitimate UI claim and the weeks must be immediately repaid to the rightful owner of the claim. In the case of "hijacked" claims, the state should employ ID verification as part of its investigation to verify the legitimate claimant's ID prior to repaying the weeks. States are also strongly encouraged to use the UI Integrity Center Integrity Data Hub's (IDH) Bank Account Verification (BAV) service to authenticate new bank account information provided on a "hijacked claim" prior to reissuing payments. The IDH's BAV service validates the status of the bank account (*e.g.*, account is open or closed) and provides a level of assurance that the individual identified as the UI claimant is the bank account owner and/or authorized user.

States that may not have the current administrative capability to move such activity to a pseudo claim may choose to temporarily mark the overpayment as "uncollectible." This ensures that unemployment ID fraud victim is not negatively impacted while the state develops a process to disassociate the fraudulent activity from the victim's SSN. Below are other actions the state may take to mitigate the negative consequences for the unemployment ID fraud victim:

- Ensure that if a future claim is filed under the victim's SSN, the claimant undergoes a secondary ID verification process (*e.g.*, include an in-person reporting requirement or other expanded ID verification alternatives). However, states should try to minimize the burden on the victim as much as possible when verifying identity.
- Ensure that the owner of the SSN is not held responsible for any overpayment and, whenever possible, is not issued a Form 1099G at the end of the year.
- Exclude the overpayment from the Treasury Offset Program and suspend any overpayment collection activity for the actual owner of the SSN.
- Do not initiate any legal actions against the actual owner of the SSN.

5. <u>Inquiries</u>. Please direct inquiries to the appropriate Regional Office.

6. <u>References</u>.

- UIPL No. 22-21, *Grant Opportunity to Support States with Fraud Detection and Prevention, Including Identity Verification and Overpayment Recovery Activities, in All*

Unemployment Compensation (UC) Programs, issued August 11, 2021, https://www.dol.gov/agencies/eta/advisories/unemployment-insurance-program-letter-no-22-21;

- UIPL No. 20-21, Change 1, *Additional State Instructions for Processing Waivers of Recovery of Overpayments under the Coronavirus Aid, Relief, and Economic Security (CARES) Act, as Amended*, issued February 07, 2022, https://www.dol.gov/agencies/eta/advisories/unemployment-insurance-program-letter-no-20-21-change-1;
- UIPL No. 16-21, *Identity Verification for Unemployment Insurance (UI) Claims*, issued April 13, 2021, https://www.dol.gov/agencies/eta/advisories/unemployment-insurance-program-letter-no-16-21; and
- UIPL No. 28-20, Change 2, *Additional Funding to Assist with Strengthening Fraud Detection and Prevention Efforts and the Recovery of Overpayments in the Pandemic Unemployment Assistance (PUA) and Pandemic Emergency Unemployment Compensation (PEUC) Programs, as well as Guidance on Processes for Combatting Identity Fraud*, issued August 11, 2021, https://www.dol.gov/agencies/eta/advisories/unemployment-insurance-program-letter-no-28-20-change-2;

7. **Attachment(s).** None.