U.S. Department of Justice
National Unemployment Insurance Fraud Task Force

Unemployment Insurance Fraud Consumer Protection Guide

September 21, 2020

This guide provides information and resources for individuals on how to protect themselves from unemployment insurance fraud and steps they can take if they suspect they have had their identity exploited by criminals.

The U.S. Secret Service, U.S. Department of Labor–Office of Inspector General (DOL-OIG), Federal Bureau of Investigation, Homeland Security Investigations, Internal Revenue Service–Criminal Investigation, U.S. Postal Inspection Service, Social Security Administration–Office of the Inspector General, and the U.S. Department of Homeland Security–Office of Inspector General, coordinating with the U.S. Department of Justice, are investigating numerous fraud schemes targeting the unemployment insurance (UI) programs of various state workforce agencies (SWAs) across the United States. Fraudsters, some of which are transnational criminal organizations, are using the stolen identities of U.S. citizens to open accounts and file fraudulent claims for UI benefits, exploiting the unprecedented expansion of these benefits provided in response to economic disruption caused by the COVID-19 pandemic.

Members of the National UI Fraud Task Force are working with SWAs, financial institutions, and other law enforcement partners across the country to fight this type of fraud, and consumers should be vigilant in light of this threat and take appropriate steps to safeguard themselves. This guide provides information and resources for individuals on how to protect themselves from UI fraud and what they can do if they suspect their identity has been exploited by criminals.

Who is at risk of becoming a victim?

- Those who have already been the victim of identity theft;
- Those who have had their personally identifiable information (PII), such as their name, date of birth, address, and social security number, exposed in a past data breach (you may have received a notice via email or regular mail about your PII being contained in a past data breach); and
- Those who have given their PII to an individual who claims to be facilitating the filing of UI claims with SWAs, often for a fee.

Signs that you may be a victim of this crime:

Many victims of this crime have no knowledge that criminals have applied for UI benefits in their name. You may only discover that you were a victim of this crime upon seeing the following red flags:

- You file a lawful UI claim on behalf of yourself, and you receive a notice that your claim was rejected because that SWA has already received a claim under your name;
- You did not apply for UI benefits, but you receive a determination letter from a SWA in your state of residence or another state regarding a UI claim filed under your name;
- You receive a notification that you failed the security verification process for your UI claim; and
- You are told by a current or former employer that a UI claim has been submitted with your PII.

What can you do if you believe you have been victimized?

- If you learn that an UI claim has been filed in your name, and you did not file the claim, report it to the relevant SWA immediately. Please refer to the state-by-state list of "Where to file a report of UI Fraud" links at the end of this guide to find the right point of contact for making the report. Reporting the crime immediately to the SWA is important if the improperly disbursed UI benefits are to be recovered.
- If you are presently working, notify your employer of the fraudulent claim, because they will also need to file documentation.
- File a complaint with the National Center for Disaster Fraud by going to https://www.justice.gov/disaster-fraud/ncdf-disaster-complaint-form or by calling (866) 720-5721.

How can you protect yourself from fraud?

- **Do not share your PII with unknown third parties.** If someone you don't know asks for your PII in order to perform some service for you, beware that the offer of services may be a scheme to collect your PII and use it for illegal purposes, including UI fraud.
- **Follow good computer hygiene and cybersecurity practices**. Ensure that the passwords to all of your financial and other accounts are unique and sufficiently complex; and change those passwords often. Wherever you can, add a second factor for authentication, such as a cell phone number, a security token, or a biometric factor, such as a fingerprint or facial scan.
- **Take advantage of credit monitoring services** if you have been notified your information was exposed in a data breach. If you do not have access to credit monitoring, use www.annualcreditreport.com, where you can get a free credit report from each credit reporting bureau once each year.
- **Place a freeze on your credit** to prohibit any new credit applications from being be opened in your name. Visit the FTC credit freeze guide for instructions. https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Please contact the DOL-OIG Hotline at https://www.oig.dol.gov/hotline.htm or (800) 347-3756 if you have questions or need more information about UI fraud.