



Raising Awareness of COVID-19 Unemployment Insurance Claim Fraud

With COVID-19 causing an unprecedented increase in unemployment insurance claims over the past few months, reports of identity theft are rising. Fraudsters are using personally identifiable information of identity theft victims who have not filed unemployment claims. Some people learn about the fraud when they receive a notice from their state unemployment benefits agency or their employer about their alleged application for benefits.

Although unemployment payments are typically deposited to accounts fraudsters control, they sometimes are sent to the legitimate accounts. If this happens to you, the fraudsters may call, text, or email to try to persuade you to send some or all of the money to them. They may also pose as your state unemployment agency, indicating the money was sent by mistake. This is a money mule scam—don't fall for it.

How to Protect Your Finances and Credit

Should this occur, it means someone is misusing your personal information, including your social security number and date of birth. Below are ways to protect your finances and credit:

1. **Report the fraud to your employer and your advisor immediately.**
2. **Report the fraud to your state unemployment benefits agency.** (Click [here](#) for a list of agency websites, searchable by state.)
 - a. An online report will save you time and be easier for the agency to process; if possible, report the fraud online.
 - b. Document who you spoke with and when, recording any confirmation or case number you receive.
 - c. Don't respond to calls, text messages, or emails asking you to wire money, send cash, or load money on gift cards. State agencies will never instruct you to repay money in this manner; anyone who tells you to do so is a fraudster.
3. **Report the fraud to the Federal Trade Commission and get help with important recovery steps.** Visit [IdentityTheft.gov](#) to place a free, one-year fraud alert on your credit, request free credit reports, and close any fraudulent accounts that have been opened in your name. It will also help you add a free extended fraud alert or credit freeze to your credit report, making it more difficult for an identity thief to open new accounts in your name.
4. **Review your credit reports often.** Check your credit reports for free through [AnnualCreditReport.com](#). This can help you recognize signs of fraud.
5. **Notify your bank and other financial institutions.**
6. **Work with your advisor to place these security protections on any accounts held with Commonwealth:**
 - a. **Soft restriction:** Money is allowed to move in and out of the account as normal. This isn't foolproof because it doesn't restrict transactions from happening.
 - b. **Hard restriction:** All money movement out of the account is stopped, including systematic withdrawal plans. Trades within the account are permitted.
 - c. **Passphrase:** If someone claiming to be you calls the Service Center, Commonwealth will ask the caller to provide the passphrase, in addition to answering normal identification verification questions, before proceeding. This passphrase is used only if you contact the Service Center; it does not affect online access to your account.