



ARE YOU THE VICTIM OF AN UNEMPLOYMENT FILING SCAM?

Have you received communication regarding your application for unemployment benefits, but you have not applied for these benefits? If yes, you may have been swept up in a nationwide fraudulent claim scheme, which uses previously stolen personal identification information to file fraudulent claims for unemployment benefits.

Here are the steps that you should take immediately:

- 1. Contact the Massachusetts Department of Unemployment Assistance ("DUA") either online through a secure form or by telephone at 877-626-6800.
 - The secure "Unemployment Fraud Reporting Form" can be completed and submitted online, and is self-explanatory.
 - You will be asked to identify yourself by name, address, date of birth, telephone number, email address and the last six digits of your social security number (entered in this manner 12-3456), or, alternatively, the number on your Massachusetts driver's license or other state-issued number.
 - Be forewarned The DUA is receiving and addressing hundreds of fraud reports at this time and your initial attempts at reporting may not succeed. Keep trying!
 - The DUA may contact you by mail, email or text regarding your report of fraud. It will not request through email or text messages any personal information such as your full social security number, bank account number or credit card information. The DUA will not request that you pay any fees. If you receive any such request, it is a scam and should be reported to the DUA.
 - The DUA will freeze the account associated with your report. The fraudulent claim will not impact your ability to apply for benefits in the future and your employer will not be assessed any charges. Any payments made by DUA before your report will not be considered as "income" for tax purposes.
- **2. File a report at your local police department and request a copy of your report.** You may need to furnish it to your creditors, credit agencies or debt collectors.
- 3. Consider reporting to the FBI.
- **4.** Report that you have been a victim of identity fraud to your credit card companies, banks and other financial institutions. Request a "fraud alert" be placed on your accounts.
- **5. Obtain your credit report.** Contact major reporting agencies Equifax, Experian and/or Transunion by calling 877-322-8228 or requesting your credit report online at **www.annualcreditreport.com**. (These reports are now available weekly through April 2021). Report and dispute any fraudulent charges.
- 6. Consider these steps through the credit reporting agencies:
 - Place a fraud alert through one or all of the agencies on your credit file.
 - Place a credit freeze with each of the agencies. (Equifax: 800-349-9960; Experian: 888-397-3742; TransUnion: 888-909-8872). *CAVEAT: If on a future date you intend to apply for a loan or credit card, you will need to "unfreeze" your credit.*

- 7. Consider enrolling in a credit monitoring program, such as Credit Karma, PrivacyGuard or other programs.
- **8.** To protect your identity, change your passwords, including on your email account(s). NOTE: Passwords that combine 12 or more letters, numbers and characters (some sites even allow spaces) in a single phrase are generally more secure and easier to remember than shorter, more complex passwords.
- 9. Review your homeowner's insurance policy to see if you have an endorsement or rider providing identity theft coverage.





