FULLY MANAGED IDENTITY THEFT PROTECTION

February Newsletter 2021

Unemployment Fraud: How it Works and How to Fight It.

Across the nation, identity thieves are exploiting the COVID-19 pandemic by committing Unemployment Benefits Fraud, which is filing for and collecting unemployment benefits fraudulently by using the identity of someone still employed. This type of scam is very difficult to detect. Sometimes the employer is the first one to know that a scam has taken place by receiving a notice of an unemployment claim from employees who are still very much employed. Let's take a look at how this scam works. It is important to know how to react quickly to minimize the damage.

Unemployment offices across the nation have been targeted for fraudulent unemployment claims even before the pandemic began; however, the activity level has drastically increased over the last year. Fraudsters count on unemployment offices being overwhelmed with claims and attempts to minimize the financial impact of the pandemic by processing claims more quickly than they might have in the past. If criminals flood a particular state with bogus claims, pressure mounts to move documents through the process, making it easier for fraudulent attempts to get approved.

How unemployment fraud works.
The identity thief collects the personal information of an individual, along with the individual's place of employment, through one or more previous data breach incidents. Unfortunately, this is all too easy. The thief files for unemployment benefits in the state of residence of the individual, impersonating the worker. The thief typically requests that the funds be deposited into a bank account set up for this purpose.

Alternatively, claims filed by scammers can result in the issuance of a check or payment card. The thief may succeed in using an alternate mailing address that directs payment to their location. Or if that doesn't work, after the fraudulent claim has been filed the scammer may contact the recipient by phone or email, posing as the state's unemployment office, instructing the unsuspecting employee to "correct the error" by transferring the funds to them.

This type of unemployment fraud is very difficult to detect. In fact, a worker may not know that they have been a victim of unemployment fraud unless:

- They apply for unemployment benefits and learn there's already an open claim in their name.
- They receive a form 1099-G listing unemployment income that's subject to federal income tax.
- They receive notice from their state unemployment office confirming that a claim has been filed.
- Or more commonly, they receive notice from their employer that someone has filed for unemployment benefits in their name.

You are not alone.
As a member of Tennessee Members 1st Federal Credit Union you have access to Fully Managed Identity Theft Recovery which provides a personal Identity Theft Recovery Advocate to work with you if you suspect identity theft or you have seen confirmed identity fraud. Your Advocate will advise you on steps to take to resolve identity theft, and when possible your Advocate will act on your behalf to perform the legwork necessary to help you dispute and recover from fraud.

How to address fraudulent claims of unemployment.
If you discover a bogus unemployment claim has been filed in your name, do the following:

1) Contact your Identity Theft Recovery Advocate. While there are limitations on what your Identity Theft Recovery Advocate can do in the case of Unemployment Fraud they can be your guide to move through the process of recovery. At the same time, they can help you uncover any other type of identity fraud that may be lurking in the shadows. Or, you may use the information below and report the fraud to your state's unemployment office and to your employer before calling an Identity Theft Recovery Advocate.

2) Either before or after you speak to your Identity Theft Recovery Advocate, notify your state's local unemployment agency. Your state's unemployment office will not allow a third-party to be on the phone or file a complaint of fraud on your behalf, so this step will be necessary to perform on your own. Some states have made this step easier by setting up a website to collect complaints of fraudulent claims. Check this option for your state before you

FULLY MANAGED IDENTITY THEFT PROTECTION

February Newsletter 2021

attempt to file a claim by telephone. Filing a complaint on the web is typically faster and more accurate.
3) Inform your employer. The state's unemployment office will contact your employer to verify the claim of unemployment. Hopefully, funds will not be released until this verification is received. If your employer notifies you of a bogus claim, ask your human resources department to report the fraudulent activity to the state's unemployment office. Make sure you also notify the unemployment agency yourself as there will need to be confirmation from both parties.

4) Be wary of anyone attempting to contact you about a fraudulent unemployment application. It is possible that your state's unemployment office will contact you regarding a report of a fraudulent unemployment claim, asking for further information. If you have already been notified by your employer of the fraudulent activity or if you have received confirmation of an application for benefits from the state, then this may be a legitimate call. However, the high incidence of unemployment, coupled with the growing awareness of rampant employment fraud, makes people susceptible to a very simple, but effective telephone scam. There may be no fraudulent application for unemployment in your name at all, but the caller makes you think that you have been a victim of unemployment fraud. The caller will go on to ask you to verify personal information, including checking account numbers, Social Security number, date of birth, etc., which is the information needed to commit many types of fraud and identity theft. If you were not a victim before the call, you may be one by the end of the call. The best course of action is to politely tell the caller that you will call back to the agency on a published number. You may also want to check with your employer to see if they have received a claim for unemployment benefits in your name. If not, this may be a scam.

5) Stay vigilant to other forms of identity theft. Your Identity Theft Recovery Advocate will help you understand the risks of other types of identity fraud. Make sure that you have activated credit monitoring and dark web monitoring and pay close attention to alerts. Get back in touch with your Identity Theft Recovery Advocate if you see any additional suspicious activity.

6) Be part of the solution. If you suspect unemployment fraud is connected to email or bogus websites or social media accounts, file a report at the FBI Internet Crime Complaint Center at www.ic3.gov.

Your Fully Managed Identity Theft Protection

Covers all types of ID Fraud
Your Fully Managed Identity Theft Recovery Services cover all types of identity fraud, even if it's not related to your accounts with us!

Free Basic Coverage
Members receive basic coverage at no cost, with opportunities for additional coverage for as low as $14 per month for families.

3 Generations of Protection
Coverage automatically extends to cover three generations of your family including coverage up to 12 months after death.

Dedicated Recovery Advocates
If you experience or suspect identity theft, a dedicated Recovery Advocate is assigned to assist you during the entire recovery process.

WERE YOU A VICTIM OF IDENTITY THEFT?

REPORT RECOVER RESTORE

If you experience or suspect you are the victim of identity theft or a data breach, visit your local Tennessee Members 1st Federal Credit Union branch or call 865-482-4343. Your contact information, as well as any details regarding your concern, will be submitted to the Recovery Care Center where a Recovery Advocate will reach out to discuss your situation and assist you during the recovery process.