Unemployment Claim Fraud Affecting 100 of Our Employees

More than 100 of our employees have been victims of unemployment claim fraud. This is happening all over the country. The U.S. Secret Service reports that a well-organized Nigerian crime ring is behind most of the fraud, with potential losses in the hundreds of millions of dollars. Washington state is seeing the most fraud, with other states showing evidence of attacks including North Carolina, Massachusetts, Rhode Island, Oklahoma, Wyoming and Florida. Many of the victims are first responders, government employees and school employees.

Employees should be aware of the threat and consider taking steps to protect themselves and reduce their risk.

If you think you may be a victim of identity theft/fraud, read and follow the suggestions below.

Contact the Washington State Employment Security Department:
https://esd.wa.gov/unemployment/unemployment-benefits-fraud
https://fortress.wa.gov/esd/file/SecureUpload/unemploymentfraud/report

You should complete ESD's online form for reporting imposter fraud. They should have the following information on hand to verify your identity.

- Last four (4) digits of your Social Security Number (SSN)
- Date of birth
- Address
- Current phone number
- Information on how you learned a fraudulent claim was filed

You can also report the fraud to ESD via phone at 1-855-682-0785 or by email at: esdfraud@esd.wa.gov. However, the online report form is currently ESD's preferred method because of the high volume of fraudulent claims it is processing. Additionally, if the fraud is reported via email, you may also be asked to provide a scanned copy of your driver's license so ESD can verify your identity**. Given the sensitivity of a driver's license number, we do not recommend sending this document via email unless the you have secure means (i.e. encrypted email)**.

Regardless of which method you use to file a report, you will also need to give ESD permission to deny or cancel the fraudulent claim. Crucially, victims of unemployment imposter fraud will not have to repay the money and will still be able to apply for unemployment benefits if needed at some future date. It is critical that you complete this step, and that it is done through ESD's official website: ESD.WA.GOV.

File a police report with Crime Check
An online or non-emergency report can be filed with Crime Check. You are also encouraged to keep a file folder or journal with the information from this incident, including any case numbers. Some government services and accommodations are available to victims of identity theft that are not available to the general public, such as getting certain public records sealed.

Contact the three major credit bureaus
Free credit reports can be obtained from Equifax, Experian, and TransUnion at AnnualCreditReport.com or by calling 1-877-322-8228. You should report that a fraudulent claim was made using your identity to the credit bureaus and should provide the bureaus with the case number from any police reports that

were filed. If desired, you can arrange to set up a fraud alert or have your credit frozen. Doing either is free by law.

A fraud alert will make it harder for someone to open new accounts using your name. To place a fraud alert, you should contact one of the three credit bureaus listed below. That bureau must then tell the other two credit bureaus.

- Experian: 1-888-397-3742
- TransUnion: 1-800-680-7289
- Equifax: 1-888-766-0008

As a victim of identity theft, you have the right to check your credit activity monthly, if desired (experts recommended everyone check their credit annually). You may also freeze your credit which is free and offers additional protection. This webpage from the Federal Trade Commission (FTC) provides links for you to set up a credit freeze with each of the three major credit bureaus.

Contact the FTC and the IRS

You may also file a short report with the FTC and should provide the FTC with the case number of any police reports you have filed.

You may also set up an IRS account with your social security number, which will prevent criminals from creating an account using your identity. The IRS can also be contacted by phone at 1-800-908-4490 to report suspected identity theft, but there may be a wait time. Another option for locking a social security number is at the Department of Homeland Security's E-Verify website.

All of this reporting may seem redundant, but it helps ensure you are identified as a victim by the local, state, and federal government.

Keep Notes

You should maintain any notes, copies of emails, etc. This paper trail can be referenced in the future for possible identity issues or inaccuracies on a credit history report. We empathize with how upsetting and time consuming this is to deal with, especially in this current COVID-19 environment.

Contact the Post Office (Bonus tip)

You can also check with your post office to make sure mail has not been redirected to a different address without your permission.

Help Prevent Identity Theft!

Even if you are still working, establish a SAW account with Employment Security to preempt one from being set up on your behalf: https://secure.esd.wa.gov/home/SAWUserRegistrations/SignUp. Using a personal email address, you can create a SAW user account with ESD. A SAW account is used by multiple Washington State agencies to conduct business with the state (such as a specialty license, business license, etc.) After creating an account, SAW will send an email to verify the email address entered. This email will include a link directing the user back to the ESD SAW website. At that point, you will enter a social security number to verify user identity and this will pair the SAW account with the email address. This will not initiate an unemployment claim, but it will associate a social security number with the secure username and password that can let a user set up an account.

Once a social security number is associated with an account created by a user, it cannot be associated with another fraudulent account. This will prevent a bad actor from using a person's name and social

security number to create a fraudulent account and associate it with a different email address. If all goes well the user will not need to take any further action. The process to create an account is straightforward and the website is easy to use.

However, the user may receive an error message stating: “The social security number (SSN) you entered already exists and is linked to this partly hidden email address: xxx@xxx.” If the email address provided is not recognizable to you, then you should assume your identity has been compromised and should follow the guidance above for reporting identity theft/security breach.

Conclusion

We know everyone is very busy and we don’t need another thing to have to manage and track. However, the above advice may prevent even more complications arising during this unusual time.