Please be aware that there has been an increase in the number of fraudulent unemployment insurance claims filed in Washington.

One way to identify if someone has fraudulently filed for unemployment in your name is to visit www.esd.wa.gov, and go through the initial registration steps as if you plan to file for unemployment. Assuming you have never filed before, and if someone fraudulently filed in your name, then you will get a warning that the SSN you entered already exists in the system.

In case you discover or believe you are victim of a fraudulent claim filing (such as being notified by your HR department or the State Employment Securities Department indicating an unemployment claim has been filed on your behalf), please review the steps below on to report this fraud:

Steps to Protect Your Financial Identity & Credit History

- Step One – Contact Human Resources
  - Contact your organization's HR staff to coordinate and report the incident to your employer.
- Step Two – Contact Your State's ESD
  - Call the State Employment Security Department (ESD) (Washington: 800-246-9763 to report the fraud or contact the ESD via an online form: https://fortress.wa.gov/esd/webform/ContactUS/)
  - You will need the following information for identity verification:
    - Last 4 of your SSN
    - Date of birth, address
    - Current phone number Information on how you learned a claim was filed on your behalf
- Step Three – Police Report
  - File an online or non-emergency report with the agency whose jurisdiction you live in.
  - Start keeping 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.
- Step Four – The Three Major Credit Bureaus
  - Obtain your free credit reports from Equifax, Experian, and TransUnion at www.annualcreditreport.com or call 1-877-322-8228
  - Report to the credit bureaus that the fraudulent claim was made using your identity and provide them with the case number from your police

report. You can have a fraud alert put on your identity or freeze your credit. Doing either is free by law.
    - A fraud alert is free and will make it harder for someone to open new accounts in your name. To place a fraud alert, contact one of the three credit bureaus. That company must tell the other two.
        - Experian: 1-888-397-3742
        - TransUnion: 1-800-680-7289
        - Equifax: 1-888-766-0008
    - Check your credit activity at least once a year. As a victim of identity-theft you have the right to check it monthly if you choose.
    - Credit Freeze – If you do not have upcoming large purchases, such as a home, you may want to freeze your credit for more protection. It is free and you can do it yourself. More information about freezing your credit can be found here.
- Step Five – FTC & IRS
    - File a short report with the FTC and give them the case number for your local police report. The FTC offers more information here.
    - Consider setting up an IRS account. If you create an account with your social security number, it will prevent criminals from creating an account using your identity.
    - Another option is to lock your social security number, which can be done here. (The next wave of this cyber-attack may be IRS tax fraud.)
    - All of this reporting seems redundant, but we want to make sure you are recognized as a victim by the local, state, and federal government. Also, the more people who report it, the more support law enforcement agents will receive to pursue the perpetrators.
- Step Six – Keep Your Notes
    - Hang on to any notes, copies of emails, etc. regarding the issue. This is the paper trail that you can reference if you face any identity issues or locate inaccuracies on your credit history sometime in the future.

Protecting Your Data and Identity

You are done dealing with the fallout from this unemployment fraud incident, but may choose to further protect yourself from cyber-crime. Below are some steps and resources that the cyber-crime detectives recommend for anyone wanting additional protections for themselves and their families.

Control Your Own Information

- Services that lock credit information can help, though you must provide companies with your own personal data, potentially creating more risk.
- There are many sites that will walk you through securing your own data. A few third-party resources are listed below. These are not associated with the City, but they are trusted resources that other victims have used successfully.
    - This workbook will walk you through a credit freeze and removing your data from data brokers and "stalker sites. The "Privacy Checklist" is a printable guide for securing devices, accounts, and personal data. You don't need to buy anything on this page, we just want to make use of their free guides.
    - The Electronic Frontier Foundation has several guides for privacy and security.
    - Most attackers use data obtained from previous internet breaches of hotel chains, entertainment services, and other widely-used digital productivity tools. That is why it is important to never use the same password twice. Get a password manager and use multi-factor authentication.
    - Use Multi-Factor Authentication (a secondary security code) on your most important accounts.
    - Most importantly, be vigilant and watch out for phishing emails, phishing fraud calls, and even things like mail/package theft, which can lead to your identity being compromised
    - Be wary of free apps/offers, which could be mining your data.
    - Additional Guides:
        - A Guide to Digital Privacy for You and Your Family
        - How to Protect Your Data as COVID-19 Scams Soar
        - Lifehacker's Complete Guide to Data Privacy
        - How to Increase Your Privacy and Security in Zoom
        - Online Security Tips for Working From Home