Dear Employee,

Washington state has identified an abnormally high rate of fraudulent unemployment claims. As an employer, we want to provide you with information that may be used to protect your personal information, should you feel you are a victim of unemployment fraud. To be clear, we are currently unaware of the actual misuse of your personal information, we are providing this information to you in an abundance of caution to assist you in protecting your personal information. The following recommendations have been released by the Seattle Police Department cyber-crime investigators. These steps are recommended for anyone who knows, or believes, they may be a victim of unemployment fraud:

**Step One – Contact HR**

* Contact our Human Resources (HR) staff to coordinate and report the incident.

**Step Two – Contact Washington State Employment Security Department, (ESD)**

* Call the [WA State Employment Security Department](https://esd.wa.gov/unemployment/unemployment-benefits-fraud) (ESD) at 800-246-9763 to report the fraud.
* You will need the following information for identity verification. o Last four (4) digits of your Social Security Number (SSN) o Date of birth
	+ Address
	+ Current phone number
	+ Information on how you learned a fraudulent claim was filed on your behalf
* You may instead contact ESD via[:](https://fortress.wa.gov/esd/webform/ContactUS/) esdfraud@esd.wa.gov . **This is ESD’s preferred method of reporting because of the high volume of fraudulent claims**. In addition to the information listed above, you may also need to provide a scanned copy of your driver’s license (so ESD can verify your identity). Given the sensitivity of your driver’s license number, we encourage you to send such information only via a secure means (i.e. encrypted email). You should give them permission to deny or cancel the fraudulent claim.

**Step Three – File a 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 – Contact the Three Major Credit Bureaus**

* Obtain your free credit reports from Equifax, Experian, and TransUnion at [Annual Credit Report](https://komonews.com/news/local/www.annualcreditreport.com) or by calling 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 bureau must tell the other two credit bureaus.

o Experian: 1-888-397-3742

o TransUnion: 1-800-680-7289

o 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](https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs) – If you do not have upcoming large purchases, such as a home, you may want to freeze your credit for additional protection. It is free and you can do it yourself. More information about credit freezes can be found at [https://www.consumer.ftc.gov/articles/0497-](https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs)  [credit-freeze-faqs.](https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs)

# Step Five – Contact the FTC & IRS

* File a short report with the Federal Trade Commission (FTC) and give them the case number for your local police report.
* Consider setting up an [IRS account. I](https://www.irs.gov/payments/view-your-tax-account)f you create an account with your Social Security number, it will better prevent criminals from creating an account using your identity.
* Another option is to lock your [Social Security number](https://www.e-verify.gov/employees) at https://[www.e-verify.gov/employees.](http://www.e-verify.gov/employees)
* All of this reporting may seem redundant, but it helps ensure you are identified as a victim by the local, state, and federal government.

# Step Six – Keep Your Notes

* Maintain any notes, copies of emails, etc. 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.

We empathize with how upsetting and time consuming this is to deal with, especially in this current COVID-19 environment. We hope you find these steps helpful to protect yourself from any further fraud and/or identity theft.

Sincerely,