WASHINGTON STATE FUSION CENTER SITUATIONAL AWARENESS BULLETIN

WSFC Tracking Number # 20-0077 May 13, 2020

(U) Criminals Exploit COVID-19 to Commit Unemployment Fraud

(U) The Washington State Fusion Center (WSFC) is providing the following information for your situational awareness. Local, State and Federal law enforcement are currently investigating a widespread fraud campaign in which victims' identities are being used to file false unemployment claims. This fraud campaign is likely capitalizing on the surge of unemployment claims relating to the current COVID-19 pandemic and has affected both the private and public sector. Victims, who have not filed unemployment claims, have received notification from their employer's Human Resources (HR) department, or the Washington State Employment Security Department (ESD), indicating an unemployment claim has been filed on their behalf.

(U) The following steps should be considered for individuals who are a victim of unemployment fraud:

(U) Step One – Contact HR

- (U) Contact your organization's HR staff to coordinate and report the incident to your employer.

(U) Step Two – Contact Washington State ESD

- (U) Report the fraud to Washington State ESD at 800-246-9763 or through their online form: https://fortress.wa.gov/esd/webform/ContactUS/
  - (U) You will need the following information for identity verification.
    - (U) Last 4 digits of your Social Security Number (SSN)
    - (U) Date of birth
    - (U) Address
    - (U) Current phone number
    - (U) Information on how you learned a claim was filed on your behalf

(U) Step Three – File a Police Report

- (U) File an online or non-emergency report with the agency whose jurisdiction you live in.

(U) Step Four – Report to the Three Major Credit Bureaus

- (U) Obtain your free credit reports from Equifax, Experian, and TransUnion at www.annualcreditreport.com or call 1-877-322-8228

(U) Tracked by: HSEC-4 and WSFC SIN-3

- (U) Report to the credit bureaus that a 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. Either can be done free of charge.
  - (U) A fraud alert will make it more difficult for someone to open new accounts in your name. To place a fraud alert, contact one of the three credit bureaus. That bureau will then notify the other two credit bureaus.
  - (U) Experian: 1-888-397-3742
  - (U) TransUnion: 1-800-680-7289
  - (U) Equifax: 1-888-766-0008
- (U) 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.
- (U) Credit Freeze – If you do not have upcoming large purchases, such as a home, you may want to freeze your credit for more protection. You can accomplish this by visiting https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

(U) **Step Five – Federal Trade Commission (FTC) & Internal Revenue Service (IRS)**

- (U) File a short report with the FTC and provide the case number from your police report https://www.identitytheft.gov/. Additional information can be found at www.ftc.gov/idtheft.
- (U) Consider setting up an IRS account at https://www.irs.gov/payments/view-your-tax-account. Setting up an account with your SSN can prevent criminals from creating an account using your identity.
- (U) Another option is to lock your SSN at https://www.e-verify.gov/employees.

(U) Step Six – Keep Your Notes

- (U) Retain any notes, copies of emails, etc. related to your reports and the fraud activity. You can reference if you face any identity issues or locate inaccuracies on your credit history sometime in the future.

(U) Actions to Further Protect Your Data and Identity

- (U) Services that lock credit information can help, though you must provide companies with your own personal data, potentially creating more risk.
- (U) There are many sites that will walk you through securing your own data. You can search "how to do opt-outs and credit freeze" or use some of the third-party resources below.
  - (U) https://Inteltechniques.com/links.html The workbook linked on the right side of the page will walk you through a credit freeze and removing your data from data brokers and stalker sites. The "Privacy Checklist" is a free printable guide for securing devices, accounts, and personal data.
  - (U) https://ssd.eff.org/en The Electronic Frontier Foundation has several guides for privacy and security.
  - (U) Most fraud is committed using 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: https://thewirecutter.com/reviews/best-password-managers/
  - (U) Use multi-factor authentication (a secondary security code) on your most important accounts: https://authy.com/guides/.

- (U) Most importantly, be vigilant and watch out for phishing emails, vishing fraud calls, and even things like mail/package theft, which can lead to your identity being compromised.
- (U) Be wary of free apps/offers, which could be mining your data.

(U) Additional Resources:

- (U) https://www.tripwire.com/state-of-security/security-data-protection/guide-digital-privacy-your-family/
- (U) https://protonmail.com/blog/coronavirus-email-scams/
- (U) https://lifehacker.com/s/dataprivacy
- (U) https://www.digitaltrends.com/computing/how-to-increase-your-privacy-security-zoom/
- (U) https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home

(U) If you have any questions, please contact the WSFC at 1-877-843-9522 or intake@wsfc.wa.gov.