Steve Sisolak
Governor

Laura E. Freed
Director

Colleen Murphy
Deputy Director

STATE OF NEVADA
DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE

515 E. Musser Street, Suite 300 | Carson City, Nevada 89701
Phone: (775) 684-0299 | admin.nv.gov | Fax: (775) 684-0298

MEMORANDUM

July 22, 2020

TO: All Agencies

FROM: Laura E. Freed, Director
Department of Administration

SUBJECT: **Unemployment Fraud & State Employees**

The Department of Administration and the Department of Employment, Training and Rehabilitation (DETR) would like to make state employees aware that there have been fraudulent unemployment claims filed in the name of some actively working state employees. This memo outlines the issue and provides direction for responding to fraudulent claims.

Background

DETR has discovered numerous fraudulent schemes related to the COVID-19 pandemic. Scammers are using unscrupulously obtained personal information—such as from the dark web—to apply for unemployment insurance and Pandemic Unemployment Assistance (PUA) benefits. The schemes target varied individuals and groups, including fraudulent claims filed in the name of some state employees. This fraud activity is not the result of any breach of DETR or other state systems; ongoing monitoring by the State Office of Information Security and other state entities has shown no indication of any breach of state systems.

The majority of these fraudulent filings related to state employees are typically discovered through DETR's verification processes before a claim is approved and paid, which stops the claim process.

State agency employers should also note that employer accounts will not be charged for fraudulent claims.

As a step to protect employee information from getting into the hands of fraud perpetrators, the Nevada Employee Directory (NED) has been removed from public access. State employees can still access NED from inside the state network.

What to do if a Fraudulent Claim has Been Filed in Your Name

State employees targeted by these schemes may receive notification from their agency regarding a claim being filed in their name. In rare cases, an employee may be contacted by DETR directly.

DETR is working cooperatively with state agencies regarding fraud reporting, and suspected fraudulent claims are immediately reported to DETR. To reduce duplicative reports and avoid additional burden to DETR staff who are already managing a massive workload volume, **state employees should not file a fraud report with DETR or contact the agency directly regarding suspected fraudulent activity**.

State employees who suspect identify theft can visit the Nevada Attorney General's website at http://ag.nv.gov/Hot_Topics/Victims/ID_Theft_Program/ for further guidance. Allegations of potential fraud involving unemployment insurance can be reported to the FBI by filing a complaint through the their Internet Crime Complaint Center (IC3), at www.ic3.gov.

Unemployment fraud is considered a felony under Nevada Revised Statutes, and the state will be following fraudulent claims up to and including prosecution and other civil remedies afforded under law.

Attached to this memo are some general tips to help you protect yourself from various forms of fraud and identify theft.

Tips for Protecting Yourself from Fraud and Identity Theft

- Never give out personal or financial information over the phone.
- Thoroughly review all financial statements for any unusual activity. Immediately contact the company if an item looks suspicious.
- Shred or destroy credit card statements, bills, insurance papers or bank statements before throwing them out.
- Do not carry your Social Security card in your wallet.
- Be wary of anyone calling to "confirm" personal or financial information. Often, these are criminals trying to obtain those facts under the guise of "confirmation".
- Release your Social Security Number only when absolutely necessary or when required by law.
- For services you are receiving, ask how you can remove unnecessary information or information that is not required.
- Check credit reports, banking information, medical information that may have details that need to be removed or secured. Put a freeze on your credit information when you are not actively applying for credit.
- Protect and update passwords to your online accounts regularly.
- When creating passwords and PINS, do not use anything that could be discovered easily by thieves. Use unique passwords for important accounts, like your bank and credit card providers.
- Memorize all your passwords and PINS, or use a secure password manager.
- Remove old accounts and passwords that are no longer in use.
- Use additional security measures provided for your accounts, like multi-factor authentication, wherever available.

Learn about **Nevada's Identity Theft Program** through the Nevada Attorney General's Office: http://ag.nv.gov/Hot_Topics/Victims/ID_Theft_Program/.

If you think an identity thief is using your Social Security Number, call the **Social Security Fraud Hotline** at (800) 269-0271.