From: Modlin, Martha O <martha_modlin@med.unc.edu>

Sent: Tuesday, February 23, 2021 12:01 PM

To: Active SOM Staff <activesomstaff@med.unc.edu>; Active SOM Faculty

<activesomfaculty@med.unc.edu>

Subject: Fraudulent Unemployment Claims

Sent on behalf of Bonnie Smith, Director, Human Resources

Good afternoon,

We want to make you aware of a large-scale scam that has erupted in the midst of the COVID-19 pandemic – imposters filing claims for unemployment benefits, using the names and personal information of people who have not filed claims. This scam is occurring across the United States, and North Carolina has not been spared from this fraudulent activity. It's suspected that the uptick in fraudulent claims by imposters is occurring because there is an increased number of assistance programs available, i.e. more money available, and the desire of federal and state agencies to disburse funds as quickly as possible to people in need. Some of these assistance programs are not run through the traditional unemployment system and so the usual safeguards against fraud are lacking. Unemployment fraud can be perpetrated by individuals acting on their own behalf, whereas other times it is linked to organized crime. Unfortunately, in most cases, all of the information required to file a fraudulent unemployment claim is available to the general public on the internet, if you know where to look, or through outside data breaches, email phishing schemes, impersonation schemes, and other methods. Here at UNC, SOM faculty have been likely targeted because of the higher salaries in the SOM as compared to most units on campus. NC residents, including UNC SOM employees, are learning about the fraud when they receive notice directly from the North Carolina Division of Employment Security (NC DES) or from UNC's Employee & Management Relations staff in the Office of Human Resources (who were notified by NC DES). When UNC receives a notice from NC DES that an active employee has filed for unemployment benefits, an EM&R representative will notify the respective employee that there is suspicious activity and will provide guidance to the employee about how to protect themselves. Individuals committing unemployment fraud can be from anywhere and most likely will have no affiliation with the University. As such, the University will not have information upon which to base an investigation and so there is no further action the University can take to address the situation, or to be of assistance to you as you pursue this matter from an individual standpoint other than provide you with the following guidance.

Below are the steps to take to help protect your finances and your credit:

- If contacted by NC DES or a representative from UNC OHR regarding suspicious activity <u>or</u> you suspect someone has used your name and personal information to apply for unemployment benefits, call the DES Hotline at 984-465-9224 or submit a report to DES so they can investigate the suspected fraud. <u>DES: Report Unemployment Fraud (nc.gov)</u>;
- 2. If you received an IRS Form 1099-G from NC DES but did not file an unemployment insurance claim, call the DES Hotline at 984-465-9224 or submit a report to DES so they can investigate the suspected fraud. DES: Report Unemployment Fraud (nc.gov);
- 3. File a police report stating you believe you are a victim of identity theft:
- 4. File a complaint with the Federal Trade Commission (FTC) at https://www.identitytheft.gov or call the FTC hotline at 877-438-4338;
- 5. Contact one of the three major credit bureaus to place a "fraud alert" on your account:
 - a. Equifax: https://www.equifax.com or 800-685-1111

- b. Transunion: https://www.transunion.com or 800-909-8872
- c. Experian: https://www.experian.com or 888-397-3742
- 6. Find resources to report and recover from identity theft at https://www.identitytheft.gov.
- 7. Review your credit reports often.

One more thing to be mindful of is that unemployment payments are usually deposited in accounts under the imposters control. However, sometimes payments are sent to the real person's account instead. If this happens to you, the imposters may call, text or email to try to get you to send some or all of the money to them. They may pretend to be a DES employee, saying the money was sent by mistake. Do not wire money, send cash, or put money on gift cards. DES will never tell you to repay money that way and so anyone asking you to is part of the scam.

We hope this information is helpful to you. We'll post it on the SOM HR website at https://www.med.unc.edu/hr/ and the SOM intranet site at https://www.med.unc.edu/intranet/.

Thanks and take care.

Bonnie