Department of Justice

U.S. Attorney's Office Middle District of Georgia

FOR IMMEDIATE RELEASE

Friday, March 12, 2021

Acting U.S. Attorney Leary Warns About Fraudsters Stealing Personal Information And Claiming COVID-19 Benefits Using Fake Websites

MACON, Ga. – The Department of Justice's National Unemployment Insurance Fraud Task Force (NUIFTF) is warning that criminals are creating websites mimicking unemployment benefit websites, including state workforce agency (SWA) websites, to steal personal information and file fraudulent unemployment insurance (UI) benefits provided as a response to the COVID-19 pandemic, said Peter D. Leary, the Acting U.S. Attorney for the Middle District of Georgia.

"Fraudsters, true to form, are taking criminal advantage of the unemployment insurance benefits provided to people in real need during the COVID-19 pandemic and committing identity theft by filing for benefits using stolen information. This crime is widespread, and citizens need to keep their guard up against phishing schemes and other attempts to steal personal information," said Acting U.S. Attorney Leary. "Our office will continue our ongoing efforts to investigate and prosecute all those committing identity theft here in the Middle District of Georgia."

The NUIFTF recently alerted citizens about the issuance of erroneous 1099-G Forms as a result of this fraud. Since UI benefits are taxable income, SWAs issue 1099-G Forms to recipients and the Internal Revenue Service (IRS) to report the amount of taxable unemployment compensation received and any withholding. Due to widespread fraud, much of it involving identity theft, citizens may receive a 1099-G indicating they collected UI benefits, when in fact they have not. In other instances, Americans may not receive a 1099-G, but later learn from the IRS or another party that their identity was used to file for UI benefits without their knowledge or consent.

There are steps that victims can take to help remedy the situation if they receive a 1099-G Form for unemployment compensation they did not receive, including filing an identity theft complaint with the Department of Justice's National Center for Disaster Fraud (NCDF). To learn more about these steps, please visit the following website: <u>https://www.irs.gov/identity-theft-fraud-scams/identity-theft-and-unemploymentbenefits</u>. To report fraud, taxpayers can complete an NCDF complaint form online at <u>https://www.justice.gov/disaster-fraud/ncdf-disaster-complaint-form</u> or by calling 866-720-5721.

To lure consumers to these fake websites, fraudsters send spam text messages and emails purporting to be from an SWA and containing a link. The fake websites are designed to trick consumers into thinking they are applying for unemployment benefits and disclosing personally identifiable information and other sensitive data. That information can then be used by fraudsters to commit identity theft.

Unless it is received from a known and verified source, consumers should never click on links in text messages or emails claiming to be from an SWA offering the opportunity to apply for unemployment insurance benefits. Instead, anyone needing to apply for unemployment benefits should go to an official SWA website, a list of which can be found

at https://www.careeronestop.org/localhelp/unemploymentbenefits/unemployment-benefits.aspx.

Schemes that use links embedded in unsolicited text messages and emails in attempts to obtain personally identifiable information are commonly referred to as phishing schemes. Phishing messages may look like they come from government agencies, financial intuitions, shipping companies, and social media companies, among many others. Carefully examine any message purporting to be from a company and do not click on a link in an unsolicited email or text message. Remember that companies generally do not contact you to ask for your username or password. When in doubt, contact the entity purportedly sending you the message, but do not rely on any contact information in the potentially fraudulent message.

If you believe you may have entered information into a fraudulent website, resources on how to protect your information can be found at: <u>www.identitytheft.gov</u>.

Further information about the SWA-imposter scheme, and other major scams targeting American consumers, can be found at the Justice Department's Transnational Elder Fraud Strike Force website: <u>https://www.justice.gov/civil/consumer-protection-branch/transnational-elder-fraud-strike-force</u>.

Members of NUIFTF include: Department of Labor Office of Inspector General, U.S. Secret Service, Homeland Security Investigations, IRS-Criminal Investigation, U.S. Postal Inspection Service, Social Security Administration Office of Inspector General and FDIC Office of Inspector General. Find out more about the NUIFTF at: <u>https://www.justice.gov/file/1319301/download</u>.

For more information about the Consumer Protection Branch,

visit <u>http://www.justice.gov/civil/consumer-protection-branch</u>. Questions can be directed to Pamela Lightsey, Public Information Officer, U.S. Attorney's Office, at (478) 621-2603 or Melissa Hodges, Public Affairs Officer (Contractor), U.S. Attorney's Office, at (478) 765-2362.

Topic(s): Elder Justice Identity Theft Component(s): USAO - Georgia, Middle