City of Parma, Ohio

LAW DEPARTMENT

7335 RIDGE ROAD | PARMA, OHIO 44129-5593 | 440-885-8132

Timothy G. Dobeck
Law Director
Prosecutor

June 15, 2020

LAW DIRECTOR ADVISORY

FRAUD ALERT – UNEMPLOYMENT BENEFIT SCAMS ON THE RISE

The unprecedented response to the COVID-19 crisis has spawned unemployment scams that endanger the financial health and the good names of people throughout Ohio and the rest of our country.

Due to the historic number of people who have lost their livelihood because of COVID-19, Ohio's rules for traditional unemployment compensation have been expanded to allow more people to receive benefits. On March 27, Congress passed the CARES Act which gives workers impacted by COVID-19 a $600 weekly supplement on top of regular unemployment payments for up to 39 weeks. The CARES Act also established the Pandemic Unemployment Assistance program (PUA) that extends jobless benefits to workers with insufficient work history, self-employed workers and other independent contractors who are traditionally not eligible for aid. Ohio alone has issued more than $1 billion in PUA payments to more than 160,000 claimants. Untold Ohioans however have fallen victim to phony PUA claims.

Law enforcement authorities have uncovered massive unemployment fraud against state agencies by both homegrown and global crime rings. The criminals range from a seasoned Nigerian cybercrime group dubbed "Scattered Canary" to individual actors operating on online forums who for $50 worth of bitcoin will sell tutorials on how to siphon unemployment benefits without getting flagged. Their schemes primarily involve using the personal information of identity theft victims to fraudulently apply for unemployment benefits. Personal identifiable information, or PII, is any data that could potentially be used to identify a particular person. Examples include, but are not limited to, a name, social security number, driver's license number, bank account number, passport number, date of birth, residential address, email address, hometown, and graduation date.

In many cases a victim's PII may have been stolen years ago as in the 2017 Equifax data breach that exposed the private data of nearly 150 million consumers. More recently, fraudsters have been brazenly calling the unemployed with false offers to help them with their claim only to misuse PII obtained from the unsuspecting victim. A substantial amount of the fraudulent unemployment benefit claims have used the personal information of first responders working in COVID-19 hotspots, government personnel and school employees. Keep in mind that all victims of identity theft, employed and unemployed alike, are equally vulnerable to unemployment benefit scams. These scams are known to routinely use a person's identifiable information to fraudulently apply for unemployment benefits in multiple states contemporaneously. States that have been targeted so far include Washington, North Carolina, Massachusetts, Rhode Island, Oklahoma, Wyoming, Florida, and Ohio. All states are likely to be affected by these scams.

Many states unfortunately have few controls in place to spot patterns in fraudulent filings, such as multiple payments routed to the same bank account, or filings made for different claimants from the same Internet address. Some states have pared back the amount of personal information required to file an unemployment claim. The risk of fraud is even higher under PUA because claimants can self-certify their unemployment qualifications. Compounding the problem are state websites that have inadvertently exposed personal details of citizens filing unemployment claims. The most egregious example of such security breach is the Arkansas Division of Workforce Services which had to temporarily shut down its benefits website after exposing the personal information of some 30,000 state residents. Ohio experienced a similar issue on May 15 when Deloitte Consulting, a vendor contracting with the Ohio Department of Job and Family Services (ODJFS) to assist the state in administering its PUA program, exposed personal information of at least two dozen unemployment applicants. Based on Labor Department estimates, the full impact of these scams may result in Ohio losing $460 million to unemployment fraud this year.

If you are or become the victim of an unemployment benefit scam, report the fraud to ODJFS immediately. You are not required to provide your name when reporting fraud. Possible fraud may be reported to ODJFS using the following methods:

Website	https://secure.jfs.ohio.gov/feedback/ouc/ouc-fraud/index.stm
Email	ucbenprotest@jfs.ohio.gov
Hotline	800.686.1555 (option 1)
Fax	614.752.4808
Mail	Benefit Payment Control P.O. Box 1618; Columbus, Ohio 43219-1618

Victims of identity theft and unemployment benefit scams should also report the fraud to the Social Security Administration by calling the Inspector General's fraud hotline at 800.269.0271 or by submitting a report online at https://oig.ssa.gov. This step is recommended because a social security number is required to file a claim for unemployment benefits. Report the identity theft also to your local police or the police in the jurisdiction where the identity theft took place. You may contact the Parma Police Department at 440.887.7300. A copy of the police report should be sent to your banks, credit card companies, and insurance providers.

After reporting the fraud, you should request all credit bureaus to freeze your credit file. A credit freeze means no one can access your credit reports or scores. And since practically no lender will extend credit without a credit check, this prevents anyone from fraudulently opening a new account in your name. You may contact the bureaus at the following service numbers:

Equifax	888.298.0045
Experian	888.397.3746
Trans Union	800.916.8800
Innovis	800.540.2505

Additionally, change the passwords to all your accounts. Use a complex string of alphanumeric characters including symbols. When creating passwords, do NOT use the last four digits of your SSN, DOB, middle name, mother's maiden name, pet's name, address, consecutive numbers, or any other information that fraudsters can discover easily. It is also vital that you scrub your personal identifiable information from all social media accounts, especially if the information is used in security questions. For more information on preventing and dealing with identity theft, please visit the Federal Trade Commission's website at www.ftc.gov/idtheft.