



Fraud Penetrating All State Unemployment Systems, IDES Taking Steps to Detect, Mitigate, and Pursue Fraudsters

July 22 2020 10:45 AM

SPRINGFIELD – IDES has uncovered and is investigating a widespread fraud scheme that is being conducted nationwide, impacting each state’s federal Pandemic Unemployment Assistance (PUA) programs, implemented as a result of the COVID-19 pandemic. PUA provides 100% federally funded unemployment benefits for hundreds of thousands of individuals who were not traditionally covered by a state’s regular unemployment insurance program, including self-employed and sole proprietors. Under this program, 39 weeks’ worth of benefits are available to PUA claimants whose claims can be backdated as earlier as February 2, 2020, with benefits ending December 26, 2020.

The Department is aggressively cracking down on this fraud network, whose dedicated team of staffers responsible for handling and investigating unemployment fraud are working directly with individuals whose identities are being used or have possibly been stolen. IDES is also working with local and federal law enforcement authorities to investigate, pursue, and prosecute those who are defrauding the unemployment insurance system.

An individual who has not filed an unemployment claim but has received a debit card or an unemployment insurance (UI) finding letter in the mail has most likely been the target of fraud. An individual’s personal identifying information is being used by fraudsters to file an unemployment claim is likely due to a prior cyber hack or data breach, such as the Equifax breach. It is imperative that individuals take the following steps if they have not filed an unemployment claim and have erroneously received an unemployment debit card or UI finding letter in the mail:

- Immediately call IDES at 800.814.0513 and when prompted:
 - o Select the English or Spanish language option
 - o Selection option 1 for claimants
 - o Selection option 5 to report identity theft
- Do not activate the debit card that was mailed to you.
- Have your credit report checked for possible suspicious activity and post a fraud alert.
- Visit the [Federal Trade Commission's website](#) to learn helpful tips on recognizing and reporting identity theft.

The increase in the fraudulent unemployment claims is believed to be coming primarily out of the Pandemic Unemployment Assistance (PUA) program. Under the ambiguous federal guidelines, which were developed in haste because of the urgency of the pandemic and issued to every state without a uniform method of implementation, the potential for fraud within this system is abundant.

One of the largest vulnerabilities within PUA is the absence of an employer on the other side of the claim to contest the claim in the event the it is fraudulent or should be protested. Under regular unemployment insurance guidelines, an employer has the ability to alert IDES if a claim has been filed in the name of an employee who is currently employed, and has the ability to protest a claim if they believe the employee does not fall into the category of having lost work through no fault of their own.

This fraud scheme is in no way connected to the PUA program access issue experienced in May. The limited data access issue of the PUA system found that one PUA claimant was able to inadvertently access personal identifying information of a limited number of claimants who had already filed an unemployment claim. Out of an abundance of caution, a year's worth of free credit monitoring was provided to any claimant whose information may have been inadvertently viewed by this one individual claimant.