PUBLICATION

Top Three Steps for Employers to Take When Facing Fraudulent Unemployment Claims

Authors: Elizabeth Ann Liner, Zachary B. Busey

April 01, 2021

Government agencies have been grappling for nearly a year with ongoing attacks directed at state unemployment programs through unique fraud schemes. The Department of Labor (DOL) has estimated that approximately $36 billion of the $360 billion benefits paid was for fraudulent claims. The passing of the American Rescue Plan Act (ARPA) means that these schemes are likely to continue and perhaps increase in frequency. Employers have played and will likely continue to play a significant role in the discovery of such schemes. What can employers do?

Federal Legislation

Before the pandemic, the most common form of unemployment fraud involved applicants receiving benefits while working and not reporting the wages that they were earning. However, the enactment of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) made lucrative federal funds available to unemployed individuals in addition to the standard state funds and extended eligibility to many individuals not usually covered, such as independent contractors and the self-employed. Legislation also lifted standard requirements for benefits such as the regular job search and the one-week waiting period. With a substantial increase in funds available and the usual checks and balances lifted, unemployment programs became prime targets for cyber-scams and fraud schemes. The recently passed ARPA extends many of the benefits made available under the CARES Act through September 4, 2021, including making additional federal funds available ($300/week).

Fraud Schemes

In a recent article, *USA Today* reported on a virtual anonymous interview with one of the fraudsters, an engineering student in Nigeria, who revealed that it was commonplace among his peers to use identity theft as a means of obtaining unemployment benefits from various state programs in the U.S. These scams are being perpetrated by unknown scammers from across the world who obtain personally identifying information (PII) for an individual and use it to apply for unemployment through a state agency. Criminals are using various techniques to obtain this PII, including purchasing it in exchange for cryptocurrency.

Unemployment benefit requests generally do not show up on credit reports. Therefore, fraud alerts on credit reports will not necessarily note stolen PII. Also, impacted individuals are not receiving notice of the unemployment application in their name because either the individual did not have an address in the system or fraudsters provided another address during the application process. In some cases, the fraudsters have physically stolen notice postcards from the individual's mailbox. As a result, the scheme often continues for weeks before discovery.

Earlier this year, the DOL announced that it will be issuing $49 million in grant funds to 28 state unemployment programs which funds are particularly earmarked for combatting fraud. However, only two days after being sworn in as U.S. Secretary of Labor, Marty Walsh was pummeled by a call from states for help thwarting unemployment fraud. With the passing of ARPA, it is likely these schemes are not over as the appeal of reduced restrictions and increased benefits will continue to draw the attention of foreign and domestic fraudsters.

Next Steps

Because of the high demand for employees in the long term care industry during the pandemic, unemployment claims may not be top of mind. However, because of the state of the unemployment system today, long term care employers should be alert to potential fraudulent claims. Employers are often the first to learn that someone is collecting benefits in the name of an individual that is currently employed. Long term care employers should be hypervigilant about unemployment claims of their employees and spread the word to increase awareness.

1. Notify your workforce. Inform employees about the prevalence of these types of scams; inform them of the fact that individuals who have previously been subject to identity theft are more susceptible; and educate them on steps to protect their PII. Suggestions for best practices for employees include the following:

- Securing an individual's social security number
- Storing personal information such as bank account numbers and dates of birth in a safe place
- Not sharing personal information, particularly over the phone
- Using security features available on mobile phones
- Creating complex passwords for accounts
- Using strong authentication questions (the Nigerian engineering student interviewed by *USA Today* admitted to obtaining maiden names)
- Watching bank accounts for unauthorized transactions, particularly any transactions by or from their state unemployment agency

2. Prepare Human Resources. Human Resources personnel should be on alert and should review any notices from state unemployment administrators with heightened scrutiny.

Employers tend to be the first to learn of these scams when an unemployment notice is received regarding an existing employee (in some instances, CEOs and upper management have shown up on unemployment notices received by employers). If you encounter such an issue have a plan to respond, including**:**

- **Notify the appropriate state unemployment administrator**. Many states now have forms for reporting this type of fraud, and most have a hotline to call. The DOL has compiled a list of those hotline numbers here.
- **Notify the DOL**. You can use the form found here.
- **Notify the employee.** Inform the affected employee that his/her PII has likely been compromised.
- **Instruct that employee.** Have the employee file a police report and report the issue to the state unemployment administrator and the DOL.
- **Assist the employee**. You may also provide information regarding resources for addressing identity theft. The Federal Trade Commission has a helpful website here.

3. Address the possibility of a data breach. If you have multiple employees experiencing this issue, you should evaluate the possibility of a data incident or other unauthorized access to your systems containing employee-related PII. If you discover an incident (or even a potential incident), it needs to be reported to your insurance carrier, and we strongly suggest involving outside legal cyber counsel. In the meantime, to guard against such incidents, employers should weigh and consider the following:

- **Conduct a risk assessment and review it**. A good starting point is to identify and understand where employee-related PII is collected, stored, and utilized within the company. From there, you can identify corresponding security protocols – or perhaps a lack thereof – and adjust those protocols accordingly. You need to learn of potential weaknesses and correct them before they are exploited.

- **Ensure that written policies address employee-related PII**. As with any employee-related issue, sufficient written policies are key. Too often, a company's policies adequately address the security and appropriate use of customer- or client-related PII, but fail to address employee-related PII.

- **Remote work and personal devices**. Now, more than ever, employees are working remotely and accessing company documents and information through personal (or quasi-personal) devices. Even company-provided devices, when used remotely, are most often connected through personal networks. Companies must ensure sufficient protocols for securing remote access to company networks. Where possible, such connections should be through a virtual private network (VPN). VPNs should be configured with multi-factor authentication (MFA) as an added security layer. With MFA enabled, even if an employee's VPN credentials are compromised, an unauthorized actor will be unable to connect through the VPN without a second factor (i.e., a code sent to an individual's smartphone, token, biometric verification, etc.).

- **Training and enforcement**. We have all experienced "Zoom fatigue" at one point or another during COVID-19. With remote work becoming part of the "new normal," companies need to adjust accordingly. Online training videos or sessions must reinforce security and remote-access protocols, such as protecting passwords and not leaving laptops unattended. These policies and best practices should also be enforced in the same manner other company policies are enforced. If an employee would be disciplined for leaving open a door or secure file room at the office, he or she should also be disciplined for failing to secure access to the company's electronic information, including employee-related PII.

If you have any questions regarding these issues, please contact the authors Elizabeth Liner and Zachary Busey, or any member of Baker Donelson's Labor and Employment Team or Data Protection, Privacy, and Cybersecurity Team.