PUBLICATION

Fraudulent Unemployment Claims on the Rise: What Should Employers Do?

Authors: Elizabeth Ann Liner, Zachary B. Busey
November 16, 2020

Government agencies are grappling with the theft of millions of taxpayer dollars through unique fraud schemes directed at state unemployment programs. Employers often are the first to discover these schemes when they learn that current employees have somehow been receiving unemployment benefits for weeks while working. What can employers do?

Nationwide Impact

In Washington, officials announced a theft of $550 million to $650 million from the state's unemployment system, of which about $300 million was recovered. Cybercriminals in Colorado were so aggressive that 75 percent of applications during a single month were ruled fraudulent. Before they were caught, thousands of inmates in Pennsylvania applied and qualified for unemployment benefits. In North Carolina, federal authorities seized more than $80,000 in funds held in local bank accounts allegedly associated with COVID-19 unemployment fraud. The account holders who aided the fraudsters appear to have been victims as well because they were led to believe they were in online romantic relationships.

These are just some of the examples of the fraud schemes. There is a multiagency effort to protect taxpayer dollars from this type of fraud. The Department of Justice (DOJ), the Department of Labor (DOL), the FBI, the U.S. Secret Service, along with state investigative bodies are working to catch the criminals perpetrating these acts. The DOJ is prosecuting three individuals in Iowa and seeking maximum sentences of up to 20 years in prison. These agencies are calling for everyone to report suspected fraud as soon as it is discovered.

Unemployment Generally

Each state administers its own unemployment compensation system and provides benefits to unemployed individuals. Most states impose a one-week waiting period and require that the individual demonstrate that they are ready and able to work, actively searching for work, and are not unemployed due to misconduct. The most common form of unemployment fraud in the past has involved applicants receiving benefits while working.

The New Form of Unemployment Fraud

However, since the enactment of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), there has been a new type of unemployment fraud plaguing the state systems involving cyber-scams and identify theft. The CARES Act made lucrative federal funds available ($600/week) to individuals unemployed due to the pandemic in addition to the standard state funds. Many states also lifted some or all of the standard qualifications such as the job search requirement 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 scams and fraud.

These scams are being perpetrated by unknown scammers who obtain personally identifying information (PII) of an individual and use the individual's PII to apply for unemployment through the state agency. Criminals are using various techniques to obtain this PII:

- email phishing schemes,

- purchasing stolen PII,
- use of PII obtained during prior data breaches,
- cold-call impersonation scams, and
- physical theft of data (i.e., dumpster diving), among others.

Unemployment benefits requests generally do not show up on credit reports. So, fraud alerts will not necessarily alert the individual to the fact that their PII has been stolen and used to apply for unemployment. The individuals are not receiving notice of the unemployment application because either the individual did not have an address in the system or fraudsters provided another address during the application process. And, in some cases the fraudsters are physically stealing the notice postcard out of the individual's mailbox. As a result, the fraudsters are able to continue to receive benefits for weeks under the individual's stolen identity before they are discovered.

What Can You Do?

Employers should be hypervigilant.

- **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.
- **Prepare Human Resources**. Human Resources personnel should be on alert and should review any notices from the state unemployment administrator 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:

- **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, report the issue to the state unemployment administrator, and to the DOL.
- **Assist the Employee**. You can also provide information regarding resources for addressing identity theft. The Federal Trade Commission has a helpful website at https://identitytheft.gov/.

Notably, 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 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. Written policies must include employee-related PII, which is often the largest source of PII maintained and used by a company.

- **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, in turn, 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 & Enforcement**. We have all experienced "Zoom fatigue" at one point or another during COVID-19. But 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.