FUNKHOUSER VEGOSEN LIEBMAN & DUNN LTD.

COVID-19 Legal Update

March 18, 2021

STOPPING COVID-19 UNEMPLOYMENT CLAIM SCAMS

By Peter T. Berk

As the pandemic continues, and unemployment benefits are extended and increased, a new type of identity theft and fraud has arisen. Identity thieves will obtain key information about an employee – including social security number, workplace, and possibly even the employee's salary. The identity thief will then use the employee's information to make a claim for unemployment benefits. In Illinois, as well as other states, such benefits are paid through a debit card mailed to the claimant. The identity thief will either try to steal the debit card from the mail, or file a change of address with the unemployment office to redirect the debit card or other payment. The thief will then try to use the money before the scam is discovered and the claim is denied. Employers and their employees must be vigilant and work together to avoid becoming victims.

How do I know if our organization/our employee is a victim?

The scam is usually uncovered in one of two ways. First, when an individual files an unemployment claim, the employer against whom the claim is filed receives a notification of the claim. In the case of the scam, the employer will receive notice of the claim, but will realize that the claim is by a current employee. Second, an employee may receive mail or another communication from the unemployment office regarding the claim – such as a copy of the claim, an address verification, correspondence regarding the debit card, or the debit card itself.

What can our organization do as an employer to protect itself and our employees?

There are a few steps an employer can and should take when it receives a fraudulent claim as part of this scam:

1. inform the employee of the claim, confirm that the employee did not file it, and provide the employee with any and all information you can about the claim (so the employee can protect himself or herself);
2. assuming it is fraudulent, report the claim as fraudulent to the unemployment office;
3. file a response to the claim, including indicating that the employee is still employed and the claim is fraudulent; and
4. check your computer system for any intruders or malicious files that may have released employee information.

FVLD

What can our organization's employees do to protect themselves?

An employee who is a victim of this scam should also take certain actions to protect themselves. These include the following:

1. the employee should report the fraudulent claim to the unemployment office – some offices have telephone hotlines and/or webpages for individuals to use to report this scam. Given the prevalence of the scam, the employee may not receive a response for some time;
2. the impacted employee should report the incident to the local police department where he or she lives, and make sure to get a police report number. This will help should the employee need to make any claim to a creditor or credit rating bureau regarding identity theft;
3. the employee should visit the Federal Trade Commission's website at www.identitytheft.gov for additional advice regarding this scam. Further, if the employee has other identity theft concerns, those can be reported here as well. The employee's state's Attorney General's website may also have helpful information;
4. the employee should obtain free copies of his or her credit reports from each of the three reporting agencies (Experian, Equifax and Transunion), and review each for errors or unknown accounts. If there are errors, unknown accounts, or other issues, the employee should report them immediately to that bureau;
5. the employee should place a fraud alert (or a credit freeze) on his or her credit report;
6. the employee should consider purchasing personal identity theft protection services, such as www.lifelock.com;
7. if the employee's data was part of a recent data breach (from your or another organization), the employee should take advantage of any offers of protection (such as additional fraud monitoring); and
8. if the employee receives a debit card related to the claim, he or she should not activate or use the card, but rather should destroy the card.

Conclusion

The ongoing pandemic has created numerous opportunities for identity thieves to exploit holes in the system or individuals' fears. It is important to be even more vigilant in these challenging times. If your business or employees have been victimized in any scam, you may also want to contact your legal advisors.

FVLD publishes updates on legal issues and summaries of legal topics for its clients and friends. They are merely informational and do not constitute legal advice. We welcome comments or questions. If we can be of assistance, please call or write Peter T. Berk at 312.701.6870 or pberk@fvldlaw.com, or your regular FVLD contact.

FVLD