Employer Beware: Avoiding Fraudulent Unemployment Claims

June 1, 2020

In the wake of the COVID-19 pandemic, the U.S. unemployment rate is at its highest level since the Great Depression. In light of the economic upheaval caused by this pandemic, in March 2020 Congress passed the largest economic stimulus package in U.S. history: the Coronavirus Aid, Relief, and Economic Security ("CARES") Act.

In addition to various types of direct payments and loan programs for businesses and individuals, the CARES Act provides workers with enhanced unemployment benefits, including Federal Pandemic Unemployment Compensation, Pandemic Emergency Unemployment Compensation, Pandemic Unemployment Assistance, and other reimbursements. These programs expand unemployment assistance to individuals who ordinarily would not be entitled to unemployment assistance or who have exhausted their benefits. These programs also provide unemployed workers with extra weekly payments in addition to existing state-provided benefits. Moreover, states have passed additional measures to provide unemployment relief. In response to Massachusetts' unemployment rate reaching as high as 24 percent—an all-time high—Governor Baker signed into law bill S.2618 which expands unemployment relief measures for both employees and employers.

In addition to providing much-needed relief, the rapidly expanded scope and availability of unemployment benefits have also created conditions ripe for fraud. Indeed, the rise in unemployment filings and the expansion of available benefits have led to a nationwide increase in the filing of fraudulent unemployment claims. Authorities suspect that criminal enterprises have been using stolen personal information collected from previous data breaches to file fraudulent claims, which are being submitted under the names of legitimate claimants as well as individuals who are still employed and never filed for unemployment benefits.

Each state has its own process for submitting and processing unemployment claims, and similar vulnerabilities for fraud and abuse. In Massachusetts, for example, once an application for unemployment benefits is filed with the Department of Unemployment Assistance ("DUA"), the DUA sends the employer a letter notifying it that the application was filed and the estimated unemployment insurance payments the employer may owe. For larger employers who have instituted widespread layoffs and furloughs—and receive a large volume of such letters—insurance payments for fraudulent claims may end up being processed alongside those for legitimate claims. In such cases, employees only learn of the fraud when they themselves receive a letter from the DUA approving their "claim" for unemployment benefits—which they never filed.

There are actions employers and employees can take to prevent these fraudulent unemployment claims from being paid:

- First, upon notification from the state unemployment agency that an application for unemployment benefits has been filed, the employer should confirm whether the named applicant is a current or former employee. If it is a current employee, then the claim is likely fraudulent. If it is a former employee, the employer should contact the former employee to confirm whether the individual filed a claim for unemployment benefits.
- Second, if it is determined that the claim is fraudulent, both the employer and the employee/former employee should immediately contact the state unemployment agency to report that the claim is fraudulent. For example, in Massachusetts, there is a webpage devoted to reporting fraudulent unemployment benefits claims, which provides a Fraud Reporting Form, the UIfraud@mass.gov email address for reporting fraudulent claims, and a telephone number. Due to reduced staff and high call volume, using the online form or email is recommended.
- Third, employees should be aware that this is evidence of a possible theft of their personal information, and they should take appropriate measures to protect their information, including alerting their banks and health insurers, signing up for credit monitoring services, and reporting the theft of their personal information to the Federal Trade Commission and separately to the IRS by filing IRS Form 14039. Such employees should also file a police report with their local law enforcement and coordinate with their employer to file the report of the data breach with the Office of Consumer Affairs and Business Regulation. In addition, the three major credit reporting agencies provide mechanisms for placing fraud alerts on accounts so that any application for a line of credit will require additional identity verification measures.
- Fourth, employers should monitor their tax accounts on a daily basis to identify unexpected claims as early as possible. In Massachusetts, for example, employers can monitor their DUA and MassTaxConnect Accounts for any suspicious activity.

The Secret Service is currently pursuing leads to shut down this fraud network. In Massachusetts, the DUA is taking its own measures to protect against this kind of fraud by requiring applicants to provide additional identifying information when filing a claim. Consequently, claimants and employers should anticipate a delay in the approval and payment of benefits.

Due to this unfortunate surge in fraudulent unemployment claims, it is important for employers to diligently monitor unemployment claims and confirm the legitimacy of any such claims with their employees and former employees.