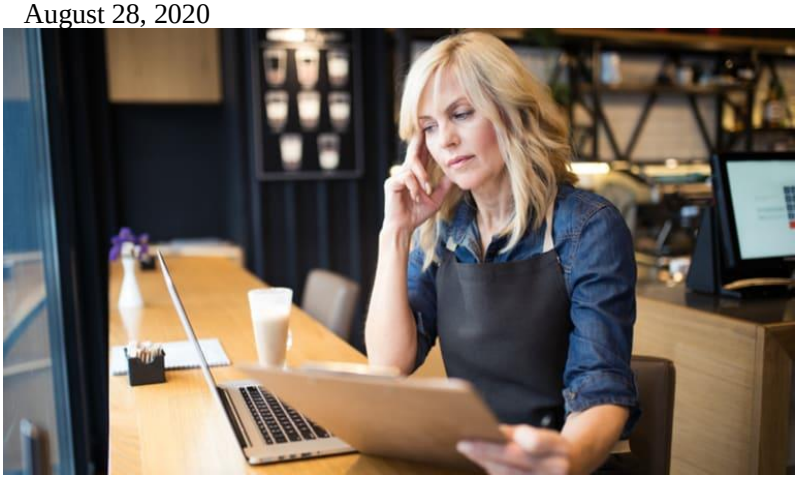
Unemployment Fraud Is on the Rise

HR should remain vigilant in reviewing claims

By Roy Maurer
August 28, 2020



The rise in unemployment filings and the expansion of jobless benefits in the wake of the ongoing COVID-19 pandemic have facilitated an explosion of fraud across the country. HR has a responsibility to respond quickly to phony unemployment claims and assist employees whose personal information has been stolen.

"With the broad expansion of unemployment benefits during the pandemic, and states racing to get them distributed, fraud was a concern from the outset," said David Fryman, a partner and member of Ballard Spahr's labor and employment group in Philadelphia. "Sure enough, states and federal entities are reporting significantly increased instances of fraudulent claims for unemployment benefits. Across a number of states, employers report receiving notifications of claims for unemployment benefits filed in the name of individuals who remain employed or employees who left the organization or retired years ago."

The Coronavirus Aid, Relief, and Economic Security (CARES) Act expanded unemployment benefits for people affected by the COVID-19 pandemic in several significant ways, including by upping the weekly benefit amount by $600 through July 31. And even though the additional $600 is no longer offered, many states are now approved to participate in a $400 extra unemployment payment program launched Aug. 8 by the Trump administration.

FBI Warning

The FBI alerted employers in July about the rise in fraudulent unemployment claims using stolen identity information. "The criminals obtain the stolen identity using a variety of techniques, including the online purchase of stolen personally identifiable information, previous data breaches, computer intrusions, cold-calling victims while using impersonation scams, e-mail phishing schemes, physical theft of data from individuals or third parties, and from public websites and social media accounts, among other methods," the agency said.

The large-scale scams involve filing claims for benefits using the names and personal information of people who have not lost their jobs, said Seena Gressin, an attorney with the Federal Trade Commission (FTC) who is focused on identity theft and fraud prevention. "The investigation is ongoing, but this much is known: The fraud is affecting tens of thousands of people, slowing the delivery of benefits to people in real need, and costing states hundreds of millions of dollars," she said. "Most people learn they're affected when they get a notice from their state unemployment benefits office or their employer about their supposed application for benefits. By then, the benefits usually have been paid to an account the criminals' control."

The prevalence of reported incidents from every corner of the country is staggering. Here are just a few of the cases:

- Georgia found more than 130,000 false claims filed in July.
- Illinois identified more than 120,000 counts of unemployment insurance fraud in August.
- Maryland announced 47,000 fraudulent claims had been uncovered in early July.
- Pennsylvania reported that 10,000 prison inmates filed for benefits across the state.

Jan Eckert, HR director at Bucklin Tractor & Implement Co., an agriculture and farm equipment dealership with locations across Kansas, recently received the third fraudulent unemployment claim among her company's workforce of 200 since the onset of COVID-19.

"I know this is a problem in Kansas, and I understand the same is true in Oklahoma, as well," she said. "I was especially concerned when I received notice of the first two in July. Both involved employees in one location. My first concern was an internal security breach, but in working with our IT [information technology] department, we could find nothing to indicate our security had been compromised. I also reached out to Paycom, who we use for our HRIS [human resource information system] and payroll functions."

Eckert said the Kansas Department of Labor (KDOL) responded to the first two claims and stopped them. "They also provided helpful information for me to share with the employees, who had apparently been impacted by identity theft," she said.

The most recent claim, filed Aug. 20, was for a former employee who retired earlier this year "after a long and successful career with the company," she said. Eckert reported it to KDOL after checking with the former worker, who denied filing it, she said.

HR's Responsibility

Due to the surge in fraudulent unemployment claims, it is important for HR to diligently monitor and confirm the legitimacy of claims, said Rebecca Harris, an attorney in the Boston office of Goulston & Storrs. "Each state has its own process for submitting and processing unemployment claims," she said.

Eckert said she monitors and responds to the claims her company receives. "For employers who do not monitor claims as closely, a fraudulent claim could end up being successful," she said.

Harris added that especially for larger employers that have instituted widespread layoffs and furloughs, 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 approving their claim for unemployment benefits—which they never filed."

The following are actions employers can take to prevent fraudulent unemployment claims from being paid:

Be alert. Let employees know about the spike in fraudulent claims and identity theft and ask them to report fraudulent benefits claims to HR as soon as they learn about them. People should exercise caution to protect against identity theft and pay careful attention to correspondence they receive related to unemployment benefits, especially if they have not applied for those benefits, Fryman at Ballard Spahr said. "Employers should be vigilant in checking their unemployment reports or advising their third-party unemployment claims administrators to do so, to guard against fraudulent claims linked to their unemployment accounts," he added.

Notify employees quickly. Harris said that HR should promptly review whether the named applicant for unemployment benefits is a current or former employee. "If it is a current employee, then the claim is likely fraudulent," she said. "If it is a former employee, the employer should contact the former employee to confirm whether the individual filed a claim for unemployment benefits."

Report the fraud. Both HR and the affected employee should work together to quickly notify both the state unemployment benefits agency and local police department of the fraud. The U.S. Department of Labor provides employers with resources on how to report unemployment fraud in each state.

Address identity theft. "The filing of a fraudulent unemployment claim is a sign that an employee's sensitive personal information is available to criminals," said Brandon Archuleta, an attorney in the Seattle office of Lane Powell. He advised employers to direct employees to file a report with the FTC, notify the major credit bureaus, review their credit report, request fraud alerts or a credit freeze, and take steps to ensure that their personal information is not used to commit additional fraud. The FTC's Gressin suggested employees visit www.identitytheft.gov to report the crime to the FTC and get step-by-step recovery help.

Review IT security. Archuleta also recommended that employers consult with their IT department to confirm that databases containing employee information have not been compromised.