Updates
May 22, 2020
Increase in Unemployment Claims Brings Heightened Risk of Fraud: How Employers and Employees Should Respond

As new unemployment claims rise, impostors seek to scam the unemployment system at the cost of the state, employees, and employers. Here's how to respond to, and lower the risk of, fraudulent unemployment claims.

Spike in Unemployment Fraud Accompanies Increased Claims to ESD

As many businesses are forced to furlough or lay off employees in the wake of COVID-19, unemployment claims have spiked precipitously. Although the number of unemployment claims filed with the Washington State Employment Security Department (ESD) per week has fallen from the early-April high of 182,000, the ESD continues to receive around 100,000 new claims per week as of May 9, 2020.

According to ESD Commissioner Suzie LeVine, the wave of new unemployment claims includes a dramatic increase in the number of fraudulent requests, prompting the ESD to pause all unemployment payments for two days in May to address the onslaught of fake claims. The ESD estimates that, in March and April 2020, fraudulent claims increased to 27 times the pre-COVID-19 rate and that $1.6 million may have been paid to fake claimants. In addition to filching government funds, fake claims, if unresolved, will increase the cost of employers' unemployment insurance.

Recent increases in state and federal benefits—including an additional $600 weekly payment from federal stimulus funds—have increased incentives to file fraudulent claims for benefits using employees' personal data, which may have been obtained during unrelated data breaches or via a phishing website posing as the ESD. Employees and employers are often unaware of the fraud until the ESD contacts them as part of its claim processing procedure.

Reactive Steps for Employers

The ESD, as well local police departments, are investing additional resources to prevent and respond to unemployment fraud. Employers that become aware of a fraudulent claim should do the following:

1. Report the fraud to the ESD by completing the Benefit Fraud Employer Reporting Template available on its website and submitting the completed form through the ESD's Employer Fraud Reporting webpage at https://fortress.wa.gov/esd/file/SecureUpload/unemploymentfraud/employer.
2. Promptly notify the affected employee and advise them to take the additional steps detailed below.
3. Notify the local police department to assist them in tracking and understanding this issue. Seattle employers can file a report online at https://www.seattle.gov/police/need-help/online-reporting.
4. Maintain records of relevant communications and filings.

The recent spate of fraudulent filings is generally assumed to use information obtained from prior data breaches or through a phishing or similar scam, so they do not necessarily indicate that the employer has suffered a breach. That said, employers should pay close attention to the data being used in a fraudulent filing for any indication that it may have come from the employer and should review their own security measures.

Reactive Steps for Employees

Employers should also advise any employees associated with a fraudulent claim to take the following steps:

1. Notify the ESD by calling 1.800.246.9763 or by completing an Imposter Fraud Report online at https://fortress.wa.gov/esd/file/SecureUpload/unemploymentfraud/report.
2. File a police report to establish a record that may be used to access protections available to victims of identity theft.
3. Check their credit report. Employees can obtain a free copy of their credit report maintained by each of the three credit reporting agencies by visiting annualcreditreport.com or by calling toll-free 1.877.322.8228.
4. Consider contacting credit reporting agencies directly to place a fraud alert or a security freeze. A fraud alert will notify any merchant checking the employee's credit history that the employee may be the victim of identity theft and that the merchant should take additional measures to verify the application. Contacting any one of the three agencies will place a fraud alert on the employee's file at all three. A security freeze restricts all creditor access to the account, but might also delay any requests the employee might make for new accounts.

Equifax: 1.800.525.6285; equifax.com/personal/credit-report-services/

Experian: 1.888.EXPERIAN (397.3742); experian.com/help

TransUnion: 1.800.680.7289; transunion.com/credithelp

5. Use the tools from the FTC at identitytheft.gov for additional recovery steps.

Preventative Measures

To minimize the risk of fraudulent unemployment claims, employers should implement the following preventative measures:

1. Request immediate notification if employees receive any communication from the ESD that they did not personally request. Make sure there is a clear point of contact for these notices.
2. Review IT security protocols to ensure that employees' personal data cannot be accessed by third parties, potentially with the aid of a cyber security vendor.
3. Increase employee training and awareness of phishing schemes.

Authors

Explore more in

Labor & Employment

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law