

## Was there a CDLE data breach?

No, there has been no data breach. Like other states, Colorado continues to see increased unemployment fraud activity. Many Colorado employers are noticing fraudulent unemployment claims being filed in the names of active employees.

Fraud within the Unemployment Insurance programs nationally has become rampant during the Pandemic. The Pandemic Unemployment Assistance (PUA) program under the CARES Act has been a relatively easier target, as it does not have the same checks and balances inherent in the state UI system. Colorado was one of the first agencies to begin an aggressive fraud detection and prevention program when this issue began to present itself. To date, CDLE has stopped over 800,000 fraudulent claims, and has likely prevented over \$7 billion in fraudulent payments. These are sophisticated criminal rings that use Personally Identifiable information, including social security numbers, to file claims on behalf of unsuspecting victims. We speculate that the sheer volume of this identity theft is the result of one or several data breaches that have occurred over the past few years, which compromised hundreds of millions of identities. In recent weeks as the Cares Act Unemployment Insurance programs expired, we suspect these fraudsters have shifted their effort to State Unemployment Insurance systems, as we saw large upticks in initial claims.

If someone is notified by their employer that a claim was filed using their information, or if they receive an unemployment debit card in the mail, they are likely a victim of identity theft and should take immediate precautions. While unemployment is relatively harmless to the victim's credit, these criminals could make other transactions using these identities, which has the potential to cause irreparable damage to the victim's credit. CDLE is committed to take every possible measure to prevent fraud within the Unemployment system, though it is an uphill battle.

## Is the form to report fraud secure?

Per the Google Team within the Governor's Office of Information Technology:

- Use of Google forms is a secure process
- Transmission of data (data in flight) is secure and encrypted
  - Between the form to the sheet
  - Via the email submit process to the recipient
- End users within CDLE (and the State at large) use multi-factor authentication to Prevent unauthorized use or logins protecting access to the data storage location

Administratively (internal) CDLE is mindful of...

- What processes are in place to protect access to the data (*Google Sheet*) location
- Who and how many people have access to the data sheet
- How is this being overseen/administered
- Communication is being encrypted through Proofpoint

## Will my premiums be impacted by fraudulent claims?

If any benefits were paid that would charge against your account prior to the claim being closed as a fraudulent claim, once the claim was closed for the fraudulent activity, your account was re-credited for any benefits that might have been paid. As such, payment of any of those benefits will not impact your experience rating when your premium rates are calculated.

## Is CDLE sending out PII?

Employer correspondence masks an employee's full SSN, showing the last 4 numbers.

## Do I need to appeal these claims benefit charges?

It is possible you received a decision on a claim that was closed due to fraudulent activity due to a program we used in our old system to try to resolve certain reported issue types that did not recognize when a claim was already closed. While our hope is to provide documentation at some point that these claims have been closed to reduce confusion and provide certainty to you, should consider submitting an appeal on any decision you received at this time to ensure the claim is closed for fraudulent activity.

## What do I do with a job separation request for an employee still on payroll?

When a claim is filed using the stolen identity of one of your employees, you receive a questionnaire by email or U.S. mail requesting information about the job separation. If your employee is still employed, and they state they did not file a claim, please complete the questionnaire as soon as possible.

Employees who are the victim of UI fraud should submit a Fraud Report online. They should visit [ColoradoUI.gov](https://colorado.gov/department-of-labor-and-employment/submit-a-fraud-report), click the "Report Fraud" button, then the "Submit a Fraud Report" button. Our website also outlines other important steps that employees who are victims of UI fraud should take.

## What happens after I submit a report?

After completing the "Submit a Fraud Report" form, the individual will not receive a follow up call or email from CDLE. While the current volume of fraud reports prevents us from following up individually on every report, our fraud investigators have received your report and will take immediate steps to close this fraudulent claim.

We understand how unsettling this experience can be. We take any fraud seriously and work daily with law enforcement and other agencies to investigate and prosecute this behavior. If you haven't yet, we encourage you to review our tips on protecting yourself against fraud.