UI Fraud
Overview
UI Fraud Overview

- The fraud we are seeing during the pandemic is a new type of fraud
- Since the inception of UI, CDLE has relied on the sanctity of a private SSN.
- Mass data breaches over the last few years changed that.
  - The identifying information is likely coming from these mass breaches, and not CDLE or an employer breach.
- We began noticing this trend in June, with the federal programs.
  - These are easier to target, no checks and balances
- We immediately implemented measures to detect and prevent fraudulent payments.
- As federal programs approached expiration 12/26, we saw a huge spike into the state system.
Why We Need Your Help

- In 2019, CDLE had 88 cases of fraud. Since March of 2020, CDLE has well over 1.2 million claims on a payment hold for suspected fraud.
- Our current strategy does not rely on preventing a fraudulent claim from being filed, but stopping payment immediately upon filing.
  - We have no way to verify if a claim is fraudulent or not until it is filed in our system.
- The one aspect that a criminal cannot control, is the employers we notify once a claim is filed.
- All employers reporting wages onto an SSN in the last two years will automatically be notified of a claim being filed under that SSN.
- We need employers to help notify victims to ensure they take necessary precautions to protect themselves.
What is Fraud?

Please report a claim as fraudulent if you receive a questionnaire for:

- An employee that is still working for you and has not suffered any loss of hours.
- Someone that has never worked for you.
- Someone with non-matching name and social security number info.
- An employee who separated in the past and confirms they did not file the claim.
What is NOT Fraud?

- It is NOT FRAUD if you receive a claim for an employee that worked for you, but you disagree that they deserve benefits. DO NOT file a fraud report for this reason, as the penalty for disputing a legitimate claim for benefits is one and half times the benefit amount.

- Please remember that a claimant does not choose which employers are sent fact-finding questionnaires. ANY employer that the claimant worked for in the last 18 months (our base period) will receive a questionnaire from CDLE. If you disagree with a finding of benefits, please proceed with the typical CDLE appeals process. Just because an employee hasn’t worked for you in a while, does not necessarily mean it is fraud.

- Submitting the fraud report on our website will hold payment on the claim pending investigation. Be aware, you may continue to receive paperwork that’s automatically generated. Rest assured, the report was received, and the claim is under investigation.
What Should Employers Do?

**DO** Immediately report the suspected fraud to CDLE via our [online form](#).

**DO** Disregard any additional correspondence from the division on these claims as these are automatically generated until we can reprogram the system to suspend these communications.

**DO** Inform the employee that they may be a victim of identity theft and direct them to our website for resources.
**What Should Employers Do?**

**DO NOT** Complete the questionnaire in MyUI Employer or the paper form you may have received. Submitting the report will hold payment on the claim, pending investigation. (SIDES users still need to respond to their electronic request)

**DO NOT** File an appeal. Payment of any fraudulent benefits will not be charged to your account (upon a finding of fraud) and will not impact your experience rating when your premium rates are calculated.

**DO NOT** Call the main UI call center at 303-318-9000. You may call the Employer Services line at 303-318-9100 should you have any questions but after completing the fraud form rest assured, the report was received, and the claim is under investigation.
What Should Victims Do?

- Put a fraud alert on their credit with the three credit bureaus and invest in credit monitoring. See other tips in the “identity theft repair toolkit” created by the Attorney General’s Office
  - Unemployment is relatively harmless to credit, but with the information these criminals have they can do much more profitable and harmful things.
  - See more here: www.stopfraudcolorado.gov/fraud-center/identity-theft.html

- Report the fraud to CDLE and US Bank through our respective forms.
  - CDLE uses a Google form, and it is secure. The form and the sheet are secure, and transmission of data (data in flight) is secure and encrypted

- Once reported, if it does not already have a payment hold, the system will flag the claim to hold payment.
Unemployment Recommendations for Restaurant Operators

Name
Kristin R.B. White
Fisher & Phillips LLP
kwhite@fisherphillips.com

April 21, 2021
Employment Law Recommendations

• Before Fraud Takes Place
  • Ensure Network Security
  • Passwords
  • Secure Systems
  • Firewalls
  • Antivirus Software
  • Educate Employees
Unemployment Claims

- Make sure you are reviewing all claims
- Respond to appropriate claims - TIMELY
- Review unemployment charge benefit statements
- Determine if fraudulent
Employment Law Recommendations

• After Fraud Occurs
  • Obligation to investigate
  • Immediately Report
  • Have Employee Take Action
  • Check Your Own System
    • Breach Response Team
    • Reporting Obligations
Questions?
Helpful Links:

- CDLE's main fraud page: https://cdle.colorado.gov/fraud-prevention
- Fraud reporting form for individuals: https://co.tfaforms.net/f/Report_Unemployment_Identity_Theft
- Fraud reporting form for employers: https://co.tfaforms.net/f/Employer_Reported_Identity_Theft
- Employer services email address: cdle_employer_services@state.co.us
- Employer email update subscription site: https://cdle.colorado.gov/employer-email-update