FinCEN ADVISORY

FIN-2020-A007 October 13, 2020

Advisory on Unemployment Insurance Fraud During the Coronavirus Disease 2019 (COVID-19) Pandemic

Detecting and preventing unemployment insurance fraud and other illicit activity related to COVID-19 are critical to safeguarding the integrity of government relief efforts.

This Advisory should be shared with:

- *Chief Executive Officers*
- *Chief Operating Officers*
- *Chief Compliance Officers*
- *Chief Risk Officers*
- *AML/BSA Departments*
- *Legal Departments*
- *Cyber and Security Departments*
- *Customer Service Agents*
- *Bank Tellers*

SAR Filing Request:

FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: "**COVID19 UNEMPLOYMENT INSURANCE FRAUD FIN-2020-A007**" and select SAR field 34(z) (Fraud - other). Additional guidance for filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to unemployment insurance (UI) fraud observed during the COVID-19 pandemic. Many illicit actors are engaged in fraudulent schemes that exploit vulnerabilities created by the pandemic. This advisory contains descriptions of COVID-19-related UI fraud, associated financial red flag indicators, and information on reporting suspicious activity.

This advisory is based on FinCEN's analysis of COVID-19-related information obtained from Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners.

Financial Red Flag Indicators of Unemployment Insurance Fraud Related to COVID-19 Relief

As unemployment claims in the United States have surged due to the pandemic, U.S. law enforcement and financial institutions have detected numerous instances of COVID-19-related UI fraud. The following are representative types of this illicit activity:

- *Fictitious employer-employee fraud:* filers falsely claim they work for a legitimate company, or create a fictitious company and supply fictitious employee and wage records to apply for UI payments;

- *Employer-employee collusion fraud:* the employee receives UI payments while the employer continues to pay the employee reduced, unreported wages;
- *Misrepresentation of income fraud:* an individual returns to work and fails to report the income in order to continue receiving UI payments, or in an effort to receive higher UI payments, an applicant claims higher wages than he/she previously earned;
- *Insider fraud:* state employees use credentials to inappropriately access or change UI claims, resulting in the approval of unqualified applications, improper payment amounts, or movement of UI funds to accounts that are not on the application; or
- *Identity-related fraud:* filers submit applications for UI payments using stolen or fake identification information to perpetrate an account takeover.[1]

As no single financial red flag indicator is necessarily indicative of illicit or suspicious activity, financial institutions should consider all surrounding facts and circumstances before determining if a transaction is suspicious or otherwise indicative of potentially fraudulent activities related to COVID-19. In line with a risk-based approach to compliance with the BSA, financial institutions also are encouraged to perform additional inquiries and investigations where appropriate.

FinCEN identified the financial red flag indicators described below to alert financial institutions to fraud schemes targeting UI programs, and to assist financial institutions in detecting, preventing, and reporting suspicious transactions related to such fraud.

Financial red flag indicators of UI fraud may include:

1 Account(s) held at the financial institution receive(s):

a. UI payments from a state other than the state in which the customer reportedly resides or has previously worked;

b. Multiple state UI payments within the same disbursement timeframe;

c. UI payments in the name of a person other than the accountholder, or in the names of multiple unemployment payments recipients;

d. UI payments and regular work-related earnings, via direct deposit or paper checks;

e. Numerous deposits or electronic funds transfers (EFTs) that indicate they are UI payments from one or more states to persons other than the accountholder(s);

f. A higher amount of UI payments in the same timeframe than similarly situated customers received.

1. *See*, FinCEN Advisory, FIN-2020-A005, "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (July 30, 2020). In some situations, fraudsters use the stolen identification information to perpetrate an account takeover. For additional information on identifying account takeover activity, *see* FinCEN Advisory, FIN-2011-A016, "Account Takeover Activity," (December 19, 2011).

2. The customer withdraws the disbursed UI funds in a lump sum by cashier's checks, by purchasing a prepaid debit card, or by transferring the funds to out-of-state accounts.

3. The customer's UI payments are quickly diverted via wire transfer to foreign accounts, particularly to accounts in countries with weak anti-money laundering controls.

4. The customer receives or sends UI payments to a peer-to-peer (P2P) application or app. The funds are then wired to an overseas account, or withdrawn using a debit card, in a manner that is inconsistent with the spending patterns of similarly situated customers.

5. Individuals quickly withdraw disbursed UI funds via online bill payments addressed to an individual(s), as opposed to businesses, as payee(s), with some individual payees receiving multiple online bill paychecks over a short time period.

6. The IP address associated with logins for an account conducting suspected UI-fraud activities does not map to the general location of stated address in identity documentation for the customer or where the UI payment originated.

7. Individuals direct UI-related EFTs, or deposit UI checks into suspected shell/front company accounts, which may be indicative of money mules transferring these funds in and out of the accounts.

8. Multiple accounts receiving UI payments at one or more financial institutions are associated with the same free, web-based email account that may appear in more than one UI application.

9. A newly opened account, or an account that has been inactive for more than thirty days, starts to receive numerous UI deposits. After a financial institution suspects UI fraud and requests additional identification documentation to verify the identity(ies) of the customer(s), queried individuals provide documents that are incorrect or forged, which may be an indicator of an account takeover or identity theft.

10. After a financial institution suspects UI fraud and conducts due diligence, it determines that the customer does not have a history of living at, or being associated with, the address to which the UI check or UI debit card is sent, or within the geographical area in which the registered debit card is being used.

Information on Reporting Suspicious Activity

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of due diligence requirements by financial institutions, is crucial to identifying and stopping unemployment insurance fraud related to the COVID-19 pandemic. Financial institutions should provide all pertinent and available information in the SAR and narrative.

- FinCEN requests that financial institutions reference this advisory by including the key term "**COVID19 UNEMPLOYMENT INSURANCE FRAUD FIN-2020-A007**" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.
- Financial institutions also should select SAR field 34(z) (Fraud - other) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19. When addressing unemployment fraud in a SAR, financial institutions should include the keywords "unemployment fraud" in SAR field 34(z).
- When filing a SAR, in addition to standard transaction data, providing the following information is highly valuable to law enforcement: relevant email addresses, IP addresses with their respective timestamps, login information with location and timestamps, cyber-related information and technical indicators, virtual currency wallet addresses, mobile device information (such as device International Mobile Equipment Identity (IMEI)), phone numbers, monikers, and description and timing of suspicious electronic communications.
- Please refer to FinCEN's Notice Related to the Coronavirus Disease 2019 (COVID-19), which contains information regarding reporting COVID-19-related crime, and reminds financial institutions of certain BSA obligations.

For Further Information

Financial institutions should send questions or comments regarding the contents of this advisory to the FinCEN Regulatory Support Section at frc@fincen.gov. To report suspected illicit activity please visit our website at https://www.fincen.gov/coronavirus, which also contains information on registering to receive FinCEN Updates.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.