Detection and Mitigation of Unemployment Insurance Fraud
Guidance for Financial Institutions

July 6, 2020

Overview:

The U.S. Secret Service and U.S. Department of Labor Office of Inspector General (DOL OIG), along with other state and federal agencies, are investigating an extensive criminal scheme involving the use of stolen personal identifying information to fraudulently claim unemployment insurance benefits. Financial institutions should be alert for suspicious transactions, and, when detected, rapidly return or preserve funds and report the suspicious activity. Financial institutions should work with appropriate law enforcement agencies to investigate potential illicit activity and to seize and return fraudulently obtained funds.

This advisory provides an update to alerts previously distributed through the Financial Crimes Enforcement Network (FinCEN). The Secret Service and DOL OIG will continue to work with FinCEN, other federal agencies, industry and trade associations, and state governments to share information regarding this activity in order to prevent fraud losses.

Detecting this scheme:

While unemployment insurance fraud is also occurring via physical checks and prepaid debit cards, the overwhelming majority of fraud is being committed via Automated Clearing House (ACH) transfers, sent to the accounts of "money mules" (these are individuals who receive and transfer illegally-obtained money on behalf of criminals; money mules may, or may not, be aware of their participation in an illicit scheme). After funds are deposited in the identified account, these funds are then withdrawn or transferred to other accounts.

Common indicators of this fraudulent scheme, which a receiving depository financial institution (RDFI) may detect, are:

- Account holder name and ACH "remit to" name do not match;
- Total unemployment deposits are in excess of $5,000 within a month;
- Unemployment deposits are paid to an account holder residing outside of the issuing state;
- The customer's account(s) receives both deposits of unemployment insurance and regular work-related earnings, such as paycheck deposits;
- Multiple unemployment insurance payments deposited into one account from the same issuing state, or from multiple issuing states;
- Unemployment deposits into one account intended for multiple unemployment benefit recipients;
- Deposited funds are quickly diverted via wire transaction to foreign accounts, particularly to accounts located in countries with poor anti-money laundering controls;
- The customer's account behavior seems atypical for an individual receiving unemployment benefits.

Reversing suspicious transactions:

Financial institutions that receive ACH transactions from fraudulent unemployment insurance benefit applications should expeditiously preserve and return these funds. This should be done in accordance with Anti-Money Laundering (AML) obligations and relevant banking laws and procedures. Specifically, RDFIs should work with the originating depository financial institution (ODFI) and the National Automated Clearing House Association (NACHA), to preserve and return funds from fraudulent unemployment insurance applications. RDFIs should partner with state workforce agencies and law enforcement to assist in confirming suspicious transactions are due to fraud. RDFIs should be aware that some state agencies, due to the pandemic, are constrained in their ability to respond in a timely manner. If any of the funds have been withdrawn and the ACH cannot be reversed, the Secret Service and DOL OIG request the RDFI preserve the remaining funds so they can be seized by law enforcement for return to unemployment insurance programs.

Current public guidance from NACHA on returning suspected fraudulent UI ACH credit entries states:

> If there is no Return Reason code that exactly matches the reason for the return, the NACHA Operating Rules allow the RDFI to select the Return Reason code that most closely approximates the reason for the return. In this scenario, Return Reason Code **R03** (No Account/Unable to Locate Account), **R17** (File Record Edit Criteria/Entry with Invalid Account Number Initiated Under Questionable Circumstances), or **R23** (Credit Entry Refused by Receiver) may be acceptable options. Please note that this use of R17 requires "QUESTIONABLE" to be inserted in the first twelve positions of the Addenda Record.

Reporting suspicious activity:

Federal and state law enforcement agencies are working collaboratively to rapidly investigate and counter this fraud scheme. RDFIs should contact their local Secret Service Cyber Fraud Task Force (CFTF), DOL OIG office, or other law enforcement agencies to conduct investigations of suspicious accounts. Law enforcement can assist with the return of funds to the appropriate unemployment insurance programs, either through administrative or judicial asset seizure processes. Law enforcement may also contact affected institutions directly to share specific information or request additional information in support of ongoing investigations.

Financial institutions should notify all federal law enforcement agencies of any contact they have had with other law enforcement agencies regarding this activity (to avoid duplication of efforts), or if they have filed a Suspicious Activity Report (SAR). Financial institutions should also preserve all information regarding the accounts associated with fraudulent unemployment benefits activity, including account opening information, transaction data, and any surveillance photos or video that may be available between February 15, 2020 and the present.

Contact the U.S. Secret Service and DOL OIG if you have questions, have information on UI fraud, or need law enforcement assistance in preventing fraud.

You can contact your local Secret Service office or Cyber Fraud Task Force (CFTF), field office contact information is available at: https://www.secretservice.gov/contact/field-offices/.

You can contact the DOL OIG Hotline at (800) 347-3756 or https://www.oig.dol.gov/hotline.htm.