NBA Nebraska Bankers Association

www.nebankers.org

Update COMPLIANCE

April 14, 2023 Vol. XXXV, No. 6

FINCEN ALERT MAIL THEFT – CHECK FRAUD: SCHEMES TARGETING THE U.S. MAIL

I. BACKGROUND

The Financial Crimes Enforcement Network (FinCEN) has issued an alert to financial institutions on the nationwide surge in check fraud schemes targeting the U.S. Mail. Fraud, including check fraud, is the largest source of illicit proceeds in the United States and is one of the anti-money laundering/countering the financing of terrorism (AML/CFT) National Priorities. In coordination with the United States Postal Inspection Service (USPIS), FinCEN has identified red flags to help financial institutions detect, prevent, and report suspicious activity connected to mail theft-related check fraud.

Bank Secrecy Act reporting for check fraud has increased significantly in the last three years. In 2021, financial institutions filed over 350,000 Suspicious Activity Reports (SARs) to FinCEN to report potential check fraud, a 23 percent increase over the number of check fraud-related SARs filed in 2020. This upward trend continued into 2022, when the number of SARs related to check fraud reached over 680,000, nearly double from the previous year's amount of filings.

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "FIN-2023-MAILTHEFT" and marking the check box for check fraud (SAR Field 34(d)).

In addition to filing a SAR, as applicable, when suspecting this type of fraud, financial institutions should refer their customers who may be victims of mail theft-related check fraud to the USPIS at 1-877-876-2455 or https://www.uspis.gov/report.

II. MAIL THEFT RISKS AND VULNERABILITIES

Criminals have been increasingly targeting the U.S. Mail and United States Postal Service mail carriers since the COVID-19 pandemic to commit check fraud. Criminals typically steal personal checks, business checks, tax refund checks, and checks related to government assistance programs, such as Social Security payments and unemployment benefits. Following the initial theft and fraudulent negotiation of the stolen checks, criminals may continue to exploit their victims by using the personal identifiable information found in the stolen mail for future fraud schemes, such as credit card fraud or credit account fraud.

Criminals committing mail theft-related check fraud generally target the U.S. Mail in order to steal personal checks, business checks, tax refund checks, and checks related to government assistance programs, such as Social Security payments and unemployment benefits. Criminals will generally steal all types of checks in the U.S. Mail as part of a mail theft scheme, but business checks may be more valuable because business accounts are often well-funded, and it may take longer for the victim to notice the fraud.

There have been cases of Postal Service employees stealing checks at USPS sorting and distribution facilities. However, according to USPIS, mail theft-related check fraud is increasingly committed by non-USPS employees, ranging from individual fraudsters to organized criminal groups comprised of the organizers of the criminal scheme, recruiters, check washers, and money mules.

Check Washers: Check washing involves the use of chemicals to remove the original ink on a check to replace the payee and often the dollar amount. Fraudsters may also copy and print multiple washed checks for future use or to sell to third-party criminals.

Money Mules: A money mule is a person (whether witting or unwitting) who transfers or moves illicit funds at the direction of or on behalf of another.

III. TYPOLOGIES OF MAIL THEFT-RELATED CHECK FRAUD AND ASSOCIATED MONEY LAUNDERING

After stealing checks from the U.S. Mail, fraudsters and organized criminal groups may alter or "wash" the checks, replacing the payee information with their own or fraudulent identities or with business accounts that the criminals control. During check washing, these illicit actors also often increase the dollar amount on the check, sometimes by hundreds or thousands of dollars. Washed checks may also be copied, printed, and sold to third-party fraudsters on the dark web and encrypted social media platforms in exchange for convertible virtual currency. In some cases, victim checks are also counterfeited using routing and account information from the original, stolen check. Illicit actors may cash or deposit checks in person at financial institutions, through automated teller machines (ATMs), or via remote deposit into accounts they control, and which they often open specifically for the check fraud schemes. Criminals may also rely on money mules and their pre-existing accounts to deposit fraudulent checks. Regardless, once the checks are deposited, the illicit actors often rapidly withdraw the funds through ATMs or wire them to other accounts that they control to further obfuscate their ill-gotten gains. The criminals may further exploit the victims by using personal identifiable information found in the stolen mail for future fraud schemes such as credit card fraud or credit account fraud.

IV. FINANCIAL RED FLAGS RELATING TO MAIL THEFT-RELATED CHECK FRAUD

FinCEN, in coordination with USPIS, has identified red flags to help financial institutions detect, prevent, and report suspicious activity connected to mail theft-related check fraud, many of which overlap with red flags for check fraud in general. As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags,

before determining if a behavior or transaction is suspicious or otherwise indicative of mail theft related check fraud. In line with their risk-based approach to compliance with the BSA, financial institutions are also encouraged to perform additional due diligence where appropriate.

- Non-characteristic large withdrawals on a customer's account via check to a new payee.
- Customer complains of a check or checks stolen from the mail and then deposited into an unknown account.
- Customer complains that a check they mailed was never received by the intended recipient.
- Checks used to withdraw funds from a customer's account appear to be of a noticeably different check stock than check stock used by the issuing bank and check stock used for known, legitimate transactions.
- Existing customer with no history of check deposits has new sudden check deposits and withdrawal or transfer of funds.
- Non-characteristic, sudden, abnormal deposit of checks, often electronically, followed by rapid withdrawal or transfer of funds.
- Examination of suspect checks reveals faded handwriting underneath darker handwriting, giving the appearance that the original handwriting has been overwritten.
- Suspect accounts may have indicators of other suspicious activity, such as pandemic-related fraud.
- New customer opens an account that is seemingly used only for the deposit of checks followed by frequent withdrawals and transfer of funds.
- A non-customer that is attempting to cash a large check or multiple large checks in-person and, when questioned by the financial institution, provides an explanation that is suspicious or potentially indicative of money mule activity.