FinCEN Financial Trend Analysis – Mail Theft-Related Check Fraud

The Financial Crimes Enforcement Network [FinCEN] issued their Financial Trend Analysis which provided threat pattern and trend information on mail theft-related check fraud incidents. With the various electronic and digital options available it is important to remember "old-school" fraud still occurs.

Mail theft-related check fraud is the fraudulent negotiation of checks stolen from the U.S. Mail. Criminals may steal different types of checks and attempt to use them for their own benefit. Once stolen, there are several ways they use the checks, including altering payees and/or amounts, using stolen checks to create counterfeit checks, fraudulently signing checks, and selling checks or its identifying information on dark web marketplaces or encrypted social media platforms. Generally, mail theft-related check fraud is a combination of two crimes: mail theft and check fraud.

While mail theft often consists of mail being stolen from USPS mailboxes or personal mailboxes, the United States Postal Inspection Service [USPIS] reported over 700 mail carriers were robbed between October 2021 and July 2023. Incidents spiked after the onset of the COVID-19 pandemic as many individuals and businesses received financial assistance via U.S. Mail. Check fraud refers to any use of paper or digital checks to fraudulently obtain funds.

FinCEN analyzed 15,427 BSA reports with more than $688 million in transactions, including both actual and attempted transactions. The analysis identified three primary outcomes after checks were stolen from the U.S. Mail: (1) altering and depositing checks; (2) using stolen checks to create counterfeit checks; and (3) fraudulently signing and depositing checks. Criminals ranged from unsophisticated to highly organized and complex, often using advanced counterfeit check technology and chemicals to remove ink from stolen checks.

BSA reporting further reflected perpetrators appeared to prefer depositing checks via methods that avoid in-person contact with bank personnel. While deposits at ATMs allow depositors to avoid in-person contact, the preferred method was via Remote Deposit Capture [RDC] as that ensures no one from the bank physically handles the check. Poorly made counterfeit checks were often made using incorrect check stock and security features. Perpetrators of new account fraud often opened new accounts online, using fraudulent identifying information or money mules to open the accounts.

OFAC Targets Funding Source of Fentanyl-Trafficking Cartel

The Office of Foreign Assets Control [OFAC] sanctioned nine Mexican-nationals and twenty-six Mexico-based entities linked to a fuel theft network generating tens of millions of dollars benefitting the Cartel Jalisco Nueva Generacion [CJNG], a violent Mexico-based drug trafficking organization responsible for a significant proportion of fentanyl and other drugs trafficked into the United States. Mexico-based drug trafficking cartels have turned to fuel theft in recent years resulting in billions of dollars of lost revenue to the Mexican government.

In related news, FinCEN issued a press release reminding financial institutions to monitor for and report suspicious transactional activity related to the illicit fentanyl supply chain, and the trafficking of illegal fentanyl and other synthetic opioids.