CHECK FRAUD: THE MULTIMILLION-DOLLAR SCHEME

Criminals committing check fraud often work together to maximize profits and leverage resources, with each participant contributing a specific skill set or playing a different role within the scheme. The combined effort can enable a group of criminals to carry out a more dynamic and complex check fraud scheme by:

- Collecting financial and personally identifiable information (PII) through open sources and data compromises
- Stealing checks and other identifying information from the mail
- Chemically washing, altering or reproducing paper checks using the stolen data
- Setting up and managing anonymized digital channels and instant messaging platforms to sell stolen checks and data
- Opening accounts and digital wallets using fake or stolen personally identifiable information (PII)
- Creating synthetic identities and counterfeit identification documents
- Recruiting people to help negotiate the fraudulent checks

USE CASE: THE $50 MILLION CHECK FRAUD SCHEME

Multiple criminals worked together for more than a year in an elaborate scheme involving mail theft, fake identities and check fraud — resulting in a $50 million fraud scheme.

As with many organized criminal efforts, this scheme relied on planning and preparation — such as stealing identities and setting up accounts that would be used to carry out the scheme while concealing the identity of the real perpetrators.

- *Stolen PII and counterfeit identification were employed to open deposit accounts used to deposit or cash fraudulent checks and set up digital wallets to receive payments for sales of stolen checks.*
- *A user profile on a digital platform was established using anonymized information. Posts boasting about this supposedly lucrative activity were used to attract followers.*
- *Checks were stolen out of the mail while en route to the intended payees.*
- *Criminals washed, altered and created counterfeit checks — thus creating fraudulent checks — using routing and account information from the stolen checks.*
- *The fraudulent checks were then cashed or deposited at the various financial institutions where the deposit accounts had been established.*

CHECK FRAUD: THE MULTIMILLION-DOLLAR SCHEME

- *Pictures of the deposit slips showing available balance information, check images and other forms of visual "proof" that the scheme was successful were then frequently posted on digital platforms to entice followers.*
- *Images of fraudulent paper checks were posted for sale on the digital platform. Payments for these sales were directed to digital wallets that were previously established.*
- *Upon discovery, financial institutions and victims reported fraudulent check activity across several states to law enforcement.*
- *Law enforcement worked with the financial institutions impacted by the check fraud losses and the identity theft victims to identify the criminals involved. The investigation uncovered more than $50 million in stolen checks connected to the group of criminals.*

THE AFTERMATH

Check fraud schemes such as this one can be extremely lucrative for criminals. The funds obtained through depositing and cashing the fraudulent checks typically result in losses for the financial institution that accepts them. Additionally, the victims of identity theft often experience long-lasting impacts because it may take a lot of time for these individuals to prove their identity, disassociate their true identities from the accounts used to facilitate the fraud, and resolve the negative impacts to their credit profiles. Ways to help minimize the impact of these types of schemes include a multi-layered approach to fraud detection that encompasses robust Know-Your-Customer (KYC) practices, as well as cross-channel account and transaction monitoring that incorporates external fraud intelligence data.

The check fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about check fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.