CHECK FRAUD CONNECTIONS TO NEW ACCOUNT FRAUD

USING NEW ACCOUNTS FOR CHECK FRAUD

One way check fraud continues to thrive is through the use of new accounts. Criminals open new accounts, or recruit someone else to open a new account, with the sole intention of depositing or cashing fraudulent checks. Fraud rates for deposits into new accounts are reported to be 17% riskier than deposits into established accounts. Once fraudulent activity has occurred and the account is considered "burnt" – due to being flagged, frozen or otherwise unusable for further fraudulent activity – the account is abandoned, and the financial institution could be in a loss position if the account balance is negative. Check fraud and new account fraud make up about 20% of the overall fraud case volume that financial institutions are dealing with on a regular basis.

NEW ACCOUNTS FUEL CHECK FRAUD

1. **New Accounts are Opened with Malicious Intent**
   Accounts are opened with fake or stolen identities, real identities or by recruiting a money mule. These accounts often appear clean and unassociated with prior fraud, helping to bypass standard fraud detection systems.
   - *Synthetic identity fraud*: Criminals create new identities using a combination of real and fake information – such as a real Social Security number with a fake name and date of birth.
   - *Identity theft*: Someone else's personal information is used to open legitimate-looking accounts without their authorization or awareness.
   - *Money mules*: An individual is recruited to open a new account at the direction of someone else, this could be the result of a scam where the mule is unwitting or complicit in the activity.
   - *Authorized party fraud*: Criminal uses their own identity to open a new account with the intent of defrauding the financial institution.
2. **Fraudulent Checks are Deposited into the New Accounts**
   - Various types of fraudulent checks are deposited – such as counterfeit checks, altered or forged checks, or other checks that have been stolen.
   - Criminals use all deposit channels to deposit fraudulent checks but there are indications that they prefer remote or "faceless" channels like ATMs and mobile deposit capture.
3. **Funds from the Fraudulent Deposits are Rapidly Withdrawn**
   - After depositing the fraudulent check, the criminals – or other complicit party – quickly withdraw cash, make purchases or transfer money via instant funds transfer to other accounts they control.
   - This scheme takes advantage of the timeframe it takes for a check to clear, making the funds from a deposit available to withdraw prior to the check being identified as fraudulent.

CHECK FRAUD CONNECTIONS TO NEW ACCOUNT FRAUD

WHY CRIMINALS PREFER NEWLY OPENED ACCOUNTS FOR CHECK FRAUD

- **Ease of Opening:** New account opening processes – including the option to open accounts online – are more convenient now than they have been in the past
- **No "Norm" Established**: New account fraud is harder to detect because the financial institution doesn't have trends, activity or history to know what is normal for that account – making it hard to verify customer intent
- **Clear history**: New accounts with new identification typically have no prior red flags or indicators that could be the onset of fraud
- **Easy to Walk Away From / Disposable**: Accounts are often abandoned once the fraud is completed.
- **Volume**: Criminals can open many accounts at many financial institutions – this allows them to spread risk and increase their chances of success.

Criminals use new accounts for check fraud because of the key advantages that help them evade detection and maximize their gains. These risks reiterate the need to incorporate strong Know-Your-Customer (KYC) practices, strengthen monitoring of new accounts and deploy advanced check fraud detection. A key consideration to combat fraudulent account opening and check fraud is incorporating siloed data into a more comprehensive view of who the new customer is and what they are doing.

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.