OVERVIEW OF DIFFERENT TYPES OF SCHEMES

Criminals are constantly evolving their tactics to perpetrate check fraud, but the schemes often follow similar trends. Check fraud could be the result of authorized fraud, such as scams that recruit money mules, or unauthorized fraud where a criminal is using stolen checks or information for their own financial gain. Maintaining awareness of the schemes being used to perpetrate check fraud can help fine tune prevention strategies, employee training, and customer education.

AUTHORIZED FRAUD – WHERE CRIMINALS COMMIT THE CHECK FRAUD DIRECTLY

Authorized fraud typically occurs when the account holder willingly sends or writes a check for the purpose of committing fraud. They are using their own identity, or a synthetic identity they created, to commit fraud against the financial institution. Common schemes connected to authorized fraud may include check kiting or paper hanging, money mules recruited by criminals (knowingly or unknowingly), or new account fraud - as shown in the example.

Scheme: The criminal opens a new account with the sole intention to commit check fraud. Once the fraud is committed, the criminal abandons the account. The check is returned unpaid, leaving a negative balance in the account that the financial institution may not be able to recover.

1
New Account Opened
Criminal opens a new deposit account.

2
Account Ages + Cash Deposits
Account ages with minimal activity other than cash deposits that continue to increase the account balance.

3
Multiple Large Checks Cashed
Criminal cashes multiple checks for large amounts using the balance in the account and then later, withdraws the funds from the account.

4
Checks Cashed are Returned
Cashed checks are returned, bringing the account balance to -$9,500 – resulting in a potential loss to the financial institution.

OVERVIEW OF DIFFERENT TYPES OF SCHEMES

UNAUTHORIZED FRAUD – WHEN CRIMINALS USE STOLEN CHECKS

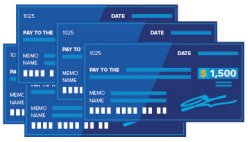
Unauthorized fraud is when someone other than the authorized person on the account is initiating fraudulent activity. In the case of unauthorized fraud, the account holder is not complicit or aware of the fraud that is taking place.

To commit unauthorized check fraud, the criminal must obtain the checks or the account information in some way. Examples include checks being stolen from the mail and the payee's signature forged on the endorsement line, or someone pretending to be the payee to negotiate the check. Fraud schemes like account takeover, impersonation and identity theft are all examples of unauthorized fraud.

Scheme: Another example is the case to the right that breaks down a common scheme by an organized group of criminals known as the "Felony Lane Gang." – the checks are stolen, forged and then cashed at a financial institution using a stolen identity. Checks that are left unsecured are vulnerable to a crime of opportunity by a perpetrator not necessarily associated with an organized crime ring.

1
Checks and ID are Stolen

Purses containing IDs and checks are stolen from cars in a parking lot.



2
Criminal Forges Stolen Checks

The criminal fills out the stolen checks and forges the maker's signature.

3
Stolen Checks are Cashed

The criminal uses the stolen ID to impersonate the account holder and cash the forged checks.

4
Account Holder Files Fraud Claims

Cashed checks are disputed by the real account holder – resulting in a potential loss to the financial institution.

The **Department of Justice** describes the **Felony Lane Gang (FLG)** as "typically a group of thieves from Florida who travel the country and target unoccupied vehicles for "smash and grab" thefts, stealing purses and using stolen identification documents and credit cards to commit financial crimes. When cashing stolen checks, they typically use the drive-thru lane farthest from the bank in an attempt to avoid detection."

OVERVIEW OF DIFFERENT TYPES OF SCHEMES

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.