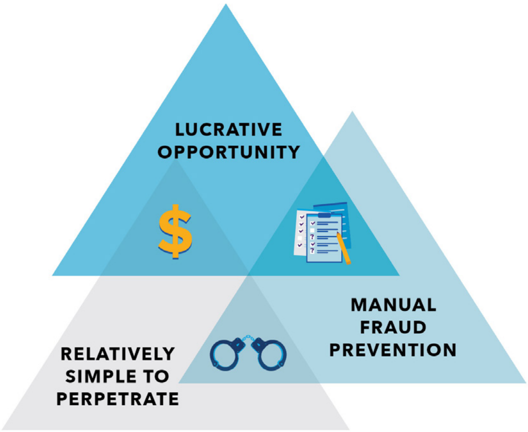
WHY CHECK FRAUD IS STILL AROUND

The relentless nature of check fraud growth and the challenges that remain year after year beg the question: *why is check fraud still around?* Although there is not a single contributing factor, check fraud continues to be a concern within the payments industry because it is:

- A **lucrative opportunity** for criminals
- Relatively **simple to perpetrate**
- **Not easy to detect:** often manual and fraudulent items can be indistinguishable from legitimate items

A deeper understanding of these challenges may help drive changes that will prevent check fraud.



OPPORTUNITY MAKES CHECKS A LUCRATIVE TARGET

The continued use of checks – with billions processed each year – provides many opportunities for criminals to target this payment method. Before checks can be fraudulently created, altered or forged, a check – or the data needed to create a fake check – needs to be obtained or fictitiously created. Criminals can gain access to data and checks in a multitude of ways, such as mail theft, data compromises and social engineering.

Mail Theft Continues to Fuel Check Fraud

Checks contain valuable information for criminals, such as account information, the institution where the maker (payer) has the deposit account, check numbers and range, and how the customer's legitimate checks look. Checks stolen from the mail may be altered, counterfeited or fraudulently endorsed and then, cashed for a criminal's own financial gain.

The sale of checks and stolen account information on the dark web, as well as widespread geographic locations and volume patterns, indicate organized activity to steal checks and perpetrate check fraud. Criminals recruit and conspire with others to participate in various roles involved in mail theft schemes. In addition, postal workers may be targeted and robbed of the mail and arrow keys they carry. Arrow keys allow access to blue mailboxes within a district and often are sold and shared among criminals.

The zip codes where check fraud occurs reveal higher levels of fraud based on the payee zip codes, rather than the payer zip codes. This indicates that checks are more often stolen at or around their intended destinations, not the point of origination. Individuals and businesses who mail checks may believe these are secure because they are placed in a secure mailbox, but may not consider risk of theft at the mail's destination.

WHY CHECK FRAUD IS STILL AROUND

Data Compromises and Social Engineering Increase Vulnerability

Every year, thousands of data breaches expose personal and financial data, such as names, addresses, birthdates, Social Security numbers and account information. Stolen data and checks can be used by criminals, shared with others or sold on the dark web for a minimal fee. Criminals use fraudulent checks created with this type of stolen information to carry out various check fraud schemes, such as cashing the fraudulent checks or depositing them into an account and then, quickly withdrawing the funds.

Continued Reliance on Checks Creates Fraud Opportunities

Checks are a preferred payment method for many businesses, as they often are considered to be a cheaper, quicker payment method and offer multiple options, such as the ability to place stop payment on a check. Especially in cases where payment is going to a school, charity or with a child, checks offer ways to control the receipt of funds and offer a paper trail of the transaction. In addition, checks avoid fees incurred by other payment types.

TECHNOLOGY, UNDERGROUND NETWORKS MAKE IT EASIER TO COMMIT CHECK FRAUD

Just like the modern-day check, early versions of checks – such as letters of credit and inscribed promissory notes that date back centuries ago – were susceptible to forgeries, counterfeiting and alterations. Unfortunately, the level of sophistication, time and effort needed to commit check fraud has been greatly reduced by technology. Countermeasures put in place throughout the years have deterred some check fraud, yet it remains a threat because it is easy to commit and lucrative for criminals.

Once the data to create checks is obtained, bad actors use a multitude of tools, resources and scams to carry out check fraud schemes. Technology used to commit check fraud is easily obtainable and relatively low cost. Within criminal networks, it also is easy to obtain how-to guides, mentors and other resources. If criminals can't create fraudulent checks themselves, they can outsource the job to another criminal through Fraud-as-a-Service.

The Use of Scams, Money Mules and Walkers

Scams and money mules (people who transfer illegally acquired money on behalf of someone else) have fueled rising check fraud volume. Criminals not only manipulate or alter checks that were legitimately issued, they also manipulate scam victims into playing a role in their schemes to facilitate check fraud. The victims may become unwitting, witting or complicit money mules.

WHY CHECK FRAUD IS STILL AROUND

Criminals also capitalize on a common practice where businesses use checks to pay their employees who may not have a deposit account. They create counterfeit checks using stolen business account information, then recruit individuals referred to as “walkers” to pose as employees and cash the counterfeit checks. This fraud scheme, often referred to as fraudulent check cashing of on-us checks by noncustomers, typically results in a loss to the financial institution because the funds literally walk out the door after the transaction is completed. (On-us checks are drawn off an account that resides with the financial institution that is cashing the check, and the payee likely does not have an account at that same institution.)

MANUAL DETECTION PROCESSES OFFER LESS EFFECTIVE PREVENTION

Identifying fraudulent checks is a manual, time-consuming effort – often requiring analysts to visually review and compare checks to detect possible fraud. While criminals continue to enhance technology used to commit check fraud by creating legitimate-looking checks, investing in the technology financial institutions can use to stop it may not always be a high priority versus competing anti-fraud efforts. In addition, information sharing between financial institutions is typically manual, delaying event reviews to identify fraud.

CONCLUSION

Most reasons that check fraud continues to be pervasive connect back to the fact that is a lucrative opportunity for criminals, relatively easy to perpetrate and difficult to detect. Dissecting each of these areas can uncover opportunities for changes that can help reduce check fraud.

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.