

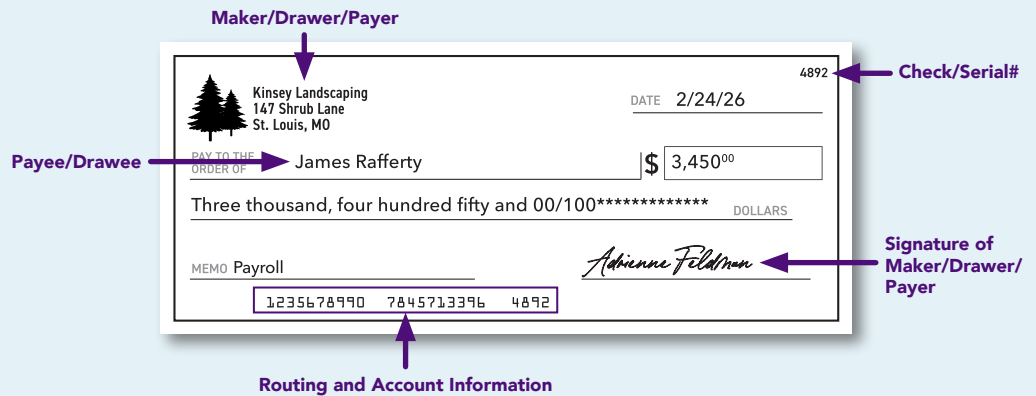
THE RISKS OF STOLEN CHECKS

Check fraud continues to rise as criminals gain access to physical checks. Once a criminal has a check, the fraud process can escalate quickly. Financial institutions can help protect their customers and improve prevention strategies by understanding this process.

1

CRIMINALS GAIN USEFUL INFORMATION

Stolen checks give criminals everything they need to initiate multiple types of fraud.



2

CHECK DATA IS USED FOR FRAUDULENT ACTIVITY

Check data is sold to other criminals or used to perpetrate other types of fraud like identity fraud.

CHECKS ARE "WASHED"

Criminals modify the payee or amount or use chemicals to alter the payee's name or dollar amount.

COUNTERFEIT CHECKS ARE CREATED

New checks using the stolen information and sometimes check stock, can be created.

3

FRAUDULENT CHECKS ARE CASHED OR DEPOSITED

Checks are cashed or deposited via various channels – such as ATMs, mobile or branches – into accounts that may be new, compromised or belong to customers knowing or unknowingly involved in check fraud.

TO HELP PREVENT CHECK FRAUD, FINANCIAL INSTITUTIONS CAN...

- Strengthen controls across all deposit channels
- Implement image-based anomaly detection
- Train employees about check fraud
- Educate customers about check safety and the risks of mailing checks
- Use cross-channel tools to identify fraud patterns

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.