Public Service Announcement

FBI & USPIS

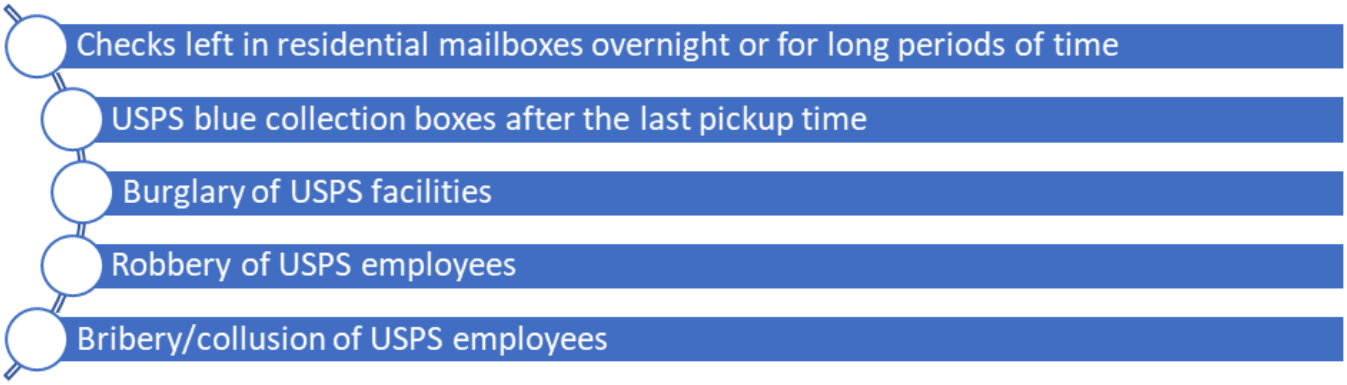
Alert Number: I-012725-PSA
January 27, 2025

Mail Theft-Related Check Fraud is on the Rise

The FBI and USPIS are warning that check fraud is on the rise, with a significant volume enabled through mail theft. Suspicious Activity Reports related to check fraud have nearly doubled from 2021 to 2023.[1] Fraudsters take advantage of regulations requiring financial institutions to make check funds available within specified timeframes, which is often too short a window for the consumer or financial institutions to identify and stop the fraud. As a result, the compromised checks clear, and the funds are withdrawn by the criminal participants before the fraud is detected.

OBTAINING THE CHECKS

Fraudsters gain access to legitimate checks and sensitive financial data by stealing mailed checks from USPS facilities or during delivery to the intended recipient. Check theft occurs several ways.



PREPARING/ALTERING THE CHECKS FOR DEPOSIT

To make the checks appear legitimate, fraudsters use check washing or other check "cooking" techniques to alter checks or create counterfeits. In other instances, checks are unaltered and deposited with forged endorsements.

Check washing involves the use of chemicals to physically alter the check, typically altering the original payee and financial amount.

Check cooking involves the digital manipulation of an image of a stolen check. Using readily available photo editing software and high-tech printers, fraudsters can manufacture checks. Check cooking allows fraudsters to manufacture multiple checks from a single check image. Often these checks are written for smaller amounts which can go undetected for longer periods of time by escaping the scrutiny or visibility of a larger check amount.

DEPOSITING THE CHECKS

Stolen checks are deposited, often by a collusive account holder who is recruited by the fraudster or sold online for a fraction of the face value to other criminal actors who deposit the checks. In many cases, financial institutions, consumers, and law enforcement agencies are not aware of the fraudulent activity until after funds have been illicitly withdrawn.

WHO IS HARMED BY CHECK FRAUD?

Businesses — Businesses could experience disruption to business activities and reputational harm due to overdue or missed payments or delays or disruption in finalizing payments when account details are compromised.

Consumers — Consumers can experience impacted credit scores for late payments for bills, account closures, stop payment fees for other outstanding checks, missed interest from refund checks, compromised personally identifiable information (PII) which may also be sold in subsequent fraud schemes, and loss of assets or investment money. Victims of fraud are often refunded some of the charges, but refunds are often delayed until investigations are complete.

Government Entities — Funds intended for citizens are intercepted and altered or forged, resulting in government funds being dispersed incorrectly. It can be a time intensive process to investigate and reissue payments to the rightful recipients of intercepted checks.

HOW TO PROTECT YOUR MAIL

- ✓ Pick up your mail promptly after delivery. Do not leave mail in your mailbox overnight or for long periods of time.
- ✓ If you are heading out of town, submit a USPS Hold Mail™ request asking your local Post Office to hold your mail until you return.
- ✓ Sign up for Informed Delivery® at USPS.com to receive daily email notifications of incoming mail and packages.

- ✓ Contact the sender if you do not receive a check, credit card or other valuable mail you are expecting.
- ✓ Consider buying and using security envelopes to conceal the contents of your mail.
- ✓ Use the letter slots inside your local Post Office to send mail. If using a blue USPS collection box, be sure to drop your mail as close to the posted pickup time as possible and before the last collection of the day.

HOW TO PROTECT YOUR CHECKS

- ✓ Use pens with indelible black ink so it is more difficult for a criminal to wash your checks.
- ✓ Don't leave blank spaces in the payee or amount lines.
- ✓ Don't write personal details, such as your Social Security number, credit card information, driver's license number, or phone number on checks.
- ✓ Use mobile or online banking to access copies of your checks and ensure they are not altered. While logged in, review your bank activity and statements for errors.
- ✓ Consider using e-check, ACH automatic payments, and other electronic and/or mobile payments.
- ✓ Follow up with payees to make sure they received your check.
- ✓ Use check positive pay if available at financial institutions to help detect and stop fraudulent checks.
- ✓ Use checks with security features to limit the effectiveness of check washing. Security features can include microprinting, holograms, heat-sensitive ink, watermarks, toner adhesion, chemically reactive paper, security screens, thermal thumbprints, void pantographs, ultraviolet overprinting, security padlock icon, and fraud warnings.
- ✓ If you believe you have been defrauded, contact your bank immediately. Consider opening a new account and closing out the compromised account to prevent future counterfeit checks being drawn off the account.
- ✓ Protect vulnerable members of your family and community. Fraudsters use high-tech, low-cost technology including printers, call spoofing technology, and AI-assisted voice recreation to fool vulnerable people into acting as unwitting accomplices.

If you think you were targeted by fraud, file a report with your bank and request copies of all fraudulent checks. Report the incident to the FBI Internet Crime Complaint Center (IC3), www.ic3.gov. If you believe you are the victim of mail theft-related check fraud, report to your local police and the United States Postal Inspection Service at uspis.gov/report or 1-877-876-2455.

[1] *SAR Filings by Industry | Filing Trend Data: Depository Institution | Exhibit 5: Number of Filings by Type of Suspicious Activity from Depository Institution Industry | Between 01 January 2014 and 31 December 2023 |*

https://www.fincen.gov/reports/sar-stats/sar-filings-industry | Accessed 18 December 2024. ↩