TRUSTAGE Fraudulent checks and deposits

Despite the numerous payment options available, losses due to fraudulent paper checks and deposits have surged.

Fraudsters have been using age-old tactics and scams to carry out their transactions — things like stealing mail and washing, altering, and counterfeiting checks.

These losses have seen significant increases in both frequency and severity:

- Stealing and altering members' issued checks or manufacturing fraudulent checks using information from legitimate checks to gain access to cash. In many cases, your members' checks are being negotiated elsewhere to bypass some of your authentication controls.
- Recruiting money mules to open accounts at credit unions to cash fraudulent U.S. Treasury checks.
- Opening fraudulent business accounts in the name of the payees listed on stolen Treasury checks, depositing these checks, and then cashing out before they're returned.

FAQs

- **Are employees aware of these fraud attempts and do they know what to be on the lookout for?**+

Check fraud is making a major resurgence and understanding the fraudulent activities, scams, and losses are an important first step in loss control. Prepare credit union employees with knowledge of check fraud schemes, build their understanding of how to identify fraudulent checks, and improve their ability to manage the risks through check acceptance and check holds.

To enhance your own policies, procedures and training, encourage your employees to take this no-cost, online **interactive training module on check fraud** from TruStage.

- **Do you use proper authentication and holds on funds related to new members and accounts?**+

To minimize these fraudulent check and deposit risks, you should:

    - Carefully review members' checks for deposit or cash — especially large dollar checks, including HELOC checks, presented for payment.

- Deploy an identity verification solution to screen and authenticate members in order to detect synthetic identities. If there are doubts as to the identity, consider using a more robust solution such as a skip trace solution.
- Place an extended check hold on the deposited check in accordance with Regulation CC or deposit to a savings account for the ability to use a longer hold.
- Limit offering debit cards or use of remote deposit capture to new members for a period of time and/or consider lower daily dollar limits on new member debit cards.
- For deposits made through remote deposit capture by new members consider stepping up your procedures for manually reviewing check images for at least the first 6 months.

- **Are you aware that you may be able to assert a presentment warranty claim against a depository institution?**+

If the transaction of cashing or depositing a fraudulent check occurs elsewhere, you may have some recourse against the depository institution depending on the circumstances surrounding the fraudulent check.

If a check has been altered or contains a forged endorsement, your credit union can assert a presentment warranty claim against the depository institution under the UCC 4-208 Presentment Warranty. This **liability for forged endorsements & alterations risk overview** provides more details on steps you can take and also includes a sample presentment warranty claim letter.

If the fraudulent activity involves a counterfeit check or forged maker signature, your recourse against the depository institution is more limited, and time-sensitive. Under UCC 4-301, the deadline for returning a forged or fraudulent check unpaid is midnight on the next banking day following the banking day of presentment.

No matter what, be sure your members understand that reporting these incidents in a timely fashion is critical. They should follow the timeline set according to your account agreement which will allow you to determine and minimize the extent of the credit union's liability.

- **Do employees know which red flags to look for to minimize risks associated with fraudulent business accounts?+**

Fraudsters are opening fraudulent business accounts at credit unions to cash stolen checks (including Treasury checks) that were issued by businesses to other businesses. The fraudulent accounts are opened in the name of the business, or a similar name, and listed as the payee on the stolen checks.

The fraudsters file fraudulent articles of incorporation with the secretary of state's office and provide this document to the credit union at account opening to prove the existence of the business entity. Credit unions can verify this documentation through the secretary of state's website.

A few red flags that may signal new business account fraud:

  - The secretary of state's filing stamp on the articles of incorporation is dated just days before the fraudulent business accounts are opened.
  - The stolen checks deposited to the fraudulent business accounts are typically dated 3 to 4 weeks before the date of the secretary of state's filing stamp on the articles of incorporation.
  - The payee's address listed on the check bears no relationship with the address used to open the fraudulent business account. For example, the payee's address listed on the check is in Georgia; however, the address used to open the fraudulent business account is in Michigan.
  - The business name listed as the payee on the stolen checks may not exactly match the name of the fraudulent business opening the account at the credit union.

Are you verifying the legitimacy of U.S. Treasury and IRS Treasury checks?+

There has been a significant increase in credit unions incurring six- or seven-figure losses involving fraudulent U.S. Treasury checks — primarily counterfeit and altered Treasury checks, although some also include forged endorsements.

Carefully review the security features of Treasury checks like the treasury seal, watermark and microprinting. In addition, you should verify the check issue information including payee using the **TIGTA's Check Integrity System** and **Treasury Check Verification System**.