TruStage™

RISK Alert

Actionable insights for bond policyholders

Awareness | **Watch** | **Warning**

Previously issued as a RISK Alert Watch on 2/15/2024

Fraudulent U.S. Treasury checks continue to drive losses

Losses involving fraudulent U.S. Treasury checks being deposited at credit unions continue to be reported. The losses are growing larger, and fraudsters are using several tactics including new member accounts, money mule accounts, and/or using mobile deposit services to make fraudulent deposits.

Many verify the checks using the Treasury Check Verification System (TCVS). You should also verify the checks, including the payees, by emailing the U.S. Treasury Inspector General for Tax Administration (checkintegrity@tigta.treas.gov) or the U.S. Treasury's Bureau of Fiscal Service (payments@fiscal.treasury.gov).

Alert details

Fraudulent U.S. Treasury checks continue to be deposited into member accounts. The fraudulent items include counterfeit checks, altered checks and checks containing forged endorsements. In many cases, fraudsters recruit money mules to open fraudulent accounts, including business accounts, in the names of the payees listed on the checks.

The fraudulent Treasury checks are frequently deposited at ATMs or via remote deposit capture. Most deposits are just under the amount allowed for remote deposit capture. The mobile deposit images typically have a similar background that appears to be a paper cutter table, and some are images on a monitor.

The money mules may open accounts at the branch or online. Often money mules have been recruited by organized crime groups through social media platforms and looking for those that have "clean" backgrounds. They promise a small cut of the money that passes through their account. Some money mules may be aware of the limitations placed on their accounts since they are new and will wait for the account to "age" (45-60 days) before depositing checks. Once the credit unions are aware of the fraud; they attempt to contact the member; however, in most cases they are unresponsive.

Withdrawals often occur at ATMs, casinos, through Zelle/CashApp transactions.

Many verify the Treasury checks using the Treasury Check Verification System (TCVS) which verifies whether the check was issued. However, the TCVS only verifies if the check was issued. It does not verify the payee listed on the check.

Some credit unions that verified the issuance of a Treasury check using the TCVS subsequently received a reclamation notice from the U.S. Treasury as the payees listed on the checks were altered, or the payee's endorsement was forged.

Date:
May 7, 2024
– previously issued February 15, 2024

Risk category:
U.S. Treasury; Check fraud; scams; money mules; mail theft; deposit account fraud; compliance; plastic card fraud

States:
All

Share with:

- Branch operations
- Executive management
- Front-line staff/tellers
- Legal/compliance
- Member services/new accounts
- Risk manager

Facing risk challenges?:
Schedule a no-cost, personalized discussion with a Risk Consultant to learn more about managing risk.

Some organizations have been able to verify Treasury checks, including the payees, by emailing the U.S. Treasury Inspector General for Tax Administration (checkintegrity@tigta.treas.gov) or the U.S. Treasury's Bureau of Fiscal Service (payments@fiscal.treasury.gov).

US Treasury checks may be returned as altered/washed of the payee or counterfeit/fictitious checks. These checks can take up to 60 days to return.

Risk mitigation

- Verify Treasury checks, including the payees, by emailing the U.S. Treasury Inspector General for Tax Administration (checkintegrity@tigta.treas.gov) or the U.S. Treasury's Bureau of Fiscal Service (payments@fiscal.treasury.gov).

  Include the date of check; serial number; check amount; payee; routing number; and attach or paste an image of the Treasury in the email.
- 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. Keep in mind, you will not be able to verify the security features on Treasury checks deposited via remote deposit capture.
- Consider limiting remote deposit capture services to new members until 6-12 months if no other services used and/or reduce the dollar amount of checks accepted via mobile deposit.
- Limit offering debit cards to new members for a period of time and/or consider lower daily dollar limits on new members debit cards.
- When opening new accounts, screen new member through an identity verification solution capable of detecting synthetic identities. If there are doubts as to the identity, consider using a more robust solution such as a skip trace solution. Consider enrolling in the Social Security Administration's electronic Consent Based Social Security Number Verification (eCBSV) Service. This service allows users to verify if an individual's SSN, name and date of birth combination matches Social Security's records.
- Avoid accepting third-party Treasury checks since the credit union would be responsible for the loss if the original payee's endorsement is forged.
- If possible, carefully examine review Treasury checks for evidence of alterations, such as cloudy bleached areas and different font types/sizes.
- Avoid accepting a Treasury check that is jointly payable to two or more payees unless the account is titled in the name of all payees and the check is properly endorsed by all payees.
- Retain the original Treasury checks for at least 18 months after imaging. You may need to refer to original checks to detect a material alteration in the event the credit union receives a notice of reclamation for accepting an altered check.
- Re-visit your check hold policy on deposits made via remote deposit capture for newer accounts (6-12 months).

Risk prevention resources:

Access the Business Protection Resource Center for exclusive risk and compliance resources (User ID and Password required).

Review these resources:

- **Liability for forged endorsement & alterations risk overview**
- **Remote deposit capture risk overview**
- **Check fraud landing page** of the Business Protection Resource Center
- RISK Alert: **Fraudulent U.S. Treasury check scams**

For additional support, call 800.637.2676 or email riskconsultant@trustage.com