

# RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.



Alert Type

Awareness

Watch

Warning

## Fraudulent Treasury Checks on the Horizon?

Stimulus payments from the Internal Revenue Service (IRS) are expected via direct deposit; however, individuals without direct deposit information on file with the IRS will receive payments via Treasury checks. The IRS plans to issue approximately 100 million paper checks at the rate of 5 million per week. Fraudsters may steal issued Treasury checks and/or manufacture counterfeit Treasury checks.

### Details

With an estimated 100 million stimulus payments to be issued via Treasury checks, fraudsters may seize the moment to create fake/counterfeit Treasury checks or steal issued Treasury checks and cash them at credit unions after opening an account.

Fraudsters who steal issued Treasury checks could forge the payee's endorsement or alter the payee.

Credit unions experienced losses in the aftermath of Hurricane Sandy when fraudsters passed counterfeit and forged Treasury checks representing Federal Disaster Assistance checks.

These are important rules on Treasury checks (Refer to [31 CFR Part 240](#)):

### Limitations on Treasury Checks ([§240.5](#)):

The Treasury is not obligated to pay a check over 12 months old.

### Counterfeit Treasury Checks ([§240.8\(c\)](#)):

The Treasury will not reclaim a counterfeit check unless the credit union failed to take all "reasonable efforts" to ensure the check is authentic. "Reasonable efforts" means, at a minimum, verifying the existence of the Treasury watermark on the original check. "Reasonable efforts" may also require the verification of other security features on the check. Refer to [U.S. Treasury Check Security Features](#).

**Altered/Forged Treasury Checks ([§240.4](#)):** When accepting a Treasury check for deposit or payment, the credit union makes the following presentment guarantees to the Treasury:

- All prior endorsements are genuine;
- The check has not been materially altered;
- Credit union has no knowledge that the signature of the drawer is forged;
- Credit union has made all reasonable efforts to ensure the check is authentic; and

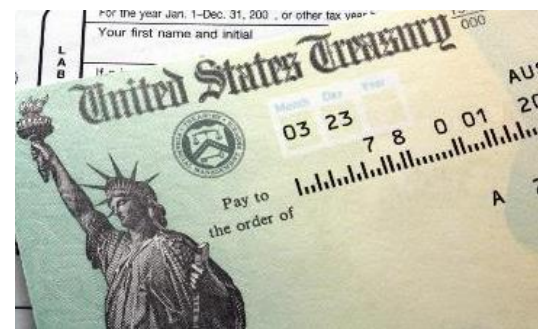
**Date:** April 21, 2020

**Risk Category:** Scams, Check Fraud; Counterfeit Checks

**States:** All

**Share with:**

- Branch Operations
- Executive Management
- Front-Line Tellers
- Risk Manager



Your feedback matters!  
**Was this RISK Alert helpful?**



# Fraudulent Treasury Checks on the Horizon?

- With respect to electronic checks, the check accurately represents all of the information on the front and back of the original check; the Treasury will not be asked to pay a check that has already been paid (no duplicate presentments); the Treasury's receipt of an electronic check will not result in the loss of the Treasury's ability to detect a material defect or alteration.

## Reclamations of Checks Paid [[§240.8\(a\)](#)]:

The Treasury has one year to pursue a breach of guarantee claim against the credit union. The one-year deadline can be extended by an additional 6 months if the payee provides notice of the forgery to the Treasury within one year of issuance.

## Reclamation Procedures ([§240.9](#)):

The Treasury will send a notice of reclamation to the credit union to recover the amount of the check in the event the credit union breaches a presentment guarantee under §240.8.

## Risk Mitigation

Credit unions should consider these loss controls when accepting Treasury checks, especially from new members:

- Retain the original Treasury checks for three years after imaging. You may need to refer to the original check to detect an alteration if you receive a notice of reclamation claiming the credit union accepted an altered Treasury check.
- Refuse Treasury checks presented more than one year after the issue date.
- Verify all of the security features on Treasury checks. Refer to [U.S. Treasury Check Security Features](#).
- Carefully examine Treasury checks for evidence of alterations, such as cloudy or bleached areas in the payee and dollar amount areas and different fonts and sizes.
- Avoid accepting third-party Treasury checks since the credit union would be responsible for the loss if the payee's endorsement is forged. Avoid accepting a Treasury check that is jointly payable to two or more payees unless the account is titled in the names of all payees and the check is properly endorsed.
- Verify US Treasury Checks using the [Treasury Check Information System \(TCIS\)](#)
- For deposits made through remote deposit capture (RDC) by new members consider stepping up your procedures for manually reviewing check images. You will not be able to verify the security features on Treasury checks deposited via RDC.
- Re-visit your check hold policy on deposits made at nonproprietary ATMs. Regulation CC allows for a five-business day hold on deposits made nonproprietary ATMs.
- When opening new accounts, screen new members through an identity verification solution. If there are any doubts as to the true identity, consider using a more robust solution, such as a skip trace solution.
- If you receive an incoming ACH stimulus payment and the member's account is closed, your best course of action is to return the ACH credit as Account Closed (return reason code R2). The Treasury's rules require financial institutions to return an ACH payment when the recipient's account is closed (refer to chapter 4 of the [Treasury's Green Book](#)).



## Risk Prevention Resources

Access CUNA Mutual Group's [Protection Resource Center](#) at [cunamutual.com](#) for exclusive risk and compliance resources to assist with your loss control efforts. The Protection Resource Center requires a User ID and password.

### Facing risk challenges?

[Schedule](#) a free personalized discussion with a Risk Consultant to learn more about managing risk.

© CUNA Mutual Group, 2020.

Insurance products offered to credit unions are underwritten by CUMIS Insurance Society, Inc., a member of the CUNA Mutual Group. This RISK Alert is intended solely for CUNA Mutual Group Fidelity Bond policyowners to prevent fraud losses. Any further distribution of this information could subject you to liability under common law and various statutes including the Fair Credit Reporting Act.

This resource was created by CUNA Mutual Group based on our experience in the credit union, insurance, and risk management marketplace. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value, and implementing loss prevention techniques. No coverage is provided by this resource, nor does it replace any provisions of any insurance policy or bond. Please read the actual policy for specific coverage, terms, conditions, and exclusions.