Allied Solutions

Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

Tax Season Fraud: Rising Threats Targeting U.S. Treasury Checks

SUMMARY

Beware of U.S. Treasury checks! Fraudsters continue to steal checks from the mail, altering the payee and amount, or creating counterfeits.

With tax season upon us, we want to warn you to be on the lookout for fraudulent Treasury checks. The U.S. Treasury's reclamation period is 18 months, so standard check holds are not effective.

There is no federal law requiring a financial institution to cash a check—even a government check. If you do accept one, financial institutions must follow Regulation CC hold guidelines. When the funds are made available, it doesn't necessarily mean the check is valid. Fake checks can take months to be discovered and untangled.

HOW TO VERIFY TREASURY CHECKS

There are two verification systems available to determine whether a Treasury check is legitimate:

Treasury Check Verification System (TCVS)
The system has been enhanced to allow financial institutions to verify payee information, making it a valuable resource in the fight against fraud. To access this enhanced service, credit unions must sign up for the secure Application Programming Interface (API). This functionality is not available on the TCVS website but becomes accessible once an API key is obtained. To enroll, credit unions must submit a terms and conditions agreement, which can be found on the Federal Reserve's website.

For questions about the TCVS API, contact the U.S. Treasury Department at: paymentintegrity@fiscal.treasury.gov

Check Integrity Initiative

Run by the Treasury Inspector General for Tax Administration (TIGTA), this fraud detection system enables credit unions to conduct in-depth analysis of potentially fraudulent checks, focusing on counterfeiting and alterations. The check integrity system allows for faster reporting of suspicious activity, helping credit unions stay ahead of fraudsters.
TIGTA has transitioned to a secure platform for submitting suspicious checks. Credit unions can now upload suspicious checks at TIGTA's Check Integrity Upload via Box.com.

For assistance using this platform or process, contact TIGTA at: checkintegrity@tigta.treas.gov

STEPS TO IDENTIFY RED FLAGS AND PREVENT LOSSES

When a check is brought to your financial institution for negotiation, review:

1. The date on the check
2. The date the account was opened at your institution
3. The date of incorporation provided at account opening (for business accounts)

If the account or business was opened after the check was issued, this is a red flag and further scrutiny of the check and account is warranted.

Pay close attention to the security features that should be present on the checks. Legitimate tax refund checks include ultraviolet (UV) printing that glows under a blacklight. There are four lines of "FMS," bracketed by the Financial Management Service (FMS) seal on the left and the United States seal on the right. If the check has been altered, the UV printing may be disrupted.

CURRENT FRAUD TACTICS FOR TAX REFUND CHECKS

We've identified three primary trends in tax refund check fraud:

1. Use of legitimate stolen checks deposited into accounts opened in the name of the original payee (individual or business)
2. Bad actors altering (or "washing") checks by changing the payee's name
3. Creation and negotiation of counterfeited checks. Bad actors are creating their own checks by purchasing check paper and printing.

In most cases, these checks are being deposited into newly opened accounts or accounts with minimal activity. Where checks are not altered or counterfeited, bad actors use stolen Personally Identifiable Information (PII) of the payee to open fraudulent accounts.

Once the checks are deposited, the criminals (or money mules—either recruited or unknowing accountholders) begin withdrawing the funds almost immediately after they are made available.

Many cases have involved using wire transfers, monetary instruments, or using P2P transfers to quickly deplete the funds before the fraud is recognized by the financial institution or the Treasury.

RISK MITIGATION RESOURCES

- If you receive a Treasury check or electronic funds transfer (EFT), the Bureau of the Fiscal Service call center can help: **1-855-868-0151, Option 2**
- For a refresher on U.S. Treasury check security features, reference this helpful graphic.
- Helpful links:
  - Fraud Risk Alert – Account Takeover Fraud is Soaring (PDF)
  - How to Validate Treasury Checks Across Deposit Channels
  - Sign up for our Let's Talk Fraud quarterly webinars
  - View additional risk resources
- Need assistance or want to request a consultation? Contact our risk specialists at risk_specialist@alliedsolutions.net

LinkedIn