Allied Solutions

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

US Treasury Fraud Risk Alert Updates

We first shared information on the fraudulent deposits of US Treasury checks in November of 2023. Since that time, we have continued to see this activity occurring at financial institutions across the country. This Risk Alert serves as a refresher on the activity and provides some additional risk mitigation resources that some financial institutions have used with success.

UPDATES

The activity in November 2023 primarily involved large Treasury checks that were proceeds from the Employee Retention Credit (ERC). We are still seeing checks tied to this program; however, the bad actors are also using other Treasury Checks, such as consumer tax refunds.

The fraudulent deposits typically followed one of these three general trends:

1. Use of legitimate stolen Treasury checks deposited into accounts opened in the name of the original payee (consumer or business) on the Treasury check.
2. Bad actors altering (washing) Treasury checks by changing the payee's name on the check to a new payee.
3. Negotiation of counterfeited Treasury checks, where bad actors are creating their own Treasury checks and printing on purchased check paper.

In almost all cases, the Treasury checks are being deposited into relatively newly opened accounts at financial institutions, though there have been cases where existing customers have perpetrated fraudulent activity on their established accounts.

Where Treasury checks are not altered or counterfeited, bad actors are establishing accounts utilizing Personal Identifiable Information (PII) of the payee to open accounts. Some are going as far as registering businesses either in different states, or using similarly spelled names, or by using the same name with a different corporate identifier after the business name such as Corporation, Company, Incorporated, or Limited.

In all cases, the criminals deposit the altered Treasury checks and begin withdrawing the funds almost immediately after they are made available. Many cases have involved using wire transfers, monetary instruments, and P2P transfers to begin depleting the funds before the fraud is recognized by the financial institution or the Treasury.

RISK MITIGATION

- When a US Treasury check is brought to your financial institution for negotiation, review the date on the check, the date that the account was opened at your financial institution, and for business accounts, check the date of incorporation that was provided at account opening. If the account was opened or business was opened after the check was issued, this should be a red flag and further scrutiny of the check and account should ensue.
- Review the history of the account and the nature of the accountholder's relationship with the financial institution. Ask yourself, "Does this type of check activity make sense for this accountholder or business?"

NOTE: *There is no federal law that requires a financial institution to cash a check, even a government check.* If you do accept the check, financial institutions are required to follow Regulation CC hold guidelines. When the funds are made available that doesn't mean it's a good check. Fake checks can take weeks to be discovered and untangled.

- If the check is deposited to a new consumer or business account (new = the accountholder had not had a transaction account with your Financial Institution within 30 days of the first deposit to the account), you can hold the excess over $5,525 in next-day availability checks – including the US Treasury check – for up to 9 business days from the banking day of deposit.
- Look to utilize other exception holds afforded by Regulation CC, such as "Reason to Doubt Collectability"
    - It is important to note that the US Treasury has 18 months to reclaim a Treasury check, so unlike most check deposits where the hold will protect you against a loss from a check returning, holding a Treasury check provides you with time to further investigate and verify the check using Treasury resources.
    - The United States Treasury does have the Treasury Check Verification System (TCVS) which allows financial institutions to verify certain information on a treasury check against their database, however it does not have the ability to verify payees.
- Pay close attention to security features (PDF download) that should be present on a legitimate US Treasury check. When a blacklight is passed over all U.S. Treasury checks, the ultraviolet (UV) printing becomes visible, and will glow. There are four lines of "FMS" bracketed by the FMS seal on the left, and the United States seal on the right. If the check is altered, the UV printing may be disturbed.
- The Treasury Inspector General for Tax Administration (TIGTA) introduced the checkintegrity@tigta.treas.gov email inbox in August 2023. This initiative serves as a crucial resource for financial institutions seeking to swiftly identify and combat counterfeit or altered Internal Revenue Service (IRS) Treasury check payments. TIGTA aims to provide responses to financial institutions within 48 hours.
- Financial institutions may also utilize the IRS External Leads Program (PDF download) which is intended to return questionable deposits to the IRS.
- If you receive a check or EFT (Electronic Funds Transfer) payment from Treasury, the Bureau of the Fiscal Service Call Center can help. The Bureau of the Fiscal Service Call Center can be reached by calling 1-855-868-0151, option 2.

RISK MITIGATION RESOURCES

- U.S. Treasury Check Security Features (PDF download)
- Treasury Check Verification System
- Check out Allied's Risk Resource Library
- Ask a Risk Specialist

The information presented in this document is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this document.

LinkedIn Instagram