Department of the Treasury
Financial Crimes Enforcement Network

Advisory

FIN-2013-A001
Issued: February 26, 2013
Subject: Update on Tax Refund Fraud and Related Identity Theft

The Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to remind financial institutions of previously-published information concerning tax refund fraud and the subsequent reporting of such activity through the filing of Suspicious Activity Reports (SARs).[1]

Identity theft can be a precursor to tax refund fraud because individual income tax returns filed in the United States are tracked and processed by Taxpayer Identification Numbers (TIN) and the individual taxpayer names associated with these numbers. Criminals can obtain TINs through various methods of identity theft, including phishing schemes and the establishment of fraudulent tax preparation businesses.[2] In response to this problem, the Internal Revenue Service (IRS) has developed a comprehensive strategy focused on preventing, detecting, and resolving instances of tax-related identity theft crimes.[3] FinCEN worked closely with the IRS to identify the following indicators of tax refund fraud.

Identifying Tax Refund Fraud

Financial institutions are critical in identifying tax refund fraud because the methods for tax refund distribution - issuance of paper checks, and direct deposit into demand deposit or prepaid access card accounts - often involve various financial services providers.[4] The number of tax refunds being distributed via direct deposit has increased significantly over the past several years

[1] Financial Crimes Enforcement Network, "Tax Refund Fraud and Related Identity Theft," (March 30, 2012), available at http://www.fincen.gov/statutes_regs/guidance/html/FIN-2012-A005.html
[2] For more information on identity theft, see e.g. "Identity Theft: Trends, Patterns, and Typologies Reported in Suspicious Activity Reports," (October 2010) at http://www.fincen.gov/news_room/rp/reports/pdf/ID%20Theft.pdf and http://www.fincen.gov/news_room/rp/files/ID%20Theft%2011_508%20FINAL.pdf; http://www.irs.gov/privacy/article/0,,id=186436,00.html?portlet=111; and http://www.ftc.gov/bcp/edu/microsites/idtheft/.
[3] Prepared Statement, Douglas H. Shulman, Commissioner, Internal Revenue Service, before the United States House of Representatives Committee on Oversight and Government Reform, Subcommittee on Government Organization, Efficiency and Financial Management, p. 2 (June 2, 2011).
[4] For more information on identifying direct deposit transactions representing Federal tax refund payments, see United States Department of the Treasury Financial Management Service, "The Green Book: A Guide to Federal Government ACH Payments and Collections," pp. 2-6 through 2-8 (August 2007, revised December 2011), available at http://www.fms.treas.gov/greenbook/pdf/GreenbookComplete.pdf.

and continues to increase annually.[5] In direct correlation, financial institutions may see tax refund fraud activity increase and related suspicious activity may be connected to direct deposit transactions. To assist financial institutions with identifying potential tax fraud, FinCEN, in consultation with the IRS and law enforcement, has identified the following red flags.[6]

- Multiple direct deposit tax refund payments, directed to different individuals, from the United States Department of the Treasury (Treasury) or state or local revenue offices are made to a demand deposit or prepaid access account held in the name of a single accountholder.
- Suspicious or authorized account opening at a depository institution, on behalf of individuals who are not present, with the absent individuals being accorded signatory authority over the account. The subsequent deposits are comprised solely of tax refund payments. This activity often occurs with fraudulent returns for the elderly, minors, prisoners, the disabled, or recently deceased.
- A single individual opening multiple prepaid card accounts in different names, using valid TINs for each of the supplied names and having the cards mailed to the same address. Shortly after card activation, Automated Clearing House (ACH) credit(s) from Treasury, state or local revenue offices, representing tax refunds, occur. This is followed quickly by ATM cash withdrawals and/or point-of-sale purchases.
- Business accountholders processing third-party tax refund checks in a manner inconsistent with their stated business model or at a volume inconsistent with expected activity. Similarly, individuals processing third-party tax refund checks through a personal account with no business or apparent lawful purpose.
- Business accountholders processing third-party tax refund checks and conducting transactions inconsistent with normal business practices, which may include:
    - A large volume of Treasury refund checks or bank checks being deposited, in contrast to other checks, such as payroll checks;
    - A large volume of refund checks bearing addresses of customers who reside in another state;
    - Multiple refund checks for the same or almost the same dollar amount;
    - Treasury refund checks or bank checks representing electronic refunds with sequential or close to sequential numbers;
    - The dollar amount of checks being deposited is not commensurate with the amount of currency being withdrawn to cover the cashing of these refund checks.

- Multiple prepaid cards that are associated with 1) the same physical address [individuals involved in criminal activity may also contact the customer service department requesting to change their address for their permanent prepaid card shortly after opening their temporary prepaid card account on-line]; 2) the same telephone number; 3) the same e-mail address; or 4) the same Internet Protocol (IP) address, which receive tax refunds as the primary or sole source of funds.

---

[5] *See* Internal Revenue Service, "2010 Filing Season Statistics" (Updated June 21, 2011), available at http://www.irs.gov/newsroom/article/0,,id=237561,00.html.

[6] Note that some of these red flags have been updated from the previous advisory, based on information received from the IRS.

- The opening of a business account for a check cashing business at a financial institution, which subsequently processed a high volume of tax refund checks issued to individuals from other states.
- A sudden increase in volume involving the cashing of tax refund checks issued to individuals from across the United States, moving through the account of an existing check cashing service.
- Individuals using bank accounts where the majority of the transactions are ACH federal tax refunds or refund anticipation loans.
- Individuals attempting to negotiate double endorsed Treasury tax refund checks with questionable identification.
- Individuals accompanying multiple parties to the bank to negotiate Treasury tax refund checks. Such items may or may not be double endorsed checks.
- The freezing or closure of a personal or business account due to suspicious activity involving either Treasury tax refund checks or ACH Treasury deposits.
- The signature/endorsement on the back of the check(s) does not match the identification of the individual conducting the transaction.
- The same signature/endorsement is used on multiple checks, with multiple names.
- Employees of financial institutions may also facilitate tax refund fraud by conducting transactions inconsistent with normal activity through the following practices:
    - Tellers who regularly process large quantities of Treasury tax refund checks. This may include one or more tellers during a specific time frame.
    - Bank employees who open multiple bank accounts that received a large quantity of Treasury tax refund checks.
    - Bank employees who did not follow proper identification procedures or accepted apparent fraudulent identification when opening an account.

Suspicious Activity Reporting

If a financial institution knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity or an attempt to disguise funds derived from illegal activity, is designed to evade regulations promulgated under the Bank Secrecy Act (BSA), or lacks a business or apparent lawful purpose, the financial institution may be required to file a SAR.[7] When completing SARs on suspected tax refund fraud, financial institutions should use the term "tax refund fraud" in the narrative section of the SAR and provide a detailed description of the activity. Due to the time sensitive nature of these transactions, a financial institution may also wish to contact their local IRS Criminal Investigation Field Office to alert them that a SAR has been filed related to tax refund fraud. In order to obtain contact information for your local IRS Criminal Investigation Field Office, financial institutions can call the FinCEN Regulatory Helpline.

Additional questions or comments regarding the contents of this Advisory should be addressed to the FinCEN Regulatory Helpline at 800-949-2732. ***Financial institutions wanting to report suspicious transactions that may relate to terrorist activity should call the Financial***

[7] *See, e.g.*, 31 CFR § 1020.320.

Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day). The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.