Department of the Treasury
Financial Crimes Enforcement Network

Advisory

FIN-2012-A005
Issued: March 30, 2012
Subject: Tax Refund Fraud and Related Identity Theft

The Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to assist financial institutions with identifying tax refund fraud and reporting the activity through the filing of Suspicious Activity Reports (SARs).

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. Fraudulent actors obtain TINs through various methods of identity theft, including phishing schemes and the establishment of fraudulent tax preparation businesses.[1] In response to this problem, the IRS has developed a comprehensive strategy that is focused on preventing, detecting, and resolving instances of tax-related identity theft crimes.[2] This Advisory is in furtherance of the comprehensive strategy.

Identifying Tax Refund Fraud

Financial institutions are critical in identifying tax refund fraud because the methods for tax refund distribution - direct deposit into demand deposit accounts, issuance of paper checks, and direct deposit into prepaid access card accounts - are often negotiated and deposited at various financial services providers.[3] The number of tax refunds being distributed via direct deposit has increased significantly over the past several years and continues to increase yearly.[4] As such, financial institutions may see tax refund fraud activity complement this trend and related suspicious activity may be more connected to direct deposit transactions. To assist financial institutions with identifying potential tax fraud, FinCEN has, in consultation with the IRS and law enforcement, identified the following red flags:

---

[1] 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/.

[2] 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).

[3] 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.

[4] *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.

- 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 fraudulent actor being named as having signatory authority. The subsequent source of funds is limited to the direct deposit of tax refunds. This activity often occurs when exploiting returns for the elderly, minors, prisoners, the disabled, or recently deceased.

- Opening multiple prepaid card accounts by one individual in different names using valid TINs for each of the supplied names, and subsequent mailing of the prepaid cards to the same address. Shortly after card activation, Automated Clearing House (ACH) credit(s) from Treasury or 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:

    - Large volume of Treasury refund checks or bank checks being deposited in contrast to few other checks being deposited, such as payroll checks;
    - Large volume of refund checks bearing addresses of customers out of state;
    - Multiple refund checks are for the same dollar amount or a few dollars off;
    - Treasury refund checks or bank checks, representing electronic refunds, are sequentially numbered or within a few numbers of each other;
    - 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 [fraudulent actors may also contact their customer service department requesting to change their address for their Permanent Prepaid Card shortly after opening their Temporary Prepaid Card 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.

- The opening of a business account for a check cashing business at a financial institution, with a subsequent high volume of tax refund checks issued to individuals from across the United States.

- A sudden increase in volume moving through the account of an existing check cashing service, involving tax refund checks issued to individuals from across the United States.

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.[5] 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.

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 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.

[5] *See e.g.* 31 CFR § 1020.320.