Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

April 02, 2015

Alert Number
I-040215-PSA

TAX RETURN FRAUD

Criminals are proficient in stealing the personally identifiable information (PII) of individuals to facilitate various fraud activities, including using stolen identity information to file fraudulent tax returns. Once the fraudsters obtain victim PII, they electronically file tax returns and set up pre-paid debit cards or bank accounts to route fraudulent returns. The balances on the pre-paid cards and bank accounts are depleted shortly after the tax refund is issued.

The fraudsters utilize multiple methods to obtain the information needed to file a tax return. The most popular methods include: computer intrusion, the online purchase of stolen PII, the recruitment of insiders who have legitimate access to sensitive information, the physical theft of computers that contain PII, the impersonation of Internal Revenue Service personnel, and the aggregation of information that is obtained through multiple publicly available Web sites.

Recent open source reporting indicates that cyber criminals also target and compromise legitimate online tax software accounts of individuals. Cyber criminals conducting this scheme modify victims' bank accounts to divert transfers to bank accounts or pre-paid cards under their control.

Victims who filed complaints with the Internet Crime Complaint Center (IC3) reported they discovered they were victims of tax refund fraud when they tried to file a return and were notified by the Internal Revenue Service that their Social Security Numbers had already been used to file a tax return. One individual reported that due to an error in direct deposit account information submitted on his return, he was issued a check. However, the victim had not yet filed a return. Others reported before they filed their return, they received notification that their returns were being audited or were under review.

A recent investigation identified a tax refund fraud ring responsible for filing approximately 644 fraudulent tax returns totaling over $1.9 million in attempted fraud. Using fraudulently obtained PII, the fraudsters submitted tax returns and requested the funds be deposited into bank accounts under their control. The group recruited college students to open accounts to collect the tax refund monies. The students withdrew funds via ATMs and counter withdrawals. The students then passed the majority of the funds to another group member and kept a portion of the refund as payment for the use of their bank accounts to conduct the scheme.

This type of fraud is a growing concern as the number of complaints filed with the IC3 has doubled from 2013 to 2014.

If you believe you have been a victim of this scam, you should reach out to your local IRS or FBI field office, and you may file a complaint with the IC3 at www.IC3.gov. Please provide any relevant information in your complaint.

Tips to protect yourself:

- Monitor your credit statements for any fraudulent activity.
- Report unauthorized transactions to your bank or credit card company as soon as possible.
- Review a copy of your credit report at least once a year.
- Be cautious of scams requiring you to provide your personal information.

	• Do not open email or attachments from unknown individuals. • Never provide credentials of any sort via email. This includes clicking on links sent via email. Always go to an official website. • If you use online tax services, double check to ensure your bank account is accurately listed before and after you file your tax return. • Ensure accounts that are no longer being utilized are properly deleted or scrubbed of sensitive information. Allowing online accounts to become dormant can be risky and make you more susceptible to tax fraud schemes.