Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

March 23, 2016

Alert Number
I-032316-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

STOLEN IDENTITY REFUND FRAUD

Each year, criminal actors target US persons and visa holders for Stolen Identity Refund Fraud (SIRF). SIRF is defined as the fraudulent acquisition and use of the Personally Identifiable Information (PII) of US persons or visa holders to file tax returns. The fraudulent tax returns are sent to bank accounts or pre-paid cards that are held under their control. SIRF is relatively easy to commit and extremely lucrative for criminal actors. While all U.S. taxpayers are susceptible to SIRF, over the past year, criminal actors have targeted specific portions of the population, including: temporary visa holders, the homeless, prisoners, the deceased, low-income individuals, children, senior citizens, and military personnel deployed overseas. This may be due to the perception by criminal actors that these individuals are less likely to be aware of or receive notification that their identity has been stolen.

After criminal actors steal PII, they use corrupt tax preparation companies or online tax software to file fraudulent tax returns with the stolen identity information at the federal and state level. The only legitimate information needed to file a fraudulent tax return is a name and social security number. This information is obtained by criminal actors through a variety of techniques, including computer intrusions, the online purchase of stolen PII, the physical theft of data from individuals or third parties, the impersonation of government officials through both phishing and cold-calling techniques, the exploitation of PII obtained through one's place of employment, the theft of electronic medical records, and searching multiple publicly available Web sites and social media. After the criminal actors electronically file fraudulent tax returns, they use pre-paid debit cards or bank accounts under their control to route fraudulent returns. The balances on the pre-paid cards and bank accounts are depleted shortly after the tax refund is issued.

Additionally, investigative information shows cyber criminals compromised legitimate online tax software accounts during the 2015 tax season. Cyber criminals modified victims' online tax software account information, diverting tax refunds to bank accounts or pre-paid cards under their control.

Many victims of SIRF do not know they have been targeted until they try to file their legitimate tax return. Many also receive notifications in the mail that their returns are being audited or are under review before they have even filed their tax returns.

If you believe you are a victim of SIRF, contact your local FBI or IRS field office. You may consult www.identitytheft.gov which can help you report and recover from identity theft. Additional resources are available at https://www.irs.gov/Individuals/Identity-Protection.

Tips to protect yourself:

- File tax returns as early as possible.
- Monitor your bank account statements regularly, as well and as your credit report at least once a year for any fraudulent activity.
- Report unauthorized transactions to your bank or credit card provider as soon as possible.
- Be cautious of telephone calls or e-mails that require you to provide your personal information, especially your birth date or social security number. If you are in doubt, do not provide the requested information.
- Do not open e-mail or attachments from unknown individuals. Additionally, do not click on links embedded in e-mails from unknown individuals.
- Never provide personal information of any sort via e-mail. Be aware, many e-mails requesting your personal information appear to be legitimate.
- If you use online tax services, ensure your bank account is accurately listed before and after you file your tax return.
- Ensure sensitive information is permanently removed from online tax software accounts that are no longer being used. Allowing online accounts to become dormant can be risky and make you more susceptible to tax fraud schemes.
- If you feel you are a victim, immediately contact the three major credit bureaus to place a fraud alert on your credit records.
- If you are a victim, file an Identity Theft Affidavit (IRS Form 14039). This form is available for download from www.identitytheft.gov.