2015 YEAR-END

Tax guide.










plante moran

audit · tax · consulting · wealth management

Fraud.

GONE PHISHING

Identity thieves are filing false returns and obtaining tax refunds — all in the name of unsuspecting taxpayers.

Michelle McHale
Partner, Forensic & Valuation Services
616.643.4059
michelle.mchale@plantemoran.com

There's an epidemic hitting taxpayers, and it's unrelated to more cumbersome tax laws. Identity thieves have been filing fraudulent returns and receiving refunds — all in the name of other taxpayers.

It's been discomforting to learn about the rising number of taxpayers who've submitted tax returns only to learn from the IRS that they had, unknowingly, already filed and received a refund. Here's how the scheme works.

Using someone else's name and Social Security number, identity thieves file a false tax return, creating fictitious W-2s showing employment and detailing that a refund is due. The online filing process is simple, allowing most thieves to file numerous fraudulent returns in a day.

The refund checks are mailed to the address or to the bank account listed on the return — and of course, neither reflects the actual taxpayer's information. While this discrepancy prevents a large number of refund requests from being processed, others get through at a cost of billions of dollars annually to the IRS and taxpayers.

This causes undue stress and hardship for the victims. If you're a tax fraud victim, the IRS freezes your refund, pending an investigation. And as mentioned on page 15, agency reductions have caused a backlog of claims that can take months to resolve — a process that leaves victims unable to obtain their refunds.

It's all possible because the thieves are able to gain access to personal information, which in many cases is offered voluntarily — albeit unwittingly. To reduce the risk of identity theft in tax-related schemes, keep the following in mind:

- **The IRS does not email taxpayers.** Don't fall victim to phishing emails that seek to extract your personal information. The temptation can be great, as identity thieves can disguise websites and emails to appear legitimate. For example, some company employees have received emails with instructions to wire funds that appear to come from company executives or board members. If you're uncertain about the authenticity of IRS-branded correspondence, contact your local IRS office to verify.
- **The IRS does not call taxpayers to request personal information.** The IRS already has your information, so there's no need to call you. As a general rule, never give out your Social Security number over the phone to someone requesting it.
- **The IRS opts for snail mail.** The IRS uses regular mail almost exclusively to correspond with taxpayers. Identity thieves understand this and also use paper correspondence to solicit personal information. If you're in doubt about the legitimacy of an IRS letter, contact your local office to verify.

The IRS is aware of the identify theft epidemic and has instituted measures that are becoming increasingly effective at preventing fraud. However, it's a cat-and-mouse game, and identity thieves are staying ahead of the chase. In the meantime, awareness and skepticism are your best tools to prevent becoming a victim.