accountingTODAY

September 1, 2016

accountingTECHNOLOGY

Avoiding Tax-Related Identity Theft

Tax-related identity theft has risen exponentially over the last couple of years. Taxpayers can become victims of identity theft in a wide variety of ways:

- Data illicitly retrieved from PCs, servers, PDAs and mobile phones that have been discarded or are being repaired;
- Computer breaches in browser security or malware such as Trojan horses or other forms of spyware;
- Hacking computer networks;
- Advertising bogus jobs to obtain applicants' personal information;
- Phishing; or
- Browsing social networking websites for personal details.

The focus of law enforcement used to be on the fraud committed rather than on whether personal identification information was used in the fraud. In more recent years, federal and state governments have enacted laws to levy separate penalties for fraud committed using stolen identity information. Changes have also been made to the Fair Credit Reporting Act allowing consumers to:

- Place fraud alerts on their credit files if they are or believe they may become victims of identity theft;
- Dispute inaccurate information; and
- Receive a free credit report once per year from each of the three credit reporting agencies.

Financial institutions are also required to establish programs designed to address suspicious patterns or practices, or specific activities, which suggest the possibility of identity theft. This requirement is called the Red Flags Rule by the Federal Trade Commission, which requires that certain businesses and organizations must implement a written identity theft prevention program designed to detect the warning signs – or red flags – of identity theft in their day-to-day operations.

All states have their own statutes that criminalize identity theft. In addition, Sections 6713 and 7216 of the Internal Revenue Code provide monetary and criminal penalties for unauthorized disclosures or use of taxpayer information by persons engaged in the business of preparing or providing services in connection with tax return preparation or who fail to properly protect their clients' personal information.
\
In one of a series of incidents over the last few years, the IRS disclosed on February 9 this year that it had been the subject of an automated malware attack compromising e-file PINs. Following this disclosure, the Senate Finance Committee passed a bill that would provide the IRS with funds to hire additional information technology professionals. It would also change the deadline for filing Forms W-2, W-3, and 1099-MISC information matching returns so that they would be reported to the IRS within 15 days of the deadline for employee and payee statements. On May 16, the House of Representatives passed a bill to create a point of contact for victims of refund fraud and an information sharing and analysis center that would help detect and prevent identity theft.

On June 7, the IRS announced that it was re-opening access to its Get Transcript Online tax record application, and access for previous users of the Identity Protection Personal Identification Number (IP PIN), Online Payment Agreement (OPA), and e-post card services, all via a new multifactor e-authentication process.

Meanwhile, the IRS has announced the establishment of a new Identity Theft Tax Refund Fraud Information Sharing & Analysis Center (ISAC) intended to centralize, standardize, and enhance the way information involving potential identity theft is collected and analyzed. The agency will also be expanding its W-2 verification code pilot program for the 2017 filing season. This involves a special code on W-2s which is entered on the tax return to confirm the accuracy and integrity of the electronically filed returns. In addition, the IRS announced in July that smaller tax return preparation companies and solo practitioners would be the focus of the next phase of the agency's ongoing battle against tax-related identity theft. Its feeling is that unregulated small preparers tend to be the most under-informed about identity theft and security issues.

In addition to safeguarding client files and information and using enhanced

security techniques to protect computer networks, filing clients' returns as early as possible in order to be notified of potentially duplicate returns helps to identify problems sooner. If a client experiences identity theft, then the following are among the actions that should be considered:

- File Form 14039 - IRS Identity Theft Affidavit;
- Report the identity theft to the Identity Protection Specialized Unit (UPSU) at 1-800-908-4490; and
- Contact Taxpayer Advocate Service (TAS) if economic hardship or unreasonable delay exists in processing information or adjusting the taxpayer's account (see Form 911).

Tax-related identity theft is likely to remain a hot topic for the foreseeable future. All practitioners will need to keep an eye out for new developments and requirements both from the IRS and from Congress, while at the same time looking for ways of increasing the security of their networks and client files.

Editor's note: A version of this article first appeared on Maddin, Hauser, Roth & Heller, P.C.'s ***blog.***

William E. Sigler is a shareholder at the Southfield, Mich.-based law firm of Maddin, Hauser, Roth & Heller, P.C. His practice involves business planning, structuring and formation of business entities, mergers and acquisitions, real property acquisitions and dispositions, contract drafting and review, employee benefit plans, executive compensation, and estate and business succession planning. He graduated from Michigan State University and the University of Detroit School of Law, where he was an editor of the Law Review.