Best Practices to Avoid Tax-Related Identity Theft

What Is Tax-Related Identity Theft?

Fraudulent tax refunds issued as a result of identity theft occur when an individual steals a victim's personally identifiable information (PII), such as a Social Security number (SSN), and files a tax return claiming to be the victim. More than 89,000 Americans filed complaints with the Federal Trade Commission (FTC) reporting tax fraud linked to identity theft in 2020. Similarly, businesses may also fall victim to tax fraud, where an individual steals a business's employer identification number (EIN) to file fraudulent returns. In both scenarios, the victims usually discover they have fallen victim to such fraud when their tax returns are rejected, or when the business receives notice about Forms W-2 they didn't file with the Social Security Administration or notices for balances due to the Internal Revenue Service (IRS) that are not owed. Most frequently, neither businesses nor individuals will have any reliable information as to how their information has been exposed. The IRS has noted such tax fraud tends to increase during tax season and time of crisis, and cybercriminals have undeniably taken advantage of the COVID-19 pandemic to unleash an unprecedented number of tax fraud schemes to steal information from taxpayers.

Common Schemes

Reports of common tax-related identity theft schemes include emails infected with phishing links that mirror bogus websites (e.g., IRS website) to trick unsuspecting victims to enter revealing personal or financial information. Most recently, the IRS issued a warning to universities and university students of scammers primarily targeting email addresses of educational institutions. Other common schemes include (i) phone calls made by callers impersonating the IRS asking for immediate payment with the threat of arrest, deportation or suspension of a business or driver's license; (ii) robo-calls claiming to suspend or cancel the victim's SSN if certain information is not provided; and (iii) phone calls made by callers impersonating the Taxpayer Advocate Service, an independent organization within the IRS that assists taxpayers to resolve tax problems.

Similarly, businesses have been warned by the IRS of certain schemes that have resulted in fraudulent tax returns. Most recently, the IRS has warned businesses of an email scam where senders use spoofing techniques to disguise an email to make it appear as if the email came from an organization executive who is requesting certain sensitive employee information, such as a list of employees and copies of their Forms W-2. An unsuspecting employee at an organization, usually an employee in the payroll or human resources department, receiving this email may provide the requested information. Certain businesses like tax professionals have also been subject to email scams attempting to steal Electronic Filing Identification Numbers (EFINs), numbers assigned to authorized IRS e-file providers. Given the amount of impersonation schemes, the IRS has issued several reminders to consumers and businesses that the IRS does not initiate contact with taxpayers via email, text messages, or social media channels to request personal or financial information, including PIN numbers, passwords or similar access information for credit cards, banks or other financial accounts.

Another common scheme the IRS has issued warnings about is identity theft via data breaches. While not every data breach results in tax-related identity theft, a breach resulting in the unauthorized access or unauthorized disclosure of sensitive information may allow cybercriminals to steal a victim's identity and file fraudulent returns. For example, breach of a tax preparer's business may result in the disclosure of tax identification numbers belonging to the tax preparer's customers or employees or the tax preparer's EIN. Given that many other federal agencies have been hacked, one could not rule out the possibility that the IRS itself may be leaking personal data. Whatever the method may be, the end goal of such schemes is to gain access and obtain sensitive personal and financial information to file fraudulent returns with the IRS or simply gain access to an individual's or business's financial account.

Related Compliance Framework and IRS Resources

Certain federal laws, like the Gramm-Leach-Bliley Act (GLBA), require companies that provide financial products and/or services, including tax preparation services, to provide their customers privacy notices that explain their information collection and sharing practices, as well as ensure the security and confidentiality of customer records and personal information. As part of its implementation of the GLBA, the FTC issued the Safeguards Rule, which requires financial institutions under FTC jurisdiction to have measures in place to protect customer information. For example, the FTC requires such institutions to (i) implement a written information security program that is appropriate to the company's size and complexity, the nature and scope of its activities and the sensitivity of the customer information it handles; (ii) designate one or more employees to coordinate the information security program; (iii) identify and assess risks to customer information in each relevant area of the company's operation and the effectiveness of its safeguards for controlling such risks; and (iv) select service providers that can maintain appropriate safeguards and oversee such providers in the provision of services. Several states, such as California, Massachusetts and New York, have enacted data security laws, most of which require businesses that own, license or maintain personal information about a resident of that state to implement and maintain "reasonable security procedures and practices" appropriate to the nature of the information to protect such information from unauthorized access, destruction, use, modification or disclosure. Massachusetts is the long-standing exception, and it has issued detailed regulatory guidance on its expectations for reasonable security. *See* 201 CMR 17.00. All fifty (50) states, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands have also enacted legislation requiring notification of security breaches involving personal information.

The Internal Revenue Code also imposes criminal penalties and/or monetary penalties against tax preparers who make unauthorized disclosures, misuse the sensitive information furnished to them, or fail to take the necessary steps to implement or correct its information security program resulting in an unauthorized disclosure. Moreover, under the American Institute of CPAs' (AICPA) code of professional conduct, tax preparers and other certified public accountants have a fiduciary duty to their clients, including the duty to safeguard client information. Therefore, a business's failure to adequately safeguard a customer's or employee's personal information resulting in tax-related identity theft may potentially result in an FTC enforcement action, an enforcement action by state AGs (depending on which state statute the business violates) and even a private action brought by an impacted customer or employee (depending on which state statute the business violates). If the business is within the scope of the AICPA, the business may also be at risk of losing its CPA license.

To better educate businesses of their legal responsibilities and better inform both individuals and businesses of how to best protect their sensitive personal and financial information, the IRS has provided several helpful resources including:

- **IRS Security Summit:** In 2015, the IRS convened a coalition of 42 state tax agencies and 20 private-sector tax industry officials (i.e., tax preparation firms, tax software developers, payroll and tax financial product processors, etc.) to fight back against criminal syndicates filing fraudulent returns or refunds. The Security Summit, organized into six working groups, have been tasked to address different areas of need, such as identifying ways to strengthen authentication practices, identifying points of vulnerability (threats/risks), increasing awareness among individuals, businesses and tax professionals on the need to protect sensitive tax and financial information, etc. Between 2015 and 2019, the number of confirmed identity theft returns stopped by the IRS declined by 68%. Unfortunately, the IRS has noted a significant increase in tax frauds, including tax-related identity thefts, during the COVID-19 pandemic.

- **Identity Theft Tax Refund Fraud – Information Sharing and Analysis Center (ISAC):** Growing out of the Summit collaboration is the ISAC, which functions as a centralized, enhanced compilation and analysis tool for member organizations to share valuable data, such as information related to data breaches, evolving tactics used to identity cybercriminals, etc. Members of the ISAC interact with trusted third-party entities, which have been evaluated and sanctioned by the IRS to facilitate the analysis and compilation of data, to transmit data into a

secure portal and/or download data submitted by other members to perform further analysis and identify patterns of identity theft. ISAC provides members with near real-time potential indicators of identity theft tax refund fraud and analysis.

- **National Tax Security Awareness Week:** Every year the IRS and its Security Summit partners designate a week as "National Tax Security Awareness Week," as part of a public awareness campaign to educate individuals, businesses and tax professionals about the importance of protecting personal, tax and financial data online and in the home. The campaign offers tips and suggestions on what individuals and businesses should do to enhance their security measures to better protect their data from identity theft.

- **IRS publications:** The IRS website has also issued several publications that provide helpful guidance to individuals and businesses, including tax preparers. For example, Publication 4557 titled "Safeguarding Taxpayer Data: A Guide for Your Business" provides tax professionals (i) a helpful summary of its obligations under GLBA and the FTC Safeguards Rule; (ii) security steps they should take to protect their data (e.g., use of security software such as anti-virus software or firewalls, strong passwords, secure wireless network, etc.); (iii) guidance on how to spot data theft (e.g., recognize phishing attacks, monitor the number of returns filed with its EFINs, etc.); and (iv) information regarding to whom they should report and how to respond to such data loss. Publication 1345 titled "Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns" provides authorized online providers of tax preparation services a summary of the rules and legal requirements it must comply with, identifies security, privacy and business standards it must adopt (e.g., minimum encryption standards for transmission over the internet, performance of vulnerability scans by independent third parties, adoption and implementation of written privacy and security programs, etc.), and other obligations (e.g., reporting of identity theft or refund fraud activity, recordkeeping and documentation requirements, etc.).

Best Practices to Safeguard Sensitive Information and Other Actionable Steps

The IRS has identified certain best practices individual taxpayers, businesses and tax preparers should follow to prevent tax-related identity theft. For example, the Security Summit has outlined the "Security Six," the must-have areas to secure taxpayer data on computers:

1. **Antivirus software (anti-malware software)**: Such software scans files or a computer's memory for certain patterns that may indicate the presence of malicious software. The software looks for patterns based on the signatures or definitions of known malware, which are often updated daily, so it is not only recommended to install and use anti-virus software, but it is important that the latest updates are installed. While anti-virus software should protect against spyware and contain anti-phishing capabilities, it cannot protect data if the computer user falls victim to a phishing attack; therefore, security awareness training (as detailed below) is still important to limit the risk of phishing schemes.

2. **Firewalls**: Firewalls provide protection against outside attackers by shielding the computer or network from malicious or unnecessary network traffic and preventing malicious software from accessing the network. Similar to anti-virus software, the IRS has noted that firewalls cannot protect data if the computer user falls for phishing scams and divulges sensitive data (e.g., usernames and passwords or personal information).

3. **Two-Factor Authentication**: This feature helps by adding an extra layer of protection, where an individual must enter a security code (i.e., a code sent via text on a mobile) in addition to the individual's username and password to access an account. Implementing this may prevent thieves that have stolen an individual's username and password from easily gaining access to the individual's account and gain access to an individual's sensitive information.

4. **Backup software/services**: Critical files and sensitive files on computers should routinely be backed up to a safe and external source not connected full-time to a network. If the external source is a hard drive, the hard drive should be stored in a secured location.

5. **Encryption of data**: Drive encryption or disk encryption transforms data on the computer into unreadable files for the unauthorized person accessing the computer. Emails being sent or received that contain personal information should also be encrypted.

6. **Virtual private network (VPN)**: Use of a VPN provides a secure, encrypted tunnel to transmit data between a remote user via the Internet and a company network, which is especially important during the COVID-19 pandemic where many more workers are teleworking from home.

Other recommended best practices include:

- **Strong and unique passwords**: Both individual taxpayers and businesses, including tax preparers, should use strong and unique passwords of eight or more mixed characters that are different for each account, and changed periodically. Therefore, if a cybercriminal acquires an individual's password, access is limited to one account as opposed to all accounts. A password manager may be handy to help individuals store, generate and manage their passwords for several different local applications and online services, although it also creates a treasure trove of passwords, so the best practice is to memorize a password that is unique for each site. This can be most easily accomplished by using a standard pass phrase and then adding a descriptor for each site. For example, one could pick a phrase such as "MichiganRocks!" and then add a phrase for each site so that for Starbucks, the phrase would be "StarbucksMichiganRocks!" or "CoffeeMichiganRocks!"

- **Secured wireless connection**: Both individual taxpayers and businesses should be cautious when allowing or granting remote access to internal networks containing sensitive data. The wireless network connection should be protected by a strong password to prevent unauthorized users gaining access to the network, and thus any sensitive data that is transferred while on the network is protected.

- **Access controls**: Businesses should design, implement, and maintain access controls that restrict access to its IT systems and applications to ensure only the necessary employees have access to taxpayer information and other sensitive data – and that former employees rapidly have their access eliminated.

- **Security awareness education**: Both individual taxpayers and business employees, including employees of tax preparers, should be educated to identify suspicious activity (e.g., phishing emails and other IRS impersonation schemes detailed above) to recognize signs of data theft, and to be informed what security measures are necessary to protect personal information.

- **IRS Identity Protection (IP PIN)**: An IP PIN is a six-digit number that prevents someone else from filing a tax return using an individual's SSN because only the taxpayer and the IRS know the designated IP PIN.

- **Track EFIN usage**: The IRS recommends that tax preparers track its EFIN usage on a weekly basis to know the number of returns filed with the tax preparer's EFIN. If the numbers are off, this may be a sign of fraudulent activity.

- **Create and implement a data security plan**: The IRS recommends that businesses, including tax preparers, implement a written data security plan as required by the FTC's Safeguards Rule that shows how the business addresses the risks it is subject to and the safeguards it uses to protect its data against breaches and identity theft.

- **Create and implement a data theft recovery plan**: The IRS recommends that businesses, including tax preparers, should create a data theft plan that they can enact should they experience a data loss, which includes notifying local law enforcement, alerting affected businesses (e.g., major credit bureaus) and impacted clients. Such a plan may also include designating a person responsible for releasing the information related to the data theft and additional steps such as offering free credit monitoring to impacted clients.

If data theft were to occur, the IRS has also identified actionable steps victims of tax-related identity theft may take.

- **Individuals**: An individual taxpayer that has fallen victim to tax-related identity theft or identity theft in general, whether or not any fraudulent tax return has been filed, may fill out an identity theft affidavit with the IRS. Upon receipt, the IRS will assign the individual's case to its Identity Theft Victim Assistance (IDTVA) organization, where the matter will be researched and resolved by an employee with specialized identity theft training. The IDTVA organization will assess the case, determine if the identity theft affects one or more tax years, address all issues related to the fraudulent return, including determining if there are additional victims. The IDTVA will then ensure the correct tax return is properly processed and remove the fraudulent return from the individual's tax records, and certain tax-related identity victims will be placed into the Identity Protection PIN program to annually receive a new, six-digit IP-PIN to file a tax return. The IRS also directs individuals to file an FTC Identity Theft Report at the FTC's identitytheft.gov website. This report contains the individual's official statement about the incident, which may be provided to businesses and credit bureaus as proof of the individual's identity theft. The individual may also input the details of its identity theft into the FTC's website to develop a recovery plan that will guide the individual step by step through recovery, including freezing the individual's bank accounts, changing account passwords, alerting credit bureaus, implementing credit-monitoring services, etc.

- **Businesses**: If a business has fallen victim to tax-related identity theft or thinks someone is using its business name or EIN to submit fraudulent tax returns or Forms W-2, the business may submit a business identity theft affidavit to the IRS. If the business has suffered a data loss related to a W-2 scam as detailed above, reporting such incident in a timely manner is critical. The IRS has found that cybercriminals who successfully steal Forms W-2 may immediately attempt to monetize their thefts by filing fraudulent tax returns claiming a refund with the stolen employee SSNs or sell the data on the Internet's black market sites to others who file fraudulent tax returns. If notified quickly, the IRS may be able to take steps that help protect the impacted employees from related identity theft. Therefore, the IRS instructs impacted businesses to email the IRS with the subject line "W2 Data Loss" in a timely manner and provides guidance on how to notify their impacted employees. The IRS also instructs impacted businesses to file a complaint with the FBI's Internet Crime Complaint Center (IC3). Lastly, because any breach of personal information may affect an individual's tax account with the state as well as the IRS, businesses are instructed to reach out to the Federation of Tax Administrators for information on how to report the impacted employees' information to the relevant state tax agencies.

Conclusion

Both individuals and businesses are at risk of tax-related identity theft. Such risk has undeniably increased during the COVID-19 pandemic as cybercriminals continue to evolve their commonly used schemes and workers continue to work remotely. Businesses and individuals should seek guidance from the IRS on how to best combat identity theft, as the IRS's website provides several invaluable resources on how to best protect personal information from such cybersecurity risk and what actionable steps an individual or business may take if identity theft were to occur.