Published on *The National Law Review* https://natlawreview.com

IRS Data Leak Hits Home: Actions for Taxpayers in the Wake of the Littlejohn IRS Data Breach

Article By:

Robert R. Pluth Jr.

Oliver R. Merrill

Melisa Seyhun

The Internal Revenue Service (IRS) has begun the process of informing over 70,000 taxpayers that their confidential tax information was leaked in a widespread breach by a former IRS contractor. Those impacted should take steps to protect against identity-theft and related abuses, assess potential damages, and consider legal action.

This past January, a former IRS contractor, Charles Littlejohn, was sentenced to five years in prison for illegally accessing and disclosing thousands of federal tax returns and related information between 2018 and 2020 (the Littlejohn Breach). The IRS is now notifying the nearly 70,000 taxpayers whose tax information was compromised in what has been described as the largest IRS breach in recent history. While the most prominent figure impacted by this disclosure was former President Donald Trump, whose tax returns were leaked to *The New York Times*, many individuals and entities are now learning that they, too, are victims of the Littlejohn Breach. Many now find themselves wondering what to do next, whether any remedies are available, and how to protect themselves from tax-related identity theft.

IRS Notices

Over the last couple of weeks, the IRS has begun the process of informing the more than 70,000 affected entities and individuals of Littlejohn's unauthorized disclosure of their tax information. Affected taxpayers have received notices (Letter 6613-A), which include a copy of Littlejohn's criminal charge, stating the taxpayer's right to civil claims, and providing little additional information. Notably, the notices provide no personalized information or details regarding which specific tax returns, and what identifying information contained therein, may have been illegally disclosed. This leaves affected taxpayers in a challenging position, knowing that they are at risk yet unsure of how to

properly assess potential damages, mitigation options, or opportunities for recourse.

Statutory Damages

Federal law provides for statutory damages which may be available to impacted taxpayers. Section 7431 of the Internal Revenue Code provides that "taxpayer may bring a civil action for damages against the United States in a district court." Section 7431 further provides that recoverable damages are limited to $1,000 "for each act of unauthorized inspection or disclosure of return or return information," plus litigation costs, unless the taxpayer can demonstrate that they sustained actual damages more than the proscribed limit because of the unauthorized act or acts. This general statutory cap on damages will likely discourage many affected taxpayers from initiating a lawsuit.

Taxpayers affected by Littlejohn Breach who are interested in taking legal action should act quickly, however, as claims must be filed within two years of the date the taxpayer discovered the data breach. The "date of discovery" is the date on which a taxpayer knows or should know of the unauthorized disclosure. For those first learning of the unauthorized disclosure via the notices recently sent by the IRS relating to the Littlejohn Breach, the period of two years begins as of the date the taxpayer received the notice.

Initial Steps to Protect Your Information

Given the scale of Littlejohn Breach, it is crucial for affected taxpayers to evaluate their tax and personal records for suspicious or unauthorized activity. Affected taxpayers are encouraged to request their tax transcript from the IRS, and to review them for fraudulent activity. The transcripts can be requested online or by mail (by filing a Form 4506-T).

The IRS provides guidance on its website for taxpayers who have had their personally identifiable information compromised in a data breach. If a taxpayer knows their information has been compromised, whether because of a data breach or otherwise, they should alert the IRS by filing an Identity Theft Affidavit (Form 14039). Upon receipt, the IRS will take steps to secure the taxpayer's account.

Furthermore, affected taxpayers should consider contacting the three major credit bureaus (Equifax, Experian, and TransUnion) to obtain, and review, their credit reports. Upon discovery of any fraudulent accounts or unauthorized activity, the taxpayer should immediately inform the credit bureaus of the suspicious activity, request implementation of a credit freeze, and contact the relevant account providers or institutions to halt further unauthorized activity and close the fraudulent accounts. Similarly, if a taxpayer suspects that their Social Security number may have been compromised, the Social Security administration should be contacted immediately.

Nine Tips to Proactively Protect Your Information

In the case of the Littlejohn Breach, individual taxpayers could do little to protect their information from unauthorized disclosure. There are many proactive ways to guard your identity and personal information, however, and implementing these protections can help ensure that risks from unauthorized activity or disclosure are identified, and mitigated, promptly.

1. Review your IRS tax transcript and credit report on an annual basis.
2. Consider applying for an Identity Protection PIN, which is required to file your tax return and

will change on an annual basis.
3. Inquire about your tax preparer’s data security and controls.
4. If you send documents electronically that contain sensitive tax information, such as your social security number of employer identification number, to your advisors, tax preparer, or others, do so on a password protected basis (conveying the password in a separate phone call) or using a peer-to-peer file transfer application.
5. Encrypt all tax records saved to your computer and cloud-based storage systems.
6. Consider insuring against identity theft.
7. Use strong and unique passwords, as well as multi-factor or two-factor authentication for all online financial accounts or online accounts that contain your financial, personal identifying, or other sensitive information.
8. Recognize and be aware of new phishing emails, and phone call and text message scams.
9. Monitor your digital footprint by periodically searching for yourself online. Report and close any fake or imitation accounts, set alerts to notify you when settings or personal information in your online accounts are changed, and ensure that tighter privacy settings (including restricting permissions) are utilized online and for mobile apps.

National Law Review, Volume XIV, Number 134