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

Protect Yourself: Action Steps Following the Largest-Ever IRS Data Breach

Article By:

Kevin Spencer

Joseph Viviano

On January 29, 2024, Charles E. Littlejohn was sentenced to five years in prison for committing one of the largest heists in the history of the federal government. Littlejohn did not steal gold or cash, but rather, confidential data held by the Internal Revenue Service (IRS) concerning the United States' wealthiest individuals and families.

Last week, more than four years after Littlejohn committed his crime, the IRS began notifying affected taxpayers that their personal data had been compromised. If you received a notice from the IRS, it means you are a victim of the data breach and should take proactive steps to protect yourself from fraud.

IN DEPTH

Littlejohn's crime is the largest known data theft in the history of the IRS. He pulled it off while working for the IRS in 2020, using his access to IRS computer systems to illegally copy tax returns (and documents attached to those tax returns) filed by thousands of the wealthiest individuals in the United States and entities in which they have an interest. Upon obtaining these returns, Littlejohn sent them to ProPublica, an online nonprofit newsroom, which published more than 50 stories using the data.

Under federal law, the IRS was required to notify each taxpayer affected by the data breach "as soon as practicable." However, the IRS did not send notifications to the affected taxpayers until April 12, 2024 – more than four years after the data breach occurred, and months after Littlejohn's sentencing

hearing.

TAKE ACTION

If you received a letter from the IRS (Letter 6613-A) enclosing a copy of the criminal charges against Littlejohn, it means you were a victim of his illegal actions. To protect yourself from this unprecedented breach of the public trust, we recommend the following actions:

1. **Consider Applying for an Identity Protection PIN**. A common crime following data theft involves using a taxpayer's social security number to file fraudulent tax returns requesting large refunds. An Identity Protection PIN (IP PIN) can help protect you from this scheme. After you obtain an IP PIN, criminals cannot file an income tax return under your name without knowing your identification number, which changes annually. Learn more and apply for an IP PIN here.
2. **Request and Review Your Tax Transcript**. The IRS maintains a transcript of all your tax-related matters, including filings, payments, refunds, extensions and official notices. Regularly reviewing your tax transcript (*e.g.*, every six to 12 months) can reveal fraudulent activity while there is still time to take remedial action. Request a copy of your tax transcript here. If you have questions about your transcript or need help obtaining it, we are available to assist you.
3. **Obtain Identity Protection Monitoring Services**. Applying for an IP PIN and regularly reviewing your tax transcript will help protect you from tax fraud, but it will not protect you from other criminal activities, such as fraudulent loan applications. To protect yourself from these other risks, you should obtain identity protection monitoring services from a reputable provider.
4. **Evaluate Legal Action**. Data breach victims should consider taking legal action against Littlejohn, the IRS and anyone else complicit in his wrongdoing. Justifiably, most victims will not want to suffer the cost, aggravation and publicity of litigation, but for those concerned with the public tax system's integrity, litigation is an option.

In fact, litigation against the IRS is already underway. On December 13, 2022, Kenneth Griffin, the founder and CEO of Citadel, filed a lawsuit against the IRS in the US District Court for the Southern District of Florida after discovering his personal tax information was unlawfully disclosed to ProPublica. In his complaint, Griffin alleges that the IRS willfully failed to establish adequate safeguards over confidential tax return information – notwithstanding repeated warnings from the Treasury Inspector General for Tax Administration and the US Government Accountability Office that the IRS's existing systems were wholly inadequate. Griffin is seeking an order directing the IRS "to formulate, adopt, and implement a data security plan" to protect taxpayer information.

The future of Griffin's lawsuit is uncertain. Recently, the judge in his case dismissed one of his two claims and cast doubt on the theories underpinning his remaining claim. It could be years before a final decision is entered.

Although Griffin is leading the charge, joining the fight would bolster his efforts and promote the goal of ensuring the public tax system's integrity. A final order in Griffin's case will be appealable to the US Court of Appeals for the Eleventh Circuit. A decision there will be binding on both the IRS and taxpayers who live in Alabama, Florida and Georgia. However, the IRS could also be bound by orders entered by other federal courts arising from lawsuits filed by taxpayers who live elsewhere. Because other courts may disagree with the Eleventh Circuit, taxpayers living in other states could file their own lawsuits against the IRS in case Griffin does not prevail.

Victims of the IRS data breach who are interested in taking legal action should act quickly. Under the Internal Revenue Code, a lawsuit must be filed within two years after the date the taxpayer discovered the data breach.

© 2025 McDermott Will & Emery

National Law Review, Volume XIV, Number 115

Source URL:https://natlawreview.com/article/protect-yourself-action-steps-following-largest-ever-irs-data-breach