

Protect Yourself From Tax Fraud

Admin User · April 4, 2026

The recent NPD data breach could impact your tax refund and increase your risk of identity theft. With tax season coming up, here's how to protect yourself.

By Kevin Knull

Imagine this: You and your spouse have been diligent savers, carefully planning for your work-optional phase. Typically, you apply for an extension and file your personal tax returns in October instead of April. Your spouse runs a profitable small business, generating about half of your family income, and the SEP IRA has been a fantastic way to enhance your retirement savings and growth plan. This year, your CPA delivers great news – you'll be receiving a tax refund of approximately \$20,000 from the IRS and about \$5,000 from the state. This unexpected windfall means you can boost your emergency fund and finance your annual ski trip.

However, when your CPA files your tax return, you're stunned to discover that the IRS claims you've already filed and received your refund! How is this possible?

The shocking answer emerges: In the summer of 2024, the National Public Data (NPD) Corporation reported that they exposed 272 million taxpayer identification numbers (TINs) and 2.9 billion records, marking the second-largest data breach in history. This breach significantly heightened the risk of tax-related identity theft, leaving most taxpayers – like you – vulnerable to fraudulent tax return filings and other financial abuses. Now, you must navigate the aftermath of this fraud and take steps to protect your financial identity moving forward.

Safeguarding Your Finances After a Data Breach

The NPD breach is a significant concern for everyone, as the exposure of sensitive information, including TINs, names, addresses and phone numbers, can lead to long-term financial risks. In addition, passwords to internal systems were inadvertently shared, further compromising taxpayer data. The need for stronger protection strategies is more critical than ever. Beyond simple credit monitoring, taxpayers should prioritize enhanced

security measures, stay informed through ongoing education, and leverage technology-driven solutions to safeguard their financial future from the growing threats of data breaches.

The Growing Threat of Tax Fraud Post-Data Breach

One of the most serious consequences of identity theft following the NPD breach is the heightened risk of fraudulent tax returns. Criminals can exploit stolen TINs to file fake returns, often claiming large refunds long before the legitimate taxpayer even becomes aware. If a fraudster files a fake return before the taxpayer, then the IRS may not detect the fraud until the legitimate return is filed, leaving the taxpayer to navigate the complex process of resolving the issue while the fraudulent refund is already long gone.

The IRS has been working to combat this type of fraud through its Stolen Identity Refund Fraud (SIRF) initiatives. In 2023, the IRS flagged over 5 million suspicious returns and blocked \$8 billion in fraudulent claims. However, with the massive number of TINs exposed in the NPD breach, 2025 is poised to see an even greater volume of fraudulent activity, especially at the start of the tax season on January 2, 2025. Taxpayers must be vigilant to protect themselves and act quickly if they suspect fraud.

The Risks of ID Theft for Taxpayers and Business

The misuse of TINs extends well beyond fraudulent tax refunds. Fraudsters can exploit stolen TINs to commit various forms of fraud, including opening unauthorized credit accounts, securing employment (which results in real tax liabilities for the taxpayer) and applying for unemployment benefits or government assistance like Social Security and Medicare. When these fraudulent claims come to light, it's the legitimate taxpayer who must navigate the consequences – often facing long delays in receiving benefits or refunds. While you can often eventually recover a stolen tax refund, the process can take years to resolve.

For businesses, the exposure of Employer Identification Numbers (EINs) poses even greater risks. Fraudsters can leverage EINs to perpetrate large-scale financial crimes, leading to unauthorized tax filings or loans the business never applied for. These incidents can inflict serious financial harm, disrupt business operations, and tarnish the company's reputation.

Protecting Yourself from Tax-Related Identity Theft

Safeguarding against tax-related identity theft requires a proactive approach that

combines enhanced security practices, fraud prevention education and better monitoring of financial accounts. Taking these steps can significantly reduce the risk of falling victim to fraud.

Key Strategies for Protection:

1. **Enhance Your Security Practices:** Strengthen your digital security by using unique, complex passwords and enabling multi-factor authentication for your financial and tax accounts. These measures make it harder for criminals to gain unauthorized access.
2. **Review IRS Notices Regularly:** Pay close attention to any IRS notices you receive, as they can be early indicators of fraudulent activity. Catching suspicious correspondence early may prevent further fraudulent filings.
3. **Monitor Financial Accounts:** Regularly review your bank and credit accounts for any unusual activity. Although this isn't directly related to taxes, monitoring your finances closely can help identify fraud across all of your accounts.
4. **File Tax Returns Early:** Submitting your tax return early minimizes the window for fraudsters to file a false return in your name. This proactive approach helps safeguard your rightful refund.

Leveraging Technology for Enhanced Fraud Protection

While traditional fraud monitoring and prevention methods remain crucial, incorporating technology-driven solutions can significantly elevate your level of protection. Some platforms now offer real-time visibility into IRS account activity, enabling early detection of suspicious actions such as unauthorized tax return filings, unexpected refunds or address changes. These systems can also notify you of any IRS fraud alerts, allowing you to act quickly.

When used as part of a comprehensive strategy, these tools provide an additional layer of security by offering alerts on unusual activity, which enables faster responses to potential threats.

It's essential to emphasize that technology should supplement – not replace – standard financial security practices. A proactive, layered approach combining both technology and traditional methods remains the most effective defense against identity theft.

Partnering with Your Financial Adviser to Prevent Tax Fraud

Your financial adviser or CPA plays a crucial role in helping you safeguard against tax fraud. By working together, you can implement a technology-driven solution that integrates directly with the IRS to monitor your IRS account activity in real time. This platform gives both you and your adviser immediate access to your tax records, allowing for continuous oversight.

With this active monitoring, your adviser can promptly identify suspicious behavior and address potential threats before they escalate into serious issues. By catching fraudulent activity early, you can prevent significant financial damage and streamline any necessary corrective measures.

Expanding your fraud prevention strategy by involving your adviser helps you build a stronger defense. Advisers can act as vigilant front-line protectors, enhancing your efforts to shield yourself from tax fraud. Speak with your adviser today about collaborating on a technology-driven solution to prevent tax fraud.

A Call for Vigilance: Taxpayers Must Proactively Protect Themselves

The NPD breach serves as a stark reminder of the vulnerabilities present in today's digital landscape. This incident highlights the urgent need for taxpayers to take proactive measures in safeguarding themselves against tax-related fraud. By combining education, robust security practices, and technology-driven solutions, individuals can effectively mitigate the risks posed by breaches and protect their financial identities.

In a world where cyber threats are constantly evolving, it's crucial to implement these suggested steps to prevent tax-related identity theft. Expand your fraud prevention strategy by integrating technology-driven solutions into your protection strategies and engaging your financial adviser or CPA to bolster your defenses against tax fraud. Now is the time to take action and protect yourself.

About the author: Kevin Knull, CFP

Kevin Knull, CFP®, is president of [TaxStatus](http://www.TaxStatus.com) (www.TaxStatus.com) and a certified financial planner focused on elevating the quality of advice in the financial services industry. TaxStatus provides frictionless, continuous IRS account monitoring and consent-based access to IRS tax records for financial professionals and the clients they serve.
