Tax identity theft: Businesses are at risk, too

Tax identity theft isn't limited to individual taxpayers — businesses are also targeted through their Employer Identification Numbers (EINs), payroll systems and tax filings. The financial impact of these crimes can be significant. Businesses may face delayed or stolen tax refunds, unauthorized payroll filings, and the time and expense of resolving IRS issues. There may even be credit damage or, if employee or customer data is compromised, reputational harm. Here's what you need to know to protect your business.

How tax identity theft happens

Business tax identity theft comes in many forms and can affect sole proprietors, corporations, partnerships and limited liability companies. For example, criminals may file fraudulent returns using a company's EIN, impersonate executives to steal employee W-2 data, or use forged IRS documents to pose as a business for financial or tax-related activity. In more advanced cases, hackers combine stolen data from breaches with synthetic identities to create entirely fake businesses capable of filing returns and securing credit.

These schemes often go undetected until the IRS rejects a legitimate tax filing or flags duplicate activity. Other warning signs may include rejected extension requests, unexpected IRS transcripts or notices, or missing IRS correspondence.

You also might receive a Letter 5263C or 6042C from the IRS. If your business receives one of these notices, don't panic — it may stem from an IRS verification issue or a filing inconsistency, such as transposed numbers on your return. But it could signal something more serious. So contact your tax advisor to help answer all the questions in the letter within the timeframe specified in the notice (typically within 30 days). In some cases, the IRS may require you to file Form 14039-B, "Business Identity Theft Affidavit," to report suspected identity theft.

How to protect your business

Tax identity theft can be costly, so prevention and early detection are critical. Consider the following seven security measures to help protect your business:

1. Prioritize cybersecurity. Your business should have a formal cybersecurity plan that provides a step-by-step approach for detecting identity theft. When breaches happen, your plan should trigger a prompt, thorough response. Review your plan regularly and update it to reflect changes in your business operations and emerging cyber risks.

2. Safeguard sensitive business data. Store employee and customer data, along with other proprietary records, such as financial statements and prior years' tax returns, in a secure location. Keep your EIN information up to date with the IRS, including the responsible party and contact details. Shred nonessential documents before throwing them out, and limit access to your EIN to parties with whom you initiated the contact. Share sensitive information via the internet or email only if the recipient is trusted (such as your lender or tax preparer) and the site is secure or the email is encrypted.

3. Guard your logins and passwords. Some businesses store account logins and passwords in a single location, which can be convenient but risky. If a dishonest employee or hacker gains access, they could reach sensitive systems, including those tied to your EIN and tax filings. Use strong security controls to protect this information.

4. Use the latest cybersecurity technology. This includes firewalls, antivirus and antimalware software, spam filters, encryption and multi-factor authentication. Also exercise common sense: Don't download files, click links or open attachments sent from unknown sources. It's also prudent to back up sensitive data to a secure, external source not connected to your network.

5. Educate employees. Conduct periodic training sessions to remind employees about the latest scams, such as phishing emails that impersonate familiar businesses or colleagues to steal sensitive information. Employees should be aware of your cybersecurity plan and each person's role if a breach occurs. Also remind them that the

IRS doesn't initiate contact by telephone, email, text or social media to request sensitive information.

6. Monitor business credit reports. It doesn't take much effort to monitor your company's profiles from the three major business credit bureaus: Equifax, Experian and TransUnion. Subscribe to their monitoring services and real-time alerts for suspicious activity, which may signal unauthorized accounts or broader identity theft affecting your business.

7. Secure your tax filings and accounts. Work with a trusted tax professional and use secure portals to share tax documents. Review IRS notices promptly and investigate any rejected filings, unexpected transcripts or unusual activity tied to your EIN.

Be proactive, not reactive

No preventive measure is 100% fail-safe, so identifying suspicious activity is also critical. Uncovering identity theft early makes it easier to address.

Contact us if you have questions about protecting your business's tax filings, employee tax data or IRS account information. We can help you review your risks, implement practical data security measures and determine the next steps if something looks suspicious.