IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

IRS highlights International Fraud Awareness Week; taxpayers urged to protect against scams, schemes

IR-2023-212, Nov. 13, 2023

WASHINGTON – As part of ongoing efforts to protect taxpayers, the Internal Revenue Service reminds people that International Fraud Awareness Week serves as an important time to protect personal and financial information from scam artists and tax schemes.

International Fraud Awareness Week, which runs through Nov. 18, is an effort to minimize the impact of fraud through awareness and education. During the special week, the IRS – including the agency's Office of Fraud Enforcement and IRS Criminal Investigation – continue working to raise awareness to fraud and scams affecting taxpayers across the country.

The IRS continues to encourage individuals, businesses and tax professionals to take time now to know the red flags of a scam, and to ensure defenses are in place to stop scammers and those who promote unscrupulous tax schemes.

Although this special week highlights international fraud, the IRS works throughout the year to raise awareness about tax scams and schemes. These efforts range from the annual Dirty Dozen list of tax scams to other tax schemes, including aggressive marketing involving Employee Retention Credit claims. In addition, the IRS, state tax agencies and the nation's tax industry work together in the Security Summit initiative to protect taxpayers, businesses and the tax system from identity thieves and related scams.

"During this special week, the IRS reminds taxpayers that we are on their side and looking out for them," said IRS Commissioner Danny Werfel. "Our work on tax scams and schemes reflects this commitment. IRS employees are working to protect honest taxpayers from scam artists, raising awareness about emerging issues and rooting out the nefarious actors that perpetrate them. With modernization funding in place, the IRS is well positioned to disrupt scams as part of our transformation efforts."

IRS Office of Fraud Enforcement: Shining a light on fraud

The IRS Office of Fraud Enforcement (OFE) promotes compliance with tax laws by strengthening the IRS response to fraud and mitigating emerging threats. This includes improving fraud detection, identifying areas of high risk, enhancing enforcement and helping develop and submit fraud referrals to IRS Criminal Investigation where appropriate.

During International Fraud Awareness Week, the IRS reminds taxpayers to be especially wary of scammers and promoters of bogus tax schemes aimed at reducing taxes or avoiding them altogether.

Many of these tax avoidance schemes are included in the 2023 IRS Dirty Dozen list and often involve unscrupulous asset protection professionals or promoters who lure people into placing their assets in offshore accounts and structures.

These promoters often sell their scams by promising that assets are out of the government's reach. They may also suggest that digital assets are untraceable and undiscoverable by the IRS and that the transactions are anonymous. In fact, the IRS has a vast array of tools to combat offshore tax evasion, including working with its international treaty partners to identify and track assets, transactions and evidence.

Improper Employee Retention Credit claims

The IRS has seen a high volume of incorrect and improper Employee Retention Credit claims and continues warning taxpayers about them. The ERC, sometimes also called the Employee Retention Tax Credit or ERTC, is a pandemic-related credit for which only certain employers qualify. The credit is not

available to individual employees.

Scam promoters are luring people to incorrectly claim the ERC with “offers” online, in social media, on the radio or through unsolicited phone calls, emails and even mailings that look like official government letters but have fake agency names and usually urge immediate action.

These unscrupulous promoters make false claims about their company’s legitimacy and often don’t discuss some key eligibility factors, limitations and income tax implications that affect an employer’s tax return.

It’s important to watch for warning signs such as promoters who say they can quickly determine someone’s eligibility without details, and those who charge up-front fees or a fee based on a percentage of the ERC claimed.

Anyone who incorrectly claims the ERC must pay it back, possibly with penalties and interest.

The only way to claim the ERC is on a federal employment tax return. The IRS continues to warn employers to not fall for aggressive marketing or scams related to the ERC. Employers should first check with their trusted tax professional before submitting an ERC claim, and the IRS has developed a special Employee Retention Credit Eligibility Checklist and Frequently Asked Questions to help people quickly determine if they might be eligible.

As part of a larger effort to protect small businesses and organizations from scams, the Internal Revenue Service created a special withdrawal process to help those who filed an ERC claim and now want to withdraw it. This new withdrawal option allows certain employers that filed an ERC claim but have not yet received, cashed or deposited a refund to withdraw their submission to avoid future repayment, interest and penalties.

The new withdrawal process follows an immediate moratorium, announced by the IRS on Sept. 14, 2023, on processing new ERC claims. The moratorium, which will last until at least the end of this year, follows concerns about ineligible ERC claims.

Know the red flags

IRS impersonation scams involve fake text messages, social media accounts, e-mail and phone calls. Knowing what to watch out for can help keep taxpayers safe.

Remember, the IRS **does not**:

- Initiate unexpected contact with taxpayers by email, text messages or social media channels to request personal or financial information.
    - Scammers attempt to use these methods of contact to con individuals, businesses, payroll and tax professionals into providing personal information, PINs, passwords and other data.
    - If a taxpayer receives an unsolicited SMS/text that appears to be from either the IRS or a program closely linked to the IRS, the taxpayer should copy the entire message and send it as an attachment to phishing@irs.gov.
- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer. The IRS does not use these methods for tax payments.
- Threaten to immediately bring in local police or other law-enforcement groups to have the taxpayer arrested for not paying.
- Demand that taxes be paid without giving the taxpayer the opportunity to question or appeal the amount owed.
- Ask for credit or debit card numbers over the phone.
- Leave pre-recorded, urgent or threatening phone messages.

- In many variations of the phone scam, victims are told if they do not call back, a warrant will be issued for their arrest. Other verbal threats include law-enforcement agency intervention, deportation or revocation of licenses.
- Criminals can fake or "spoof" caller ID numbers to appear to be anywhere in the country, including from an IRS office, which makes it difficult for taxpayers to verify the actual caller's number.
- Fraudsters have spoofed local sheriff's offices, state departments of motor vehicles, federal agencies and others to convince taxpayers the call is legitimate.
- Any taxpayer receiving a scam phone call should hang up immediately and not give out any information.
    - Contact the Treasury Inspector General for Tax Administration to report the call at IRS Impersonation Scam Reporting.
    - Report the caller ID and/or callback number to the IRS by sending it to phishing@irs.gov with the subject "IRS Phone Scam."

Watching for these common scams can keep people from becoming victims of identity theft. Individuals should protect their sensitive personal information that can be used to file fraudulent tax returns and steal refunds.

Small businesses are big targets

Businesses of all types and sizes, especially small businesses, need to be aware cybercriminals could target their businesses with scams to steal passwords, divert funds or steal employee information.

The IRS continues to see instances where small businesses, including tax professionals, face a variety of identity-theft related schemes that try to obtain information to file a business tax return or use customer data for identity theft.

Businesses, including tax professionals, are encouraged to follow best practices from the Federal Trade Commission, including to:

- Use multi-factor authentication.
- Set security software to update automatically.
- Back up important files.
- Require strong passwords for all devices.
- Encrypt devices.

In partnership with the IRS, the Security Summit initiative is at the forefront of protecting taxpayers, businesses and the tax system from identity thieves. Working together as the Security Summit, the IRS, state tax agencies and the nation's tax industry have taken numerous steps to warn people to watch out for common scams and schemes.

Report fraud

To report an abusive tax scheme or a tax return preparer, people should mail or fax a completed Form 14242, Report Suspected Abusive Tax Promotions or Preparers, and any supporting materials to the IRS Lead Development Center.

Mail:

Internal Revenue Service Lead Development Center
Stop MS5040
24000 Avila Road
Laguna Niguel, California 92677-3405
Fax: 877-477-9135

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Alternatively, taxpayers and tax practitioners may send the information to the IRS Whistleblower Office for possible monetary reward.

For more information, see Abusive Tax Schemes and Abusive Tax Return Preparers.

Resources

- Tax Scams and Consumer Alerts on IRS.gov.

-30-