

**JEANMARIE F. MOORE, CPA, CITP, AND SCOTT D. SCHINDEWOLF**  
Klatzkin

# It's tax season, beware of tax scams

# RISKS

**Insurance agents and other professional service providers must protect their client's sensitive data. This includes everything from their personal contact information to their Social Security number, bank account information, coverage and other types of sensitive information like the names of family members.**

All professional insurance agents should be held accountable for client data security. This can include simple measures like having all computers go into sleep mode, to requiring that laptops are locked away and never left in a potentially dangerous place such as a car.

Agents should never use public Wi-Fi, review a sensitive document in a public place, or share passwords with anyone. Make sure all your employees have a different password for every app they use in the course of doing business. Insurance agencies that are victims of a data breach can face financial, legal and other consequences if sensitive personal and financial client-related information is stolen. A data breach is just one type of a fraudulent scheme used to victimize agents and clients. The IRS and other officials frequently issue warnings on other fraudulent schemes.

## Popular tax scams

As published on the IRS's website ([www.irs.gov](http://www.irs.gov)) the following are typical tax scams that agents need to be aware of to provide guidance to their clients:

**Suspended or canceled Social Security number.** Con artists threaten to suspend or cancel the victim's Social Security number by stating that the victim owes the IRS money in taxes. Fraudsters frighten people into returning Robocall voicemails by threatening to cancel the person's Social Security number if the person does not pay the overdue taxes immediately. If someone receives a call threatening to suspend his or her Social Security number for an unpaid tax bill, the person should hang up the telephone. According to the IRS, fraudsters carrying out this scheme demand:

- immediate payment using a specific method such as a prepaid debit card, iTunes gift card or wire transfer;
- payment to a person or organization other than the U.S. Treasury; and/or
- the taxes be paid without giving the taxpayer the opportunity to question or appeal the amount owed.

The scammer also threatens to contact local police or other law-enforcement agencies to have the taxpayer arrested for nonpayment immediately.

*Advice for agents to their clients.*

Agents should advise their clients of this scam, and the fact that the IRS does not use any of these methods to collect tax payments. Nor will the IRS call to demand taxes to be paid immediately. Instead, the IRS mails a notice to address these situations. Agents also should advise clients to never give out sensitive information over the telephone unless they are positive the caller is legitimate.

**Impersonating the IRS.** IRS imposters have sent unsolicited emails to taxpayers. The email subject line may be a variation of "Automatic Income Tax Reminder" or "Electronic Tax Return Reminder." According to the IRS, the emails include links to a website that are similar to [www.irs.gov](http://www.irs.gov). These emails include false information regarding a taxpayer's refund, electronic return or tax account. The emails contain a "temporary password" to access the files, which is a malicious file.

*Advice for agents to their clients.*

Once again, agents should advise clients that the IRS does not send unsolicited emails and never emails taxpayers about the status of refunds.

**"Ghost" tax preparer.** This scheme involves a "ghost" preparer who is paid to prepare a taxpayer's tax return, but who refrains from signing the return (i.e., electronically or on paper). By law, anyone who prepares

or assists in preparing federal tax returns for compensation must have a valid Preparer Tax Identification Number.

Returns filed without a PTIN are considered self-prepared. Information on the return is assumed to have come from the self-preparer, including the bank routing and account numbers. Scammers submit their bank account information instead of the taxpayer's information. Then the refund is deposited into the perpetrator's account instead of the taxpayer's account.

*Advice for agents to their clients.* Agents should make clients aware that “ghost” preparers may require cash payment and then neglect to give a receipt. Advise clients to review their returns carefully and check that their direct deposit information is correct.

**Tax transcripts and other financial documents.** A surge of fraudulent emails impersonating the IRS, banks or other financial institutions uses tax transcripts or financial documents to encourage victims to open documents containing malware. Businesses fall victim, when an unsuspecting employee opens the malware. Entire networks can be infected, causing all kinds of issues and possible security breaches.

*Advice for agents to their clients.* Agents should advise employees and clients not to open attachments from people unless they are confident that the sender is legitimate. Educate employees and clients on how to identify fraudulent emails and establish rules on opening documents. Make sure to send information to clients using encrypted email.

**False pleads to help victims of natural disasters.** Criminals and scammers are known to take advantage of generous taxpayers who want to help victims of major disasters. The IRS warns taxpayers that fraudulent schemes usually start with unsolicited contact by telephone, social media, email, or in-person using a variety of tactics. Fake websites are used to impersonate legitimate charities and trick people into sending money or providing personal financial information. A scammer also may claim to work for, or on behalf of, the IRS to help victims file casualty loss claims and get tax refunds.

*Advice for agents to their clients.* Agents should remind clients to go directly to a legitimate charity's website by typing in its domain name. Never open a link sent via email or advertised online. It could lead to a fake site that is almost identical to the real one. To know if a website is secure, make sure the “lock” icon is present.

There are many other schemes that fraudsters use to victimize innocent people. The IRS publishes its “Dirty Dozen” list of the top 12 scams annually. The 2019 Dirty Dozen are:

1. Falsifying income and creating bogus documents
2. Inflating deductions or credits
3. Promises of inflated refunds
4. Tax return preparer fraud
5. Identity theft
6. Phone scams
7. Phishing
8. Charitable contribution scams


9. Improper claims for business credits

10. Failure to report offshore funds

11. Frivolous tax arguments

12. Abusive tax shelters, trusts, and conservation easements

Agents should consider sharing information on the latest scams, which have been identified by the IRS, with their clients as these schemes are brought to the attention of the public. Just one successful attack can put you or a client in a compromising position with significant financial consequences. Be diligent, mindful of questionable email or voice communication, conscientious about verifying that the sender is legitimate, and avoid opening suspicious emails or accepting suspicious telephone calls.

Agents can find information and useful guides on what to do if fraud is suspected at [irs.gov/identity-theft-fraud-scams](https://www.irs.gov/identity-theft-fraud-scams). Agents also should report instances of IRS-related phishing attempts and fraud to the Treasury Inspector General for Tax Administration at (800) 366-4484 or [tigta.gov](https://www.tigta.gov). Or, use The Federal Commission's FTC Complaint Assistant ([FTC.gov](https://www.ftc.gov)). Taxpayers who experience tax-related identity theft may file an Identity Theft Affidavit (Form 14039). 

*Moore is a certified public accountant and partner with Klatzkin with more than 30 years of experience in the field of accounting. She is the firm's technology partner and holds the Certified Information Technology Professional designation. Reach her at [jmoore@klatzkin.com](mailto:jmoore@klatzkin.com). Schindewolf is Klatzkin's IT Manager, responsible for oversight and management of the firm's IT infrastructure. Reach him at [sschindewolf@klatzkin.com](mailto:sschindewolf@klatzkin.com).*