



Identifying and Avoiding Tax Scams

Every year during tax season the Internal Revenue Service (IRS) releases the “[Dirty Dozen](#)” list of tax scams. With the increased number of data breaches, we encourage our clients to remain vigilant when sharing their personal data and responding to demands for tax payments. Here are some tips to help you avoid tax scams and identity theft.

You know it’s a tax scam if...

- You receive an unexpected deposit in your bank account from the U.S. Treasury and then receive a call from the IRS claiming to have made the deposit in error and asking that you return it to a third-party collection agency.
 - Do not return the money to the scammer. You may be a victim of identity theft. Contact your tax return preparer and your financial institutions. See [Protecting Your Credit After a Data Breach](#).
 - The scammer may have filed a fraudulent tax return in your name and directed the improper refund into your account.
 - If so, follow these instructions to return the money directly to the U.S. Treasury: [Tax Topic Number 161 - Returning an Erroneous Refund](#).
 - Note that if a fraudulent tax return has already been filed in your name for this year, you may have to file your actual return on paper rather than electronically. You may also have to attach an [Identity Theft Affidavit](#).
- You receive an unexpected phone call claiming to be from the IRS, demanding immediate payment of a tax bill and perhaps threatening arrest or other negative consequences if you do not. They may also demand that you provide personal information.
 - The IRS never calls a taxpayer to initiate an audit or demand personal information. The IRS always sends letters via the U.S. Postal Service. A lengthy period of correspondence must take place before the IRS can legally demand any payment.
 - Bogus callers may use fake caller ID numbers, IRS titles, employee identification numbers, and even websites to make themselves seem official. They may also be in possession of your stolen personal or financial information and try to use that to trick you into thinking they are legitimate.
 - Never send a tax payment to a third party. All tax payments should be sent directly to the U.S. Treasury.

For more information about what to do in this situation, including how to confirm that certain IRS correspondence is genuine, see [Report Phishing and Online Scams](#).





You can report tax scams here:

- The Treasury Inspector General for Tax Administration (TIGTA): online at "[IRS Impersonation Scam Reporting](#)" or by calling 800-366-4484.
- The Federal Trade Commission: online at "[FTC Complaint Assistant](#)".
- Report an unsolicited email claiming to be from the IRS, or an IRS-related component like the Electronic Federal Tax Payment System, to the IRS at phishing@irs.gov.
- For more information see [Report Phishing and Online Scams](#).

Contact Us

For more information, please contact a member of our Private Client Group, or the author of this advisory:

Paul M. Cathcart, Jr.
617.557.9737
pcathcart@hembar.com

Charles R. Platt
617.557.9757
cplatt@hembar.com

Private Client Group

Brad Bedingfield
Joseph L. Bierwirth, Jr.
Brian C. Broderick
Paul M. Cathcart
Dennis R. Delaney
Nancy E. Dempze
Mark B. Elefante
Kevin M. Ellis
Charles Fayerweather
Joan Garrity Flynn
Nancy B. Gardiner
Stephen W. Kidder
Harry F. Lee
Edward Notis-McConarty

Arthur B. Page
Charles R. Platt
Michael E. Porter
Michael J. Puzo
John J. Siciliano
Kurt F. Somerville
Sarah M. Waelchli

Of Counsel
Timothy F. Fidgeon
Frederic J. Marx
R. Robert Woodburn, Jr.
Raymond H. Young

www.hembar.com

Copyright © 2018 Hemenway & Barnes LLP

This advisory is provided solely for information purposes and should not be construed as legal advice with respect to any particular situation. This advisory is not intended to create a lawyer client relationship. You should consult your legal counsel regarding your situation and any specific legal questions you may have.