WARNING: IRS PHONE SCAM

As of January 2016, more than 896,000 taxpayers reported to the Treasury Inspector General for Tax Administration ("TIGTA") that they received calls from individuals impersonating the IRS in an attempt to scam taxpayers. The TIGTA identified at least 5,000 victims who have lost an estimated $26.5 million from these scams.

"When you get a call from a party claiming to be the IRS, your first instinct is not to assume fraud. In fact, you're not really sure what to do because you assume the IRS only has legitimate reasons to contact taxpayers. We are issuing this Client Alert to put you on notice of these IRS scams and provide you with instructions if you are faced with one of these fraudulent situations," stated Emily A. Parker, Partner at Thompson & Knight and former Acting Chief Counsel and Deputy Chief Counsel for the IRS.

This Client Alert focuses on the IRS and TIGTA's warnings about these phone calls, including characteristics of the phone calls, typical IRS behavior, and what to do if you are contacted by one of these fraudulent callers.

Characteristics of the Fraudulent Call:

- Manipulating the Caller ID system and making the incoming phone call appear to be coming from the IRS.
- Sounding legitimate during the call's introduction by reciting a fake name, IRS badge number, and even the last four digits of the taxpayer's Social Security number.
- Telling the taxpayer that tax is immediately owed and should be paid through a prepaid debit card, wire transfer, or PayPal account.
- Demanding personal information from the taxpayer such as Social Security numbers, banking information, and contact information, and claiming that the information is needed to secure a refund for the taxpayer.
- Using an aggressive or hostile tone when demanding information from the taxpayer.
- Using threats of arrest, deportation, or other legal action to convince the taxpayer to give the caller what he or she wants.
- Sending a fake IRS e-mail to the taxpayer reiterating some of the information recited to the taxpayer during the call.

The IRS Will Never:

- Call to demand immediate payment over the phone, nor will the agency call about taxes owed without first having mailed you a bill.
- Threaten to immediately bring in local police or other law-enforcement groups to have you arrested for not paying.
- Demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe.
- Require you to use a specific payment method for your taxes, such as a prepaid debit card.
- Ask for credit or debit card numbers over the phone.

What to Do If You Receive a Call from Someone Claiming to be from the IRS:

- Do not give out any information. Hang up immediately.
- Contact TIGTA to report the call. Use their "IRS Impersonation Scam Reporting" webpage or call 800.366.4484.
- If you know you owe taxes, or you think you might owe taxes, call the IRS at 800.829.1040. If you know you do not owe taxes or have no reason to think that you owe any taxes, then call and report the incident to TIGTA at 800.366.4484.
- You can file a complaint using the FTC Complaint Assistant. If the complaint involves someone impersonating the IRS, include the words "IRS Telephone Scam" in the notes.

ADDITIONAL WARNING ABOUT E-MAIL PHISHING SCAMS

The IRS also warned taxpayers about different forms of e-mail phishing scams. The IRS reported an approximate 400 percent surge in phishing and malware incidents during the 2016 tax season. The scam is designed to trick taxpayers into thinking the e-mails are official communications from the IRS or others in the tax industry, including tax software companies.

Characteristics of an E-Mail Phishing Scheme:

- Seeking information related to refunds, filing status, confirmation of personal information, ordering transcripts, and verification of PIN information.
- Sending e-mails containing links that the taxpayer is encouraged to click. These e-mail links send taxpayers to sites designed to imitate an official-looking website, such as IRS.gov. The sites also may carry malware, which can infect the taxpayer's computer and allow criminals to access the taxpayer's files or track the taxpayer's keystrokes to gain information.

The IRS Will Never:

- Initiate contact with you by e-mail or any other type of electronic communication, such as text messages, emails, pop-up messages, and social media channels to request personal or financial information.
- Ask for your PIN, passwords, or similar confidential access information for credit card, bank, or other financial accounts.

What to Do If You Receive a Phishing E-Mail:

- Do not reply to the message.
- Do not give out your personal or financial information.
- Forward the e-mail to phishing@irs.gov, then delete it.
- Do not open any attachments or click on any links. They may have malicious code that will infect your computer.

Please contact the Thompson & Knight attorney with whom you regularly work or any of the following attorneys to discuss the information contained in this Client Alert.

CONTACTS:

Mary A. McNulty
214.969.1187
Mary.McNulty@tklaw.com

Emily A. Parker
214.969.1502
Emily.Parker@tklaw.com

Roger D. Aksamit
713.951.5885
Roger.Aksamit@tklaw.com

John R. Cohn
214.969.1420
John.Cohn@tklaw.com

Todd D. Keator
214.969.1797
Todd.Keator@tklaw.com

Jana M. Benson
214.969.1706
Jana.Benson@tklaw.com