**Beware of Tax Scams**

Dear [Client Name],

I hope this letter finds you well. As your trusted tax professional, I am writing to inform you about the increasing prevalence of tax scams and to provide you with important information to help protect you from becoming a victim.

Tax scams are becoming more sophisticated and can target anyone, regardless of their financial situation. It is essential to remain vigilant and informed to safeguard your personal and financial information. Below, I have outlined some common tax scams and provided tips on how to recognize and avoid them.

**Common Tax Scams**

**IRS Impersonation Scams:** Scammers pose as IRS officials and contact taxpayers via phone, email, or mail, demanding immediate payment for taxes. They often use threats of arrest, deportation, or license revocation.

**What to do**: The IRS will never call you to demand immediate payment. If you receive such a call, hang up immediately and report it to the Treasury Inspector General for Tax Administration (TIGTA).

**Refund Scams**: The scammer contacts the victim, usually by phone, claiming to be from a retailer or online platform. They inform the victim of an unauthorized purchase and offer a refund. The scammer then requests personal information or remote access to the victim's computer to process the refund. In some cases, the scammer claims to have refunded too much money and asks the victim to return the excess amount, often via wire transfer or gift cards.

**What to do**: Do not provide personal information or remote access to your computer to unsolicited callers. Verify the legitimacy of the call by contacting the company directly using official contact information.

**Phishing Scams**: Fraudulent emails or websites trick recipients into providing personal information, such as Social Security numbers, credit card details, and passwords. These scams often appear as legitimate communications from financial institutions or the IRS.

What to do: Do not click on links or download attachments from unknown or suspicious emails. Always verify the sender’s identity.

**Tech Support Scams**: Scammers pretend to be tech support from well-known companies, convincing victims that their computers are infected with viruses or malware. They gain remote access to the victim's computer and steal personal information or install malicious software.

**What to do**: Never grant remote access to your computer to unknown individuals. Contact the company directly using official contact information.

**Tax-Related Identity Theft**: Scammers use stolen personal information to file fraudulent tax returns and claim refunds. Victims usually discover the scam when they try to file their legitimate tax return and find that one has already been filed in their name.

**What to do**: File your tax return as early as possible. If you suspect identity theft, contact the IRS immediately.

If you receive any communication claiming to be from the IRS or another tax authority, please do not respond or provide any personal information. Instead, contact me directly at [Your Phone Number] or [Your Email Address] for verification and assistance.

Your security and peace of mind are my top priorities. By staying informed and cautious, we can work together to prevent these scams from affecting you and your family.

**If you know anyone who has been scammed or is having any issues with the IRS please have them contact me as soon as possible.**

Sincerely,

[Your Name]

[Your Title]

[Your Company Name]