Client Notification Letter — Telephone Scam

<Date>

<Client Representative>
<Client Name>
<Client Address>

RE: Telephone Scam

Dear <Client Representative>,

The Internal Revenue Service (IRS) continues to warn taxpayers to guard against sophisticated and aggressive phone scams targeting taxpayers, as reported incidents of this crime continue to rise nationwide. Each year, millions of individuals have their identities stolen, and these phone scams are yet another opportunity for potential identity theft to occur.

It is important to remember that the IRS follows certain procedures that are designed to protect the privacy of taxpayers and does not initiate contact with taxpayers via phone or email asking for personal or financial information. As such, it is essential that you always be alert to potential identity theft if you receive a call or email from someone claiming to be an IRS agent or a member of the Criminal Investigation Division (CID) of the IRS.

What is the typical scenario for these scam calls?

The IRS has noted a few patterns in these calls, such as:

- Scammers use fake names and IRS badge numbers. They generally use common names and surnames to identify themselves.
- Scammers may recite the last four digits of your Social Security number.
- Scammers "spoof" or imitate the IRS toll-free number on caller ID to make it appear that it's the IRS calling.
- Scammers sometimes send bogus IRS emails to some potential victims to support their bogus calls.
- Potential victims sometimes hear background noise of other calls being conducted to mimic a call center.
- After threatening potential victims with jail time or a driver's license revocation, scammers hang up; others soon call back pretending to be from the local police or Department of Motor Vehicles, and the caller ID supports their claim.

What should I do if I receive one of these scam calls?

If you get a phone call from someone claiming to be from the IRS, hang up immediately and **do not**, under any circumstances, provide any information over the phone to the caller. If you are not sure whether you have a legitimate tax issue outstanding, you can contact the IRS directly at 1-800-829-1040, or if you prefer, you can contact our firm for assistance.

Where do I go if I think I have been the victim of this scam?

If you have received a phone call from someone claiming to be from the IRS or the CID, report the incident to the Treasury Inspector General for Tax Administration (TIGTA) at 1-800-366-4484. If you've been targeted by this scam, you should also contact the Federal Trade Commission and use their "FTC Complaint Assistant" at FTC.gov and add "IRS Telephone Scam" to the comments of your complaint. In addition, there are a number of other steps you might want to take immediately to protect your assets and banking accounts as well as your personal identification. Please see the attached list for steps to take if you believe that your Social Security number may have been compromised.

As always, please feel free to call me if you have any questions.

Sincerely,

_____
<Accountant Name>

Steps to Take If You Believe That Your Social Security Number May Have Been Compromised

1. Verify that the Social Security Administration ("SSA") has all of your current information (address, telephone number, employer if applicable, etc.) on file by calling 1-800-772-1213. Follow any steps necessary to correct the information on file.

2. If the SSA's current information matches yours, call the IRS identity theft hotline at 1-800-908-4490 to determine whether a return was filed using your Social Security number. In the event a false return has been filed, follow any suggestions the Service makes.

3. Verify your address with the IRS. If you need to change the address, File IRS Form 8822 – Change of Address to update the Service's records.

4. If you would like the IRS to mark your account to identify questionable activity, file IRS Form 14039 – Identity Theft Affidavit.

5. Consider requesting a copy of a fraudulent return with IRS Form 4506.

6. Contact your financial institutions regarding a fraud alert and take appropriate actions advised by the institutions.

7. Contact at least one of the three credit bureaus to place a fraud alert and get a free copy of your credit report with that agency:

    a. Equifax: 1-800-525-6285, or https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp

    b. Trans Union: 1-800-680-7289, or http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page

    c. Experian: 1-888-397-3742, or https://www.experian.com/fraud/center.html

You are permitted one free credit report per bureau per year. You may want to space out the reports requested from the individual credit bureaus in order to maximize your monitoring efforts. Initially, a 30–60–90 day window for actual fraud or ID theft is very helpful. In subsequent years, request a report from a different agency approximately every 3–4 months.

8. Review your credit report for inquiries from companies you have not contacted, accounts you did not open, and debts on your accounts that you cannot explain.

9. Contact the Federal Trade Commission: https://www.ftccomplaintassistant.gov/ or 1-877-438-4338.

10. File a police report with local law enforcement.