Letterhead

[date]

[name]
[address]
[address]

NOTICE OF DATA BREACH

Dear [name]:

We are writing to provide you with information about suspicious activity involving some MSA Accounting, CPA Professional Corp. clients.

What Happened?

After receiving reports that some MSA Accounting, CPA Professional Corp. clients or their employees have received letters from the IRS telling them that someone had filed or attempted to file a 2016 tax return that was not authorized and experiencing unusual activity during this filing season with an escalated number of rejected returns, we immediately changed all of our passwords as a precaution. Further, we notified the IRS of the activity and contacted local IT professionals who ran 'deep scans' on our system. The scans found *no* malicious activity. As a further precautionary measure, we hired specialized forensic IT consultants to investigate.

On April 11, 2017, the specialized forensic IT firm completed its investigation, including a thorough examination of all 8 of our network systems and available network logs. The specialized forensic IT firm found no evidence of a breach of the security of our network. Although no breach was found, however, given the activity some clients experienced, we wanted to notify you of the events.

What Information Was Involved?

If you are an individual, this information on our system may have included your: name, date of birth, telephone number(s), address, Social Security number, all employment (W-2) information, 1099 information (including account number if provided to us), direct deposit bank account information (including account number and routing information if provided to us), and any supporting documents you may have provided including health care.

If you are an entity, this information on our system may have included your: company name, Federal Employer Identification Number, address, telephone number; employee and/or 1099-recipient information (including account number if provided to us); bank or brokerage account information if provided to us; and partner, shareholder/officer or beneficiary names, addresses, and Social Security numbers.

What We Are Doing.

We immediately changed all of our passwords as a precaution, notified the IRS of the suspicious activity, and contacted local IT professionals who ran 'deep scans' on our system, all of which have found *no* malicious activity. Further, we hired a specialized forensic IT firm to investigate and we have notified the FBI.

What You Can Do.

Given the nature of the information potentially involved, we recommend the following steps be taken:

1. Change all bank account numbers that you have provided to us, or at a minimum monitor all such bank activity. These would include direct deposit and electronic fund transfer account details or scanned copies of bank statements and form 1099's.

2. Establish free 90 day fraud alerts with the three credit reporting bureaus. Their telephone numbers and websites are:

Equifax P.O. Box 740241 Atlanta, GA 30374 1-888-766-0008 https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp	Experian P.O. Box 2104 Allen, TX 75013 1-888-397-3742 https://www.experian.com/fraud/center.html	TransUnion P.O. Box 2000 Chester, PA 19022 1-800-680-7289 http://www.transunion.com/fraud-victim-resource/place-fraud-alert

3. Consider placing a credit freeze on your accounts which will make it more difficult for someone to open an account. For more information visit: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

4. If you suspect identity theft, report it to the Federal Trade Commission at https://identitytheft.gov and law enforcement. The FTC also provides detailed and specific information about identity theft at their website, which we recommend you review.

Lastly, you are entitled to a free credit report every year from each of these agencies at: www.annualcreditreport.com

For More Information.

In our 28 years of business, this is our first direct encounter with potential unauthorized access to our system. Protecting your information is incredibly important to us, as is addressing this matter with the information and assistance you may need. If you have any questions or concerns, please do not hesitate to call us at (951) 735-6266, e-mail at moni@msacpatax.com, or write us at 2960 Tarocco Drive, Corona, California 92881.

Very truly yours,

MSA Accounting, CPA Professional Corp.

Further Information about Identity Theft Protection

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax:	1-888-766-0008, www.equifax.com
Experian:	1-888-397-3742, www.experian.com
TransUnion:	1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.