[[COMPANY] LETTERHEAD]

[Insert name]
[Insert address]

Notice of Data Breach

Dear [**Insert name**],

Mark Schaefer Associates, LLP ("MSA") was recently the victim of a break-in resulting in the theft of two external hard drives which may have contained certain personal information about you. This information was maintained by MSA in connection with the accounting services it provides to individuals and employers. We are providing this notice to inform you and other potentially affected individuals of the incident and to call your attention to steps you can take to help protect yourself and your personal information. We apologize for any inconvenience this may cause you and assure you we are working diligently to address this incident.

What Happened
On September 9, 2017, MSA discovered it was the target of a break-in which resulted in the theft of two external hard drives among other low value items which do not have the capability to store information or data. The hard drives, which were maintained under lock and key, may have included certain data elements of personal information for MSA's clients and/or the employees of MSA's clients.

What Information Was Involved
The personal information subject to this incident may include name, address, Social Security number, and financial information from prior to 2013. Based on the other items stolen as part of the break-in, it appears the hard drives were targeted for their street value as opposed to the data contained therein.

What We Are Doing
Immediately upon discovering the break-in and theft, we commenced an investigation to define the scope of this incident and determine what, if any, personal information may have been maintained on the hard drives. As a result of the incident, we filed a police report with the Pasadena Police Department. Additionally, we worked with our internal response team to recreate the data on the hard drives in an effort to obtain relevant contact information for those potentially affected.

As an added precaution, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion® , one of the three nationwide credit reporting companies. **To receive these services you must enroll within 60 days of the date of this letter.**

To enroll in this service, go to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the Activation Code provided at the top of this letter, and follow the three steps to receive your credit monitoring service online within minutes. If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one yearof unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

We treat all sensitive client information in a confidential manner and are proactive in the careful handling of such information. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring. Theft of data and similar incidents are difficult to prevent in all instances, however, we will be reviewing our systems and making improvements where we can to minimize the chances of this happening again.

What You Can Do

We are sending this advisory to you and other individuals to make you aware of this incident so that you can take steps to protect yourself and minimize the possibility of misuse of your information. In addition to enrolling in the credit monitoring service mentioned above, set forth below are steps you can take to protect your identity, credit and personal information.

For More Information

If you have questions or concerns you should call [Insert Number] from 6:00 am to 6:00 pm Pacific Time, Monday through Friday. Again, we apologize for this situation and any inconvenience it may cause you.

Sincerely,

[Insert name and title]

What You Should Do to Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to avoid identity theft, obtain additional information, and protect your personal information:

1. Contacting the nationwide credit-reporting agencies as soon as possible to:

- Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. To place a 90 day fraud alert on your credit file, log into the Equifax Member Center and click on the fraud alert tab, visit www.fraudalerts.equifax.com or call the auto fraud line at 1-877-478-7625, and follow the simple prompts. This fraud alert will remain on your credit file for 90 days.
- Place a "security freeze" on your credit account. This means that your credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, you must write by certified or overnight mail (see addresses below) to each of the three credit reporting agencies, or through the electronic or Internet method made available by the credit reporting agencies. Credit reporting agencies charge a $5 fee to place or remove a security freeze, unless you provide proof that you are a victim of identity theft, in which case there is no fee. A copy of your police report or an investigative report or written FTC complaint documenting identity theft must be included to avoid a fee. In your request, you also must include (documentation for both the spouse and the victim must be submitted when requesting for the spouse's credit report) (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial as well as Jr., Sr., II, III, etc.,) address, Social Security number, and date of birth; (iii) if you have moved in the past 5 years, the addresses where you have lived over the prior 5 years; (iv) proof of current address such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable (vi) payment by check, money order or credit card (Visa, Master Card, American Express or Discover cards only.)
- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
- Receive a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com/consumer	www.transunion.com

2. Contacting the Federal Trade Commission ("FTC") either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is:

   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580

3. If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

4. If you believe you are a victim of identity theft you should immediately report same to law enforcement and/or your state attorney general.

5. The IRS also offers Identity Protection: Prevention, Detection and Victim Assistance which can be found at: https://www.irs.gov/Individuals/Identity-Protection.

6. *North Carolina Residents*: The contact information for the North Carolina Attorney General is: Address: North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699; Telephone: (919) 716-6400; website: www.ncdoj.com/.

7. *New Mexico Residents*: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to http://consumersunion.org/pdf/security/securityNM.pdf