December 5, 2016

Dear [Recipient's Name]:

I value your business and respect the privacy of your information, which is why, as a precautionary measure, I am writing to let you know about a data security incident that occurred on November 15, 2016 and involves your personal information.

The breach involved an unknown and unauthorized person accessing and downloading client files saved on an online Citrix ShareFile server. The ShareFile system is password protected and used in the place of email to ensure that confidential information is accessed only by authorized parties. However, an unauthorized person hacked the Citrix system and accessed the information saved on their servers. The information accessed by the unauthorized person primarily includes QuickBooks files and summary statements of tax returns. More specifically, some of the information accessed includes client names, social security numbers, personal tax identification numbers, and mailing addresses. I am unsure at this time whether the information as accessed was encrypted on Citrix's server such that the data is unreadable, so I am giving this notice out of an abundance of caution.

I am working with law enforcement and forensic investigators and will notify you if there are further significant developments. I have implemented additional security measures, including an additional level of password protection, to prevent the reoccurrence of such a breach and to protect the privacy of my clients. With the assistance of an Information Technology professional, I have also conducted a thorough analysis of my office network files, and no breach to these files has been detected. Extensive diagnostic tests have confirmed that my personal systems have not been compromised in any way.

I am notifying you so you can take action to minimize or eliminate potential harm. I strongly advise you to take measures to help prevent and detect any misuse of your information.

As a first step, I recommend that you closely monitor your financial accounts. If you see any unauthorized activity, you should promptly contact your financial institution. If you see any unauthorized activity on your credit reports, I also suggest that you report any unauthorized activity to the Federal Trade Commission by calling 1-877-438-8228 (1-877-IDTHEFT) or online at www.identitytheft.gov.

As a second step, you may want to contact the three U.S. credit reporting agencies (Equifax, Experian, and TransUnion) to obtain a free credit report from each by calling 1-877-322-8228 or by logging onto www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends you check your credit reports periodically. Checking your credit reports periodically can help you spot a problem and address it quickly.

To protect yourself from the possibility of identity theft, Ariz. Rev. Stat. Ann. §44-1698 (2008) allows you to place a security freeze on your credit files. By placing a freeze, someone who

fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name.

You will need to contact the three U.S. credit reporting agencies to place the security freeze. When you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily or permanently lift the freeze.

To obtain a security freeze, contact the following agencies:

Equifax: 1-888-298-0045
TransUnion: Fraud Victim Assistance Department, P.O. Box 6790 Fullerton, CA 92834
Experian: Send an email to BusinessrecordsVictimassistance@experian.com

I will keep you informed of any developments in the investigation that may be of importance to you. If you have further questions or concern, please contact me at this telephone number 702-265-1159.

Sincerely,

Robin McQuown, CPA