[redacted]

Mr. Karberg,

I am writing to notify you of a possible email breach we have reason to believe occurred recently. In accordance with PIPA, I'm including along with this correspondence the email we are sending to our clients and an information page we're providing regarding what to do in the case of possible identity theft.

We are sending this correspondence to about 3000 clients, not all of whom are Maryland residents, but most are as we practice in MD and service MD, VA, and Washington DC along with some clients who have moved to other states, but still retain our services.

The nature of the breach

As close as we can gather, an email account was compromised and used to login in to the email system from an unknown location, giving access to all documents and emails in that account. It is not clear if it was just one email account or various. All accounts had password changes and have been migrated off site to office 365.

Remediation Efforts

Remediation includes migration to office 365 from an on premises hosted exchange system, with multi factor authentication being added as well. Additionally, state of the art anti virus has been secured in the form of Sophos virus protection, replacing Symantec software. Passwords to email accounts were also changed and made unique to that account only.

There is a possibility for next tax season of using a cloud based repository for tax documents instead of having them sent by email. This is being currently tested.

Thank you for your time.

Best
Josh Levine
Jeffrey Levine
Evan Levine

Subject Line: Levine TaxCo. Possible Email Security Breach

Dear Client,

We hope everyone is healthy and having a fun summer. We're writing because unfortunately we have reason to believe that our email system may have been breached. LevineTaxCo has a security firewall in place, but a recent fake email we received has prompted us to notify you of a potential data security breach.

This notice is being sent to you pursuant to the Personal Information Protection Act ("PIPA"), Md. Code Ann., Commercial Law §14-3504 to notify you of the potential data security breach and to provide information to help you protect yourself. Although the potential breach was through an email, it is possible that any financial or identity documents or information exchanged between you and our firm by email transmission may have been compromised.

While we can't know for certain that this happened and have no evidence of inappropriate use of your specific personal information, we are letting you know so you can be extra vigilant about your email inboxes regarding phishing and scam attempts you may receive and so you can take action to guard against any potential identity theft or fraud, including contacting the three major credit reporting companies.

We value our relationship with you and sincerely regret any inconvenience or concern this incident may cause. Keeping your personal data secure is of the utmost importance to us. To mitigate the chance of future security issues we've upgraded our system to leverage Microsoft Office 365 cloud-based email, which has built-in protections. Additionally, we'll be implementing a portal for document upload and delivery to keep documents out of the email system entirely.

We want to make you aware of steps you can take to guard against identity theft or fraud. We recommend that you review your credit and debit card account statements as soon as possible to determine if there are any discrepancies or unusual activity listed. You should remain vigilant and continue to monitor your statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect any fraudulent transactions have taken place, you should immediately call the bank or credit institution that issued the credit or debit card.

We recommend you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. The government makes it possible for each person to annually obtain a copy of his or her credit report for free from each of the three major credit report agencies. If you haven't requested a copy of your credit report within the last year, you can request copies of your credit reports online at no cost at www.AnnualCreditReport.com. That central site allows individuals to request a free credit report once every 12 months from each of the nationwide consumer credit report companies: Equifax, Experian and TransUnion. If you see anything on your credit reports that you don't understand, call the credit agency immediately. We have also enclosed an "Information about Identity Theft Protection" reference guide that describes additional steps you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection, and details on how to place a fraud alert or a security freeze on your credit file.

If you have questions, please email us at appointments@levinetaxco.com. We apologize for any inconvenience this may cause and will look forward to seeing you later this year.

Best,
Jeff & Evan Levine

INFORMATION ABOUT IDENTITY THEFT PROTECTION

Credit Reports. You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

You may also elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax General: 1-800-509-8495 Credit Reports: 800-685-1111 Fraud Alert: 888-766-0008 Other: 1-888-378-4329 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian General: 1-888-397-3742 Credit Reports: 888-397-3742 Fraud Alert: 888-397-3742 www.experian.com P.O. Box 9554 Allen, TX 75013	TransUnion General: 1-800-680-7289 Credit reports: 877-322-8228 Fraud Alert: 800-680-7289 Other: 1-800-888-4213 www.transunion.com Fraud Victim Assistance Dept P.O. Box 2000 Chester, PA 19016-2000

Fraud Alerts on Your Credit File: There are two types of fraud alerts 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 about to be, a victim of identity theft. An initial fraud alert stays on your credit report for up to one year. 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. Contact the credit reporting agencies listed above to activate an alert.

Freezing Your Credit File: You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. To place a security freeze on your credit report, contact the three major credit reporting agencies using the contact information provided above. In order to request a security freeze you will have to provide specific information and documentation, which may include: your full name, Social Security number and date of birth; addresses where you have lived over the last five years; proof of current address, such as a current utility or telephone bill; a legible photocopy of a government issued identification card; and if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Information About Preventing Identity Theft from the FTC/State Attorney General: The Federal Trade Commission (FTC) provides information at www.ftc.gov/idtheft. The FTC can be reached by phone at 1-877-438-4338; (202) 326-2222; TTY 1-866-653-4261 or by writing to FTC, 600 Pennsylvania Ave., NW. Washington, DC 20580. Your State Attorney General may also provide information. Maryland residents can contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023. Washington, DC residents can obtain information about steps to avoid identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

Protect Yourself from Phishing Scams: Learn to recognize phishing scams. Do not open emails from unknown senders and be sure not to click on strange links or attachments. Never enter your username and password without verifying the legitimacy of the request by contacting the sender by tele0phone or other methods. Replying to the email is not a safe way to confirm. Visit https://www.consumer.ftc.gov/articles/0003-phishing for more information of these types of scams.