Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

October 12, 2020

Sent Via Mail

Re: Security Incident Notification

Dear Attorney General Gordon MacDonald,

I am writing on behalf of PricewaterhouseCoopers LLP ("PwC", "we", "us", or "our") located at 300 Madison Avenue New York, NY 10017-6204 to inform you of a matter that may have impacted the personal information of two residents of the State of New Hampshire. On September 14, 2020, we became aware that a member of a PwC account team serving our client, Brookside Mezzanine Partners ("Brookside"), inadvertently sent an email with an attachment containing two New Hampshire residents' tax information to the incorrect recipient due to a typographical error. Upon being made aware of this error, we promptly took steps to investigate the issue and confirmed that this was an isolated occurrence caused by a human error. We have sent a further communication to the recipient email address indicating that the message was sent in error and requesting that it be deleted. The information at issue includes tax information and other personal information such as: name (first name, last name, and middle initial), tax address (legal residence for tax purposes), Social Security number (or in some cases Employment Identification Number), and the individual's share of taxable income from Brookside.

The individual at PwC responsible for this issue has been removed from the Brookside account and that individual's access to Brookside information has been revoked. In addition, the remaining members of the Brookside account team will receive re-training on our privacy and data protection policies. Further, we are working with our internal information security team to set-up monitoring of suspicious websites for the file that was sent inadvertently to the incorrect email address.

Although PwC is not currently aware of any evidence indicating that unintended recipient was seeking to acquire, access, or misuse the personal information, PwC has decided out of an abundance of caution to notify individuals whose personal information covered by N.H. Rev. Stat. § 359-C:19 may have been impacted as a result of the error.

PwC is coordinating with its vendor Equifax to send the notification letters to the potentially affected individuals on October 12, 2020. A sample copy of the notification letter is enclosed. In addition to providing information regarding credit reporting agencies, security freezes, fraud alerts, and other identity theft prevention tools, PwC is offering the individuals 24 months of Equifax services as described in attached Equifax document.

Please feel free to contact me if you have any questions or require additional information.

Sincerely,

Brian Kim

Managing Director
Ethics & Compliance
(201) 927 4450
brian.s.kim@pwc.com

Rob Bertrand
PricewaterhouseCoopers LLP
2001 Market St., Suite 1800
Philadelphia, PA 19103

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>>
<<Country>>

October 12, 2020

Dear <<Name 1>>:

I am writing to make you aware of a matter that involves your personal information. At this time, we have no reason to believe that your personal information has been or will be used in an unauthorized way, but we are informing you out of an abundance of caution.

What Happened?

On September 14, 2020, PricewaterhouseCoopers LLP ("PwC", "we", "us", or "our") became aware that a member of the PwC account team serving our client, Brookside Mezzanine Partners ("Brookside"), inadvertently sent an email with an attachment containing your tax information to the incorrect recipient due to a typographical error. Upon being made aware of this error, we promptly took steps to investigate the issue and confirmed that this was an isolated occurrence caused by a human error. We have sent a further communication to the recipient email address indicating that the message was sent in error and requesting that it be deleted.

What Information Was Involved?

The information at issue includes tax information and other personal information such as: your name (first name, last name, and middle initial), tax address (legal residence for tax purposes), Social Security number (or in some cases Employment Identification Number), and your share of taxable income from Brookside.

What We are Doing.

The individuals at PwC responsible for this issue have been removed from the Brookside account and their access to Brookside information has been revoked. In addition, the remaining members of the Brookside account team will receive re-training on our privacy and data protection policies. Further, we are working with our internal information security team to set-up monitoring of suspicious websites for the file that was sent inadvertently to the incorrect email address.

In addition, we are offering you 24 months of complimentary identity theft prevention services through Equifax. If you wish to enroll in these complimentary services, please see the attached Equifax document for instructions and your activation code. The enrollment period ends on December 31, 2020, so please make sure to enroll prior to that date to take advantage of these services.

What You Can Do.

In addition to enrolling in the identity theft prevention services, we recommend that you remain vigilant and take steps to protect yourself from identity theft by reviewing your account statements and by checking your credit report from one or more of the national credit reporting agencies periodically. Under the Fair Credit Reporting Act, you are entitled to obtain a free annual credit report (once every 12 months) from each of the nationwide credit reporting companies—Equifax, Experian, and TransUnion. To do so, please go to www.annualcreditreport.com or call 1-877-322-8228. If you notice any suspicious activity, you should promptly report such activity to the proper law enforcement agencies.

For More Information.

Please see below for important information about additional resources. If you have further questions or concerns please contact me at robertson.bertrand@pwc.com.

Sincerely,

Robertson Bertrand

Robertson Bertrand

ADDITIONAL RESOURCES

As stated above, you may obtain a free copy of your credit report from each of the three credit reporting agencies by visiting www.annualcreditreport.com. You can request information regarding fraud alerts, security freezes, and identity theft from the following credit reporting agencies, but note that fees may be involved for some of these services. Please see below for the contact information of the credit reporting agencies:

- Equifax, https://www.equifax.com/personal/credit-report-services, 1-800-525-6285, P.O. Box 740256, Atlanta, GA 30374
- Experian, https://www.experian.com/help, 1-888-397-3742, P.O. Box 9554, Allen, TX 75013
- TransUnion, https://www.transunion.com/credit-help, 1-800-680-7289, P.O. Box 2000, Chester, PA 19016

To place a security freeze on your credit, you may need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
- Social Security number
- Date of birth
- The addresses where you have lived over the prior five years
- Proof of current address such as a current utility bill or telephone bill
- A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.)

In addition to a security freeze, you may consider placing a fraud alert on your credit files. Adding a fraud alert to your credit report file makes it more difficult for someone to get credit in your name by requiring creditors to follow certain procedures. However, this may also delay your ability to obtain credit. No one is allowed to place a fraud alert on your credit report except you. To place a fraud alert on your file, contact one of the three nationwide credit reporting agencies; the first agency that processes your fraud alert will notify the others to do so as well.

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything that you do not understand, call the credit reporting agency at the telephone number on the report and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

You can also receive information from the Federal Trade Commission ("FTC") regarding fraud alerts, security freezes, your rights under the Fair Credit Reporting Act, and how to avoid and report identity theft: https://www.consumer.ftc.gov, 1-877-438-4338, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580.

Additional information:

- New York residents may contact the New York State Office of the Attorney General: https://ag.ny.gov/consumer-frauds-bureau/identity-theft, 1-800-771-7755. New York residents may also contact the New York Department of State Division of Consumer Protection: https://www.dos.ny.gov/consumerprotection, 1-800-697-1220.
- Under Massachusetts law, Massachusetts residents have a right to obtain a police report, if available.
- North Carolina residents may contact the North Carolina Attorney General's Office: https://ncdoj.gov/ ,, 1-919-716-6400, 114 West Edenton St., Raleigh, NC 27603. Residents may also find additional information regarding steps to take to prevent ID theft from this source.