

STATE OF NH
DEPT OF JUSTICE
2021 FEB 22 PM 12: 58

BakerHostetler

Baker & Hostetler LLP

Key Tower
127 Public Square, Suite 2000
Cleveland, OH 44114-1214

T 216.621.0200
F 216.696.0740
www.bakerlaw.com

William H. Berglund
direct dial: 216.861.7416
wberglund@bakerlaw.com

February 19, 2021

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Young's Holdings, Inc. ("Young's"), and its subsidiary, Wilson Daniels LLC ("Wilson Daniels"), to notify you of a data security incident involving one New Hampshire resident.¹ Young's and Wilson Daniels' headquarters are in Aliso Viejo, CA and Napa, CA, respectively.

Young's recently completed an investigation into suspicious activity originating from two employee email accounts. Upon discovering this, Young's immediately took measures to secure the email accounts, contacted law enforcement, and launched an investigation with the assistance of a cybersecurity firm. The investigation determined that an unauthorized person accessed the employees' email accounts at various times between October 15, 2020 and October 27, 2020, and created a rule whereby certain emails from one of the accounts were forwarded to an unknown email address. The rule was removed as soon as it was discovered. The investigation did not determine the full scope of the specific emails or attachments in the two email accounts that were actually accessed or downloaded by the unauthorized person. Out of an abundance of caution, Young's searched all emails and attachments that could have been accessed or downloaded to identify individuals whose information was accessible to the unauthorized person. On January 4, 2021, Young's determined that an email or attachment that was accessible to the unauthorized person contained certain information pertaining to one New Hampshire resident, including the resident's name and payment card number.

¹ This notice does not waive Young's Holdings, Inc.'s objection that New Hampshire lacks personal jurisdiction over it regarding any claims related to this data security incident.

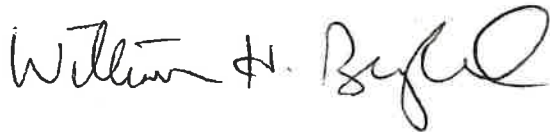
February 19, 2021
Page 2

Beginning today, February 19, 2021, Young's will mail a notification letter to the New Hampshire resident via First Class U.S. mail. A sample copy of the notification letter is enclosed. Young's is recommending that the individual remains vigilant to the possibility of fraud by reviewing their account statements for unauthorized activity. Young's has also established a dedicated telephone number that individuals may call with related questions.

To further protect personal information, Young's has taken additional steps to enhance its existing electronic security protocols and is re-educating its staff for awareness of these types of incidents.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink that reads "William H. Berglund". The signature is written in a cursive style with a large, stylized "W" and "B".

William H. Berglund
Counsel

Enclosure



PRIVATE CLIENT GROUP

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>>:

At Wilson Daniels, we understand the importance of protecting the information we maintain. I am writing to inform you of an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you may consider taking.

We recently completed an investigation into suspicious activity originating from two employee email accounts belonging to Wilson Daniels employees who have email correspondence with Private Client Group Services staff. As soon as we became aware of the suspicious activity, we immediately took measures to secure the email accounts, contacted law enforcement, and launched an internal investigation. A cybersecurity firm was engaged to assist in a full forensic analysis of this incident. The investigation determined that an unauthorized person accessed the employees' email accounts at various times between October 15, 2020 and October 27, 2020, and created a rule whereby certain emails from one of the accounts were forwarded to an unknown email address. We removed the rule as soon as we became aware of it.

The investigation did not determine the full scope of the specific emails or attachments in the two email accounts that were actually accessed or downloaded by the unauthorized person. Out of an abundance of caution, we searched all emails and attachments that could have been accessed or downloaded to identify individuals whose information was accessible to the unauthorized person. We determined that an email or attachment that was accessible to the unauthorized person contained your <<b2b_text_1(DataElements)>>.

Although we cannot confirm your information was actually viewed by the unauthorized person, or that it has been misused, we encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you see charges or activity you did not authorize, please contact your financial institution immediately. For more information on how to help safeguard your identity and steps you can take to help protect personal information, please see the additional information provided in this letter.

Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. To further protect personal information, we have taken additional steps to enhance our existing electronic security protocols and re-educate our staff for awareness on these types of incidents. We are also working actively in the development and implementation of new payment processing protocols, including engaging the services of a payment portal provider module for all Private Client Group transactions as a further safeguard. We anticipate introducing this in time for our 2021 sales offerings.

If you have any questions, please call 707.963.9661 Monday through Friday from 9:00 A.M. through 5:00 P.M. Pacific Time or email us at collectors@wilsondaniels.com.

Sincerely,

Mike Hoagland
Vice President, Private Client Group Services

Additional Steps You Can Take

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general 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 are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for 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.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Wilson Daniels' mailing address is 1300 Main Street, Suite 300, Napa, CA 94559 and the phone number is 707.963.9661.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia: You may contact and obtain information from your attorney general at: *Office of the Attorney General for the District of Columbia*, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov> .