

RECEIVED

OCT 23 2020

CONSUMER PROTECTION

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

October 22, 2020

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, H-M Company, Inc. ("H-M Company"), to notify your office of a security incident involving one New Hampshire resident. H-M Company is a commercial laundry equipment parts, products, and services company based in Cincinnati, Ohio.

H-M Company conducted an investigation into suspicious activity originating from a small number of H-M Company employee email accounts. As soon as H-M Company became aware of the activity, it immediately took measures to secure the email accounts and launched an internal investigation. A cybersecurity firm was engaged to assist in a full forensic analysis of the incident. The investigation determined that an unauthorized person accessed the H-M Company employees' email accounts at various dates between at least April 8 and July 8, 2020. The investigation did not determine whether any of the emails and attachments in the employee accounts were viewed by the unauthorized person; however, H-M Company was not able to rule out that possibility. H-M Company searched the full contents of the accounts to identify individuals whose information may have been accessible to the unauthorized person. On September 3, 2020, H-M Company determined that an email or attachment in the accounts contained the personal information of one individual who was subsequently found to be a New Hampshire resident, including the resident's name and payment card number.

October 22, 2020

Page 2

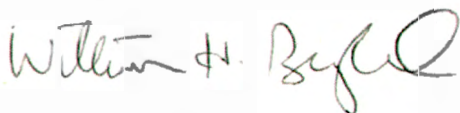
Beginning today, October 22, 2020, H-M Company will mail written notification to the New Hampshire resident via first class U.S. Mail. A sample copy of the notice letter is enclosed.¹

H-M Company is recommending that the individual remain vigilant to the possibility of fraud by reviewing their account statements for unauthorized activity. H-M Company has also established a dedicated phone number that the individual may call with related questions.

To further protect personal information, H-M Company is taking steps to enhance existing security protocols and re-educating staff for awareness on these types of incidents.

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

Sincerely,

A handwritten signature in cursive script that reads "William H. Berglund".

William H. Berglund
Counsel

Enclosure

¹ This report does not waive H-M Company's objection that New Hampshire lacks personal jurisdiction over it related to any claims that may arise from this incident.



<<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>> <<middle_name>> <<last_name>> <<suffix>>,

H-M Company understands the importance of protecting the personal information of our customers and employees. I am writing to inform you of an incident that involved some of your information. This letter explains the incident, measures we have taken, and some steps you can take in response.

We have conducted an investigation into suspicious activity originating from a small number of H-M Company employee email accounts. As soon as we became aware of the activity, we immediately took measures to secure the email accounts and launched an internal investigation. A cybersecurity firm was engaged to assist in a full forensic analysis of the incident. The investigation determined that an unauthorized person accessed the H-M Company employees' email accounts at various dates between at least April 8, 2020 and July 8, 2020.

The investigation did not determine whether any of the emails and attachments in the employee accounts were viewed by the unauthorized person; however, we were not able to rule out that possibility. We searched the full contents of the accounts to identify individuals whose information may have been accessible to the unauthorized person. On September 3, 2020, we determined that an email or attachment in the accounts contained your <<b2b_text_1(ImpactedData)>>.

While we are not aware of any misuse of information contained in the email accounts, we encourage you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements for any unauthorized activity. For more information on steps you can take to protect your personal information, please see the additional information provided in this letter.

We regret that this occurred and apologize for any inconvenience. To further protect personal information, we are taking steps to enhance our existing security protocols and re-educating our staff for awareness on these types of incidents. If you have any questions, please call 513-281-3832, Monday through Friday between 9:00 a.m. and 5:00 p.m. Eastern Time.

Sincerely,

Roger Heldman
CEO

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.