

BakerHostetler

RECEIVED

APR 08 2020

CONSUMER PROTECTION

Baker & Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

William R. Daugherty
direct dial: 713.646.1321
wdaugherty@bakerlaw.com

April 7, 2020

VIA OVERNIGHT MAIL

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

Re: Notice of Security Incident

Dear Attorney General MacDonald:

We are writing on behalf of our client, Cornerstone Building Brands, Inc. ("Cornerstone"). As noted in Cornerstone's prior notification to your office on September 11, 2019, Cornerstone's investigation into a security incident determined that an unauthorized person accessed two employees' email accounts. Upon learning of the incident, Cornerstone immediately took steps to secure the accounts, launched an investigation, and a cyber security firm was engaged to assist. The investigation determined that an unauthorized person accessed the two email accounts at various times between April 1 and April 2, 2019 and may have accessed or viewed certain emails and attachments in the email accounts. Cornerstone conducted a thorough review of the emails and attachments that may have been accessed or viewed and, on August 16, 2019, determined that the emails or attachments contained the names of eight New Hampshire residents. Those eight residents were notified on September 11, 2019 pursuant to N.H. Rev. Stat. Ann. § 359-C:20.

Cornerstone recently identified correct mailing addresses for additional individuals whose information was contained in the email accounts involved. Today, Cornerstone will send a notification letter via First Class Mail to the additional New Hampshire resident whose personal information contained in emails or attachments in the email accounts included their name, financial account number, and payment card number. The total number of New Hampshire residents notified about this incident is nine. This notice is being provided in accordance with N.H. Rev. Stat. Ann. § 359-C:20. A sample copy of the notice is also provided. Cornerstone is providing a call center for the individuals to call with questions regarding the incident.

April 7, 2020

Page 2

To help prevent a similar incident from occurring in the future, Cornerstone is providing additional data-security training to employees and enhancing existing security measures.

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

Sincerely,

A handwritten signature in black ink, appearing to read "William R. Daugherty". The signature is fluid and cursive, with a large, stylized initial 'W'.

William R. Daugherty

Partner

Attachment



<<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>>,

At Cornerstone Building Brands, Inc. ("Cornerstone") we are committed to protecting the privacy of personal information. We are writing to inform you about an incident involving some of your information. This notice explains the incident, measures we have taken, and steps you can take in response.

Our investigation into a security incident determined that an unauthorized person accessed two employees' email accounts. Upon learning of the incident, we immediately took steps to secure the accounts, launched an investigation, and a cybersecurity firm was engaged to assist. Our investigation determined that an unauthorized person accessed the email accounts at various times between April 1, 2019 and April 2, 2019 and may have accessed or viewed certain emails and attachments in the email accounts. We conducted a thorough review of the emails and attachments that may have been accessed or viewed and determined that the emails or attachments contained some of your personal information, including your <<ClientDef1(Impacted Data)>>. This matter did not involve your email account.

As a precaution, we have arranged for Kroll to provide identity monitoring at no cost to you for one year. Kroll has experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. For more information on how to safeguard your identity and Kroll services, including instructions on how to activate your complimentary one-year membership, please visit the below website.

Visit <https://krollbreach.idMonitoringService.com> to activate and take advantage of your identity monitoring services.

*You have until **June 18, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

We regret this incident occurred and any inconvenience it may cause. To help prevent a similar incident from occurring in the future, we are providing additional data-security training to employees and enhancing existing security measures. If you have any questions, please call 1-833-716-3396, Monday through Friday, from 6:00 a.m. to 3:30 p.m. Pacific Time.

Sincerely,

Cornerstone Building Brands, Inc.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

Regardless of whether you choose to take advantage of the complimentary identity monitoring, 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:

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

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

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

If you are a resident of Maryland or North Carolina, you may contact and obtain information from your state attorney general at:

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023 / (410) 576-6300 (for calls originating outside Maryland), www.oag.state.md.us

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, 919-716-6400 / 1-877-566-7226, www.ncdoj.gov

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: 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 are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one (1) 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 (7) years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

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