BakerHostetler

Baker&Hostetler LLP

1170 Peachtree Street
Suite 2400
Atlanta, GA 30309-7676

T 404.459.0050
F 404.459.5734
www.bakerlaw.com

John P. Hutchins
direct dial: 404.946.9812
jhutchins@bakerlaw.com

March 15, 2022

VIA EMAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Formella:

We are writing on behalf of our client, Holden International ("Holden"), to notify your office of a cybersecurity incident. Holden headquarters is located at 117 South Cook Street, #382; Barrington, Illinois 60010.

On June 24, 2021, Holden became aware of a data incident. Upon becoming aware of this incident, Holden took immediate steps to secure its systems, began an investigation, and a third-party cybersecurity firm was engaged to conduct this investigation. The investigation determined that an unauthorized actor accessed the Holden email system in April 2021, and August 2021, and accessed the user account of a Holden employee. Holden conducted a thorough review of the account that was accessed, and on February 22, 2022, determined that the name, financial account number, and medical information of one New Hampshire resident was involved.

On March 7, 2022, Holden mailed a notification letter to the New Hampshire resident in accordance with N.H. Rev. Stat. Ann. § 359-C:20[1], via United States First-Class mail. A copy of the notification letter is enclosed. A dedicated, toll-free call center has been established for individuals to call with questions about the incident.

To help prevent a similar incident from occurring in the future, Holden has implemented measures to enhance information security, including adding additional layers of security around user access to all systems, including multi-factor authentication. Holden has also audited all systems and connected devices and moved all servers to a more secure environment.

[1] This report does not waive Holden's objection that New Hampshire lacks regulatory authority over it related to any claims that may arise from this incident.

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

Sincerely,

John P. Hutchins

John P. Hutchins
Partner

Enclosure

HOLDEN®
SALES TRANSFORMATION, CONSULTING, AND TRAINING

<<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>>,

We are writing to inform you of an incident that may have involved some of your information. This notice explains the incident, the measures we have taken in response, and some steps you may consider taking in response.

On June 24, 2021, Holden International became aware of a data incident. Holden International took immediate steps to secure its systems, began an investigation, and a third-party cybersecurity firm was engaged to conduct this investigation. The investigation determined that an unauthorized actor accessed the Holden International email system in April 2021, and August 2021, and accessed the user account of a Holden International employee. Holden International conducted a thorough review of the account that was accessed, and on February 22, 2022, determined that some of your information was involved, which included your <<b2b_text_1(name, data elements)>>. The investigation was not able to determine whether the unauthorized actor actually viewed or acquired your specific information contained in the accounts; however, we cannot rule out that possibility.

We want to notify you of this incident and assure you that we take it very seriously. We apologize for any concern or inconvenience this incident may cause. To help prevent a similar incident from occurring in the future, we have implemented measures to enhance our information security, including adding additional layers of security around user access to all systems, including multi-factor authentication. We have also audited all systems and connected devices and moved all servers to a more secure environment. For more information on identity theft prevention, please see the additional information provided with this letter. Additionally, we have created a dedicated call center to answer any questions you may have about the incident and our response. If you have any questions, please call 1-855-541-3558, Monday through Friday, between 9:00 a.m. and 6:30 p.m. Eastern Standard Time, excluding major U.S holidays.

Sincerely,

Christine E. Holden
Managing Partner

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.