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

November 30, 2022

VIA E-MAIL: DOJ-CPB@DOJ.NH.GOV

Attorney General John M. 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, Crown Uniform & Linen Service ("Crown"), to notify you of a cybersecurity incident involving residents of New Hampshire.

Crown identified a cybersecurity incident involving unauthorized access to some of its systems. Crown immediately took steps to secure its systems and engaged a cybersecurity firm to assist with an investigation. The investigation determined that an unauthorized party gained access to some of Crown's systems between August 29, 2022 and September 6, 2022. Crown conducted a review of the data in the systems involved. On September 29, 2022, Crown determined that the data in the systems involved contained personal information that may have affected the names, Social Security numbers, driver's license numbers, direct deposit information, 401k information and/or medical information pertaining to workers' compensation and FMLA claims, drug testing and/or physicals of 195 New Hampshire residents.

On November 30, 2022, Crown is notifying affected New Hampshire residents via U.S. mail in accordance with N.H. Rev. Stat. Ann. § 359-C:20.[1] A copy of a notification letter is enclosed. Crown is providing complimentary credit monitoring to individuals whose Social Security numbers or driver's license numbers may have been involved through Experian IdentityWorks Credit 3B. Crown is also encouraging individuals to remain vigilant by reviewing their accounts for unauthorized activity.

[1] This notice does not waive Crown Uniform & Linen Service's objection that New Hampshire lacks personal jurisdiction over it regarding any claims related to this incident.

To help prevent something like this from happening again, Crown has enhanced its existing security protocols and technical safeguards by implementing an endpoint detection and response tool.

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

Sincerely,

John P. Hutchins
Partner

Return Mail Processing
PO Box 999
Suwanee, GA 30024

November 30, 2022

7 1 1537 **********SNGLP
SAMPLE A. SAMPLE - Master
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Dear Sample A. Sample:

Crown Uniform and Linen Service addressed a security incident that may have involved some of your information. This letter explains the incident, the measures we have taken, and some steps you may consider taking in response.

On August 30, 2022, our IT support provider identified a data security incident and immediately took steps to secure our systems and begin an investigation. We engaged a cybersecurity firm to assist. The investigation determined that an unauthorized party gained access to some of our systems between August 29, 2022 and September 6, 2022. We conducted a review of data in the systems involved and determined that some systems contained certain personal information. On September 29, 2022, we determined that some of your personal information may have been contained in one of the systems involved, including your name, Social Security number, driver's license number, direct deposit information, 401k information and/or medical information pertaining to workers' compensation and FMLA claims, drug testing and/or physicals.

We are offering you a complimentary one-year membership to Experian's® IdentityWorks℠. This product helps detect possible misuse of your personal information and provides you with identity protection support. For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you may consider taking, please see the pages that follow this letter.

We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you see charges or activity that you did not authorize, please contact the relevant financial institution or credit bureau to report the activity immediately.

We regret any inconvenience or concern this incident may cause. We have enhanced our existing security protocols and technical safeguards by implementing an endpoint detection and response tool to help prevent issues like this in the future. We have established a dedicated call center to help answer frequently asked questions you may have about the incident. Please call (888) 829-6550, Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays) for up-to-date information about the incident.

Sincerely,

Plato Spilios
Co-President

Activate IdentityWorks Credit 3B Now in Three Easy Steps

To activate your membership and start monitoring your personal information please follow the steps below:

1. ENROLL by: **February 28, 2023 (**Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**:

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 829-6550** by **February 28, 2023.** Be prepared to provide engagement number as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.
Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **(888) 829-6550.** If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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.identitytheft.gov

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 credit bureaus, 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 do so.

***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.

Crown can be reached at 800-221-2725. Its mailing address is 15 Technology Way, Nashua, NH 03060.

Maryland Residents: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York Residents: 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