

BakerHostetler

RECEIVED

MAY 03 2021

CONSUMER PROTECTION

Baker & Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Anthony P. Valach
direct dial: 215.564.2588
avalach@bakerlaw.com

April 30, 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 Kettle Cuisine ("Kettle") to notify you of a security incident involving seven New Hampshire residents.

Kettle Cuisine recently concluded an investigation into a ransomware incident involving certain computer system's on Kettle's network. Upon discovering the incident, Kettle immediately took steps to secure its systems, began an investigation, and a cybersecurity firm was engaged to assist. The investigation determined that an unauthorized actor obtained access to Kettle Cuisine's systems between November 3, 2020 and December 7, 2020 and acquired a limited amount of files from certain servers. The investigation determined that an unauthorized actor gained access to some network servers, and specifically to files that may have contained some personal information of seven New Hampshire, including their names, Social Security numbers, and driver's license numbers.

On April 29, 2021, Kettle Cuisine began mailing written notifications to those individuals whose information may have been involved, including seven New Hampshire who are being notified of the incident in writing, in accordance with N.H. Rev. Stat. Ann. § 359-C:20.¹ A sample letter is attached. Kettle Cuisine is offering the eligible individuals complimentary credit monitoring, fraud consultation, and identity theft restoration services through Kroll for one year. Kettle Cuisine will also recommend that the notified individuals remain vigilant to the possibility of fraud by reviewing their financial account statements for unauthorized activity.

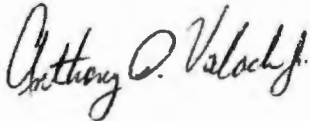
¹ This notice does not waive Kettle Cuisine's objection that New Hampshire lacks personal jurisdiction over Kettle Cuisine regarding any claims related to this incident.

April 30, 2021

Page 2

Kettle Cuisine has established a toll-free number where all notified individuals can obtain further information regarding this incident. To help prevent a similar incident in the future, Kettle Cuisine deployed new tools to monitor activity on its network to protect the business and safeguard personal information. Kettle Cuisine also implemented additional internal controls and safeguards, made changes to user access and email protocols, and provided additional training to our system users.

Sincerely,

A handwritten signature in cursive script that reads "Anthony P. Valach".

Anthony P. Valach
Counsel

Enclosure



<<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>>:

Kettle Cuisine recognizes the importance of protecting our employees' information. We are writing to notify you that we recently identified and addressed an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and additional steps you may consider taking in response.

We recently concluded an investigation into a ransomware incident involving unauthorized access to certain computer systems on Kettle's network. Upon discovering the incident, we immediately took steps to secure our systems, began an investigation, and a cybersecurity firm was engaged to assist. The investigation determined that an unauthorized actor accessed our systems between November 3, 2020 and December 7, 2020, and acquired a limited amount of files from certain servers. We reviewed the content of the files acquired by the unauthorized person and, on March 10, 2021, we discovered that the files included information relating to some of our employees. We completed a review of those files and discovered that some of your information was involved in the incident, including your <<b2b_text_1(ImpactedData)>><<b2b_text_2(ImpactedDataCont)>>

While we have no evidence that your information has been misused, we wanted to let you know this happened and assure you we take it very seriously. In an abundance of caution, we are offering you a complimentary one-year membership of Kroll's identity monitoring services. This product includes Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

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

You have until July 30, 2021 to activate your identity monitoring services.

Membership Number: <<Member ID>>

For more information on identity theft prevention, including instructions on how to activate your complimentary one-year membership, as well as information on additional steps you can take in response to this incident, please see the additional information provided in this letter.

We are notifying you of this incident and sharing the steps that we are taking in response. To help prevent a similar incident in the future, we are implementing several changes to enhance our existing security measures, including measures designed to prevent a recurrence of such an attack and to protect the privacy of our employees. We deployed new tools to monitor activity on our network to protect the business and safeguard personal information. We also implemented additional internal controls and safeguards, made changes to user access and email protocols, and provided additional training to our system users. Should you have any further questions or concerns regarding this matter, please contact 1-XXX-XXX-XXXX, Monday through Friday, 9:00 am to 6:30 pm, Eastern Time.

Sincerely,

James Reed

James Reed
Chief Financial Officer
Kettle Cuisine



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.

If your health insurance information was involved, it is also advisable to review the billing statements you receive from your health insurer or healthcare provider. If you see charges for services you did not receive, please contact the insurer or provider immediately.

Additional information for residents of the following states:

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

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 above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.