

BakerHostetler

RECEIVED

OCT 23 2020

CONSUMER PROTECTION

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

David E. Kitchen
direct dial: 216.861.7060
dkitchen@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, Savers, Inc., to notify your office of a security incident involving two New Hampshire residents.

Savers' investigation into an email phishing incident recently determined that an unauthorized party could have accessed information contained in a single Savers employee email account. Upon learning of the potential incident, Savers quickly took steps to secure the employee's email account and began an investigation with the assistance of a cybersecurity firm to determine the scope of the incident. Savers' investigation determined that an unauthorized person accessed the account between June 28, 2020 and July 3, 2020. The investigation was not able to conclusively determine which emails or attachments were viewed by the unauthorized person. Accordingly, Savers conducted a review of the emails and attachments that may have been viewed and determined on September 21, 2020 that the names and financial account numbers of two New Hampshire residents were contained in the account.

On October 22, 2020, Savers began sending notice to all potentially affected individuals, including to the New Hampshire residents. A sample copy of the notification is enclosed. Savers is encouraging potentially affected individuals to closely monitor their account statements and to notify the financial institution immediately if fraudulent transactions are suspected. Savers has provided a telephone number for potentially affected individuals to call with any questions they may have about the incident.

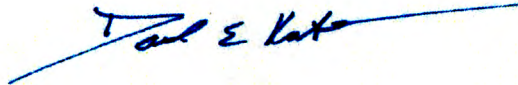
October 22, 2020

Page 2

To further protect personal information, Savers has implemented additional safeguards and technical security measures and is providing additional training to employees.

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

Sincerely,

A handwritten signature in blue ink that reads "David E. Kitchen". The signature is written in a cursive style and is positioned above a horizontal line.

David E. Kitchen
Partner

Enclosure



<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>><<State>><<Zip>>

<<Date>>

<<Country>>

Dear <<Name 1>>:

At Savers, we understand the importance of protecting the personal information that we maintain. We are writing to inform you of a security incident that may have involved some of your information. This notice explains the incident, measures we have taken and some steps you can take in response.

We have concluded our investigation into an email phishing incident that targeted one Savers employee. Upon learning of the potential incident, we quickly took steps to secure the employee's email account and began an investigation with the assistance of a cybersecurity firm to determine the scope of the incident. Our investigation determined that an unauthorized person accessed the account between June 28, 2020 and July 3, 2020. The investigation was not able to conclusively determine which emails or attachments were viewed by the unauthorized person. Accordingly, we conducted a review of the emails and attachments that may have been viewed and, on September 21, 2020, determined that they contained your <<variable data>>.

Although, to date, we have no evidence that your information has been misused, we assure you that we take this incident very seriously. We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. For more information on additional steps you can take to help protect yourself, please see the additional information provided with this letter.

We sincerely regret any inconvenience caused by this incident. We have implemented additional safeguards and technical security measures to further protect personal information and are providing additional training to employees. If you have any questions, please call 1.800.259.0004 or email us at PeopleServices@savers.com.

Sincerely,

Richard Medway
General Counsel and Chief Compliance Officer

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.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland: 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

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

New York: 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>

Rhode Island: This incident involves 4 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov