

BakerHostetler

RECEIVED
JAN 16 2019
CONSUMER PROTECTION

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

January 15, 2019

VIA OVERNIGHT MAIL

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Foster:

We are writing on behalf of our client, Graeter's Ice Cream, the operator of <https://www.graeters.com>, to notify you of a security incident involving New Hampshire residents.

Graeter's Ice Cream was recently made aware by the payment card networks of patterns of unauthorized charges occurring on cards after they were legitimately used on Graeter's website, <https://www.graeters.com>. In response, Graeter's launched an investigation with assistance from a cybersecurity firm. On December 17, 2018, our investigation identified unauthorized code that had been added to the checkout page on Graeter's website. Findings from the investigation indicate that the code may have been present from June 28, 2018 to December 17, 2018, and capable of copying information entered by customers during the checkout process. The information entered during checkout that the unauthorized code could have potentially copied includes first and last name, address, telephone number, fax number, payment card type, payment card number, expiration date, and card verification code. Purchases made in a Graeter's Ice Cream store were not involved in this incident.

Today, Graeter's Ice Cream is notifying 42 New Hampshire residents via U.S. mail in substantially the same form as the enclosed letter.¹ Graeter's Ice Cream is advising potentially impacted individuals to remain vigilant and review their financial account statements for

¹ This report is not, and does not constitute, a waiver of Graeter's Ice Cream's objection that New Hampshire lacks personal jurisdiction over the company related to this matter.

Attorney General Joseph Foster
January 15, 2019
Page 2

suspicious activity. Graeter's Ice Cream is also providing a telephone number for individuals who received a notification letter to call with any questions they may have.

To help prevent this type of incident from happening again, Graeter's Ice Cream is taking steps to enhance its security environment, including forcing password resets and scanning its website for malicious code.

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 "Craig Hoffman", with a long horizontal line extending to the right.

Craig Hoffman
Partner

Enclosure



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Dear <<Name 1>>:

At Graeter's Ice Cream, we value the relationship we have with our customers and understand the importance of protecting customer information. We are writing to inform you that we recently identified and addressed an incident that may have involved your payment card information. This notice explains the incident, measures we have taken in response, and some additional steps you may consider taking.

What Happened?

We were recently made aware by the payment card networks of patterns of unauthorized charges occurring on cards after they were legitimately used on Graeter's website, <https://www.graeters.com>. In response, we launched an investigation with assistance from a cybersecurity firm. On December 17, 2018, our investigation identified unauthorized code that had been added to the checkout page on our website. Findings from the investigation indicate that the code may have been present from June 28, 2018 to December 17, 2018, and capable of copying information entered by customers during the checkout process on our website. Purchases made in a Graeter's Ice Cream store were not involved in this incident.

What Information Was Involved?

The information entered during checkout that the unauthorized code could have potentially copied includes first and last name, address, telephone number, fax number, payment card type, payment card number, expiration date, and card verification code. We are notifying you because you placed an order on our website using the payment card(s) ending in <<Variable Data>> during the relevant time period.

What We Are Doing.

We deeply regret any inconvenience or concern this incident may cause you. To help prevent a similar incident from occurring in the future, we are taking steps to enhance our security environment, including forcing password resets and scanning our website for malicious code.

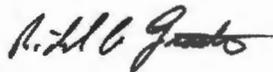
What You Can Do.

We encourage you to closely review your payment card account statements for any unauthorized activity. You should immediately report any unauthorized charges to the bank that issued your card because payment card networks rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. Information on additional steps you can take can be found on the following pages.

For More Information.

If you have any further questions or concerns, please call 877-209-9591, Monday through Friday, between the hours of 8:00 a.m. and 8:00 p.m. C.T.

Sincerely,

A handwritten signature in black ink, appearing to read "R. A. Graeter". The signature is fluid and cursive, with the first name "Richard" and last name "Graeter" clearly distinguishable.

Richard A. Graeter
President
Graeter's Ice Cream

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 Centre, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

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 90 days. 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. 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

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.