BakerHostetler

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

July 23, 2019

VIA OVERNIGHT MAIL

Office of the Attorney General
33 Capitol St.
Concord, NH 03301

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Graeter's Ice Cream Company ("Graeter's"), to notify your office of a security incident involving New Hampshire residents.

Graeter's began an investigation of its e-commerce website after a guest called to report that an unauthorized charge occurred on the guest's payment card after the guest used it to make a purchase from Graeter's website, https://www.graeters.com. A leading cybersecurity firm was then engaged to determine what had happened and what information may have been involved. By June 28, 2019, findings from the investigation indicated that the code may have been present from December 30, 2018 to June 13, 2019 and may have been capable of copying information entered by customers during the checkout process. The information entered during the checkout process that could have been copied includes first and last name, address, telephone number, payment card number, expiration date, and card verification code.

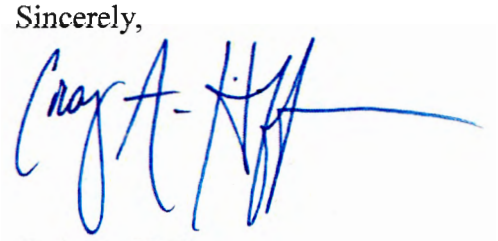
Today, Graeter's is notifying 24 New Hampshire residents via U.S. mail in substantially the same form as the enclosed letter.[1] Graeter's is advising individuals to remain vigilant and review their financial account statements for suspicious activity. Graeter's is also providing a telephone number for individuals who received a notification letter to call with any questions they may have.

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

To help prevent this type of incident from happening again, Graeter's is taking steps to enhance the security of its e-commerce environment, including through the use of six additional security scans. In addition, in the early fall, Graeter's will be moving to a new e-commerce platform that will use iframe technology so that payment card data will not be entered on its servers.

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

Sincerely,



Craig A. Hoffman
Partner

Attachment

IRRESISTIBLE

SINCE Graeter's 1870

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Graeter's Ice Cream is a fourth-generation family run business dedicated to carrying on the tradition of making hand-crafted, hand-packed ice cream. Our guests mean a great deal to us, and as stewards of the business entrusted to us by our family, we work hard to make the entire Graeter's experience satisfying and memorable for every guest. It is because of our personal connection to our guests that I wanted to take a moment to write to you on behalf of Graeter's to let you know that we recently identified and addressed an incident that may have involved your payment card information. This notice explains the incident, the measures we have taken in response, and some additional steps you may consider taking.

What Happened?

We recently began an investigation of our e-commerce website after a guest called to report that an unauthorized charge occurred on their payment card after they used it to make a purchase from our website, https://www.graeters.com. A leading cybersecurity firm was then engaged to determine what had happened and what information may have been involved. By June 28, 2019, findings from the investigation indicated that the code may have been present from December 30, 2018 to June 13, 2019 and may have been capable of copying information entered by guests during the checkout process. We are notifying you because you placed an order on our website during that time.

What Information Was Involved?

The information entered during the checkout process that could have been copied includes first and last name, address, telephone number, payment card number, expiration date, and card verification code for the payment card(s) ending in <<ClientDef1(Last 4 of Card Number)>>.

What We Are Doing.

After an attack on our e-commerce site last year, we implemented a number of security enhancements. In spite of these measures, this incident occurred due to a vulnerability in the code of our third-party e-commerce platform, which is used by thousands of e-commerce sites. In response to this incident, we have implemented a number of additional security measures, including using an expanded set of six different security scans on our environment. In the early fall, we'll be moving to a new e-commerce platform that will use iframe technology so that payment card data will not be entered on our servers. And we will continue to look for additional ways to protect our guests' information.

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 network 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.

We deeply regret that this occurred and apologize for any inconvenience. If you have any further questions or concerns, please call 1-833-963-0521, Monday through Friday, between the hours of 9:00 a.m. and 6:30 p.m. ET.

Sincerely,

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

If you are a resident of Connecticut, Maryland, or North Carolina, you may contact and obtain information from your state attorney general at:

- *Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag
- *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 Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, www.ncdoj.gov

If you are a resident of 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 below. You also have a right to place a security freeze on your credit report, as described below.

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 one (1) 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. 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.

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). Here is a summary of your major rights under FCRA. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., 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.