



Craig S. Horbus
Attorney at Law
Direct Dial 330.434.7563
chorbus@brouse.com

March 23, 2020

RECEIVED

MAR 31 2020

CONSUMER PROTECTION

VIA CERTIFIED U.S. MAIL

Gordon J. MacDonald, Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, New Hampshire 03301

Re: Data Breach Notification

Dear Sir or Madam:

We are writing to provide you with information about a recent data security incident involving our client Enerco Group, Inc., DBA Mr. Heater, Inc., Heatstar by Enerco and HeatstarAG (“Enerco”), pursuant to requirements under New Hampshire Revised Statutes Sec. 359-C:20(VI). This incident affected the personal information of ten (10) New Hampshire residents. While Enerco takes data security very seriously and has established policies to mitigate risks, including technical, administrative, and physical safeguards, its website was compromised and some customers’ personal information was unlawfully obtained.

Enerco has been in the infrared combustion technology industry since 1957 and is based in Ohio, specifically located at 4560 West 160th Street, Cleveland, Ohio 44135. Part of its business is to sell heating products to consumers and other businesses through which some sales are transacted through its secure website. While its system does not store payment card information, the unauthorized third party may nonetheless have been able to access and acquire information used to pay for purchases in its online store through what it has suspected was some type of data scraping tool deployed by cybercriminals through malicious code at some point between October 31, 2019 and December 26, 2019. Enerco discovered this breach in the late afternoon on Friday, February 7, 2020 and upon notice from Visa of a suspected fraudulent pattern involving its customers, at which time Enerco immediately began an internal investigation and risk mitigation plan pursuant to its internal policies.

Enerco’s investigation revealed that the personal information potentially involved may have included first and last names, shipping and billing addresses, phone numbers, email addresses, and credit card information including account number, expiration date, and three-digit security code.

Our client takes this matter very seriously. Upon learning of the incident, Enerco took immediate measures to contain and neutralize the vulnerability and immediately began a forensic investigation to determine the extent of the third party criminal conduct. It has also deployed,

Gordon J. MacDonald, Attorney General
New Hampshire Department of Justice
March 23, 2020
Page 2

and continues to deploy, additional security procedures to prevent future attacks. Finally, Enerco engaged our firm as cyber security legal counsel to guide it through this process. Enerco will be sending notice to New Hampshire's affected consumers pursuant to the state's data privacy laws informing them of the necessary information potentially involved, on or about March 30, 2020. This notice will also provide recommendations for monitoring an individual's credit report and other financial transactions to avoid any fraudulent activity as a result of this data breach and a toll free number to call with questions about the incident. Enerco will also provide free credit monitoring to any customer whose data was breached for twenty-four (24) months in an effort to help mitigate any further misuse of the information. A copy of this letter is attached for your reference.

Enerco has removed the malicious code and continues to review its internal policies and conduct post-incident activities to ensure appropriate response and future protection against data theft and cyber-crime.

Please feel free to contact me with any questions regarding this matter.

Sincerely,



Craig S. Horbus

CSH/rjh

Enclosure: Copy of Consumer Notice

cc: Jessica Siejka (w/enclosure)

1090803.1

<<Date>>

<<First Name>> <<Last Name>>

<<Address1>> <<Address2>>

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

To Enroll, Please Call: 800-939-4170 Or Visit: https://ide.myidcare.com/customending ; https://app.myidcare.com/account-creation/protect Enrollment Code: <<XXXXXXXXXX>>

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to you to let you know about a security incident that may involve your personal information. We are providing this notice out of an abundance of caution and to inform you of steps you can take to help protect your information.

What Happened

Between October 31, 2019 and December 26, 2019, our web server was breached and order information was potentially collected. While our system does not store payment card information, the unauthorized third party may nonetheless have been able to access and acquire information used to pay for purchases in our online store. Though you may have contacted our Support Center directly via phone, our online store uses the same system which our Technical Support Team also utilizes to place phone orders.

What Information Was Involved

The personal information potentially involved may have included first and last names, shipping and billing addresses, phone numbers, email addresses, and credit card information including account numbers, expiration dates, and three-digit security codes. Please note that you are receiving this notification only because an attempted transaction occurred in our system during the potentially exposed time period; we cannot confirm your actual information was in fact involved in the potential incident.

What We Are Doing

We take this matter very seriously and apologize for any inconvenience caused. Upon learning of the incident, we took immediate measures to contain and neutralize the vulnerability and immediately began a forensic investigation to determine the extent of the third party criminal conduct. We have also deployed, and continue to deploy, additional security procedures to prevent future attacks. Finally, we have engaged cyber security legal counsel to guide us through this process.

In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare™ services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare™ will help you resolve issues if your identity is compromised.

What Actions You Can Take

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare™ services by calling 800-939-4170 or going to <https://ide.myidcare.com/customending;https://app.myidcare.com/account-creation/protect> and using the Enrollment Code provided above. MyIDCare™ experts are available Monday through Friday from 5 am - 5 pm Pacific Time. Please note the deadline to enroll is [Enrollment Deadline].

1. Website and Enrollment. Go to <https://ide.myidcare.com/customending;https://app.myidcare.com/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the Credit Monitoring Provided as Part of Your MyIDCare™ Membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare™ will be able to assist you.

3. Telephone. Contact MyIDCare™ at 800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review Your Credit Reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare™, notify them immediately by calling or by logging into the MyIDCare™ website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the Three Credit Bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Equifax

P.O. Box 740241
Atlanta, Georgia 30374
1 (866)349-5191
www.equifax.com

Experian

P.O. Box 4500
Allen, Texas 75013
1 (888) 397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, Pennsylvania 19016-2000
1 (888) 909-8872
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Please call 800-939-4170 or go to <https://ide.myidcare.com/customending>;
<https://app.myidcare.com/account-creation/protect> for assistance or for any additional questions you may have.

We remain committed to protecting your personal information. We again sincerely apologize for any inconvenience caused by this incident. We are undertaking measures to further secure your personal information, and are continuously monitoring our processes to prevent similar incidents in the future.

Sincerely,

R. Jeffrey Bush, President
Enerco Group Inc., D.B.A. Mr. Heater Inc., Heatstar by Enerco, HeatstarAG

Other Important Information

RESIDENTS OF IOWA: State law advises you to report any suspected incidents of identity theft to local law enforcement or the attorney general.

RESIDENTS OF MARYLAND: You can obtain information from the Federal Trade Commission and the Office of the Attorney General about steps you can take to avoid identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1 (888) 743-0023
www.oag.state.md.us

Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, D.C. 20580
1 (202) 326-2222
www.ftc.gov/idtheft

RESIDENTS OF MASSACHUSETTS: You have the right to obtain a police report.

RESIDENTS OF NEW MEXICO: You have rights pursuant to the Fair Credit Reporting Act in order to ensure accuracy, fairness, and privacy of the information contained in your credit report.

RESIDENTS OF NORTH CAROLINA: You can obtain information from the North Carolina Office of the Attorney General and the Federal Trade Commission about preventing identity theft.

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1 (877) 566-7226
www.ncdoj.gov

Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, D.C. 20580
1 (202) 326-2222
www.ftc.gov

RESIDENTS OF OREGON: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission.

RESIDENTS OF RHODE ISLAND: State law advises you that you may file or obtain a police report and that the state Attorney General can be contacted at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
1 (401) 274-4400
www.riag.ri.gov

RESIDENTS OF VERMONT: Consumers in Vermont are entitled to one free credit report each year from each credit reporting agency. Information on how to obtain a free credit report is available at <https://www.annualcreditreport.com/index.action>.

RESIDENTS OF WYOMING: This notice was not delayed as a result of any law enforcement investigation.