March 20, 2020

VIA OVERNIGHT DELIVERY

Attorney General Gordon J. MacDonald
Office of the Attorney General
State of New Hampshire
33 Capitol Street
Concord, New Hampshire 03301

NOTICE OF DATA BREACH

Dear Attorney General MacDonald:

We are writing to notify you of a recent data security incident involving twelve (12) New Hampshire residents.

On January 22, 2020, Zerbee, LLC, a provider of office supplies and office services solutions, was notified by a payment card brand that it may have experienced a security incident involving unauthorized access to certain customer payment card information. Upon receiving this information, Zerbee commenced an investigation.

Based on its investigation, Zerbee determined that malicious code was present on Zerbee's website between October 22, 2019 and January 7, 2020. During that time, the malicious code allowed unauthorized access to the payment card information of Zerbee customers, including customers' credit card number, expiration date, cardholder name, and card verification value (CVV) number. In some cases, the malicious code also allowed unauthorized access to certain information such as customers' name, email, phone number, and/or billing/shipping address. Other information such as Social Security Number, passport, or driver's license number was not accessed.

We have taken steps to determine how the incident occurred and to ensure appropriate action is being taken in response. Among other things, Zerbee performed a forensic analysis of its website and reviewed relevant transactions to determine potentially impacted customers. Zerbee takes the protection of its customers' personal information very seriously, and will continue to take steps to reduce the likelihood of a similar incident.

On March 20, 2020, Zerbee notified by mail the twelve (12) customers who are residents of New Hampshire that used a payment card on the Zerbee website during the October 22, 2019 through January 7, 2020 timeframe that their payment card information may be at risk. We used the mailing address associated with their credit card billing address as entered on the Zerbee website. A copy of the notification letter is included with this correspondence.

ZERBEE
BUSINESS PRODUCTS

If you have any questions regarding this incident or if you desire further information or assistance, please do not hesitate to contact us at 855-493-7233 and 6645 James Avenue North, Minneapolis, MN 55430.

Sincerely,

Pete Soderling
President

Enclosure

[DATE]

[CUSTOMER NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]

NOTICE OF DATA BREACH

Dear Customer:

We value your business and respect the privacy of your information. We are writing to let you know about a recent incident that may have involved your personal information. This notice explains the incident, the measures we have taken in response, and some additional steps you may consider taking.

What Happened?

On January 22, 2020, Zerbee, LLC, learned that it may have experienced a security incident involving unauthorized access to certain customer payment card information. Upon receiving this information, Zerbee commenced an investigation into the incident.

Based on its investigation, Zerbee determined that malicious code was uploaded to Zerbee's website allowing unauthorized access to certain payment card information used on Zerbee's website. Zerbee's investigation determined that the malicious code was present on Zerbee's website between October 22, 2019 and January 7, 2020. As such, Zerbee is notifying customers that used a payment card on the Zerbee website during this timeframe that their payment card may be at risk.

What Information Was Involved?

The malicious code allowed unauthorized access to payment card information from your transaction on Zerbee.com, including your credit card number, expiration date, cardholder name, and card verification value (CVV) number. In some cases, the malicious code also allowed access to certain information such as your name, email, phone number, and/or billing/shipping addresses.

What We Are Doing

Upon learning of the incident, Zerbee promptly commenced an investigation. We have taken steps to determine how the incident occurred and to ensure appropriate action is being taken in response. Zerbee takes the protection of your personal information very seriously, and will continue to take steps to reduce the likelihood of a similar incident.

What You Can Do

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major

credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

In addition, you may contact the Federal Trade Commission (FTC) or law enforcement, such as your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
https://www.identitytheft.gov/

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime and in case you are asked to provide copies to creditors to correct your records.

For more information on identity theft prevention and certain state-specific information, please see the information about additional steps you can take that follow this letter.

For More Information

We apologize for any inconvenience caused by this incident. If you have any questions regarding this incident or if you desire further information or assistance, please do not hesitate to contact us at 855-493-7233 and 6645 James Avenue North, Minneapolis, MN 55430.

Sincerely,

Pete Soderling
President

Additional Steps you Can Take

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide credit reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the credit reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major credit reporting agencies to request a copy of your credit report at:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374-0241, www.equifax.com, (866) 349-5191
- *Experian*, P.O. Box 2002, Allen, TX 75013, www.experian.com, (888) 397-3742
- *TransUnion*, P.O. Box 2000, Chester, PA, 19016, www.transunion.com, (800) 916-8800

Fraud Alerts

You may obtain information from the FTC and the credit reporting agencies about fraud alerts. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last one year. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. Contact information related to fraud alerts for the three major credit reporting agencies is included below:

- *Equifax*, P.O. Box 105069, Atlanta, GA 30348-5069, www.equifax.com, (800) 525-6285
- *Experian*, P.O. Box 9554, Allen, TX 75013, www.experian.com, (888) 397-3742
- *TransUnion*, P.O. Box 2000, Chester, PA, 19016, www.transunion.com, (800) 680-7289

Security Freeze

You can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. There is no fee to place

or lift a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. You may contact the nationwide credit reporting agencies regarding a security freeze at:

- *Equifax*, P.O. Box 105788, Atlanta, GA 30348-5788, www.equifax.com, (888) 298-0045
- *Experian*, P.O. Box 9554, Allen, TX 75013, www.experian.com, (888) 397-3742
- *TransUnion*, P.O. Box 160, Woodlyn, PA 19094, www.transunion.com, (888) 909-8872

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 hour 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 hour 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 the 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.

State Specific Information

IF YOU ARE A MARYLAND RESIDENT: In addition to the FTC, you may also obtain information about avoiding identity theft from the Maryland Attorney General's Office. The office can be reached at:

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

IF YOU ARE A NORTH CAROLINA RESIDENT: In additional to the FTC, you may also obtain information about preventing identity theft from the North Carolina Attorney General's Office. The office can be reached at:

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com

IF YOU ARE A NEW YORK RESIDENT: You may also obtain information about preventing identity theft from the New York Department of State's Division of Consumer Protection and the New York State Attorney General. These offices can be reached at:

New York State Division of Consumer Protection,
123 William Street
New York, NY 10038- 3804
or
One Commerce Plaza,
99 Washington Ave.,
Albany, NY 12231-0001
(800) 697-1220
www.dos.ny.gov/consumerprotection

OR

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
(800) 771-7755
https://ag.ny.gov