POLSINELLI

900 W. 48th Place, Suite 900, Kansas City, MO 64112 • 816.753.1000

July 7, 2023

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)
The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: ***Notification of Data Security Incident***

Dear Attorney General MacDonald:

We represent MAC Pizza Management, Inc. ("MAC Pizza"), 12633 State Highway 30, College Station, Texas, 77845, in connection with an incident that may have involved the personal information of one (1) New Hampshire resident. MAC Pizza is reporting the incident pursuant to N.H. REV. STAT. ANN. § 359-C:20. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to this submission. While MAC Pizza is notifying you of this incident, MAC Pizza does not waive any rights or defenses relating to the incident, this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE INCIDENT

On April 17, 2023, MAC Pizza discovered that it was the victim of a ransomware attack. Upon discovering the incident, MAC Pizza promptly began an investigation, notified law enforcement, and worked to secure its systems. MAC Pizza also engaged a forensic security firm to assist with its investigation and confirm the security of its computer systems. The forensic investigation recently concluded and determined that an unknown, unauthorized third party accessed MAC Pizza's computer systems at times between April 14, 2023 and April 22, 2023 and may have accessed and acquired certain documents from MAC Pizza's systems as a part of the incident.

MAC Pizza reviewed the contents of the potentially acquired documents to determine if they contained any personal information. On June 21, 2023, MAC Pizza completed its review and determined that the potentially acquired documents contained one (1) New Hampshire resident's . The investigation determined that the unauthorized access was limited to MAC Pizza's corporate files and did not involve or

compromise customer or consumer information or store technology platforms. At this point, MAC Pizza is not aware of any fraud or identity theft to any individual as a result of this incident.

NUMBER OF RESIDENTS NOTIFIED

MAC Pizza is notifying the one (1) New Hampshire resident of the incident by US first-class mail today, July 7, 2023. The notification letter includes information on ways the individuals can protect themselves against potential fraud and identity theft, as well as a telephone number they can call if they have any questions regarding the incident. Enclosed is a copy of the notice that is being sent.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, MAC Pizza promptly began an investigation, notified law enforcement, and worked to secure its systems. MAC Pizza also engaged a forensic security firm to investigate and confirm the security of its email and computer systems. MAC Pizza is undertaking efforts to reduce the risk of a similar incident occurring in the future, including enhancing its technical security measures. Finally, as discussed above, MAC Pizza is notifying the resident and providing them with information on how to protect against fraudulent activity and identity theft.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Alexander D. Boyd

Enclosure

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Name>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

July 7, 2023

Dear <<Name 1>>:

<<RE: NOTICE OF DATA BREACH>>

MAC Pizza Management ("MAC Pizza") values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved some of your personal information. This letter explains the incident, the steps we have taken in response, and provides information on steps you may take to help protect your information, should you feel it is appropriate to do so.

What Happened? On April 17, 2023, we discovered that we were the victim of a cyber-attack. Upon identifying the issue, we promptly began an investigation, notified law enforcement, and worked to secure our systems. We also engaged a forensic security firm to assist with our investigation and confirm the security of our computer systems. The forensic investigation determined that an unknown, unauthorized third party accessed our computer systems at times between April 14, 2023 and April 22, 2023. The investigation indicated that the third party may have accessed and acquired certain documents from our systems during this period.

What Information Was Involved? We reviewed the contents of the potentially acquired documents to determine if they contained any personal information. We recently determined that the documents contained personal information that included . The information could also include .

What We Are Doing. In addition to the actions described above, we have taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures.

What You Can Do. While we have no evidence that your personal information has been misused, you can find information on steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please contact us by phone at: or you can contact us at: MAC Pizza Management, 12633 State Highway 30, College Station, TX, 77845.

Sincerely,

MAC Pizza Management

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Rhode Island Residents: We believe that this incident affected 4 Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.