NIXON PEABODY LLP
ATTORNEYS AT LAW

NIXONPEABODY.COM
@NIXONPEABODYLLP

Jenny L. Holmes
Associate
T 585-263-1494
jholmes@nixonpeabody.com

1300 Clinton Square
Rochester, NY 14604-1792
585-263-1000

March 18, 2020

VIA EMAIL AND OVERNIGHT MAIL

Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

To Whom It May Concern:

On behalf of Banfi Products Corporation ("Company"), I am writing to notify you of a security incident involving an inadvertent disclosure of personal information that may have affected six (6) New Hampshire residents.

On February 28, 2020, the Company discovered that the computer systems were hacked in a ransomware attack. At approximately 4:00 a.m. that morning, the Company's IT team started to receive alerts from the computer systems that routine jobs were failing and daily jobs were not connecting to the servers. The IT team immediately contacted the Company's third-party network support team and asked them to investigate the problem. They informed the Company that the computer systems were hacked and infiltrated by ransomware. Upon further investigation, the Company learned that certain machines and servers had certain files encrypted and locked so that the Company could not access the files. The Company promptly engaged third-party security vendors and expert forensic teams to investigate the source of the ransomware in order to stop the attack and contacted outside counsel and its insurance carrier. The Company also notified local law enforcement and have been cooperating with their requests. The team has worked continuously to ensure that the attack was contained and that the Company was able to safely run the computer systems again.

Since this incident, the IT team has changed every employee's office password and installed a higher level virus scanning agent on all machines and servers. The Company also enhanced the firewall security function and installed two-factor authentication for every user. The third-party vendor forensic teams continue their study of the computer system's e-mail logs and firewall logs and will report further to us when they have additional information. The Company plans on reviewing the current security policies and procedures to learn from this incident and help prevent another incident in the future.

NIXON PEABODY LLP
ATTORNEYS AT LAW

NIXONPEABODY.COM
@NIXONPEABODYLLP

This week, the Company will send a letter to the affected individuals informing them of this incident. The form of the notification letter to be sent to the affected New Hampshire residents is enclosed.

If you should have any additional questions or need further information regarding this incident, please do not hesitate to contact me at 585-263-1494.

Sincerely,

Jenny L. Holmes

Enc.

NOTICE OF DATA BREACH

March 18, 2020

To Whom It May Concern:

At Banfi Products Corporation, we take your privacy and data security very seriously. We are writing to notify you of a security incident involving some of your personal information.

What Happened?

On February 28, 2020, we discovered that our computer systems were hacked in a ransomware attack. At approximately 4:00 a.m. that morning, our IT team started to receive alerts from the computer systems that routine jobs were failing and daily jobs were not connecting to our servers. Our IT team immediately contacted our third-party network support team and asked them to investigate the problem. They informed us that our computer systems were hacked and infiltrated by ransomware. Upon further investigation, we learned that certain machines and servers had certain files encrypted and locked so that we could not access the files. We promptly engaged third-party security vendors and expert forensic teams to investigate the source of the ransomware in order to stop the attack and contacted our outside counsel and insurance carrier. We also notified law enforcement and have been cooperating with their requests. Our team has continued to work around the clock to ensure that the attack was contained and that we were able to safely run our computer systems again.

Because we had a complete set of backups on the cloud, we were able to retrieve all of the encrypted and locked information. At the advice of counsel, our insurance carrier, and our security vendors, we did not pay the ransom to the hackers. The information was already accessed and paying the ransom did not guarantee the hackers would not use the information.

What Information Was Involved

We maintain certain personal information about our employees, former employees, dependents of employees or former employees, and certain job applicants in order to process payroll, provide health insurance benefits, and complete required tax reporting. Therefore, the hackers may have had access to your personal information, including your name, birthdate, address, e-mail, social security number and financial information.

What We Are Doing

Since this incident, our IT team has changed every employee's office password and installed a higher level virus scanning agent on all machines and servers. We also enhanced the firewall security function and installed two-factor authentication for every user. Our third-party vendor forensic teams continue their study of our computer system's e-mail logs and firewall logs and will report further to us when they have additional information. We plan on reviewing our current security policies and procedures to learn from this incident and help prevent another incident in the future.

You have received this notice as a former employee, spouse or dependent child of a former employee of Banfi. We are extremely sorry that this incident occurred.

What Can You Do?

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

While we believe there is a low risk of unauthorized use of this information, we advise you to remain vigilant by reviewing your account statements and monitoring your credit reports regularly. If you see unauthorized activity on your account statements, you should contact your financial institution or payment card issuer directly. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities and/or the Federal Trade Commission (FTC).

For More Information.

For further information and assistance, please contact Judi Brenenson at 516-686-2579 or Denise Caputo at 516-686-2578. Please also review the attached additional information for helpful steps you can take to protect your identity.

Please let us restate that we take very seriously our responsibility to safeguard your personal information. We sincerely apologize for any worry this situation may cause you.

Sincerely,

Judith Brenenson
Vice President, Human Resources

Important Identity Theft Information:

Additional Steps You Can Take to Protect Your Identity

The following are additional steps you may wish to take to protect your identity.

Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. When you receive your credit report, look it over with care. If you notice anything suspicious – accounts you did not open, inquiries from creditors that you did not initiate, personal information such as a home address or Social Security number that is not accurate – or you see anything you do not understand, call the credit reporting agency at the number listed in the report. If you find fraudulent or suspicious activity in your credit reports, you should promptly report the matter to the proper law enforcement authorities. Follow the steps recommended above for reporting fraudulent or suspicious activity to law enforcement.

You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service. P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax Credit Information Services, Inc.	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 4500	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
(888) 685-1111	(888) 397-3742	Chester, Pennsylvania
www.equifax.corn	www.experian.com	(800) 888-4213
		www.transunion.com

Consider Placing a Fraud Alert

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:	Report Fraud:	1.888.766.0008
Experian:	Report Fraud:	1.888.397.3742

TransUnion: Report Fraud: 1.800.916.8800

Security Freeze for Credit Reporting Agencies

You may wish to request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. 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. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $10.00, (or in certain states such as Massachusetts, no more than $5.00), each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the following addresses:

- Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348
- Experian Security Freeze, P.O. Box 9554, Allen, TX 75013
- TransUnion Security Freeze, Fraud Victim Assistance Department, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016

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

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft
- If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Don't send cash through the mail.

The credit reporting agencies have three business days after receiving your request 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 freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include (1) proper identification (name, address, and Social Security number), (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities 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 three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze all together, you must send a written request to each of the three credit bureaus by mail 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 three business days after receiving your request to remove the security freeze.

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Suggestions If You Are a Victim of Identity Theft

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

- Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1.877.IDTHEFT (1.877.438.4338); online at http://www.ftc.gov/idtheft; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from: http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.

- Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log

of your conversations with creditors, law enforcement officials, and other relevant parties.

Take Steps to Avoid Identity Theft

Further information can be obtained from the FTC about steps to take to avoid identity theft through the following paths: http://www.ftc.gov/idtheft; calling 1.877.IDTHEFT (1.877.438.4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

State-Specific Information

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at http://www.oag.state.md.us/idtheft/index.htm, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, calling 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at http://www.atg.state.vt.us.