Buchanan
Ingersoll·Rooney

Jason R. McLean
412 562 1474
jason.mclean@bipc.com

Union Trust Building
501 Grant Street, Suite 200
Pittsburgh, PA 15219-4413
T 412 562 8800
F 412 562 1041

September 28, 2021

Via Email and Mail

Office of the Attorney General
Consumer Protection and Antitrust
Gateway Professional Center
1050 E Interstate Avenue Suite 200
Bismarck, ND 58503-5574
Email: ndag@nd.gov

Re: Notice of Breach

Dear Attorney General:

We represent Wm. G. Roe & Sons, Inc. ("Wm. G. Roe & Sons") and are writing to notify your office of a breach that may affect some personal information relating to two (2) North Dakota residents. This notice may be supplemented with new significant facts learned subsequent to its submission. By providing this notice, Wm. G. Roe & Sons does not waive any rights or defenses regarding the applicability of North Dakota law, the applicability of the North Dakota data breach notification statute, or personal jurisdiction.

Nature of the Breach

In mid-June 2021, an unscrupulous hacker obtained access to portions of Wm. G. Roe & Sons' computer system. This unauthorized access initially manifested as a ransomware attack, and W. G. Roe & Sons' took immediate measures to secure its system and prevent further damage to its network and data. Wm. G. Roe & Sons retained a third-party cybersecurity team to assist with the recovery of its systems. Upon further forensic investigation into the extent and cause of the incident, Wm. G. Roe & Sons discovered that the attackers conducted certain data exfiltration activities in their network prior to launching the malware. The attackers may have taken a data file containing certain current and former employee information, although the cybersecurity professionals were unable to confirm this. The personally identifiable information in the data file included names and social security numbers.

Notice to North Dakota Residents

On or about September 28, 2021, the Wm. G. Roe & Sons began providing written notice of this breach to potentially affected individuals, which includes two (2) North Dakota residents. Written notice is being provided in substantially the same form as the letter attached here as Exhibit A.

Other Steps Taken and To Be Taken

As soon as Wm. G. Roe & Sons became aware of this situation, it engaged expert assistance to stop further unauthorized access to its systems and accelerated its plan to install additional security measures across its environment. Wm. G Roe & Sons also engaged a cybersecurity forensic expert to investigate

whether any files were accessed or removed by the threat actor. The investigator could not rule out the possibility that the data file containing employee information had been compromised. Wm. G. Roe & Sons then searched for updated address information for all potentially affected individuals, who are either current or former employees.

To help relieve concerns and restore confidence following this incident, Wm. G. Roe & Sons has secured the services of Kroll to provide identity monitoring at no cost to affected individuals for one year. Kroll has extensive experience helping people who have sustained potential compromise of their personally identifiable information. The identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Thank you for your attention to this matter, and should you require any further information, please do not hesitate to contact me.

Very truly yours,

Jason R. McLean, Esq.

Enclosure

EXHIBIT A

FLORIDA FRUITS & JUICES
SINCE 1927

Wm. G. Roe & Sons, Inc.

PACKERS • PROCESSORS • GROWERS • MARKETERS
SPECIALIZING IN FRESH CITRUS AND FRESH BLUEBERRIES

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Wm.G. Roe & Sons, Inc. recently experienced a data security incident that may have involved unauthorized access to some of your personal information. We want you to know about this incident, although we are not certain that any of your information was in fact taken or misused. We also want to provide you with some resources to help protect your personal information, and to offer to pay for one year of credit monitoring and identity restoration should you chose to take advantage of these services.

What Happened: An unscrupulous hacker obtained access to portions of our computer system and appears to have accessed and possibly taken a data file containing employee information. We engaged a cybersecurity forensic firm to conduct an investigation, but they were unable to determine with certainty whether your information was actually taken by the unauthorized person. Still, we recognize that you will want to know this occurred so you can consider taking appropriate precautions.

What Information Was Involved? The personal information in the data file included your name and Social Security number.

Our Response: As soon as we became aware of this situation, we engaged expert assistance to stop further unauthorized access to our systems and accelerated our plan to install additional security measures across our environment. We also engaged a cybersecurity forensic expert to investigate which, if any, files were accessed or removed by the threat actor. The investigation was inconclusive and the investigator could not rule out the possibility that the data file containing employee information had been compromised.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **December 30, 2021** to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

Additional information describing your services is included with this letter.

What Else You Can Do to Help Protect Your Information: We encourage you to be on the alert for incidents of identity theft and fraud by monitoring your account statements and credit reports for suspicious activity and reviewing the attached information under the caption, “Additional Steps to Help Protect Your Information.”

For More Information: We encourage you to sign up for the free identity monitoring services by going to **https://enroll.krollmonitoring.com** and using your personal Membership Number contained within this letter.

We deeply regret the concern or inconvenience this matter may cause you. We take data protection very seriously and are committed to protecting the privacy of information stored in our systems. We recognize that you may have questions that have not been addressed in this letter. If you have additional questions, please contact us at 863-251-4017.

Sincerely,

Wm. G. Roe & Sons, Inc.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Additional Steps to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and 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 incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission ("FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 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 also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com

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

Security Freeze: You have the right to place a security freeze on your credit file. This will prevent new credit from being opened in your name without your express authorization. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit

file with each credit reporting agency. There is no fee to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the Federal Trade Commission or from your state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to your state Attorney General.

Federal Trade Commission (FTC): The FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www. identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and, TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them as explained on their website. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

Fair Credit Reporting Act (FCRA): You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Maryland residents: You can contact the State Attorney General at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov .

For New York residents: You can contact the State Attorney General at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For North Carolina residents: You can contact the State Attorney General at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.