



Brian T. Sniffen
971.347.1410 direct line
brian.sniffen@wildwoodlaw.com

3519 NE 15th Ave, Ste 362
Portland, Oregon 97212
www.wildwoodlaw.com
Office: 503.564.3049

April 15, 2022

VIA EMAIL

(ndag@nd.gov)

Office of Attorney General
600 East Boulevard Avenue, Dept 125
Bismarck, North Dakota 58505-0040

Subject: Notice of Data Security Incident

Dear All:

This firm represents Bob's Red Mill Natural Foods, Inc., an Oregon-based food manufacturer with its headquarters at 13521 SE Pheasant Ct., Milwaukie, Oregon 97222. Pursuant to North Dakota law, we are writing to notify you of a data-security incident that Bob's Red Mill recently suffered. This incident may have impacted three North Dakota residents.

What happened?

Bob's Red Mill recently learned that, between February 23 and March 1, 2022, malicious software was used to "scrape" purchase-related information entered into its website. This information typically goes directly (and via secure protocols) to its payment processor – but the scraping software is intended to interfere with that. Immediately upon learning of the issue, Bob's Red Mill began an investigation and took steps to fix the problem. It has isolated and removed the malicious software such that website purchases are again secure.

Initially, Bob's Red Mill had no evidence that any of the information was acquired (e.g., downloaded or exfiltrated from the website). Nor did it have any indication that the information had been used in any way – such as to make fraudulent purchases. But it continued to look into the incident. On March 22, Bob's Red Mill received a call from a customer who indicated that they incurred a fraudulent charge. Bob's Red Mill received a number of similar reports this month. We do not know if these fraudulent charges are related to the website incident, but it now appears possible that payment-card (and other) information may have been acquired. Bob's Red Mill is therefore providing notice to you and impacted North Dakota residents (a copy of the consumer notice is enclosed) so they can take

steps to protect themselves. Bob's Red Mill is sending consumer notifications as quickly as possible: it plans to mail notification letters to North Dakota residents this week or next week.

What information was involved?

The scraping software appears to have impacted data entered when customers made purchases from the Bob's Red Mill website. The following information therefore appears to have been involved: payment-card number, expiration date, CVV number, billing address and shipping address, including name and street address, e-mail address, phone number, and purchase amount.

Bob's Red Mill believes that this incident was limited to its website and limited to the period from February 23 - March 1, 2022. It does not believe any of its physical/in-person point-of-sale terminals have been impacted, or that purchases made outside the February 23-March 1 window have been impacted. There is also no information to indicate that Social Security numbers, driver's license numbers or other government-issued ID numbers, dates of birth, or other sensitive personal information or online account credentials have been compromised. As a result, Bob's Red Mill believes this incident presents a low risk of identity theft.

What Bob's Red Mill is doing

As an organization, Bob's Red Mill is committed to ensuring the security of its customers' personal information. The steps it has taken to address this incident include:

- When it first learned of this incident, it immediately began an investigation and took steps to fix the problem – such as identifying, isolating, and removing the malicious software.
- It immediately notified, and will work with, its payment processor to reduce the likelihood of this type of incident happening again.
- It immediately notified the payment-card brands it works with (American Express, Discover, Mastercard, and Visa) and will work with them to reduce the likelihood of this type of incident happening again.
- It already devotes significant resources to data security, including the security of payment systems.
- It will learn from this incident and use the information uncovered during its investigation to further bolster its data security and incident-response processes.

Office of Attorney General
April 15, 2022
Page 3 of 3

If you have any questions, please contact me at (971)347-1410 or
brian.sniffen@wildwoodlaw.com.

Best regards,

A handwritten signature in blue ink, appearing to read "B. Sniffen". The signature is fluid and cursive, with the first letter of the last name being a large, stylized "S".

Brian T. Sniffen

Enclosure



[DATE]

<Name>

<Address Line 1>

<Address Line 2>

<City>, <State> <Zip Code>

Subject: Notice of data breach. Please read this entire letter.

Dear <Name>,

We are writing to notify you about a data-security incident that may have affected the credit card (or other payment card) you used when making a purchase on our website, BobsRedMill.com (<https://www.bobsredmill.com/>).

This letter contains important information about what happened, including steps you should take to reduce the risk that any fraudulent transactions are completed with your card. The privacy and security of our customers' information is important to us, and we apologize for the concern and inconvenience this incident may cause you.

What happened?

We recently learned that, between February 23 and March 1, 2022, malicious software was used to "scrape" purchase-related information entered into our website. This information typically goes directly (and via secure protocols) to our payment processor – but the scraping software is intended to interfere with that. Immediately upon learning of the issue, we began an investigation and took steps to fix the problem. We have isolated and removed the malicious software such that website purchases are again secure.

Initially, we had no evidence that any of the information was acquired (e.g., downloaded or exfiltrated from the website). Nor did we have any indication that the information had been used in any way – such as to make fraudulent purchases. But we continued to look into the incident. On March 22, we received a call from a customer who indicated that they incurred a fraudulent charge. We received a number of similar reports this month. We do not know if these fraudulent charges are related to our website incident, but it now appears possible that payment-card (and other) information may have been acquired. We are therefore providing you with this notice so you can take steps to protect yourself.

Bob's Red Mill Natural Foods, Inc.

13521 SE Pheasant Court, Milwaukie, OR 97222

PHONE: (503) 654-3215 • (800) 349-2173 • FAX: (503) 653-1339 • [bobsredmill.com](https://www.bobsredmill.com)

FLOURS • OATMEAL • BARS • GRAINS • BAKING MIXES • GRANOLAS

What information was involved?

The scraping software appears to have impacted data entered when customers made purchases from our website. The following information therefore appears to have been involved: payment-card number, expiration date, CVV number, billing address and shipping address, including name and street address, e-mail address, phone number, and purchase amount.

We believe that this incident was limited to our website and limited to the period from February 23 - March 1, 2022. We do not believe any of our physical/in-person point-of-sale terminals have been impacted, or that purchases made outside the February 23-March 1 window have been impacted. There is also no information to indicate that Social Security numbers, driver's license numbers or other government-issued ID numbers, dates of birth, or other sensitive personal information or online account credentials have been compromised. As a result, we believe this incident presents a low risk of identity theft.

If you are receiving this letter, it is because we believe your purchase-related information may have been among the data impacted by the malicious software between February 23 and March 1.

What we are doing

As an organization, we are committed to ensuring the security of our customers' personal information. The steps we have taken to address this incident include:

- When we first learned of this incident, we immediately began an investigation and took steps to fix the problem – such as identifying, isolating, and removing the malicious software.
- We immediately notified, and will work with, our payment processor to reduce the likelihood of this type of incident happening again.
- We immediately notified the payment-card brands we work with (American Express, Discover, Mastercard, and Visa) and will work with them to reduce the likelihood of this type of incident happening again.
- We already devote significant resources to data security, including the security of payment systems.
- We will learn from this incident and use the information uncovered during our investigation to further bolster our data security and incident-response processes.

Please note that this letter was not delayed because of a law-enforcement investigation.

What you can do

Monitor your payment-card accounts and report any unauthorized transactions or other suspicious activity to the applicable card brand or card issuer.

Bob's Red Mill Natural Foods, Inc.

13521 SE Pheasant Court, Milwaukie, OR 97222

PHONE: (503) 654-3215 • (800) 349-2173 • FAX: (503) 653-1339 • bobsredmill.com

FLOURS • OATMEAL • BARS • GRAINS • BAKING MIXES • GRANOLAS

You should be vigilant and regularly review and monitor your payment-card account statements and immediately report any suspicious activity to the applicable card brand or card issuer.

Monitor your credit reports.

As with your payment-card account statements, you should regularly review your credit reports and report any suspicious activity or inaccurate information to the applicable credit-reporting agency and the company that furnished the suspicious or inaccurate information. You have the right to obtain a copy of your credit report for free once a year from one of the national credit-reporting agencies.

You may obtain your free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 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 purchase additional credit reports by contacting one or more of the three following national credit-reporting agencies:

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 800-685-1111, www.equifax.com

Experian: P.O. Box 9532, Allen, TX 75013, 888-397-3742, www.experian.com

TransUnion: P.O. Box 1000, Chester, PA 19022, 800-888-4213, www.transunion.com

You may also obtain information regarding fraud alerts and security freezes from the foregoing credit-reporting agencies and the Federal Trade Commission ("FTC").

Report any suspicion of identity theft to regulators.

If you ever suspect that you are the victim of identity theft, please report that to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center: 600 Pennsylvania Avenue, NW, Washington, DC 20580, 877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Other important information

Be aware.

We will never contact you by phone or e-mail to ask for payment-card information or other sensitive personal information. If you ever receive a call, e-mail, or text message purporting to be from Bob's

Bob's Red Mill Natural Foods, Inc.

13521 SE Pheasant Court, Milwaukie, OR 97222

PHONE: (503) 654-3215 • (800) 349-2173 • FAX: (503) 653-1339 • bobsredmill.com

FLOURS • OATMEAL • BARS • GRAINS • BAKING MIXES • GRANOLAS

Red Mill and asking for such information, it is likely a scam. If you are ever in doubt, please call us at the number listed below to confirm the legitimacy of the call, e-mail, or text message.

We are including some state-specific information as an enclosure to this letter. You should review the enclosure to see if any of the additional information pertains to you.

For more information

If you have any questions or would like more information about this incident, please contact us at 971-233-8799, Monday – Friday, from 9:00a.m. – 4:00p.m. Pacific Time.

We appreciate your business and trust, and sincerely apologize for this incident and the inconvenience or concern it may cause.

Sincerely,

Bill Lozier
Chief Operating Officer

Enclosure

Bob's Red Mill Natural Foods, Inc.

13521 SE Pheasant Court, Milwaukie, OR 97222

PHONE: (503) 654-3215 • (800) 349-2173 • **FAX:** (503) 653-1339 • bobsredmill.com

FLOURS • OATMEAL • BARS • GRAINS • BAKING MIXES • GRANOLAS

ENCLOSURE – STATE-SPECIFIC INFORMATION

District of Columbia Residents. Under federal law (15 U.S.C. § 1681c-1), you have the right to obtain a credit freeze – also known as a security freeze – on your credit file. There is no charge for a credit freeze (or for temporarily lifting or permanently removing the freeze). To request a security freeze, you must contact each of the credit-reporting agencies listed in the body of our letter. You should be prepared to provide the following information in connection with your credit-freeze request:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.), Social Security number, and date of birth;
2. If you have moved in the past five years, the addresses where you have lived over the previous five years;
3. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
4. A legible photocopy of a government-issued ID card;
5. Social Security card, pay stub, or Form W-2; and
6. If you are a victim of identity theft, a copy of the police report, investigative report, or complaint to a law-enforcement agency concerning the theft.

You can obtain more information about fraud alerts, credit freezes, and preventing identity theft by contacting the FTC at the information listed in the body of our letter, visiting the FTC's website at <https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts>, contacting one of the credit-reporting agencies listed in the body of our letter, or contacting the Office of the Attorney General for the District of Columbia ("AGDC").

The AGDC can be reached at the following:

<https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft>, 202-727-3400, 400 6th Street, NW, Washington, DC 20001.

Maryland Residents. The Maryland Attorney General ("MAG") can be reached at the following: <https://www.marylandattorneygeneral.gov/pages/identitytheft/default.aspx>, 1-888-743-0023, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202.

In addition to the FTC, you can obtain information from the MAG regarding steps you can take to prevent identity theft.

New Mexico Residents. Under the federal Fair Credit Reporting Act ("FCRA"), you have several rights – including the following:

1. You must be told if information in your file has been used against you;
2. You have the right to know what is in your file;
3. You have the right to ask for a credit score;
4. You have the right to dispute incomplete or inaccurate information;
5. Consumer-reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information;
6. Consumer-reporting agencies may not report outdated negative information;
7. Access to your file is limited;
8. You must give your consent for reports to be provided to employers;
9. You may limit "prescreened" offers of credit and insurance you get based on information in your credit report;
10. You have the right to obtain a security freeze, or place a fraud alert, on your credit report;
11. You may seek damages from violators; and
12. Identity-theft victims and active-duty military personnel have additional rights.

Additional information regarding your rights under the FCRA can be found here: <https://www.consumerfinance.gov/learnmore/>.

North Carolina Residents. The North Carolina Attorney General's Office ("NCAG") can be reached at the following:

<https://ncdoj.gov/protecting-consumers/protecting-your-identity/>, 1-877-5-NO-SCAM, and 9001 Mail Service Center, Raleigh, NC 27699-9001.

In addition to the FTC, you can obtain information from the NCAG regarding steps you can take to prevent identity theft.

Rhode Island Residents. You have the right to file a police report if you ever experience identity theft or fraud. If you file a police report, or if a police report is filed regarding this incident, you have a right to obtain a copy of that report.

You also have the right to request a credit freeze – also known as a security freeze – as outlined under the "District of Columbia Residents" section above.

The Rhode Island Attorney General can be contacted at:

www.riag.ri.gov, 401-274-4400, 150 South Main Street, Providence, RI 02903.

West Virginia Residents. For information regarding how to place a credit freeze – also known as a security freeze – see the information outlined in the "District of Columbia Residents" section above. You may also be eligible for a fraud alert. There are two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling any of the three credit-reporting agencies listed in the body of our letter. There is no charge for a fraud alert.