PIERSON FERDINAND

TARA TURNER
PARTNER

333 SE 2nd Avenue, Suite 2000
Miami, FL 33131

Direct: 1.786.558.2100
Email: Tara.Turner@pierferd.com

CONFIDENTIAL

May 11, 2026

VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Pierson Ferdinand LLP represents Millborn Seeds, Inc. ("Millborn"), located at 2132 32nd Avenue, Brookings, SD 57006, with respect to a data security incident described in more detail below. The purpose of this letter is to notify you of a data security incident in accordance with New Hampshire's data breach notification statute. Millborn takes the security and privacy of the information in its control seriously and is taking steps to prevent a similar incident from occurring in the future.

1. Description of the Incident.

On or about January 21, 2026, Millborn experienced a data incident, which may have affected the information of New Hampshire residents (the "Incident"). Millborn has since worked diligently to determine what happened and what information may have been impacted as a result of this Incident.

Based upon the evidence available, an investigation conducted by third-party forensic specialists determined the incident occurred on or around January 21, 2026, through January 28, 2026, and was discovered on or around January 28, 2026. Following the investigation, a data mining exercise was conducted of the potentially impacted data set to identify the potentially impacted individuals and what elements of their personally identifiable information may have been affected so that an informed notification could be provided.

As of this writing, Millborn has not received any reports of fraud or identity theft related to this matter.

PIERSON FERDINAND

2. Number of New Hampshire Residents Affected and Information involved.

The incident involved the personal information of one (1) New Hampshire resident. The information involved in the incident includes New Hampshire resident's name, credit/debit card number and CVV/expiration date.

3. Notification.

A letter was mailed to the affected New Hampshire residents by USPS First Class Mail on May 6, 2026. The notification letter provides resources and steps the individual can take to help protect his/her information. The notification letter also offers complimentary identity protection services, including 12 months of credit monitoring, and fully managed identity theft recovery services. Those services are offered through Kroll, a global leader in risk mitigation and response with experience helping people who have sustained an unintentional exposure of confidential data. A copy of the notification letter sent to the impacted individual is included with this correspondence.

4. Steps taken to address the Incident.

Upon discovery of the Incident, Millborn worked with cybersecurity counsel and forensic experts to investigate how the Incident occurred and what information may have been impacted.

Millborn also implemented additional security measures to secure its environment in an effort to prevent a similar event from occurring in the future. Millborn is also notifying the affected individuals and providing them with steps they can take to protect their personal information.

5. Contact information.

Millborn remains dedicated to protecting information within its control. If you have any questions or need additional information, please do not hesitate to contact me at tara.turner@pierferd.com or (786)-558-2100.

Very truly yours,

Tara Turner

Tara Turner, Esq.
Pierson Ferdinand LLP

Enclosure: Consumer Notification Letter

Millborn Seeds, Inc

Return to Kroll
P.O. Box 3826
Suwanee, GA 30024

2
XXXXXXXXXX XXXXXXXXXXXX
XXX XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXX, NH XXXXX-XXXX

SCAN TO ENROLL

May 6, 2026

Notice of Data Incident

Dear Xxxxxxxxxx Xxxxxxxxxxxx:

Millborn Seeds, Inc. ("Millborn") experienced a data incident which may have affected your personal information. Based on our current review, we have no indication that your personal information has been or will be used inappropriately, but we wanted to make you aware of the incident, the measures we have taken in response, and to provide details on the steps you can take to help protect your information. We take the protection and proper use of your information seriously and are working to prevent a similar incident from occurring again in the future.

What Happened

On or about January 28, 2026, Millborn became aware of a compromise to an employee's email account, which may have resulted in the exposure of personal information contained within that account. We promptly launched an investigation, engaged a national cybersecurity firm to assist in assessing the scope of the incident and took steps to mitigate the potential impact to our community. A third-party forensic investigation determined the incident occurred on January 21, 2026, to January 28, 2026.

What Information Was Involved

Following a diligent review of the data potentially impacted, we determined the elements of your personal information that may have been included are your XXXX, XXXXXXXXXXXXXXXXXXXX, XXXX, and XXXXXXXXXX.

Please note that we have no evidence at this time that any of your personal information has been or will be misused as a result of the incident.

What We Are Doing

Upon discovering the incident, we promptly launched an investigation and engaged a national cybersecurity firm to assist in assessing the scope of the incident. As part of our ongoing commitment to the security of information, we are evaluating opportunities to further secure our systems to prevent a similar event from occurring again in the future, including increasing security measures to prevent unauthorized access and protocols to ensure that data is transmitted securely.

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 12 months. 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.

These services provide you with 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'll 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. 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. Activating these services will not affect your credit score.

What You Can Do

To enroll in the complimentary services we are offering you, please visit **https://enroll.krollmonitoring.com** and follow the instructions provided. You have until **August 4, 2026** to activate your identity monitoring services. When prompted, please provide the following membership number: **XXXXXXXXX-X**.

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

At this time, we are not aware of anyone experiencing fraud as a result of this incident. As data incidents are increasingly common, we encourage you to always remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following pages, which contain important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

What can I do on my own to address this situation?

If you choose not to use these services, we strongly urge you to do the following:

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)	**Equifax (1-800-525-6285)**	**TransUnion (1-800-680-7289)**
P.O. Box 4500	**P.O. Box 740241**	**P.O. Box 2000**
Allen, TX 75013	**Atlanta, GA 30374**	**Chester, PA 19016**
www.experian.com	www.equifax.com	www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204).
- Be sure to promptly report any suspicious activity to Millborn Seeds, Inc.

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft.

For More Information

Please know that the protection of your personal information is a top priority, and we understand the inconvenience and concern this incident may cause. Representatives can be reached at (844) 403-4624 between the hours of 8:00 a.m. to 5:30 p.m. Central time, Monday through Friday, excluding major U.S. holidays. Please have your membership number ready.

Sincerely,

Marcus Heemstra

Marcus Heemstra
Millborn Seeds, Inc.

Additional Important Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348 equifax.com/personal/credit-report-services/	Allen, TX 75013 experian.com/freeze/center.html	Woodlyn, PA 19094 transunion.com/credit-freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.

Implementing an Identity Protection PIN (IP PIN) with the IRS:

To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. If you want to request an IP PIN, please note: you must pass an identity verification process; and Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register to validate your identity.

Some items to consider when obtaining an IP PIN with the IRS:

- An IP PIN is valid for one calendar year.
- A new IP PIN is generated each year for your account.
- Logging back into the Get an IP PIN tool, will display your current IP PIN.
- An IP PIN must be used when filing any federal tax returns during the year including prior year returns.

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Vermont*: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For residents of *New Mexico*: 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.

For Residents of *Washington, D.C.*: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.gov

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts and Rhode Island*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.