



ROPES & GRAY LLP
191 NORTH WACKER DRIVE
32nd FLOOR
CHICAGO, ILLINOIS 60606-4302
WWW.ROPESGRAY.COM

October 31, 2024

Matthew R. Cin
T +1 312 845 1357
matthew.cin@ropesgray.com

BY E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Data Incident

Dear Attorney General Brown:

We write on behalf of our client, BINA Farm Inc. (“BINA”), a 501(c)(3) nonprofit organization, to inform you of a security incident that may have affected the personal information of two (2) Maryland residents.

On March 4, 2024, BINA discovered that it was the target of a security incident in which an unknown intruder gained access to a BINA employee’s email account and a portion of BINA’s cloud storage (the “incident”). Upon discovery of the incident, which started approximately February 28, 2024, and lasted through March 4, 2024, BINA engaged external counsel and third party cybersecurity forensic experts, and launched a thorough investigation. That investigation determined that two (2) Maryland residents’ information may have been affected. Specifically, the individuals’ name, date of birth, driver’s license number, insurance policy number, and vaccination records may have been accessed by the intruder.

In the period since the discovery of the intrusion, BINA has implemented enhanced safeguards to help prevent another incident. These include resetting all user passwords, enabling enhanced logging to quickly detect malicious activity, and requiring multi-factor authentication for remote access.

As of this date, BINA is not aware of any improper use of any of the potentially impacted personal information. Nevertheless, as a precautionary measure, BINA is notifying potentially affected individuals on October 31, 2024.

October 31, 2024

As part of the notice package, BINA is offering complimentary 24-month credit monitoring to all individuals who are receiving a notification letter. Additional information on credit monitoring services and a telephone number that consumers may call for further information and assistance is included in the attached sample notification made to the potentially affected parties. If you have any questions, please reach out to us at +1 (312) 845-1357.

Sincerely,

A handwritten signature in blue ink, appearing to read "Matthew Cin".

Matthew R. Cin



BINA Farm Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
DB09294

0_0000464



October 31, 2024

Notice of Data Breach

Dear [REDACTED],

We are writing to share information with you about a cyber incident regarding BINA Farm Inc. ("BINA") that may have affected your personal information. While we are not aware of any actual or attempted misuse of the information, we are providing you with information about the security incident and additional measures you can take if you wish to do so.

What Happened?

On February 28, 2024, an unknown intruder gained unauthorized access to a BINA employee's email account and may have had access to a portion of BINA's cloud storage environment. This intrusion was detected on March 4, 2024, at which point the intruder's access was eradicated. After reviewing those files, some of your personal information was identified as being contained within the potentially affected dataset.

What Information May Have Been Involved?

Personal information which may have been exposed includes name, contact information, social security number, driver's license or military identification card number, and certain medical information.

What We Are Doing.

Upon discovery of the incident, BINA took steps to identify, contain and remediate the issue, including by locking down its systems and strengthening security controls. BINA also engaged a leading forensics firm to determine the means of ingress and what information (if any) may have been accessed by the intruder, and took steps to safeguard our systems and information, including by resetting passwords for all personnel accounts with access to the potentially affected environment and launching a thorough investigation of the unstructured data in the relevant email accounts.

What You Can Do.

Although we are not aware of any fraudulent activity associated with your personal information, as a protective measure, we are providing notice of this incident so that you may take further steps to help protect your personal information should you feel it is appropriate to do so.

We always encourage you to regularly review your financial accounts and report any suspicious or unrecognized activity. The enclosed “General Information About Identity Theft Protection” provides further information about steps that individuals can take. Federal regulatory agencies recommend vigilance for the next 12 to 24 months and that you report any suspected incidents of fraud to the relevant financial institution.

Other Important Information.

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. We are also providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company, specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to **<https://bfs.cyberscout.com/activate>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **75E3713090F6**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

If you have any additional questions related to this letter, please contact our dedicated assistance line at 1-800-405-6108 and supply the fraud specialist with your unique code listed above. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

Sincerely,

BINA Farm Inc.



GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

It is always advisable to regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. 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, P.O. Box 740241, Atlanta, Georgia 30374-0241, 1.800.685.1111, www.equifax.com

Experian, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742, www.experian.com

TransUnion, Consumer Disclosure Center, P.O. Box 1000, Chester, PA 19016, 1.800.916.8800, www.transunion.com

Fraud Alert: You may contact 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:	1.800.685.1111
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.680.7289

Security Freeze for Credit Reporting Agencies: You may 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. It is free to place, lift or remove a security freeze. You must separately place a security freeze on your credit report at each credit bureau. To do so, you must contact the credit bureaus by phone, mail, or secure electronic means:

Equifax: P.O. Box 105788, Atlanta, GA 30348, 1.888.298.0045, www.Equifax.com

Experian: P.O. Box 9554, Allen, TX 75013, 1.888.397.3742, www.Experian.com

TransUnion: P.O. Box 160, Woodlyn, PA 19094, 1.800.916.8800, www.TransUnion.com

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 request a freeze online or by phone, the agency must place the freeze within one business day. The credit bureaus have three business days after receiving a request by mail to place a security freeze on your credit report, and they must also send 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 contact the credit reporting agencies and include (1) proper identification; (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.

You also 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 https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf or www.ftc.gov.

Steps You Can Take 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 (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.

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 helpful to log conversations with creditors, law enforcement officials, and other relevant parties.

Additional Steps to Avoid Identity Theft: The FTC has further information about steps to take to avoid identity theft at: <http://www.ftc.gov/idtheft>; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

State Specific Information

District of Columbia residents may contact the District of Columbia Attorney General at 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and <https://oag.dc.gov/>.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, calling the Identity Theft Unit at 1.410.576.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202.

New York residents may contact the New York Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

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 <https://ncdoj.gov/protecting-consumers/protecting-your-identity/>, calling 1.919.716.6000 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

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 <https://ago.vermont.gov/>.