Schwabe
WILLIAMSON & WYATT®

December 7, 2018

Colin Folawn
Admitted in Washington and Oregon
T: 206-407-1500
cfolawn@schwabe.com

VIA FIRST CLASS MAIL

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

RE: Cybersecurity Incident Notification
Our File No.: 125014-221195

Dear Attorney General MacDonald:

On behalf of our client, Farmer Bros. Co. ("FBC"), we writes to notify you of a cybersecurity incident involving three New Hampshire residents.

On September 18, 2018, FBC became aware of a potential cyber incident involving unauthorized third-party access to multiple FBC email accounts. Upon learning of this incident, FBC immediately worked to restore the security of the email accounts and began a thorough investigation through a nationally-recognized cyber incident response team to identify what information was stored in the affected systems. Based on the investigation, on November 15, 2018, FBC determined that the affected systems contained the name, driver's license number, and social security number of three residents of New Hampshire.

Commencing on December 11, 2018, FBC is mailing notification letters to the three New Hampshire residents in accordance with N.H. Rev. Stat. Ann. § 359-C:20 in substantially the same form as the attached letter. FBC has provided contact information that the potentially affected individual can use to contact FBC with questions. FBC is also recommending that the potentially affected individual remain vigilant to the possibility of fraud by reviewing their account statements and credit reports for unauthorized activity.

FBC takes the privacy and security of personal information very seriously. Upon learning of the incident, FBC immediately reset the passwords for the affected email accounts and implemented stronger password policies. To help prevent this type of incident from happening again, FBC is working to improve the security of its network and data to protect from other unauthorized access to sensitive personal and financial information. In particular, FBC has taken measures to enhance the protections of FBC's company email accounts against access by unauthorized individuals conducting similar criminal activity in the future. In addition, FBC is educating its employees on measures they can take to ensure the protection of sensitive personal information.

Please do not hesitate to contact me if you have any questions about this matter.

Best regards,

SCHWABE, WILLIAMSON & WYATT, P.C.

Colin Folawn

CJF:res
Enclosure

PDX\125014\221195\CJF\24408220.1

To Enroll, Please Call:
(866) 887-1306
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<XXXXXX>>

C/O ID Experts
P.O. Box 10444
Dublin, OH 43017-4044

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 11, 2018

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We take the security of your information seriously, and want to let you know about a cyber incident potentially related to your personal and/or financial information.

What Happened

On September 18, 2018, Farmer Bros. Co. ("Farmer Brothers") became aware of a cyber incident in which multiple Farmer Brothers company email accounts were accessed by an unauthorized third party. After conducting a thorough investigation through a nationally-recognized cyber incident response team, which concluded in November, it was discovered that some of those email accounts contained your personally identifiable information and/or financial information. However, due to technical limitations inherent in standard commercial email systems, we were unable to determine whether your personal and/or financial information was actually accessed, viewed, or copied by an unauthorized third party.

Nevertheless, out of an abundance of caution, and in accordance with individual state security breach notification laws, we are providing this notice to you as a potentially affected party. The following information and resources are being provided to you at no cost, to assist with protecting and monitoring your information for any potential unauthorized activity.

What Information Was Involved

The investigation conducted by the cyber incident response team revealed that the types of information at issue varied widely. The types of personal and/or financial information that may have been accessed include *one or more of the following*, depending upon the affected individual: name, address, Social Security number, driver's license number, date of birth, payment card number, payment card security access code (CVV) and/or expiration date, email address, passport number, phone number, bank account number, bank routing number, and individual taxpayer identification number.

What We Are Doing

We have taken measures to enhance the protections of our company email accounts against access by unauthorized individuals conducting similar criminal activity in the future. We are also working to further improve the security of the Farmer Brothers network and data systems to protect against other unauthorized access attempts.

In addition, we are offering to you identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do

Although we have no indication your information was actually accessed, copied, or misused, we encourage you to remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your free credit reports. We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (866) 887-1306 or going to https://app.myidcare.com/account-creation/protect, using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday between 5 A.M. and 5 P.M. Pacific Time. Please note the deadline to enroll is March 11, 2019.

Again, at this time, there is no conclusive evidence that your personal or financial information has been actually accessed, copied, or misused. However, we encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal and financial information.

You also are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling on online, so please do not discard this letter.

Please call (866) 887-1306 or go to https://app.myidcare.com/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Michael H. Keown
CEO and President
Farmer Bros. Co.

(Enclosure)

MyIDCare

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at (866) 887-1306 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: 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 a violator. 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. You can 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.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.