Farmgirl FLOWERS™

May 9, 2018

New Hampshire Department of Justice
Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General MacDonald:

On April 29th, 2018, Farmgirl Flowers, Inc., discovered that it's system were recently compromised and as a result, the personal information of some of your state's residents may have been disclosed.

The details of the incident are as follows:

- On April 26, 2018 an executable file containing rogue code was inserted by unknown persons into the Farmgirl Flowers website's checkout page. The code was designed to download an executable file to the user's browser while on the Farmgirl Flower's website and capture any information entered by a customer at the checkout page and send that data to a remote endpoint.
- The code was removed on April 29, 2018.
- Between April 26th, 2018 and April 29th, 2018 the personal information of 1,870 individuals may have been compromised, including 4 residents of your state.
- The types of information that may have been compromised are: name, billing address for a credit card, telephone number, email address, and credit card information including card number, name on card, issuer, expiration date, and security code.

Upon learning of the unauthorized access, Farmgirl Flowers took immediate measures to remove the code and to investigate and implement additional security measures to prevent a similar incident from occurring.

To address the incident, Farmgirl Flowers is taking the following actions:

- We are implementing vigorous, whitelist-based access controls and password policies, as well as deploying a more robust intrusion detection system. All company technical and operational security is being audited and, where necessary, redesigned.
- We plan to notify all of potentially affected customers, including 4 residents of your state, by letter mailed on May 10, 2018.
- We are also offering these individuals 24 months of credit monitoring, fraud alert, and identity repair services provided by AllClear ID. Additional details about the affected individuals are available upon request. A copy of a letter we are sending to residents to your state is enclosed. We have also provided notice to credit reporting agencies, the FBI, and local law enforcement in San Francisco, California.

We regret this situation occurred, and will be working to reduce the risks of similar situations happening in the future. If you have any questions, please contact Christina Stembel at (415) 602-9099 or christina@farmgirlflowers.com.

Sincerely,

Christina Stembel

Farmgirl FLOWERS™
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00061
00002 ACD1234
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 11, 2018

Re: NOTICE OF DATA BREACH

We are so sorry to inform you that we recently became aware of a data breach that may have compromised your personal information. We understand how important your privacy is, and we take the protection of your information very seriously. Our company is built on honestly, trust, and transparency, which is why I'm reaching out personally to let you know about what happened and what we're doing to address it.

What Happened?

On April 29, 2018, at approximately 4:00 p.m. (all times PST), we learned that there was unauthorized access by electronic means to our data by a person or persons whose identities remain unknown. The unauthorized access occurred sometime between 1:00 p.m., on April 26, 2018, and 3:08 p.m., on that same date. The unauthorized access involved the insertion of rogue code into our checkout page. The code was designed to capture the name, billing address, phone number, and email address of certain customers, and also their credit card information, and then send that data to a remote endpoint. The customer order dates for potentially compromised information are April 26, 2018, at 1:00 p.m., until April 29, 2018, at 4:10 p.m. Although we cannot be sure that any of your information was accessed or misappropriated, we are sending you this notice to make you aware of the situation and to provide you with other helpful information.

What Information Was Involved?

The information that was accessed without authorization could have included your name, billing address for a credit card, telephone number, email address, and credit card information including card number, name on card, issuer, expiration date, and security code.

What Are We Doing?

We take our obligation to safeguard your personal information very seriously. Upon learning of the potential unauthorized access, we conducted an examination of the breach and employed technical measures to help ensure that further breaches do not occur in the future. We are implementing vigorous, whitelist-based access controls and password policies, as well as deploying a more robust intrusion detection system. All company technical and operational security is being audited and, where necessary, redesigned. We are also notifying the FBI and local law enforcement in San Francisco, California, of the situation and we intend to fully cooperate with law enforcement if they determine that further investigation of the situation is warranted.

What You Can Do?

Given the nature of the information involved, we recommend that you:

- Review and monitor your account statements and order a credit report. Under federal law, all citizens are entitled to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, call toll free at 1-877-322-8228 or visit www.annualcreditreport.com. If you wish to contact the credit reporting agencies directly, their contact information is as follows:

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
1-888-766-0008	1-888-397-3742	1-800-680-7289

- If you do become aware of any unauthorized use of your credit card, make sure to report that to your bank or card issuer immediately. You may also wish to report the unauthorized activity to the FBI, the federal Attorney General's Office, your local police and/or the Attorney General's Office for your state of residence.
- You can contact the Federal Trade Commission to learn more about how to protect yourself in the event you become a victim of fraud or identity theft:

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

- You may also contact the Office of the Attorney General of the United States:

U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530-0001
202-514-2000
www.justice.gov/contact-us

- You may also consider placing a fraud alert or credit freeze on your credit file. A fraud alert helps protect you against an identity thief opening a new credit account in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The merchant can then take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any of the credit reporting agencies identified above. You may obtain more information about fraud alerts by contacting the Federal Trade Commission or the credit reporting agencies identified above. You may also consider placing a credit freeze, also known as a security freeze, on your file. A credit freeze, or security freeze, is designed to prevent potential creditors from accessing your credit file at the credit reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a freeze, which generally range from $5-20. *Unlike a fraud alert, you will need to separately place a freeze at each consumer reporting agency.* For more information on freezes, you may contact either the FTC or the credit reporting agencies identified above. The instructions for placing a freeze differ from state to state, and the credit reporting agencies can provide more information on the requirements. These agencies may ask you to provide the following in connection with any such request: your full

name with middle initial, social security number, date of birth, all addresses where you have lived for the past five years, a copy of government issued identification, and proof of your current residential address, such as a utility bill.

- You may also have additional rights under the Fair Credit Reporting Act or other federal or state consumer protections laws.

- As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

  AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-704-6250 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

  AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-704-6250 using the following redemption code: Redemption Code.

  Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

- Additional information for residents of Maryland, North Carolina and Rhode Island:

  - **For residents of Maryland:** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:
    - **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

  - **For residents of North Carolina:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:
    - **North Carolina Attorney General's Office,** Consumer Protection Division
      9001 Mail Service Center, Raleigh, NC 27699-9001,
      1-877-5-NO-SCAM, www.ncdoj.gov

  - **For residents of Rhode Island:** You may contact the office of the Attorney General for The State of Rhode Island:
    - **Rhode Island Attorney General's Office**
      150 South Main Street
      Providence, Rhode Island 02903
      (401) 274-4400
      www.riag.gov
    - Residents of Rhode Island have the right to file or obtain police reports
    - Fees may be applicable for services provided by credit reporting agencies

For More Information

If you have further questions or concerns about this incident, you can contact AllClear ID at 1-855-704-6250, Monday through Saturday, 6:00 a.m. to 6:00 p.m. Pacific Time (excluding U.S. holidays).

We at Farmgirl Flowers truly value you, and the trust that we have established with our customers, and reiterate that we take our obligation to protect your personal information very seriously. We've set up a toll-free line where our Customer Service Manager, Ernest Parker, would love to talk to you about the situation. Please feel free to reach out with questions or additional information.

Very truly yours,

Christina M. Stembel

Christina Stembel
Chief Executive Officer
Farmgirl Flowers, Inc.

Information about Identity Theft Protection

We recommend that you 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: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("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, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

The next 2 paragraphs are regarding incidents involving personal health information. Disregard if not applicable to your situation.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Fraud Alerts: There are also 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 the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 24 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 24 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	**Mail**	**Phone**
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077