

FLOWERS

Vineyard & Winery

June __, 2015

[Customer Contact Information]

Dear *[Valued Customer]*,

Thank you for your continued support of the Flowers Vineyard & Winery. We value the trust you have placed in us and greatly appreciate your enthusiasm for our wines.

We are writing to inform you that our third-party ecommerce provider, Missing Link Networks, Inc. (MLN), was the subject of a recent data security incident. MLN notified us of this incident on May 27, 2015. You are receiving this letter because your credit card number on file may have been among the data compromised. MLN informs us that customer names, payment card numbers, related payment addresses and dates of birth may have been compromised during the window of April 1, 2015 to April 30, 2015. Since MLN is widely used in the wine industry, you may be hearing from other wineries whose data was compromised in the same incident.

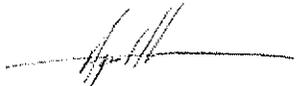
We take this incident very seriously and after we received the information from MLN, we immediately began our own investigation. MLN assures us that it has contained the incident, and that there has been no further unauthorized access of our customer data. MLN informs us that it has been cooperating with law enforcement and has notified the card brands about the situation.

In addition to the suggested actions that you may read below, we would like to offer you one year of credit monitoring services at no cost to you. To activate credit monitoring, please go to <http://www.protectmyid.com/protect> and enter Activation Code [Activation Code] by December 31, 2015. The toll-free number for offline enrollment is 866-751-1324 and Engagement # is PC94731. Membership benefits can be found below.

We pride ourselves on the long-term relationships we have built with our customers and are very sorry for any inconvenience this may cause you. Additional details related to this incident can be found at <http://www.ecellar1.com/faq>.

If you have any questions, please do not hesitate to reach out to us at 707-847-3661.

With our sincerest apology,



Agustin Francisco Huneus
Managing Partner

ADDITIONAL INFORMATION

In addition to offering you the fraud remediation services described in our cover letter at no cost to you, we encourage you to consider the following other proactive steps designed to detect and prevent financial or identity theft or other misuse of your personal information:

Review Your Credit Reports

You should 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 105139, Atlanta, GA 30374-0241, 1-800-685-1111, www.equifax.com

Experian, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com

TransUnion, P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

When you receive your credit reports, review them carefully for any sign of fraud, such as accounts or creditor inquiries that you did not initiate or do not recognize, debts that you cannot explain, medical debt collection notices from health care providers, or a home address or 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.

Review Your Payment Card and Associated Financial Account Statements

We recommend you remain vigilant with respect to reviewing your card and financial account statements, and promptly report any suspicious activity or suspected identity theft to the bank, as well as to any proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission (FTC).

Fraud Alerts

There are also two types of fraud alerts that you can place on your credit report to put 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: 1-800-525-6285, www.equifax.com

Experian: 1-888-397-3742, www.experian.com

TransUnion: 1-800-680-7289, www.transunion.com

Credit or "Security" Freezes

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 put on 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.*

The instructions for how to establish a credit freeze differ from state to state. You may contact the three major credit reporting companies listed above (TransUnion, Experian, and Equifax) to find out more information.

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.

What if You Find Evidence of Identity Theft or Other Suspicious Activity?

We are offering free identity theft repair and fraud remediation services to our customers who are affected by this incident. For more information please see the instructions on the cover letter.

In addition, we recommend that you promptly report any suspicious activity or suspected identity theft 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 regulatory authorities 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 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

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is **not** required for enrollment in ProtectMyID.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in ProtectMyID:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors the Experian file for indicators of fraud.
- **Internet Scan:** Alerts you if your information is found on sites containing compromised data.
- **Address Change Alerts:** Alerts you of changes to your mailing address
- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE:** You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet Protection:** Get help replacing credit, debit, and medical insurance cards.

Once you have completed enrollment in ProtectMyID, you can receive alerts on your mobile phone by downloading the BillGuard mobile app for FREE. Use your ProtectMyID membership login credentials to sign in to the app in order to access - in one place - both your ProtectMyID alerts and BillGuard features, including monitoring against fraud on your current credit and debit card accounts. Visit protectmyid.com/billguard to learn more.

If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 866-751-1324.