

Dear [Name]:

Thank you for your continued support of Kosta Browne, LLC. We 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 breach on May 27, 2015. You are receiving this letter because the credit card number that you used to purchase wine from Kosta Browne may have been among the data compromised. It appears that customer names, credit card numbers, related payment addresses and dates of birth may have been compromised during the window of April 1, 2015 - 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 assure you that we take the privacy and security of your information very seriously. When MLN informed us of this incident, we immediately took steps to address the issue. We have required MLN to delete all existing credit card information for Kosta Browne customers. MLN informs us that they are cooperating with law enforcement and the security compromise has been contained. Furthermore, MLN has reported the matter to the various credit card companies.

In addition to alerting you to the incident, we are offering you data breach resolution services at no cost to you. We have engaged Experian®, the largest credit bureau in the US, to offer you complimentary Fraud Resolution and identity protection for one-year. Please email or call us to receive an offer code to activate these services. Additional information about steps you can take to protect your accounts and your identity is attached to the end of this message.

We take very seriously our duty to safeguard the personal information of our valued members. We sincerely regret any inconvenience this incident has caused and we welcome you to contact us at 707.827.4796 or send us an email at kb@kostabrowne.com with your questions.

Thank you again for your continued support of Kosta Browne.

Sincerely,

Jennifer Downing

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](tel: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](tel:1-800-685-1111), www.equifax.com

Experian, P.O. Box 2002, Allen, TX 75013, [1-888-397-3742](tel:1-888-397-3742), www.experian.com

TransUnion, P.O. Box 6790, Fullerton, CA 92834-6790, [1-800-916-8800](tel: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](tel:1-800-525-6285), www.equifax.com

Experian: [1-888-397-3742](tel:1-888-397-3742), www.experian.com

TransUnion: [1-800-680-7289](tel: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.

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

We are offering free identity theft repair and fraud remediation services to KBW list members who are affected by this incident.

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