Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

August 19, 2024

VIA E-MAIL

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

Re: Notice of Data Event

To Whom It May Concern:

We represent Crimson Wine Group ("Crimson") located at 5901 Silverado Trail, Napa, CA 94558, and are writing to notify your office of an incident that may involve certain personal information relating to one (1) Maryland resident. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Crimson does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On June 30, 2024, Crimson became aware of a cyber security incident in which an unauthorized third party gained access to certain systems in Crimson's network. Upon becoming aware of this incident, Crimson initiated an investigation into the nature and scope of the incident. The investigation determined that unauthorized access to certain Crimson systems occurred, and that certain information on Crimson's systems may have been viewed or taken without authorization between June 26, 2024 – June 30, 2024. On or around July 15, 2024, Crimson determined that some of the information involved may include personal information.

The information that could have been subject to unauthorized access may include name and Social Security Number.

Notice to Maryland Resident

On or about August 19, 2024, Crimson began providing written notice of this incident to one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Crimson moved quickly to investigate and respond to the incident, assess the security of Crimson systems, and identify potentially affected individuals. Further, Crimson notified federal law enforcement regarding the event. Crimson is also working to implement additional safeguards and training to its employees. Crimson is providing access to credit monitoring services for one (1) year, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Crimson is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Crimson is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/ao1
Enclosure

EXHIBIT A

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 19, 2024

L8531-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF [Extra1]

Dear Sample A. Sample:

Crimson Wine Group ("Crimson") writes to notify you of an event that may involve some of your personal information. We are providing you with notice of the event, steps we have taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? On June 30, 2024, Crimson became aware of a cyber security incident in which an unauthorized third party gained access to certain systems in our network. Upon becoming aware of this incident, Crimson initiated an investigation into the nature and scope of the incident. The investigation determined that unauthorized access to certain Crimson systems occurred, and that certain information on our systems may have been viewed or taken without authorization between June 26, 2024 – June 30, 2024. On or around July 15, 2024 we determined that some of the information involved may include personal information. In an abundance of caution, we are notifying individuals whose personal information may have been involved in this event.

What Information Was Involved? The information that may have been viewed or taken may include your name, Social Security number and financial account information. We have no evidence that identity theft or fraud has occurred as a result of this event.

What We Are Doing? We take this event and the security of personal information in our care seriously. Upon discovering the network disruption, we took steps to secure the network, investigate the activity, and determine the scope of impacted information. Our immediate response to this event also included prompt notification to federal law enforcement authorities.

As an added precaution, we are providing you with [Extra2] months of complimentary access to credit monitoring and identity restoration services through Experian, as well as guidance on how to better protect your information. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions included within the enclosure to this letter.

What You Can Do. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call our dedicated assistance line at 1-833-919-4739, Monday through Friday from 6 am – 6 pm Pacific Time, excluding U.S. holidays. You can also write to us at 5901 Silverado Trail, Napa, CA 94558.

Sincerely,

Jen Locke
Chief Executive Officer

0000001

ENGAGE#

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [Extra2] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Extra2] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra2]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** November 29, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-919-4739 by November 29, 2024. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra2]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.

[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity

0000001

theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

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

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

December 13, 2024

VIA E-MAIL

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

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent Crimson Wine Group ("Crimson") located at 5901 Silverado Trail, Napa, CA 94558. We are supplementing Crimson's previous notice to your office on August 19, 2024. The investigation into this matter is ongoing and as such this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Crimson does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

As detailed in the August 19, 2024 notice to your office, on June 30, 2024, Crimson became aware of a cyber security incident in which an unauthorized third party gained access to certain systems in Crimson's network. Upon becoming aware of this incident, Crimson initiated an investigation into the nature and scope of the incident. The investigation determined that certain information on Crimson's systems may have been viewed or taken without authorization between June 26, 2024 – June 30, 2024.

On or around July 15, 2024. Crimson determined that some of the information involved may have included personal information. On August 19, 2024, Crimson began providing written notice to the initial set of individuals identified, including one (1) Maryland resident.

Following additional data review, on or around November 8, 2024, Crimson identified additional individuals whose personal information was present in the data involved.

The information that could have been subject to unauthorized access may include name and Social Security Numbers, driver's license or state ID numbers, financial account information, payment card information and medical information.

Notice to Maryland Residents

On or about December 13, 2024, Crimson provided written notice of this incident to one hundred ten (110) additional Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Crimson moved quickly to investigate and respond to the incident, assess the security of Crimson systems, and identify potentially affected individuals. Further, Crimson notified federal law enforcement regarding the event. Crimson is also working to implement additional safeguards and training to its employees. Crimson is providing access to credit monitoring services for one (1) year, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Crimson is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Crimson is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/ao1
Enclosure

EXHIBIT A

CRIMSON
WINE GROUP
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

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

December 13, 2024

NOTICE OF <<Variable Text 1: Subject Line>>

Dear <<First Name>> <<Last Name>>:

Crimson Wine Group ("Crimson") writes to notify you of an event that involves some of your personal information. We are providing you with notice of the event, steps we have taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? On June 30, 2024, Crimson became aware of a cyber security incident in which an unauthorized third party gained access to certain systems within our network. Upon learning of this, Crimson initiated an investigation into the nature and scope of the incident. The investigation determined that certain information on our systems may have been viewed or taken without authorization between June 26, 2024 – June 30, 2024. On or around December 9, 2024, we determined that some of the affected information included personal information. As part of the investigation, there was a review of the files involved to identify those whose personal information may be involved. Following that we worked to locate address information where needed. This process was substantially completed on or about November 8, 2024. We are notifying individuals whose personal information may have been involved in this event.

What Information Was Involved? The information that may have been viewed or taken may include your name, and <<Variable Text 4: Data Elements>>. We have no evidence that identity theft or fraud has occurred as a result of this event.

What We Are Doing. We take this event and the security of personal information in our care seriously. Upon discovering the network disruption, we took steps to secure the network, investigate the activity, and determine the scope of impacted information. Our response to this event also included prompt notification to federal law enforcement, and we are continuing to cooperate with law enforcement authorities.

As an added precaution, we are providing you with <<Variable Text 3: Service Length>> months of complimentary access to credit monitoring and identity restoration services through IDX, as well as guidance on how to better protect your information. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions included within the enclosure to this letter. Please note the deadline to enroll is March 13, 2025.

What You Can Do. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call our dedicated assistance line at 1-866-711-4721, Monday through Friday from 6 am to 6 pm Pacific Time, excluding U.S. holidays. You can also write to us at 5901 Silverado Trail, Napa, CA 94558.

Sincerely,

Jen Locke
Chief Executive Officer, Crimson Wine Group

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

1. **Website and Enrollment.** Scan the QR image or go to https://app.idx.us/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 IDX identity protection 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, IDX will be able to assist you.

3. **Telephone.** Contact IDX at 1-866-711-4721 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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. We encourage consumers to review their 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.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 11 Rhode Island residents that may be impacted by this event.