



**J. LOHR**  
VINEYARDS & WINES

February 13, 2007

Attorney General's Office  
Attn: Mary Gould, Legal Assistant  
Consumer Protection Bureau  
33 Capitol Street  
Concord, NH 03301

Dear Ms. Gould:

I am writing on behalf of J. Lohr Vineyards and Wines ("J. Lohr") to inform you of a security breach affecting one New Hampshire resident. On December 19, 2007, a thief broke into a locked office at the Company's headquarters and stole two computers. J. Lohr promptly reported the theft to the San Jose (California) Police Department, which is investigating the theft.

J. Lohr worked diligently to reconstruct the information stored on the stolen computers. J. Lohr has been able to determine that one of the computers contains the name and social security number of J. Lohr employees, including, as noted above, one New Hampshire resident. J. Lohr currently anticipates notifying affected employees on or before February 15, 2007, of this incident. A copy of the letter that will be sent to affected New Hampshire residents is attached.

If you have any questions concerning the matters discussed above, please do not hesitate to call me.

Very truly yours,

James Schuett  
Vice President - Finance

**J. LOHR**  
VINEYARDS & WINES  
**1000 LENZEN AVENUE**  
**SAN JOSE, CA 95126**

February 13, 2008

[Name of Employee]  
[Street Address]  
[City/State/Zip]

Dear [NAME OF EMPLOYEE]

J. Lohr Vineyards and Wines ("J. Lohr") recognizes the importance of safeguarding its personnel information. Even the most rigorous safeguards, however, can not guarantee protection against criminal conduct.

Our Company recently was victimized by such conduct, and we regret to have to say that this criminal conduct might have a direct impact on you. A thief recently broke into a J. Lohr office and stole two company computers. We immediately reported the theft to the San Jose Police Department. The police are investigating the theft, and we are cooperating fully in the investigation.

We have worked to reconstruct the information stored on the stolen computers. We have determined that one of the computers contained information about participants in our Company ESOP, including the names, addresses, Social Security Numbers (SSN) and dates of birth of current and former J. Lohr employees, including yours.

At this point, we have no reason to believe that the theft was directed at the information stored on this computer. We also have received no reports to date, indicating that the information stored on this computer has been misused. We are in the process of evaluating steps that can be taken to make a recurrence of this incident less likely.

J. Lohr recognizes that the theft of your personal information, and any related inconvenience, might be upsetting. We regret that this incident has occurred, and we apologize for any inconvenience it may cause you.

To lessen the potential inconvenience to you and to reduce the risk that you might be victimized by identity theft, we have arranged for **one year of free credit monitoring through ConsumerInfo.com, Inc, an Experian® company**. This product, known as **TripleAlert<sup>SM</sup>**, provides daily monitoring of your credit report with each of the three national credit bureaus and will notify you of key changes that may indicate fraudulent activity. You also will receive monthly all-clear notifications.

You have ninety (90) days from the date of this letter to activate this membership. We encourage you to activate your credit monitoring membership quickly. Please visit

<http://partner.experiandirect.com/triplealert/> and enter the activation code provided below. You will be instructed on how to initiate your online membership. Your Credit Monitoring Activation Code: [insert activation code]

In addition to this credit monitoring membership, **we have contracted with National ID Recovery (NIDR) to provide the following services *free of charge to you*:**

- NIDR will help you obtain free credit reports from each of the national credit bureaus and to place a “fraud alert” on your credit report with each of the national credit bureaus. Just call **1-800-836-5379** to take advantage of this service;
- NIDR will work to answer any questions you might have concerning the security breach;
- If you do become a victim of identity theft within one year of the date of this letter, NIDR will work to recover your identity for you;
- Additional educational resources on how to protect yourself from identity theft and on related topics are available at [www.nationalidrecovery.com/m/jlohr](http://www.nationalidrecovery.com/m/jlohr).

The Federal Trade Commission (FTC) recommends that potential victims of ID theft periodically check their credit reports and account statements. You should consider canceling any accounts that reflect suspicious activity as well as reporting the suspicious activity to your local law enforcement agency.

You can find additional information about protecting yourself against the possibility of ID theft at the FTC’s Web site ([www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)). The Commission also maintains an identity theft hotline number (toll free) 877-438-4338. You can file an ID theft complaint with the FTC through that number or by mailing it to the Federal Trade Commission, Consumer Response Center, Room 130-B, 600 Pennsylvania Avenue, N.W. Washington, D.C., 20580. You also can consult your state’s consumer protection board concerning the availability of additional protections under state law, such as a security freeze.

If you have any questions, please call **1-800-836-5379**. Again, we apologize for any inconvenience that this incident may cause you.

Very truly yours,



James Schuett  
Vice President - Finance