

RECEIVED

FEB 13 2020

CONSUMER PROTECTION

# BakerHostetler

## Baker&Hostetler LLP

2929 Arch Street  
Cira Centre, 12th Floor  
Philadelphia, PA 19104-2891

T 215.568.3100  
F 215.568.3439  
www.bakerlaw.com

Anthony P. Valach  
direct dial: 215.564.2588  
avalach@bakerlaw.com

February 12, 2020

### VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

*Re: Security Incident Notification*

Dear Attorney General MacDonald:

We are writing on behalf of our client, Terlato Wine Group (“Terlato”), to notify your office of a security incident involving one New Hampshire resident.

Terlato recently concluded its ongoing investigation into a phishing email incident involving unauthorized access to employee email accounts. Upon learning of the incident, Terlato promptly secured the accounts and a leading cyber security firm was engaged to assist with the investigation. The investigation determined that an unauthorized actor may have accessed the employee email accounts between the dates of August 22, 2019 and September 13, 2019. Terlato conducted a comprehensive review of the emails and attachments that may have been viewed by the unauthorized actor and determined on December 9, 2019, that an email or attachment containing personal information of one New Hampshire resident was in the accounts, including the name, Social Security number and driver’s license number. Although there is no evidence that the personal information was accessed or viewed, Terlato is notifying the New Hampshire resident out of an abundance of caution.

On February 12, 2020, Terlato mailed written notifications to the potentially affected New Hampshire resident in accordance with N.H. Rev. Stat. Ann. § 359-C:20 in substantially the same form as the enclosed letter. Terlato is offering the individual a complimentary one-year membership to credit monitoring and identity theft protection services through Experian. Terlato also provided a telephone number for potentially affected individuals to call with any questions they may have about the incident.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver  
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

February 12, 2020

Page 2

To help prevent a similar incident from occurring in the future, Terlato is providing additional training to our employees regarding phishing emails and implementing additional technical cybersecurity measures.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink that reads "Anthony P. Valach". The signature is written in a cursive style with a large initial "A".

Anthony P. Valach  
Counsel

Enclosure



<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

Terlato Wine Group Ltd. ("Terlato") is committed to safeguarding the information it maintains. We are writing to inform you that we recently identified and addressed a security incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

Our ongoing investigation of a phishing email incident recently determined that an unauthorized party could have accessed certain emails contained in a limited number of Terlato employee email accounts. Upon learning of the incident, we promptly secured the employee email accounts and a leading cyber security firm was engaged to assist with the investigation. Our investigation determined that an unauthorized actor may have accessed the employee email accounts between the dates of August 22, 2019 and September 13, 2019. We conducted a comprehensive review of the emails and attachments that may have been viewed without authorization and determined on December 9, 2019, that an email or attachment contained your <<b2b\_text\_1 (impacted data)>>. We have no evidence that your personal information was accessed or viewed, however, we wanted to alert you of the incident out of an abundance of caution.

Although there are no reports that any of the information involved in this incident was misused, we encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. As a precaution, we have arranged for Kroll to provide identity monitoring at no cost to you for one year. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. For more information on Kroll Identity Monitoring, including instructions on how to activate your complimentary one-year membership, please visit the below website:

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until [Date] to activate your identity monitoring services.

Membership Number: <<Member ID>>

We regret any inconvenience or concern this may cause you. To help prevent an incident like this from happening in the future, we are providing additional training to our employees regarding phishing emails and implementing additional technical cybersecurity measures.

If you have any questions, please call 1-???-???-???? Monday through Friday between the hours of 8:00 a.m. and 5:30 p.m., Central Time.

Sincerely,

Nick Alex  
Chief Financial Officer

## **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You've been provided with access to the following services<sup>1</sup> from Kroll:

### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

### ***Fraud Alerts and Credit or Security Freezes:***

**Fraud Alerts:** There are two types of general fraud alerts 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 one year. 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.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

**Credit or Security Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

*How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

***Additional information for residents of the following states:***

**Maryland:** The Terlato Wine Group's address is 900 Armour Dr., Lake Bluff, IL 60044. You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, [www.oag.state.md.us](http://www.oag.state.md.us)

**New York:** You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

**North Carolina:** You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)