

December 31, 2014

PRIVILEGED & CONFIDENTIAL

VIA U.S. MAIL

Joseph Foster  
Office of the New Hampshire Attorney General  
Attn: Security Breach Notification  
33 Capitol Street  
Concord, NH 03301

Re: Notice of Data Security Event

Dear Mr. Foster:

We represent the La Jolla Group, Inc., 14350 Myford Road, Irvine, CA 92606, and are writing to notify you of a data security incident that compromised the security of personal information of eleven (11) New Hampshire residents. The La Jolla Group's investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, the La Jolla Group does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

#### Nature of the Data Security Event

La Jolla Group is a management company that provides management services in connection with the operation of ecommerce websites for O'Neill, Metal Mulisha, and FMF apparel brand licensees. On or about December 3, 2014, the La Jolla Group learned of potential unauthorized access to the checkout page of these three brands' respective websites. Upon learning of this issue, La Jolla Group immediately launched an investigation and took steps to prevent any further potential for unauthorized access. Independent computer forensic experts were retained to assist in La Jolla Group's investigation and confirmation of what information may have been accessed without authorization.

Although the investigation is ongoing, it was confirmed on December 29, 2014 that a malicious script was placed on the La Jolla Group's system leading to the compromise of the security of certain customer personal information, including the customer's name, address, phone number, email address, credit card number, CVV2 data and credit card expiration date. This information is provided by the customer when making a purchase, or preparing to make a purchase, at the three brands' e-commerce websites.

#### Notice to New Hampshire Residents

On January 2, 2015, the La Jolla Group will mail written notice to affected customers, which included eleven (11) New Hampshire residents, about this incident and the steps they can take to protect themselves. Written notice will be provided in substantially the same form as the letter attached here as *Exhibit A*.

#### Other Steps Taken and To Be Taken

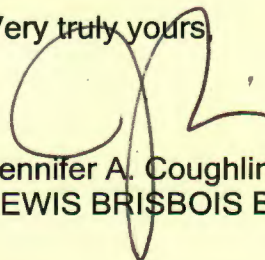
The La Jolla Group takes this matter, and the security of the personal information in its care, seriously and has taken measures to ensure that this type of exposure does not occur again. Upon discovery, the malicious script was quickly removed from the La Jolla Group's systems and the company is monitoring its systems for any signs of further attempts by unauthorized individuals to access customer personal information.

In addition to providing written notice of this incident to affected individuals as described above, each affected individual is being offered access to one free year of triple-bureau credit monitoring and identity restoration services provided through AllClear ID. The La Jolla Group is providing each individual with information on how to protect against identity theft and fraud. Further, the La Jolla Group is providing written notice of this incident to other state regulators, the card brands, and consumer reporting agencies where required.

#### Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at [REDACTED]

Very truly yours,

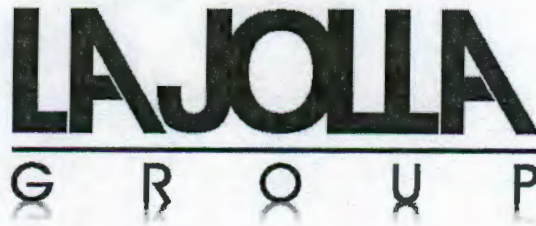


Jennifer A. Coughlin of  
LEWIS BRISBOIS BISGAARD & SMITH LLP

JAC:lm



# EXHIBIT A



January 2, 2015

First Name Last Name

Address

City, State Zip

Dear First Name Last Name,

La Jolla Group, a management company that provides management services in connection with the operation of ecommerce websites to certain apparel brand licensees, is writing to notify you of a data security incident that affects the security of your personal information, and to make you aware of resources available to support you.

**What happened?** On December 3, 2014, we learned of potential unauthorized access to the checkout page of the client\_def 1 website, client\_def 2. When we learned of this issue, we immediately launched an investigation and took steps to prevent any further potential for unauthorized access. We retained independent computer forensic experts to assist in our investigation and confirmation of what information may have been accessed without authorization. Although our investigation is ongoing, we confirmed on December 29, 2014 that the security of certain information relating to you was compromised as a result of this incident. This information includes your name, address, phone number, email address, credit card number, CVV2 data and credit card expiration date – all provided when you placed, or prepared to place, an online order at client\_def 2 between November 30, 2014 and December 3, 2014. **This incident did not compromise the security of your Social Security number, which we never request you provide to us as part of the purchasing process.**

**What We Are Doing.** We remediated the issue that gave rise to the incident. We retained independent computer experts to assist in our investigation into what happened and what information is at risk. We've taken steps to prevent something like this from happening again.

**What You Can Do.** Enclosed is helpful information on how to protect against identity theft and fraud. As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

- **AllClear SECURE:** The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call «DID\_Phone» and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear ID maintains an A+ rating at the Better Business Bureau.
- **AllClear PRO TBO:** This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use the PRO TBO service, you will need to provide your personal information to AllClear ID. You may sign up online at [enroll.allclearid.com](http://enroll.allclearid.com) or by phone by calling «DID\_Phone» using the following redemption code: {RedemptionCode}.

You can also review the enclosed information for additional ways to protect against identity theft and fraud. Should you have any questions about the content of this letter, enrollment in the AllClear Pro TBO product, or ways you can protect



yourself from the possibility of identity theft, please call our confidential hotline between 9 a.m. and 9 p.m. EST, Monday to Saturday at 1-877-403-0281.

The security of our customers' personal information is one of our highest priorities. We are sorry for any inconvenience and concern this incident may cause you.

Sincerely,

A handwritten signature in cursive script, appearing to read "Cristy Abella".

Cristy Abella  
La Jolla Group

## ADDITIONAL STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

You may also take action directly to further protect against possible identity theft or other financial loss. We encourage you to be vigilant by reviewing your account statements regularly and monitoring your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below. Information regarding security freezes is also available from these agencies.

Equifax  
P.O. Box 105069  
Atlanta, GA 30348  
800-525-6285  
[www.equifax.com](http://www.equifax.com)

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

TransUnion  
P.O. Box 2000  
Chester, PA 19022-2000  
800-680-7289  
[www.transunion.com](http://www.transunion.com)

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, [www.ncdoj.gov](http://www.ncdoj.gov). **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16<sup>th</sup> Floor, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/), 1-877-ID-THEFT (1-877-438-4338); 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.