LEECHTISHMAN
LEECH TISHMAN FUSCALDO & LAMPL

February 28, 2017

Laurel Brandstetter
lbrandstetter@leechtishman.com

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster:

Please be advised that Leech Tishman Fuscaldo & Lampl represents Roxy Trading, Inc. ("Roxy"), the parent company of Chimes. We are writing to notify you of potential unauthorized access of personal information involving three New Hampshire residents.

On January 22, 2017, a hacker gained access to Roxy's server and installed a form of "malware" known as "ransomware" to block access to their files. Among the files on the server that was hacked was a password-protected file with customer payment information. After breaching Roxy's system, the hacker demanded a ransom to restore access to the system. Roxy made payment and access was restored. The customer file subject to the ransomware contained names, business addresses, business phone numbers, email addresses, and credit card numbers.

Roxy's IT team has conducted a complete investigation and found no evidence that any data was removed from the server. We have no evidence that the personal information has been used fraudulently.

We provided notice to all affected customers. A copy of that notice is attached for your review and consideration. A one-year of Protect My ID Membership has been offered to all affected customers.

Should you have any questions or concerns, please do not hesitate to contact me directly.

Sincerely,

LEECH TISHMAN FUSCALDO & LAMPL, LLC

Laurel Brandstetter, Esquire

Chimes, Roxy Trading Inc.
389 N. Humane Way
Pomona, CA 91768
(T) 626.610.1388 (F) 626.610.1339

February 22, 2017

##C6265-L01-0123456 **********SNGLP
SAMPLE A SAMPLE
123 ANY ST
ANYTOWN, US 12345-6789

We are contacting you regarding a recent data security incident that occurred at Roxy Trading Inc., the parent company of Chimes, specifically a "ransomware attack" on one of our company servers. In light of this attack, there is a ***theoretical*** possibility that your name, business address, business phone number, email address, and credit card number were exposed to a party external to our company.

Specifically, on January 22, 2017, a hacker gained access to our server and installed a form of "malware" known as "ransomware" to block access to our files. Among the files on the server that was hacked was a password-protected file with customer payment information. After breaching our system, the hacker demanded a ransom to restore access to our system. We made payment and access was restored.

Our IT team has conducted a complete investigation and found no evidence that any customer data was removed from the server. However, we have also been advised that due to the nature of the attack, this possibility cannot be absolutely foreclosed.

Ransomware is extremely widespread. According to a 2016 survey by Kasperky Lab, more than 2/3s of small and medium-sized business have had files damaged by this kind of malware. (Source: https://business.kaspersky.com/cryptomalware-report-2016/5971/)

We understand that many companies do not send breach notification to their customers in situations like this. ***However, while we have no evidence that your information was compromised, a hacker did gain access to our system and we feel that that it is important to inform you of the potential compromise of your information, regardless of any legal obligation.***

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 these issues, please reach out to an Experian agent (which information we will provide below). If, after discussing your situation with an agent, it is determined that fraud resolution support is needed then an Experian Fraud Resolution agents are 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.)

0123456

Please note that this offer is available to you for one-year 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.experian.com/fraudresolution. You will also find self-help tips and information about identity protection at this site.

While Fraud Resolution assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through ProtectMyID® Alert as a complimentary one-year 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**: **2/19/2018** (Your code will not work after this date.)
Visit the ProtectMyID website to enroll: **www.protectmyid.com/redeem**
Provide your **activation code**: ABCDEFGHI

If you have questions about the incident, need assistance with fraud resolution that arose as a result of this incident or would like an alternative to enrolling in ProtectMyID online, please contact Experian's customer care team at 877-371-7902 by 2/19/2018. Be prepared to provide engagement number **PC106524** as proof of eligibility for the fraud resolution services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is **not** required for enrollment in ProtectMyID.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in ProtectMyID:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.experian.com/fraudresolution for this information.

We sincerely regret this incident and any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at (626) 610-1388 x 135.

Sincerely,

Sieng Elvis Saetang
President
Roxy Trading, Inc. / Chimes

*Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

C6124-L01