McCARTER &ENGLISH
ATTORNEYS AT LAW

June 7, 2017

RECEIVED
JUN 08 2017
CONSUMER PROTECTION

VIA FEDEX

CONFIDENTIAL

Mr. Gordon J. MacDonald
Attorney General
NH Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Notification of Data Breach – Jewelry.com

Scott S. Christie
Partner
T. 973-848-5388
F. 973-297-3981
schristie@mccarter.com

McCarter & English, LLP
Four Gateway Center
100 Mulberry Street
Newark, NJ 07102-4056
T. 973.622.4444
F. 973.624.7070
www.mccarter.com

Dear Mr. MacDonald:

We are writing to notify you of the unauthorized access of personal information involving 34 New Hampshire residents.

On May 16, 2017, Jewelry.com, a division of Richline Group, Inc., discovered that beginning on or about November 16, 2016, unknown individuals gained access to Jewelry.com through the unauthorized use of an account belonging to one of its employees. Jewelry.com learned about the potential problem through Wells Fargo Merchant Services, LLC, who advised Jewelry.com that it had been identified by Discover as a common point of purchase for holders of Discover credit cards who subsequently experienced fraud on their accounts.

After conducting an investigation and review of Jewelry.com's systems, Jewelry.com discovered that on November 16, 2016 and March 23, 2017, an account belonging to one of its employees was used to access the administration portal of the Jewelry.com's Magento eCommerce platform and create a second user account. This new user account added JavaScript code to the Jewelry.com website's global footer to capture credit card payment information as it was entered on the shopping cart pages. The information was transmitted to a server located at twitterbuttons.com.

Jewelry.com currently believes that during the period from November 16, 2016, through May 1, 2017, the intruders misappropriated credit card information (including name, billing address, credit card number, expiration date, and CVV number).

Immediately following the discovery of the data security breach, Jewelry.com removed the malicious code from its website, the compromised employee account was terminated, and the affected computer was disabled and unplugged from the

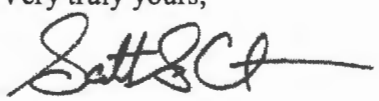
company's network. Jewelry.com also has taken additional steps to contain the breach and to enhance the security of the company's network.

Jewelry.com has retained the law firm of McCarter & English, LLP to assist with remediating the issue and to address applicable legal obligations arising from the breach. We have reported the incident to the appropriate federal and state law enforcement authorities. At present, all indications are that Jewelry.com's database of customer information remains secure.

To date, Jewelry.com has made no public disclosure of the intrusions in order not to compromise any criminal investigation. Jewelry.com filed a complaint with the FBI through its Internet Crime Complaint Center concerning the intrusions affecting its website. We plan on providing notice to residents of this state affected by this breach shortly. A copy of the letter we plan to send to the residents of this state affected by this breach is enclosed.

If you have any questions or need further information, you may reach me at schristie@mccarter.com or 973-848-5388.

Very truly yours,



Scott S. Christie

JEWELRY.COM
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name1>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

RE: Important information about your recent purchase at Jewelry.com

Dear Valued Customer,

We are writing to share with you important information about an incident involving our online boutique, Jewelry.com, as well as the steps we are taking in response to this incident, and recommended actions for you to take.

On May 16, 2017 Jewelry.com discovered that, beginning on or about November 16, 2016, unknown individuals gained access to our online boutique through the unauthorized use of an account belonging to one of our employees. Unfortunately, and despite all the security measures implemented on the website, the intruders were able to install malicious software on the Jewelry.com website which was used to capture credit card payment information as it was entered on our shopping cart page. The intruders were able to access information associated with online purchases through our Jewelry.com website between November 16, 2016 and May 1, 2017.

The compromised information includes debit and credit card numbers, card holders' names, card holders' billing addresses, passwords, security codes and expiration dates. While not all debit and credit cards used during this time period were necessarily affected, out of an abundance of caution we are notifying you of this incident.

Immediately following the discovery of the data security breach, we removed the malicious software from the Jewelry.com website, the compromised employee account was terminated, and the affected computer was disabled and unplugged from the company's network. We also have taken additional steps to contain the breach and to enhance the security of the company's network.

We have retained the law firm of McCarter & English, LLP to assist with remediating the issue and to address applicable legal obligations arising from the breach. We also have reported the incident to the appropriate federal and state law enforcement authorities. At present, all indications are that our database of customer information remains secure.

If you already have been contacted by your card issuing bank concerning this matter, then your bank is aware of the problem and has protected your account. If not, we encourage you to be vigilant and regularly review your banking and payment card statements, other financial accounts, and credit report, and report any suspicious or unrecognized activity immediately to the relevant financial institutions and/or law enforcement authorities. You can follow the recommended steps on the following pages to learn more about how to protect your debit and credit card information.

We at Jewelry.com take the security of our customers' information very seriously and truly regret any inconvenience that this incident may have caused you. Should you have any questions, please do not hesitate to call 800-436-1892 from 9:00 a.m. to 5:00 p.m. EST.

We thank you for your patronage, your understanding and your patience.

Sincerely,

JEWELRY.COM

J.P. Dowd
Vice President Engineering

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

1. **Telephone**. If you already have been contacted by your card issuing bank concerning this matter, then your bank is aware of the problem and has protected your account. If not, contact your card issuing bank to speak with a representative about the appropriate steps to take in protecting your card.

2. **Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228.

   If you discover any suspicious items, notify your card issuing bank immediately. In the unlikely event that you fall victim to identity theft as a consequence of this incident, they will work on your behalf to identify, stop and reverse the damage quickly.

   You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

3. **Place Fraud Alerts with the three credit bureaus.** You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

   Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	www.transunion.com

   It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. Please note that no one is allowed to place a fraud alert on your credit report except you, so please follow the instructions above to place the alert.

4. **Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to $5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338).

California Residents: Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 1-888-743-0023.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, Telephone: 1-919-716-6400.

Rhode Island Residents: Office of the Attorney General, 4800 Tower Hill Road, Suite 152, Wakefield, RI 02879, www.riag.ri.gov, Telephone: 1-401-782-4150.