womblebonddickinson.com

WOMBLE BOND DICKINSON

May 3, 2019

Attorney General Gordon MacDonald
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Via Federal Express

Theodore F. Claypoole
Partner
Direct Dial: 404-879-2410
E-mail: Ted.Claypoole@wbd-us.com

Re: Notice of Data Exposure Incident Affecting New Hampshire Residents

Dear Attorney General MacDonald:

Pursuant to the New Hampshire Revised Statutes Annotated § 359—C:20 (the "Act"), we are writing to notify you on behalf of our client of an incident that may have exposed the personal information of 67 New Hampshire residents. We are providing the required information below.

General Description of the Incident

Salt Life recently confirmed through forensic experts that unauthorized malware intrusions of its system captured customer payment information. Salt Life believes that payment cards used to make a purchase on its eCommerce website www.saltlife.com between December 12, 2018 and March 12, 2019, as well as from 7:30 AM ET to 9:30 AM ET on April 11, 2019 may have been exposed to these intrusions. While Salt Life does not store customer payment card information on its system, we believe such information may have been exposed as it was being entered by the customer.

Number of New Hampshire Residents Affected

Sixty-seven New Hampshire residents may have been affected by the incident. On May 1, 2019, Salt Life sent these residents notice pursuant to the Act via e-mail. A template copy of the notification is enclosed along with this letter.

Type of Personal Information That May Have Been Affected

Salt Life believes the malware associated with the intrusions may have allowed access to customer payment card information. No social security data was exposed in the intrusions, nor does Salt Life believe that any other personal information beyond payment card information was exposed.

Steps Salt Life Has Taken or Plans to Take Relating to the Incident

Salt Life has removed the malware associated with the intrusions from its system and has taken actions to secure its website by working with recognized data security experts to conduct a thorough investigation of

the incident and determine additional measures designed to build stronger protections against future incidents of the nature.

Company Contact Information

Salt Life, LLC
Justin Grow
Vice President
322 S. Main Street
Greenville, SC 29601
(864) 232-5200, ext. 6604
Justin.grow@deltaapparel.com

If you have any questions, please feel free to contact me.

Best regards,

Womble Bond Dickinson (US) LLP

Ted Claypoole tk

Theodore F. Claypoole
Partner

Enclosure

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Notice of Data Incident

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

We are writing to inform you of a data security incident involving Salt Life customer payment information. Salt Life greatly values your business and deeply regrets that this incident occurred.

What Happened?

Salt Life recently confirmed through forensic experts that unauthorized malware intrusions of Salt Life's system captured customer payment information. We believe that a payment card you used to make a purchase at the Salt Life eCommerce website www.saltlife.com may have been exposed in these intrusions. Salt Life does not store your payment card information on its system but we believe your information may have been exposed as it was being entered to make a purchase at the Salt Life eCommerce website www.saltlife.com. We want you to be aware that because of this incident, there is a possibility of fraudulent charges on your credit or payment card. Salt Life has provided notice to your card company.

What Information Was Involved?

Salt Life believes that the malware associated with the intrusions may have allowed access to your payment card information. **No social security data was exposed in these intrusions, nor do we believe that any other personal information beyond payment card information was exposed.**

What Are We Doing?

We have removed the malware associated with the intrusions from our system and taken actions to secure our website by working with recognized data security experts to conduct a thorough investigation of the Incident and determine additional measures designed to build stronger protections against future incidents of this nature. Although the risk of data security incidents cannot be eliminated altogether, we have taken procedural, policy, and technical steps to help minimize the risk of this type of event.

To help relieve concerns and restore confidence following this incident, we have engaged Kroll to provide identity monitoring services at no cost to you for 1 year. The offered credit and identity monitoring services through Kroll include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.
*You have until **July 28, 2019** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-800-491-9358. Additional information describing your services is included with this letter.

What Can You Do?

Please review the enclosed "Additional Resources" information included with this letter. This information describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

We recommend that you remain vigilant for incidents of identity theft and fraudulent charges by reviewing account statements and monitoring free credit reports, as detailed below. If you notice suspicious activity in your financial records, you should report it immediately to any financial institution involved. You may also ask your bank to replace your card at any time with a new card identified with a different set of numbers.

For more information.

If you have questions, please call 1-800-491-9358, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

On behalf of Salt Life, we sincerely apologize for any inconvenience this issue might have caused.

Sincerely,

Justin Grow
Vice President

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 61 Rhode Island residents impacted by this incident.

Kroll. | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] 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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. 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.