NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2758
kris.kleiner@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

June 15, 2017

By Certified Mail
Return Receipt Requested

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, Southern Tide, to inform you of a potential security incident involving personal information for certain Southern Tide customers that may have affected approximately seventeen New Hampshire residents. Southern Tide is notifying these individuals and outlining some steps they may take to help protect themselves.

Southern Tide recently learned that an unauthorized individual was able to gain access to portions of its website and may have been able to access certain customer information as a result. The incident could affect certain personal information, including name, address, email address, telephone number, payment card account number, expiration date, and card verification code for certain individuals that made purchases on the website between April 27, 2017 and May 23, 2017 or between June 5, 2017 and June 7, 2017. This incident did not affect transactions at any retail locations.

Southern Tide takes the privacy of personal information seriously, and deeply regrets that this incident occurred. Upon learning of the incident, Southern Tide promptly took steps to address the situation, including engaging outside forensic experts to assist in investigating and remediating the situation. Southern Tide has removed the malware and replaced and reconfigured various components of its website servers to enhance the security of its systems. While Southern Tide is continuing to review and enhance its security measures, the incident has now been contained and is no longer affecting transactions on the website.

Affected individuals are being notified via written letter which will begin mailing on or around June 15, 2017. A form copy of the notice being sent to the affected New Hampshire residents is included here for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2758 or kris.kleiner@nortonrosefulbright.com.

Very truly yours,

Kristopher Kleiner

KCK
Enclosure

[SOUTHERN TIDE LETTERHEAD]

[DATE]

[ADDRESS]

Dear [NAME],

Notice of Data Security Incident

Southern Tide recently became aware of a potential security incident that may affect the personal information of some customers who made a purchase on the SouthernTide.com website using a credit card or debit card. We are providing this notice as a precaution to let you know about the incident and tell you about some steps you can take to help protect yourself. We take the security of our customers' information very seriously and we are sincerely sorry for any concern this may cause you.

What Happened

We were recently alerted to a potential security incident involving our website. Based upon an extensive forensic investigation, it appears that an unauthorized individual gained access to portions of our website and placed malicious software that was designed to capture credit card or debit card information.

What Information Was Involved

We believe that the incident could have affected certain information (including name, address, email address, telephone number, credit card or debit card account number, expiration date, and verification code) of customers who made a credit card or debit card purchase on the website between April 27, 2017 and May 23, 2017 or between June 5, 2017 and June 7, 2017. According to our records, you made a credit card or debit card transaction on the website during that timeframe and, as a result, your information may be affected. Please note that because we do not collect sensitive personal information like Social Security numbers, this type of sensitive information was not affected by this incident nor did this incident affect transactions made through PayPal or at any of our retail locations.

What We Are Doing

We take the privacy and security of our customers' information seriously, and deeply regret that this incident occurred. We took steps to address and contain this incident promptly after it was discovered, including engaging independent forensic experts to assist us in investigating and remediating the situation. We have removed the malware and replaced and reconfigured various components of our website servers to enhance the security of our systems. While we are continuing to review and enhance our security measures, the issue has now been resolved and is no longer affecting transactions on our website.

What You Can Do

We recommend that you review your credit card/debit card account statements to determine if there are any discrepancies or unusual activity listed. We urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not recognize, you should immediately notify the issuer of the credit or debit card as well as the proper law enforcement authorities. In instances of credit or debit card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

Although Social security numbers and other sensitive personal information were not at risk in this incident, as a general practice we recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. As an additional precaution, we are providing an "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection.

For More Information

For more information about this incident, or if you have additional questions or concerns about any of this, you may contact us directly at 800-478-2218 between 9:00 a.m. and 5:00 p.m. Eastern time, Monday through Friday. The entire Southern Tide team values your business and appreciates your support.

Sincerely,

Christopher Heyn
Chief Executive Officer, Southern Tide

Information about Identity Theft Protection

Review Accounts and Credit Reports: You can also regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You can obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of North Carolina: You can obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island You can obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

Fraud Alerts: There are two types of fraud alerts that 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 at least 90 days. 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)
General Contact:
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:
P.O. Box 740256, Atlanta, GA 30374
Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
General Contact:
P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
General Contact:
P.O. Box 105281
Atlanta, GA 30348
877-322-8228

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872