

August 14, 2019

Via Email: doj-cpb@doj.nh.govAttorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification Pursuant to N.H. Rev. Stat. Ann. § 359-C:20

Dear Attorney General MacDonald:

This firm represents Pelican Products, Inc. (“Pelican”), and we are writing on behalf of our client to notify you of a breach of security involving six (6) New Hampshire residents that may have been impacted by a malicious code placed on Pelican’s ecommerce website, which is operated and managed by a third party ecommerce service provider, SureSource LLC d/b/a BrandShop.

NATURE OF THE UNAUTHORIZED DISCLOSURE

On or about July 16, 2019, we were alerted by a third party that a malicious code may be present on our ecommerce website. The malicious code was designed to intercept credit card data and billing/shipping information from customer transactions. It is important to note that neither Pelican nor BrandShop are aware of any actual exfiltration or misuse of this information. We promptly alerted SureSource of the suspicious script potentially running on the ecommerce website store.pelican.com, operated and maintained by SureSource. SureSource immediately launched an investigation to determine the nature and scope of the incident, and began working with third-party cybersecurity experts. The investigation determined that a malicious script was present on the store.pelican.com website from June 28, 2019 until July 16, 2019, when BrandShop took the site down. Please also note that, no Social Security number, drivers’ license numbers, or account passwords were involved or exposed.

STEPS WE ARE TAKING RELATED TO THE INCIDENT

We are working closely with BrandShop to be sure appropriate measures and safeguards are in place to avoid a similar occurrence in the future. Pelican and SureSource have removed the malicious code, and Pelican’s ecommerce site is operational again. In response to this incident, Pelican notified federal law enforcement and implemented additional security measures to help protect the privacy of individuals’ information that it maintains.

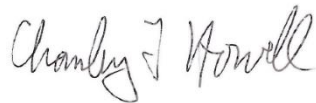
AUSTIN
BOSTON
CHICAGO
DALLAS
DENVERDETROIT
HOUSTON
JACKSONVILLE
LOS ANGELES
MADISONMEXICO CITY
MIAMI
MILWAUKEE
NEW YORK
ORLANDOSACRAMENTO
SAN DIEGO
SAN FRANCISCO
SILICON VALLEY
TALLAHASSEETAMPA
WASHINGTON, D.C.
BRUSSELS
TOKYO

Page 2

Pelican plans to mail a notification to the potentially affected New Hampshire residents on or before August 16, 2019. Enclosed is a sample copy of the notice that was sent to that individual. Pelican provided the potentially affected New Hampshire residents with credit monitoring and identity theft protection through Experian®, at no cost to the individual for one (1) year.

If you have any further inquiries concerning this notification, please do not hesitate to contact me.

Sincerely,



Chanley T. Howell
Partner

CTH:

Enclosures: Sample Notification Letter



Pelican Products, Inc.
23215 Early Avenue
Torrance, CA 90505

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

WHAT HAPPENED?

On or about July 16, 2019, Pelican Products was made aware that a malicious script may be present on our website store.pelican.com.

We utilize an outside vendor, SureSource LLC d/b/a BrandShop (“SureSource”), to operate and maintain our website. Upon learning of the malicious script, we promptly alerted SureSource and began an investigation to determine the nature and scope of this event. To assist in this process, SureSource began working with third-party cybersecurity experts. The investigation concluded that a malicious script was present on the website from June 28, 2019 to July 16, 2019, and the script was designed to intercept credit card data and billing/shipping information from customer transactions.

Although we did not uncover any evidence of data actually being intercepted or misused by the script, out of an abundance of caution we are notifying all Pelican customers who entered their debit or credit card information on store.pelican.com during this timeframe.

WHAT INFORMATION WAS INVOLVED?

The type of data that could have been intercepted by the script includes your full name, credit or debit card information, and possibly your billing or shipping address. **No** Social Security numbers, drivers’ license numbers or account passwords were involved or exposed. As noted above, we do not have any evidence of actual interception or misuse of any of your information, but, as a valued customer of Pelican, we are notifying you out of an abundance of caution.

WHAT WE ARE DOING

We take the trust you’ve placed in us seriously. Since learning of this incident, we have been working with SureSource by conducting an investigation, working with a leading security forensics firm, and implementing enhanced security measures to help prevent this type of incident from happening



again. We have also notified Federal law enforcement. This notice was not delayed due to our notification of law enforcement.

To help protect your identity, we are offering a complimentary one-year (unless a different period is required under applicable law) membership of Experian's® IdentityWorksSM. This product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: November 30, 2019 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experian.com/consumer-products/identity-theft-and-credit-protection.html>
- Provide your activation code: [INSERT CODE]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by November 30, 2019. Be prepared to provide engagement number [ENGAGEMENT #] as proof of eligibility for the identity restoration services by Experian.

Additional Details Regarding Your 12-Month Experian IdentityWorks Membership:

Pelican will provide Experian Identity Restoration support as set forth in this letter to you for one year from the date of this letter. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site. A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only. Offline members will be eligible to call for additional reports quarterly after enrolling.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers. The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (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).

At your own cost and expense, and in addition to or as an alternative to above, you may also enroll in an online three-bureau credit monitoring service to access your credit report and credit score and receive notifications if there are any critical changes to your credit files. Such a service could also include access to an identity restoration program that provides assistance in the event that your identity is compromised and identity theft insurance.

WHAT YOU CAN DO

We strongly encourage you to carefully examine your credit card account statements. Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information), which provides additional information on ways you can protect your information.

FOR MORE INFORMATION

Pelican is a brand built on the highest of quality and customer service. You, our customers, are the core of our business, and without you we wouldn't be who we are today. We sincerely regret any concern this may cause you. For more information, please call us at 1-844-805-8142 between 8:00 a.m. – 8:00 p.m. Eastern Monday through Friday.

Best,

Pelican Products, Inc.



Steps You Can Take to Further Protect Your Information

Review Your Account Statements & Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). To file a report with the FTC, go to www.identitytheft.gov, call 1-877-ID-THEFT (877-438-4338), or write to the FTC Bureau of Consumer Protection, 600 Pennsylvania Ave., NW, Washington, DC 20580. Reports filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. You may wish to review the tips provided by the FTC on how to avoid identity theft. A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at www.ftc.gov/bcp/edu/microsites/idtheft/.

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>, or you can elect to purchase a copy of your credit report by contacting one of the three national credit-reporting agencies. Contact information for the three national credit-reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion
(800) 680-7289
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report

We recommend placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Other Important Information

Security Freeze



You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit-reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three (3) major consumer-reporting agencies listed above. To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960

<https://www.equifax.com/personal/credit-report-services/>

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

<https://www.experian.com/freeze/center.html>

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

<https://www.transunion.com/credit-freeze>

In order to request a security freeze, you will need to provide some or all of the following information to the credit-reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five (5) years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or up to three (3) business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.



To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three (3) credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to remove the security freeze.

For Residents of Hawaii, Michigan, Missouri, New Mexico, North Carolina, Vermont, Virginia, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For Residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, West Virginia, and Wyoming: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit-reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov.

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023 (toll-free in Maryland), (410) 576-6300, www.oag.state.md.us.

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze.

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at: North



Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free in North Carolina) (919) 716-6400, www.ncdoj.gov.

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392 (toll-free in Oregon), (503) 378-4400, <http://www.doj.state.or.us>.

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at: 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>. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze.

For West Virginia Residents. You may obtain further information as to the types of information Pelican and SureSource collects from individuals generally, and what specific information Pelican or SureSource collects and maintains about you (if any), by calling us at 1-844-805-8142 between 8:00 a.m. – 8:00 p.m. Eastern Monday through Friday.