July 31, 2020

Robert Walker
601.499.8083 (direct)
Robert.Walker@wilsonelser.com

VIA EMAIL DOJ-CPB@doj.nh.gov;
Attorneygeneral@doj.nh.gov

Attorney General Gordon McDonald
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
DOJ-CPB@doj.nh.gov

Re: Data Security Incident

Dear Attorney General McDonald:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Ferris Marketing, Inc. ("Ferris"), a computer and office equipment wholesaler, with respect to a potential data security incident involving Night Owl Security Products LLC ("Night Owl"), a subsidiary of Ferris, (hereinafter, the "Incident") described in more detail below. Ferris takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security Incident.

On May 29, 2020, Ferris was alerted by Visa Inc. ("VISA") that Night Owl's retail website - https://nightowlsp.com/ - was the last Common Point of Purchase ("CPP") for credit cards legitimately used to purchase products from Night Owl which were later used to make fraudulent purchases using VISA payment cards.

Upon further investigation by Ferris, Ferris discovered on June 5, 2020 that this Incident was likely caused by an unknown cyber attacker's malicious insertion of a script onto Night Owl's website which allowed the cyber attacker to orchestrate a credit card fraud scheme against those who made purchases on Night Owl's website after the malicious script was dropped on or around November 1, 2019 and before it was removed on June 5, 2020.

At this time, Ferris has no evidence to indicate that the individual responsible for the cyber incident viewed or otherwise acquired any personal information belonging to New Hampshire residents other than names, addresses, and any payment card information previously used to make a purchase on Night Owl's website.

2. Number of New Hampshire residents affected.

On or about July 13, 2020, Ferris finished identifying fifty-three (53) New Hampshire residents who were potentially affected by this Incident. Incident notification letters addressed to these individuals were mailed on July 31, 2020, via First Class Mail. A sample copy of the Incident notification letter being mailed to

potentially affected residents of New Hampshire is included with this letter.

3. Steps taken.

On June 5, 2020, the same day that Ferris identified the malware infection on Night Owl's retail website, Ferris removed the infection and shut down public access to Night Owl's retail website. During the following twenty days, Ferris took steps to ensure the security of Night Owl's website including the migration to a different hosting provider as well as the performance of upgrades to its network and software. Night Owl's website reopened for public use on June 26, 2020.

Ferris has taken steps to prevent a similar event from occurring in the future. These steps include strengthening Ferris's cybersecurity posture by implementing enhanced software monitoring programs and firewall protection to resist the future occurrence of any similar cybersecurity events.

Ferris has also gone to great lengths to identify and notify any individuals who were potentially impacted as result of this Incident including the hiring of a third-party vendor to arrange for any potentially affected individuals in New Jersey to receive credit monitoring and identify theft protection services for twelve (12) months.

4. Contact information.

Ferris remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at Robert.Walker@wilsonelser.com or (601) 499-8083.

Very truly yours,

Robert Walker

EXHIBIT A

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

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

<<Date>>

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident involving www.nightowlsp.com, a retail website maintained by Night Owl Security Products LLC ("Night Owl"), a subsidiary of Ferris Marketing, Inc. ("Ferris"), which may have resulted in the disclosure or misuse of your payment card information. We take the security of your personal information very seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter contains information about the incident and steps you can take to protect your information.

What Happened

On May 29, 2020 Ferris was first alerted to evidence that Night Owl's retail website was the last Common Point of Purchase ("CPP") for payment cards identified as having been legitimately used to purchase products from Night Owl which were then later used to make fraudulent purchases from other retailers. Upon further investigation, Ferris discovered on June 5, 2020 that this event was likely caused by an unknown cyber attacker's unauthorized insertion of a malicious script onto Night Owl's website on or around November 1, 2019 which allowed the cyberattacker to acquire payment card information of Night Owl customers who made purchases on Night Owl's website.

Upon discovery of the malicious script, Ferris immediately took steps to protect Night Owl customers, including the swift removal of the malicious script on June 5, 2020 and the immediate suspension of public access to Night Owl's retail website for approximately twenty (20) days during which Ferris thoroughly investigated the incident and ensured that the Night Owl website is a secure retail environment for our customers.

At this time, Ferris has no evidence to indicate that the individual responsible for the cyber incident viewed or otherwise acquired any personal information belonging to you other than your name, address, and any payment card information you have previously used to make a purchase on Night Owl's website. Ferris strongly recommends that you should remain vigilant and monitor your accounts for suspicious or unusual activity.

What We Are Doing

Ferris is committed to ensuring the security of all information in our control, and we are taking steps to prevent a similar event from occurring in the future. This includes strengthening our cybersecurity posture. Specifically, we are performing additional hardening of our network, platforms, and software, as well as the implementation of enhanced software monitoring programs and firewall protection to prevent the future occurrence of any similar cybersecurity events.

As a safeguard, we have arranged for you to enroll in a complimentary, online credit monitoring service (*my*TrueIdentity) for twelve (12) months provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

What You Can Do

To enroll in this service, go to the *my*TrueIdentity website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Activation Code>>** and follow the three steps to receive the credit monitoring service online within minutes. If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode **<<Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 855-917-3582 Monday – Friday, 9:00am to 9:00pm Eastern Standard Time.

Sincerely,

Tom Matthews
Acting CFO
Ferris Marketing, Inc.

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: 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,* and *West Virginia*:
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 residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

***For residents of Maryland, Rhode Island, Illinois, New York,* and *North Carolina*:**
You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.
Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, https://www.marylandattorneygeneral.gov/
Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov
North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226, www.ncdoj.gov
Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave., NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft
New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224, 1-800-771-7755, https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

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

More information can also be obtained by contacting the Federal Trade Commission listed above.