CLARK HILL

Clark Hill
130 East Randolph Street
Suite 3900
Chicago, IL 60601
T 312.985.5900
F 312.985.5999

clarkhill.com

Melissa K. Ventrone
T 312.360.2506
F 312.517.7572
Email: mventrone@clarkhill.com

March 12th, 2019

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Dear Attorney General MacDonald:

We represent International Vapor Group, Inc. ("IVG") with respect to a data security incident involving the potential exposure of certain personally identifiable information described in more detail below. IVG is committed to answering any questions you may have about the data security incident, its response, and steps it has taken to prevent a similar incident in the future.

1. Nature of security incident.

IVG has been investigating a possible compromise of its e-commerce website. On December 31, 2019, IVG's forensic investigators informed IVG that payment card data processed through its vaporfi.com and directvapor.com websites between January 19, 2018 and June 30, 2018 were at "intermittent" risk of compromise. In other words, the forensic vendor found that cards were occasionally at risk of compromise during the above period. IVG asked its forensic vendor if it could identify the specific windows in which the payment cards were at risk, but the vendor was unable to do so. IVG then hired a nationally recognized computer forensic firm to determine the specific dates in which payment card information may have been compromised. This information was provided to IVG on March 1, 2019. While the analysis as to which cards, specifically, were at risk is ongoing, IVG has proceeded with sending letters to potentially impacted individuals that may have entered their payment card information on the sites during specific windows of vulnerability. Information at risk may include the cardholder's name, credit or debit card number, expiration date, security code, and order details.

2. Number of residents affected.

48 residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on March 12, 2019 (a copy of the form notification letter is enclosed).

3. Steps taken or plan to take relating to the incident.

DIRECTVAPOR®
vaporfi

C/O ID Experts
P.O. Box 10444
Dublin, OH 43017-4044

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

March 12, 2019

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing you to notify you of a security incident that may have affected your name and credit or debit card information. International Vapor Group ("IVG") values and respects the privacy of your information, and sincerely apologizes for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information.

1. What happened and what information was involved?

We recently learned from our forensic investigators that some credit or debit cards used on directvapor.com or vaprofi.com between January 19, 2018 and June 30, 2018 may have been compromised. From the investigation, it appears an unauthorized individual may have gained access to our e-commerce site and inserted malicious code that occasionally captured credit and debit card information for purchases made through our websites. Credit or debit card information submitted over the phone or purchase made at a retail store were not affected and remain secure. Information at risk includes your name, address, credit or debit card number, expiration date and card verification code.

2. What we are doing and what you can do.

IVG has taken significant steps to enhance the security of its systems and prevent a similar incident from happening again. This includes upgrading system hardware, changing the way certain software and system processes work, implementing a new monitoring program, and moving its servers to AWS with additional security. To help protect your information, you should closely monitor your bank account statements and immediately contact your financial institution if you notice any suspicious activity. More information on protecting your identity is available below.

3. For more information.

If you have any questions or concerns, please call at (888) 262-1559 Monday through Friday, 7:00 a.m. – 7:00 p.m. Central Time. Your trust is a top priority for IVG, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Nick Molina
Chief Executive Officer

U.S. State Notification Requirements

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 by contacting any one or more of the following national consumer reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 105139	P.O. Box 2002	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
1-800-685-1111	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

You may also 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.

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, as well as the Federal Trade Commission.

For residents of *Maryland, Illinois, North Carolina,* and *Rhode Island*:
You can obtain information from the Maryland, North Carolina, and Rhode Island Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Attorney General	**North Carolina Attorney General**	**Rhode Island Attorney General**	**Federal Trade Commission**
Consumer Protection Div.	Consumer Protection Div.	Consumer Protection Div.	Consumer Response Center
200 St. Paul Place	9001 Mail Service Center	150 South Main Street	600 Pennsylvania Avenue, NW
Baltimore, MD 21202	Raleigh, NC 27699-9001	Providence, RI 02903	Washington, DC 20580
1-888-743-0023	1-877-566-7226	(401) 274-4400	1-877-IDTHEFT (438-4338)
www.oag.state.md.us	www.ncdoj.com	www.riag.ri.gov	www.identityTheft.gov

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 at one of the three major credit bureaus by phone and also via each credit bureau'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 credit bureaus is below. As of September 21, 2018, fraud alerts will now last one year, instead of 90 days. Fraud alerts will continue to be free and identity theft victims can still get extended fraud alerts for seven years.
Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.
Security Freeze: 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, each credit reporting agency has a dedicated web page for security freezes and fraud alerts or you can request a freeze by phone or by mail. 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 may also require 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. Effective September 21, 2018, placing a freeze on your credit report is now free for all United States citizens.

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	http://www.experian.com/freeze	www.transunion.com

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