Writer's email: MLittle@pooleshaffery.com

November 9, 2018

**VIA U.S. CERTIFIED MAIL-RETURN RECEIPT REQUESTED, AND E-MAIL TO: SECURITYBREACH@ATG.WA.GOV**

Office of Attorney General
State of Washington
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

**RE: PRELIMINARY NOTICE OF POTENTIAL SECURITY BREACH**

To Whom It May Concern:

Please be advised that this office represents Thesy, LLC, a California limited liability company ("Thesy"). We ask that you please direct all correspondence and inquiries regarding the issues addressed below to our office.

Thesy operates an e-commerce business through its website www.elementvape.com (the "Website"). It has come to our attention that the Website was subject to a data security incident which is described in greater detail below (the "Breach Event"). Thesy takes the privacy and security of its customer's information very seriously and is taking steps to prevent a similar incident from occurring in the future. The following provides a basic summary about the Breach Event based on the information we have obtained as of the date of this letter. Please note that this information is subject to change, as our investigation into the Breach Event is ongoing.

**Brief Description of the Breach Event**

On September 20, 2018, Thesy discovered that a third-party intruder inserted malicious codes into the Website's shopping cart e-commerce software platform creating a window of intrusion between December 6, 2017 and June 27, 2018 wherein the personal information of Thesy's customers who made transactions on the Website may have been at risk of unauthorized access. Upon this discovery, Thesy ran a search of all consumer transactions that took place on the Website during the window of intrusion. It was during this process that Thesy determined that the personal information—namely, the credit card information—of certain Washington residents may be subject to potential unauthorized access. However, we have not been provided with specific evidence that the personal information of Washington residents was in fact acquired illegally or that any such information was used for any fraudulent purpose as a result of the Breach Event.

**The Number of Washington Residents Potentially Affected by the Breach Event**

As of the date of this letter, approximately 5,907 Washington residents are potentially affected by the Breach Event. This number may be subject to change as Thesy and our office continue our investigation into the scope of the Breach Event.

Thesy takes this incident very seriously. It has taken affirmative steps to prevent a similar situation from arising in the future and to protect the privacy and security of its customer's personal information. These steps have included implementing security patches to the shopping cart, removing the malicious code from Thesy's e-commerce platform, and mitigating vulnerabilities with the Website by, among other things, increasing security monitoring along with existing SSL encryption technology for all transactions on the Website.

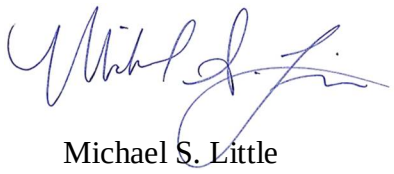
Furthermore, to protect these Washington residents who may have been affected by the Breach Event, Thesy will notify such Washington residents in writing and offer identity theft protection / mitigation services at no cost to them. Please find enclosed an anonymized draft of the notice letter that was sent, on or about November 2, 2018 and/or November 5, 2018, via U.S. Mail to Washington residents whose personal information may have been compromised as a result of the Breach Event.

Should you have any questions, we ask that you please direct all correspondences related to the Breach Event to counsel for Thesy:

Poole & Shaffery, LLP
Attn: Michael S. Little, Esq.
25350 Magic Mountain Parkway, Suite 250
Santa Clarita, CA 91355
Phone: (661) 290-2991
Fax: (661) 290-3338

Sincerely,

POOLE & SHAFFERY, LLP



Michael S. Little

MSL:ams
cc: Thesy, LLC (via email only)
Andrew M. Sevanian (via email only)

Enclosure

[INSERT THESY,LLC | ELEMENT VAPE LOGO] <<Date>>

<<ClientFirstName>><<ClientMiddleName>><<ClientLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>><<ZipCode>>

NOTICE OF DATA BREACH

Dear <<ClientFirstName>><<ClientLastName>>,

Thesy, LLC is committed to maintaining and protecting the security and privacy of the personal information provided to us by our customers. We are writing to inform you of an incident potentially involving the disclosure of information you provided to us. While we have no evidence that any of your information has been used inappropriately, we wanted to notify you of this incident and advise you of steps we have taken in response.

What Happened?

On September 20, 2018, we discovered that a third-party intruder inserted malicious codes into our website's e-commerce software platform creating a window of intrusion between December 6, 2017 and June 27, 2018 wherein personal information of our customers may have been accessed. We immediately conducted an investigation into this matter wherein the breach was contained on June 27, 2018 and the malicious code was removed from our e-commerce platform and vulnerabilities were mitigated.

What Information Was Involved?

While it has not been confirmed that any personal information was in fact taken by the third-party intruder, we determined that credit card information of customers who made transactions on our website between December 6, 2017 and June 27, 2018 was at-risk.

What We Are Doing.

We deeply regret this incident occurred and any inconvenience or concern this may cause you. To date, we are not aware of any reports of identity fraud resulting from this incident nor do we have any evidence to suggest that your personal information has actually been misused. We take our obligation to safeguard your personal information very seriously and have implemented measures to help prevent this type of issue in the future. For your protection and security, we have also notified law enforcement of the incident. We wanted to make you aware that your personal information may be in the possession of an unauthorized individual and explain the steps we are taking to safeguard you against identity theft.

In order to help relieve any such concerns and restore confidence following this incident, we have contracted with LifeLock, a Symantec company, to make available at no cost to you for one year its LifeLock Defender™ Preferred solution. As you may be aware, LifeLock is an industry leader in providing credit and identity theft monitoring and remediation services and products. Their incident response team has extensive experience in assisting people who have sustained an unintentional exposure of their personal information.

LifeLock Defender™ Preferred is specifically designed to protect your personal information as well as your financial standing and personal identity. In the unlikely event that you are impacted by this incident, LifeLock will take all steps necessary to respond to, remediate and rectify the situation.

**To activate your membership and get protection at no cost to you:**

1. Go to www.LifeLock.com and click on the red **START MEMBERSHIP** button.
2. You will be taken to another page where, below the three protection plan boxes, you can enter the promo code: **THESY1810** and click the APPLY button.
3. On the next page, enter your Member ID. (Your Member ID is **<<MEMBER ID>>**).
4. Click the red **START YOUR MEMBERSHIP** button.
5. You will receive a confirmation email after enrollment (be sure to follow all directions in this email).

**You will have until December 30th, 2018 to enroll in this service.**

Once you have completed the LifeLock enrollment process, the service will be in effect. Your LifeLock Defender™ Preferred membership includes:

- ✓ LifeLock Identity Alert® System†
- ✓ Live, US-Based Priority Member Support 24/7
- ✓ Stolen Funds Reimbursement up to $25,000 *
- ✓ Personal Expense Compensation up to $25,000 *
- ✓ Service Guarantee for Lawyers and Experts up to $1 million *
- ✓ Identity Restoration Support
- ✓ Annual Three-Bureau Credit Reports & Credit Scores[1]
  The credit scores provided are VantageScore 3.0 credit scores based on Equifax, Experian and TransUnion respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.
- ✓ Three-Bureau Credit Monitoring[1,2]
- ✓ Address Change Verification
- ✓ Bank Account Takeover Alerts†
- ✓ Dark Web Monitoring
- ✓ Fictitious Identity Monitoring
- ✓ Credit Card, Checking and Savings Account Activity & Application Alerts†

1 Credit reports, scores and credit monitoring may require an additional verification process and credit services will be withheld until such process is complete.

2 For LifeLock Defender™ Preferred Three-bureau Credit monitoring, credit monitoring from Experian and TransUnion will take several days to begin.

† LifeLock does not monitor all transactions at all businesses.

* Indicates features included within the Million Dollar Protection™ Package††† No one can prevent all identity theft.

We are also providing you with the attached Recommended Steps to help Protect your Information, which identifies other measures that you can take to protect yourself from identity theft. It also includes contact information for the Federal Trade Commission, state Attorneys General, and the three major credit bureaus, should you wish to contact them as well.

What You Can Do.

In addition to utilizing the LifeLock solution, which we strongly encourage you to take advantage of, we also caution you to be vigilant in protecting your personal information. By way of example, you might change all of your

website and computer passwords, check your bank and credit card statements to see if there have been any unusual or unauthorized transactions or activity, and take similar remedial measures that only you can do, as suggested on the attached document. You should also report any suspected incidents of identity theft to local law enforcement or the attorney general.

To protect yourself from the possibility of identity theft, we recommend that you immediately place a fraud alert on your credit files. A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud. When you or someone else attempts to open a credit account in your name, the lender should take measures to verify that you have authorized the request.

Please rest assured that our customers', employees' and their families' well-being and the security of your personal information are our highest priorities. We apologize for any inconvenience this incident may cause you and thank you for your understanding and patience.

For More Information.

If you have any questions or need additional information about this notice, we have set up a dedicated support line through LifeLock, available 24/7/365. Please feel free to give us a call at XXX-XXX-XXX.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Kenny Sy
CEO – Thesy, LLC
www.elementvape.com

**Recommended Steps to Help Protect Your Information**

It is recommended 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.

You can obtain information from the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. The FTC can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

**Fraud Alerts**: You can place fraud alerts with the three major credit bureaus by phone and also via their websites. 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.

**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, or 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, 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. The consumer reporting agency may charge a small fee to place, lift, or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

| **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.freeze.equifax.com | www.experian.com/freeze | http://freeze.transunion.com |
| 800-525-6285 | 888-397-3742 | 800-680-7289 |

**If you live in Maryland, please read the additional notice below that applies to you:**

You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.marylandattorneygeneral.gov

**If you live in North Carolina, please read the additional notice below that applies to you:**

You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

North Carolina Attorney General
Department of Justice
9001 Mail Service Center
Raleigh, NC 27699-9001
(919) 716-6400
http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx

**If you live in Oregon, please read the additional notice below that applies to you:**

You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

Oregon Attorney General
Department of Justice – Consumer Protection
1162 Court Street NE
Salem, OR 97301
(877) 877-9392
https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/data-breaches

**If you live in Rhode Island, please read the additional notice below that applies to you:**

You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

Rhode Island Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401) 274-4400
http://www.riag.ri.gov/consumerprotection/about.php