

# CLARK HILL

---

Melissa K. Ventrone  
T 312.360.2506  
Email: [mventrone@clarkhill.com](mailto:mventrone@clarkhill.com)

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

December 21, 2020

*Via <https://appengine.egov.com/apps/nics/Maine/AGReportingForm>; Online Form*

Attorney General Aaron Frey  
Office of the Attorney General  
6 State House Station  
Augusta, ME 04333

Attorney General Aaron Frey:

We represent Vaporfi.com and Directvapor.com (collectively “affected entities”) with respect to a data security incident involving the potential exposure of certain personally identifiable information described in more detail below. All affected entities, headquartered in Florida, are eCommerce entities that sell, among other things, vaporizer pens and E-Cigarettes. The affected entities are committed to answering any questions you may have about the data security incident, their response, and steps taken to prevent a similar incident in the future.

## **1. Nature of security incident.**

On September 23, 2020, the affected entities became aware of suspicious activity associated with their online check-out page. The affected entities immediately began an internal investigation and determined that an unauthorized user had gained access to their online payment platform and credit and debit card information entered between September 14, 2020 through September 23, 2020 may have been at risk of compromise. From the investigation, it appears information at risk may have included customer names, credit or debit card numbers, expiration dates, and security codes or card verification codes.

## **2. Number of residents affected.**

Cumulatively, Three (3) Maine residents may have been affected and is broken down as follows:

Entity	Residents Impacted
Vaporfi.com	1
Directvapor.com	2

December 21, 2020

Page 2

All impacted individuals were notified of the incident by notification letter mailed via regular mail on December 21, 2020 (a copy of the form notification letter is enclosed).

**3. Steps taken relating to the incident.**

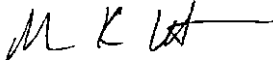
The affected entities fixed the vulnerability, audited its systems, and installed additional controls to further enhance the system's security.

**4. Contact information.**

The affected entities take the security of the information in their control seriously and are committed to ensuring this information is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at [mventrone@clarkhill.com](mailto:mventrone@clarkhill.com) or (312) 360-2506.

Very truly yours,

CLARK HILL

A handwritten signature in black ink, appearing to read 'M K Ventrone', with a horizontal line extending to the right.

Melissa K. Ventrone  
Partner

Enclosure



C/O IDX  
P.O. Box 1907  
Suwanee, GA 30024

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

December 16, 2020

### Notice of Data Security Incident

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

We are writing you to inform you of a recent data security incident experienced by Vaporfi.com (“VF”) that may have impacted your personal information, including your name and credit or debit card information. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

#### What Happened:

On September 23, 2020, VF became aware of suspicious activity associated with its online check-out page. We immediately began an internal investigation and determined that an unauthorized user may have gained access to information entered into the check-out page of Vaporfi.com between September 14, 2020 through September 23, 2020. On October 13, 2020, we completed our investigation and determined that your information may have been impacted by this incident.

#### What Information Was Involved:

Information at risk may have included your name, address, credit or debit card number, expiration date, security code or card verification code, and purchase information.

#### What We Are Doing:

We are taking steps to help prevent this type of incident from occurring in the future. Since the incident, we fixed the vulnerability, audited our systems, and installed additional controls to further enhance our system’s security. We also implemented multi-factor authentication for remote access to our system. We are confident that customers can make purchases safely on our website.

#### What You Can Do:

You should carefully review the credit and debit card statements for any payment cards you used on our website between September 14, 2020 through September 23, 2020. If you identify any suspicious activity, immediately contact your financial institution.

**More Information:**

For questions, please call 1-833-754-1792 Monday through Friday from 9 AM – 9 PM Eastern Time. Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

*Matt Nahanee*

Matt Nahanee

Vice President, Consumer Experience



## Recommended Steps to Help Protect Your Information

**1. Telephone.** Contact IDX at 1-833-754-1792 to gain additional information about this event.

**2. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**3. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax'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 bureaus is as follows:

### Credit Bureaus

Equifax Fraud Reporting  
1-866-349-5191  
P.O. Box 105069  
Atlanta, GA 30348-5069  
[www.equifax.com](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**4. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**5. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



C/O IDX  
P.O. Box 1907  
Suwanee, GA 30024

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

December 16, 2020

### Notice of Data Security Incident

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

We are writing you to inform you of a recent data security incident experienced by Directvapor.com (“DV”) that may have impacted your personal information, including your name and credit or debit card information. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

#### What Happened:

On September 23, 2020, DV became aware of suspicious activity associated with its online check-out page. We immediately began an internal investigation and determined that an unauthorized user may have gained access to information entered into the check-out page of Directvapor.com between September 14, 2020 through September 23, 2020. On October 13, 2020, we completed our investigation and determined that your information may have been impacted by this incident.

#### What Information Was Involved:

Information at risk may have included your name, address, credit or debit card number, expiration date, security code or card verification code, and purchase information.

#### What We Are Doing:

We are taking steps to help prevent this type of incident from occurring in the future. Since the incident, we fixed the vulnerability, audited our systems, and installed additional controls to further enhance our system’s security. We also implemented multi-factor authentication for remote access to our system. We are confident that customers can make purchases safely on our website.

#### What You Can Do:

You should carefully review the credit and debit card statements for any payment cards you used on our website between September 14, 2020 through September 23, 2020. If you identify any suspicious activity, immediately contact your financial institution.

**More Information:**

For questions, please call 1-833-754-1792 Monday through Friday from 9 AM – 9 PM Eastern Time. Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

*Matt Nahanee*

Matt Nahanee

Vice President, Consumer Experience





## Recommended Steps to Help Protect Your Information

**1. Telephone.** Contact IDX at 1-833-754-1792 to gain additional information about this event.

**2. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**3. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax'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 bureaus is as follows:

### Credit Bureaus

Equifax Fraud Reporting  
1-866-349-5191  
P.O. Box 105069  
Atlanta, GA 30348-5069  
[www.equifax.com](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**4. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**5. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.