



<< Date >> (Format: Month Day, Year)

<<first_name>> <<last_name>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>

NOTICE OF DATA BREACH

Dear eJuice Direct Customer:

We value your business and respect the privacy of your information, which is why we are writing to let you know about a cybersecurity incident involving the eJuice Direct e-commerce website that may have allowed an unauthorized third party to acquire a copy of personal information you entered into the website.

WHAT HAPPENED?

A malicious script was injected into the website by an unauthorized third party that may have allowed access to personal information you entered into the website between August 15, 2020 and August 25, 2020, and between October 28, 2020 and July 7, 2021.

While we cannot definitively confirm that your personal information was affected, it is possible that it might have been as your transaction(s) occurred during the above referenced period. If it was, this might have exposed you to a risk of fraudulent transactions being carried out using your personal information.

WHAT INFORMATION WAS INVOLVED?

The data accessed included payment card details (card number, CVC/CVV and expiration date). Other information was not compromised.

WHAT WE ARE DOING.

Upon discovering the incident, we immediately contracted with a leading cybersecurity firm to conduct a thorough forensic investigation and will notify you if there are further significant developments. We have implemented additional security measures to prevent the reoccurrence of such a breach and to protect the privacy of our customers. The additional security measures include the following:

- The malicious script has been removed from the website;
- Multi-Factor Authentication (MFA) has been enabled for all administrative accounts on the website;
- A Web Application Firewall (WAF) has been enabled and configured to provide additional security.

WHAT YOU CAN DO.

We are notifying you so that you can take action which will assist to minimize or eliminate potential harm. We strongly advise you to take preventive measures to help prevent and detect any misuse of your information.

FOR MORE INFORMATION.

We sincerely apologize for the inconvenience this incident has caused you. Please be advised that we will keep you informed of any developments in the investigation which may be of importance to you.

If you have any questions about the incident, please contact us at 224-220-3222, Monday through Friday from 9:30 a.m. to 5:00 p.m. Central Time or notice@ejuicedirect.com.

eJuice Direct

Recommended Steps to Help Protect Your Information

1. Monitor financial accounts. As a first step, we recommend that you closely monitor your financial accounts and if you see any unauthorized activity, you should promptly contact your financial institution. We also suggest that you submit a complaint with the Federal Trade Commission by calling 1.877.438.8228 (1.877.IDTHEFT) or online at www.ftccomplaintassistant.gov.

2. Review your credit reports. As a second step, you may want to contact the three U.S. credit reporting agencies (Equifax, Experian, and TransUnion) to obtain a free credit report from each by calling 1.877.322.8228 or by logging onto www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit reports periodically can help you spot a problem and address it quickly.

3. Place Fraud Alerts with the three credit bureaus. 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

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
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. If you are a victim of identity theft, you have the right an extended fraud alert which is good for 7-years.

A credit freeze does not apply to any person or entity, or its affiliates, or collection agencies acting on behalf of any person or entity that you have an existing account or loan with and requests information in your credit report for the purpose of reviewing or collecting outstanding balances on a credit card or other credit account, loan, or other bills. This information includes activities related to account maintenance, monitoring credit line increases, loan and account upgrades, and loan approvals.

The credit reporting agencies have 3-business days after receiving your request to place a credit freeze on your credit report. The credit reporting agencies must also send written confirmation to you within 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 of or a temporary or permanent lifting of the credit freeze to allow creditors to access your credit report.

4. **Place a security freeze.** You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement or telephone bill.

5. **Obtain additional information.** You can obtain additional information about the steps you can take to avoid identity theft from the following agencies.

California Residents: This notification was not delayed by law enforcement. Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, <https://www.oag.dc.gov/>, 1-202-727-3400.

Iowa Residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, 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, 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, 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, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, 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, Telephone: 401-274-4400. Approximately 21 Rhode Island residents were impacted in this data security incident.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Colorado, Georgia, Maine, Maryland, New Jersey, and Vermont Residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

Tennessee residents:

TENNESSEE CONSUMERS HAVE THE RIGHT TO OBTAIN A SECURITY FREEZE

You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze must be requested in writing by certified mail or by electronic means as provided by a consumer reporting agency. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. If you are actively seeking a new credit, loan, utility, or telephone account, you should understand that the procedures involved in lifting a security freeze may slow your applications for credit. You should plan ahead and lift a freeze in advance of actually applying for new credit. When you place a security freeze on your credit report, you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or authorize the release of your credit report for a period of time after the freeze is in place. To provide that authorization you must contact the consumer reporting agency and provide all of the following: (1) The personal identification number or password; (2) Proper identification to verify your identity; and (3) The proper information regarding the period of time for which the report shall be available. A consumer reporting agency must authorize the release of your credit report no later than fifteen (15) minutes after receiving the above information. A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account, that requests information in your credit report for the purposes of fraud control, or reviewing or collecting the account. Reviewing the account includes activities related to account maintenance. You should consider filing a complaint regarding your identity theft situation with the federal trade commission and the attorney general and reporter, either in writing or via their web sites. You have a right to bring civil action against anyone, including a consumer reporting agency, which improperly obtains access to a file, misuses file data, or fails to correct inaccurate file data.