[GREEN AMERICA LOGO]

<<Return Mail Address>>

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>> <<Date>>
<<City>>, <<State>> <<Zip>>
<<Country>>

NOTICE OF [DATA EVENT] / [DATA BREACH]

Dear <<Name 1>> <<Name 2>>:

Green America is writing to notify you of a recent data security event that occurred at DC Health Link that may impact the privacy of some of your information. DC Health Link is a third-party health care enrollment entity which stored data for Green America to assist in enrolling and obtaining health insurance for Green America employees and dependents. This event did not occur at Green America, nor did it impact the security of Green America's computer systems. We are providing you with information about the incident and steps you may take to protect against misuse of your information, should you feel it necessary to do so.

What Happened? In March of 2023, we learned that a data security incident occurred at DC Health Link when contacted by certain employees. We have not been notified by DC Health Link. We understand that on March 6, 2023, DC Health Link learned data for some DC Health Link users was exposed on a public forum. DC Health Link immediately began working to determine the nature and scope of the incident and launched an investigation with the assistance of third-party forensic specialists. We further understand that DC Health Link then provided notice directly via email to certain individuals. DC Health Link is providing updates on this event at: https://www.dchealthlink.com/data-breach.

Once Green America became aware of the incident, we immediately undertook a review to determine what data was shared with DC Health Link, and out of an abundance of caution, we are providing notice to all employees who had accounts with DC Health Link and their beneficiaries whose data may have been affected by this incident at DC Health Link.

What Information Was Involved? DC Health Link reports the data that relates to you and may have been affected by this incident includes your name and name of your dependents enrolled on DC Health Link, Social Security Number, Date of Birth, Gender, Address, Email, and Phone Number. Further, according to DC Health Link, additional information exposed included Plan name, Premium Amount, APTC, Coverage Start and End Dates, Race/Ethnicity, Citizenship, HBX ID.

What We Are Doing? Upon learning of this incident, Green America moved quickly to investigate and respond.

We also want to make you aware of the credit and identity monitoring product that DC Health Link is offering. Details for enrollment are in the email from DC Health Link. Please contact [name] at [contact info] if you don't have this information.

What You Can Do? We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. You may also review the information contained in the attached "Steps You Can Take to Help Protect Your Information."

For More Information. We regret any concern this incident may cause, and recognize that you may have questions that are not addressed in this letter. If you have additional questions or concerns, please call our dedicated assistance line at xxx-xxx-xxxx. This toll-free line is available Monday – Friday from _:00 am to _:00 pm _ Eastern Time. Individuals may also write to Green America at 1612 K Street NW, Suite 600, Washington D.C. 20006.

Sincerely,

[NAME]
[TITLE]
Green America

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

Visit the Experian IdentityWorks website to enroll:

For adult DC Health Link customers (18 and over), go to https://www.experianidworks.com/3bplus

- Activation Code: G9NXF76MB
- Engagement Number: B087357
- Product: Experian IdentityWorks – Credit Plus 3B

For DC Health Link customers who are minors (under 18), go to https://www.experianidworks.com/minorplus

- Activation Code: XCV4FPB3G
- Engagement Number: B087358
- Product: Experian IdentityWorks – Minor Plus

You will need to provide the **Activation Code** listed above for the adult or minor monitoring services you are selecting. If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(877) 890-9332.** Be prepared to provide the **Engagement Number** listed for your services above as proof of eligibility for the identity restoration services by Experian. If asked for a "Client Name" mention **District of Columbia Health Benefit Exchange Authority.**

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help

888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are two (2) Rhode Island residents impacted by this incident.