**CareFirst BlueCross BlueShield**
**Community Health Plan**
**District of Columbia**
1100 New Jersey Ave. SE
Suite 840
Washington, D.C. 20003
**www.carefirstchpdc.com**

[March X, 2021]

[Name]
[Addressee Address 1]
[Addressee Address 2]
[Addressee Address 2]
[City], [State], [Zip]

**Notice of Security Event**

Dear [Name]

CareFirst BlueCross BlueShield Community Health Plan District of Columbia (CareFirst CHPDC), formerly Trusted Health Plan, is writing to tell you about an event that may have impacted your information. We want you to know what we are doing to protect you and how you can protect yourself.

What Happened

On January 28, 2021, we learned that someone attacked our computer systems. They stole personal information. We informed the Federal Bureau of Investigation and started our own inquiry. We also hired an expert computer security company, CrowdStrike, to help us. We found that a foreign cybercriminal group is likely responsible.

CHPDC also notified the D.C. Department of Health Care Finance (DHCF). DHCF, with the assistance of the District's Privacy and Security Official within the Office of the Attorney General, is monitoring our inquiry to identify necessary actions and improvements.

What Information Was Stolen

As a provider, you received payment from CHPDC for services provided to D.C. Medicaid enrollees. The stolen information may have included personal and/or business information about you, such as your full name, business address and Social Security number or tax identification number, whichever number you use for tax purposes.

If you receive any emails from anyone stating that they have your personal or business information, please do not click on any links or attachments that may be in the email. Please

This program is funded in part by the Government of the District of Columbia Department of Health Care Finance.

delete the emails. The links or attachments may have software in them that can harm your computer or device.

What We Are Doing

When we learned about the attack on our systems, we immediately took action to isolate the affected computers and protect personal information. We called in the expert computer security company, CrowdStrike, who assisted us in taking a series of steps designed to further protect personal information, including changing every password, monitoring for signs of data misuse, and finding out how the attack happened to avoid it from happening again. We also stopped operations that share information with our business partners.

To help protect your identity, we are offering a free two-year membership in Experian's® IdentityWorks℠. This product monitors all three credit bureaus, helps detect possible misuse of your personal information and provides detection and theft resolution. This product also includes insurance and identity restoration.

To activate your membership, please follow the steps below:

- **Visit** [URL] to enroll.
- Provide your **activation code**: **[code]**
- Ensure that you **enroll by**: **June 30, 2021**(Your code will not work after this date.)

Please do not share this information. These links and codes are only for you.

If you do not have internet access, or need assistance, please contact Experian at [phone number] and provide this engagement #: **[engagement number]** to enroll at no cost.

What You Can Do

There are other things you can do to protect yourself from identity theft. Please read the information we have attached to learn more.

For More Information

We are committed to protecting your privacy. CHPDC will not contact you by email or phone about this event. If you receive inquiries by phone, email, text or social media that say they are about this event, they are **not** from us. Do not click on any links in email messages or provide any personal information in response.

If you have questions, please contact Experian at [insert contact phone number]. You can also reach us by email at chpdcanswers@carefirst.com or by mail at CHPDC Privacy Office, P.O. Box 14858, Lexington, KY 40512. You may also contact us directly at 202-821-1100.

You can also find enrollment information and other information about this incident at www.chpdcanswers.com.

Sincerely,
[SIGNATURE GRAPHIC]
George Aloth
CEO, CareFirst BlueCross BlueShield Community Health Plan District of Columbia

**Steps You May Take to Protect Yourself Against Potential Misuse of Information**

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may 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. You may also obtain a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

**Equifax:** P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com

**Experian:** P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com

**TransUnion:** P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports. We also recommend that you promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission (FTC). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

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

**Fraud Alerts:** There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for 7 years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

**Equifax:** 1-888-766-0008, www.equifax.com

**Experian:** 1-888-397-3742, www.experian.com

**TransUnion:** 1-800-680-7289, fraud.transunion.com

**Credit Freezes:** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Placing, lifting, and/or removing a credit freeze from your account is completely free and will not affect your credit score. Please contact the three national credit reporting agencies as specified below to find out more information:

**Equifax:** P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

**Experian:** P.O. Box 9554, Allen, TX 75013, www.experian.com

**TransUnion:** P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the three national credit reporting agencies listed above.

The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day, and year); current address and previous addresses for the past 5 years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state, or military ID card, and a copy of a utility bill, bank, or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

**For residents of the District of Columbia**: You may also contact the District of Columbia Office of the Attorney General: Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001, (202) 442-9828, https://oag.dc.gov/.

**For residents of Maryland**: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

**For residents of Massachusetts**: If you are a Massachusetts resident, you also have a right to request a police report about this incident.

**For residents of New York**: You may also obtain information about security breaches and preventing and avoiding identity theft from the New York Office of the Attorney General: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/.

**For residents of North Carolina**: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

**For residents of Oregon**: You may also contact the Oregon Office of the Attorney General: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, 1-877-877-9392, help@oregonconsumer.gov, www.doj.state.or.us.

**For residents of Rhode Island**: You also may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, Consumer Protection Unit 150 South Main Street, Providence, RI 02903, (401)-274-4400, http://www.riag.ri.gov. You may also be able to file or obtain a police report about this incident.