

P. Todd Cioni, Vice President  
Chief Compliance, Ethics & Privacy Officer

CareFirst BlueCross BlueShield  
1501 S. Clinton Street  
Baltimore, MD 21224  
Tel. 410.528.7170  
Fax 410.720.6081  
Email: todd.cioni@carefirst.com

STATE OF NH  
DEPT OF JUSTICE  
2015 MAY 26 AM 11:32



May 20, 2015

The Honorable Joseph Foster  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

Dear Attorney General Foster:

This letter is to provide you with information regarding an unauthorized access or use of personal information involving 7 New Hampshire residents ("affected brokers"). CareFirst is providing you with information regarding the unauthorized access or use as required by New Hampshire Statute §369-C:20, I(b).

As part of CareFirst's ongoing information technology (IT) security efforts in the wake of recent cyberattacks on other health insurers, CareFirst engaged the services of Mandiant, one of the world's leading cybersecurity firms, to conduct an end-to-end assessment of our IT environment. This assessment included multiple, comprehensive scans of our IT systems and related devices for evidence of any cyberattack.

During the Mandiant assessment, on April 21, 2015, Mandiant discovered that a cyberattack occurred and likely resulted in a limited unauthorized access to a database on June 19, 2014. The database stores data that is used in the operation of a website used by brokers who are registered with CareFirst. Mandiant has completed its review and found no indication of any other prior or ongoing attack or evidence that other personal information was accessed.

More specifically, the investigation determined that the attackers could have potentially acquired the unique user name used by the broker to log into the website, as well as the broker's name and his/her Social Security number.

However, it is important to realize that user names must be used in conjunction with a password the broker created to gain access to the website. The database in question did not include passwords because CareFirst fully encrypts and stores these in a separate system as a safeguard against just such attacks. Since no passwords were accessed, the user name created by the broker cannot be used to access the website. It is also critical to note that the database accessed did not include financial, banking, medical, or any other information about the broker.

At this time CareFirst has no evidence that the information contained in the database has been misused.

Approximately 1.1 million current and former CareFirst members and individuals who do business with CareFirst online who registered to use CareFirst's websites prior to June 20, 2014 are affected by this incident.

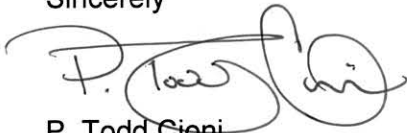
We have notified Experian, Equifax and TransUnion of the incident.

CareFirst is providing the affected brokers with a summary of the incident as well as an opportunity to enroll for two (2) years of credit monitoring at CareFirst's expense.

We have included a copy of the notification letter(s) being sent to the affected brokers within the next 7 business days.

Please do not hesitate to contact me, if you have any questions about this incident.

Sincerely

A handwritten signature in black ink, appearing to read "P. Todd Cioni", with a stylized flourish at the end.

P. Todd Cioni

Attachment: Broker Notification Letter



The CareFirst BlueCross BlueShield  
family of health care plans.

Return Mail Processing Center  
PO Box 414  
Claysburg, PA 16625-7802

Chet Burrell  
President and Chief Executive Officer

May 22, 2015



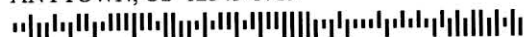
##B0148-L07-0123456 0001 00000001 \*\*\*\*\*3-DIGIT 123

SAMPLE A SAMPLE

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



Dear Sample A Sample,

I am writing to inform you that CareFirst BlueCross BlueShield ("CareFirst") was the target of a sophisticated cyberattack. It is possible that some of your personal and/or business information – as explained below – may have been accessed by the attackers.

We regret the concern this may cause you. I am writing to provide you with information regarding the attack, the steps we are taking to protect your information, and the steps you should take to do the same.

#### What happened and what is CareFirst doing about it?

As part of CareFirst's ongoing information technology (IT) security efforts in the wake of recent cyberattacks on other health insurers, CareFirst engaged the services of Mandiant, one of the world's leading cybersecurity firms, to conduct an end-to-end assessment of our IT environment. This assessment included multiple, comprehensive scans of our IT systems and related devices for evidence of any cyberattack.

Through this assessment, on April 21, 2015, Mandiant initially discovered that a cyberattack occurred and likely resulted in a limited unauthorized access to a database on June 19, 2014. The database includes data that is used in the operation of CareFirst's Broker Portal website. Mandiant has completed its review and found no indication of any other prior or ongoing attack or evidence that other personal information was accessed.

More specifically, the investigation determined that the attackers could have potentially acquired the unique user name assigned to you by CareFirst that you use to log into the Broker Portal, as well as your name, Social Security number and email address.

It is important to realize that user names must be used in conjunction with a password you created to gain access to the Broker Portal. The database in question did not include passwords because CareFirst fully encrypts and stores these in a separate system as a safeguard against just such attacks. Since no passwords were accessed, the user name you created cannot be used alone to access your data through the Broker Portal. It is also critical to note that the database accessed did not include address, medical claims, employment, credit card, financial, or any other information about you or your business.

0123456



Please note if you are also a CareFirst member who has registered through the CareFirst website you may receive a second letter in your capacity as a member.

## What should you do now?

We do not have any evidence that your information has been misused and we believe that the likelihood of such misuse is low. However, as an added protection, we are providing you with two years of free credit monitoring and identity theft protection services through Experian's® ProtectMyID® Alert. These services help detect possible misuse of your personal information and provide you with identity protection services focused on immediate identification and resolution of identity theft. Enrollment is completely free and will not affect your credit score. Due to privacy laws, we are unable to enroll you directly.

### Activate ProtectMyID Now in Three Easy Steps

1. ENSURE That You Enroll By: **October 31, 2015** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: [www.protectmyid.com/carefirst](http://www.protectmyid.com/carefirst)**
3. PROVIDE Your Activation Code: **ABCDEFGHI**

If you have questions or need an alternative to enrolling online, please call 888-451-6562 and provide this engagement #: **[engagement number]**.

For more information and FAQs about how this event directly affects our brokers, go to the broker homepage on CareFirst.com and login. After you login you will see a link to click for broker-specific information.

In addition, we recognize that you may be a member of CareFirst as well. CareFirst has created a dedicated public website ([www.carefirstanswers.com](http://www.carefirstanswers.com)) where you can find more information about this event and its impact on CareFirst members.

### A Special Word of Caution

Please note, CareFirst will not contact you by email or make unsolicited phone calls to you about this attack. Therefore, if you receive inquiries by phone, email or social media purporting to be related to this attack, they are not from CareFirst and you should not click on any links in email messages or provide any personal information in response. Authentic emails from CareFirst related to your health care coverage will contain a link to [www.carefirst.com](http://www.carefirst.com), where you will be required to provide a user name and password to access the site and any content referenced in the message.

### Information About Preventing Identity Theft

We recommend that you remain vigilant to guard against the possibility of fraud and identity theft by reviewing your credit card, bank and other financial statements for any unauthorized activity. You may obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report free of charge once every 12 months, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax  
PO Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
1-800-525-6285

Experian  
PO Box 2002  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
1-888-397-3742

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

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission and the Maryland Office of the Attorney General are as follows:

Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
1-877-438-4338

Maryland Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
<http://www.oag.state.md.us/idtheft/>  
1-410-528-8662

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes.

Again, we urge you to take the actions outlined above to further safeguard your information. We are deeply sorry for any concern this attack causes you, but wanted you to know the nature and extent of it, and to make you aware of the steps we are taking to protect your information at all times.

Sincerely,



Chet Burrell  
President & Chief Executive Officer

0123456



B0148-L07