CareFirst
The CareFirst BlueCross BlueShield family of health care plans.

Broker FAQs – For Use on Broker Portal and with Brokers
May 20, 2015

What happened?
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 its IT environment. This assessment included multiple, comprehensive scans of our IT systems and related devices for evidence of any cyberattack.

Part way through this assessment, on April 21, 2015, Mandiant discovered that a sophisticated cyberattack occurred that likely resulted in a limited unauthorized access to a database on June 19, 2014. The database stores data that members and other individuals used to access CareFirst's website. Mandiant has completed its review and found no indication of any other prior or subsequent attack or evidence that other personal information was accessed.

Who is responsible for this attack?
CareFirst reported the attack to the Federal Bureau of Investigation (FBI) and is cooperating with the investigation. Any inquiries regarding the investigation should be directed to the FBI.

What information was accessed and how does it affect me and my business?
The investigation determined that the attackers could have potentially acquired brokers' Social Security Number (SSN) as well as your user name to access CareFirst online services and your email address. No financial or credit information was affected.

We understand that any compromise of your SSN is a cause for concern. Every broker user who registered to do business with CareFirst prior to June 20, 2014 will receive a letter from CareFirst. We are providing two free years of credit monitoring and identity theft protection through Experian.

It is important to know that your user name created as part of the registration process to access www.carefirst.com must be used in conjunction with the associated password you created. Without the associated password, the username alone cannot be used to access the website or the underlying information. No passwords were accessed in this attack because passwords are stored in a separate database and are encrypted as a safeguard against just such attacks.

How do I know if I have been affected?
Brokers whose accounts were created for access to www.carefirst.com prior to June 20, 2014 are affected by this incident. CareFirst is mailing letters to all affected brokers. If you are affected you will receive a letter in the next 7 to 10 days which will include your personalized code and instructions for how to enroll in the offered protections.

In addition, if you are a CareFirst member and you created a user account on www.carefirst.com to manage your personal coverage with CareFirst prior to June 20, 2014, you are affected and will receive a separate letter.

What reassurances can CareFirst provide regarding its online security?
In today's environment, no business of any size or scope can offer ironclad reassurances about IT security. Given the size and scale of cyberattacks against major United States businesses documented in the last year, it is evident that the sophistication and scale of cyberattacks continues to grow.

CareFirst – like every other major business – constantly identifies and prevents attempted attacks on its IT infrastructure. This is a 24-7, year round exercise.

As part of our continuing IT security efforts and in the wake of documented cyberattacks against major national health care companies earlier this year, CareFirst engaged Mandiant, one of the world's leading cybersecurity firms to conduct a comprehensive assessment of its IT environment and – specifically – to search for any evidence or trace of ongoing or past attacks on our systems. It was this exhaustive set of scans that led to the discovery of this attack. Mandiant has completed its review and found no indication of any other prior or ongoing attack or evidence that other personal information was accessed.

What is CareFirst doing to strengthen its online security?
In addition to the deep assessment of our environment by Mandiant, CareFirst has also engaged Mandiant to perform a complete analysis of our overall security program and controls. CareFirst has an aggressive security program that is routinely reviewed by internal staff, external auditors, and specialized security firms. All recommendations provided by Mandiant in their assessment have either already been completed or are in progress.

How does this affect CareFirst members?
The investigation determined that the attackers could have potentially acquired the unique user name members created as part of their registration to use CareFirst's online services, as well as their name, birth date, email address, and subscriber identification number. The database accessed by attackers contained no member Social Security numbers, medical claims, employment, credit card, or financial information.

The member information accessed as part of this attack is of limited utility to others. For example, the user name created by a member as part of the registration process for www.carefirst.com can only be used in conjunction with an associated, member-created password. Without the associated password the user name alone cannot be used to access the website in order to gain access to any underlying information. No passwords were accessed in this attack because passwords are stored in a separate database and are encrypted as a safeguard against just such attacks.

Only CareFirst members who created online accounts at www.carefirst.com prior to June 20, 2014 are potentially affected by this attack. Members who enrolled to use CareFirst online services on or after June 20, 2014 are not affected because their enrollment occurred after the date of the unauthorized access. Affected members will receive letters from CareFirst. Additional member information can be found at www.carefirstanswers.com.

What is CareFirst doing to alert affected members?
Approximately 1.1 million CareFirst members who registered to CareFirst's online services at www.carefirst.com are potentially affected. CareFirst has made a public announcement regarding this matter, and has established www.carefirstanswers.com as an online source of information.

Beginning May 22, 2015 CareFirst will begin mailing letters to all affected members. These letters will include personalized codes to allow the members to enroll in the credit monitoring and identity theft protections being offered.

Did this affect all lines of CareFirst business or is it limited to groups or others?
This incident did not impact members of CareFirst Administrators or the Standard and Basic Plans of the Federal Employee Program.

I received my letter of notification, how do I activate my free protection?
Go to www.carefirstanswers.com or call 888-451-6562. Please be sure to have the engagement number and activation code included in your letter. Individuals calling internationally may call 479-573-7373. You may enroll any time prior to October 31, 2015.

I have not yet received a letter. How can I access the protections being offered?
Only users registered online with CareFirst prior to June 20, 2014 are affected. Please note, the link to enroll in protections at www.carefirstanswers.com will not be available to members or brokers affected until they receive a letter with a personalized code.

What else should I do to protect my personal or business information?
If you receive a letter from CareFirst, be sure to activate the credit monitoring and identity theft protection or business credit monitoring being offered.

You should be aware that you may receive scam and phishing emails claiming to be from CareFirst in relation to this attack. If you receive an email claiming to be related to this attack you should take the following steps:

DO NOT reply to the email or reach out to the sender/s in any way.
DO NOT enter any information on any website that may open, if you have clicked on a link in the email.
DO NOT open any attachments included in the email.

You can learn more about protecting yourself online at:
www.staysafeonline.org

Why did CareFirst announce this attack on May 20 if it was discovered earlier?
We first learned of the attack on April 21, 2015 when the review was partially complete. This was when Mandiant discovered that a cyberattack occurred and likely resulted in a limited unauthorized access to a database. It was necessary to complete the comprehensive forensic information technology (IT) review of all of CareFirst's systems to understand the nature of the attack, the information potentially accessed, and the members who were affected. In addition, the comprehensive review was necessary to determine that there was no evidence of any other prior or ongoing attacks and to take steps necessary to ensure the integrity of the system.

Does this attack affect members of other Blue Cross Blue Shield plans?
No. The information potentially accessed included only those CareFirst members who created online accounts on www.carefirst.com prior to July 2014.