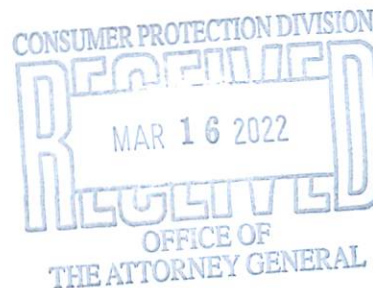


P. Todd Cioni, Vice President  
Chief Compliance, Ethics & Privacy Officer

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



March 10, 2022

The Honorable Brian E. Frosh  
Attorney General, State of Maryland  
Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202  
Email: idtheft@oag.state.md.us

Dear Attorney General Frosh:

This letter is to provide you with information regarding an unauthorized access or use of personal information involving 44 Maryland residents ("impacted individuals"). CareFirst Inc. is providing you with information regarding the unauthorized access or use as required by Maryland Code §14-3501 et seq.

On September 29, 2021, CareFirst identified suspicious login activity regarding our Member Portal. To protect our systems and data, CareFirst took our Member Portal offline to allow for investigation of the activity. It was discovered that CareFirst's Member Portal was being subjected to a Credential Stuffing attack.

### What is a Credential Stuffing Attack?

A 2020 security study found more than 15 billion username and password credentials available on the dark web.<sup>1</sup> These credentials are published by threat actors from more than 100,000 website breaches. In a Credential Stuffing attack, the threat actor utilizes a network of what can be thousands of computers to use these leaked credentials in an attempt to find valid combinations in the target website. This is what was observed on our Member Portal.

It is important to note that when this results in successful access to an account, it is done utilizing the individuals' login ID and password, making it difficult to differentiate between a member's appropriate access or an unauthorized third party.

After extensive analysis of logs and other forensic data by both internal CareFirst analysts and CareFirst's incident response firm, it was determined that the objective of the attack, based on repeated log patterns, was to redeem reward points through Sharecare (our Wellness program vendor). We believe this was attempted using credentials likely obtained from the dark web. Using data forensics, we determined that a foreign attacker utilized a network of several thousand computers in this attack.

On January 28, 2022, CareFirst confirmed that the event impacted a total of 44 Maryland residents as follows:

- Rewards points for 36 members were fraudulently redeemed - our records indicate that no other PHI was accessed. Social Security Numbers or credit card information are not stored on the Member Portal or Sharecare site. The rewards points were redeemed as eGift cards redirected to a third party's email

<sup>1</sup> Digital Shadows, From Exposure to Takeover: The 15 billion stolen credentials allowing account takeover (2020), <https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover>

...the ... of the ...  
...the ... of the ...  
...the ... of the ...  
...the ... of the ...  
...the ... of the ...  
...the ... of the ...  
...the ... of the ...  
...the ... of the ...  
...the ... of the ...  
...the ... of the ...

10-10-10

address. For impacted members, the erroneously redeemed points will be restored. We provided members with a notification including offering credit monitoring. A sample of the letter is attached.

- For eight (8) members our records indicate a successful login and potential access to member's data, which included PHI. No credit card, bank account information or Social Security Numbers are stored in the Member Portal. The information that could have been accessed includes member name, address, member number, explanation of benefits and claims information (excluding, diagnosis code and CPT code). No rewards points were redeemed. We provided members with a notification including offer credit monitoring. A sample of the letter is attached.

#### **What actions did CareFirst undertake?**

CareFirst took actions to block this attack using the specific characteristics of the attack and implemented a number of additional security controls which we were able to confirm stopped the attack. To help mitigate the risk of future attacks, CareFirst has implemented multi-factor authentication

*requiring a member to enter a one-time code delivered to their email or mobile device to log into their account.* CareFirst also engaged its cybersecurity incident response firm and federal law enforcement. With the consent of our cybersecurity incident response firm and in consultation with federal law enforcement, we re-enabled the Member Portal access on October 1, 2021.

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

Sincerely,



P. Todd Cioni