FENWICK & WEST LLP

SILICON VALLEY CENTER 801 CALIFORNIA STREET MOUNTAIN VIEW, CA 94041

TEL 650.988.8500 FAX 650.938.5200 WWW.FENWICK.COM

June 13, 2019

TYLER NEWBY

EMAIL TNEWBY@FENWICK.COM

Direct Dial (415) 875-2495

VIA OVERNIGHT MAIL

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of Data Breach

Dear Attorney General MacDonald:

This firm represents my client, Castlight Health ("Castlight" or the "Company"), and I write on its behalf, pursuant to New Hampshire Rev. Stat. §§ 359-C19-C21, to inform you that a data breach has occurred. On April 25, 2019, Castlight determined that an unknown bad actor attempted to impersonate Castlight users to gain access to approximately 71 user accounts on Castlight's application. Based on its investigation, the Company does not believe that the bad actor obtained login credentials through a compromise of its system. Instead, the attempted access was conducted by a bad actor who appeared to be using email and password combinations from other data breaches that are available for illicit download on the internet.

The information that may have been compromised as a result of the unauthorized access includes the personal information and unsecured health information that is displayed in a user's Castlight account. This information may include first and last name, address, date of birth, email address, phone number, health information and health insurance information.

Pursuant to New Hampshire Rev. Stat. §§ 359-C19-C21, notification was sent to the 1 affected New Hampshire resident in substantially the form attached hereto on June 10, 2019.

Please do not hesitate to contact Jennifer Chaloemtiarana (jchaloemtiarana@castlighthealth.com) or Annie Sun (asun@castlighthealth.com) with any questions, or if you need additional information.

Sincerely,

FENWICK & WEST LLP

/s/ Tyler Newby

Tyler Newby

cc: Jennifer Chaloemtiarana, Esq.
Annie Sun, Esq.

[Date]
[Affected Individual or Representative Name]
[Address Line 1]
[Address Line 2]
[City, State Zip Code]

Re: Notice of April 2019 Data Breach

Dear [AFFECTED INDIVIDUAL]:

You may have recently received an email from us regarding suspicious activity connected to your Castlight account and we are writing to provide additional information about the incident.

What Happened?

On April 25, 2019, we detected an unknown individual attempting to use your Castlight login information to gain access to your Castlight account. We do not believe that the unknown individual obtained your login information through a compromise of our systems. Instead, we believe the individual used email and password combinations, likely obtained from other data breaches available for illicit download from the internet, to access your account. This is commonly known as "credential stuffing," and individuals who use the same email and password combination across multiple accounts are most at risk of such attacks.

What Information Was Involved?

Information which may have been compromised as a result of the unauthorized access includes personal and protected health information. This includes information displayed to you, about you and your dependent(s), if applicable, when you log into your Castlight account. This may include: first and last name, address, date of birth, email address, phone number, health information, and health insurance information.

What We Are Doing?

Castlight values your privacy and takes this incident very seriously. We have taken the following steps to protect your information and help prevent this from happening again:

- We froze your account access immediately. Because of this action and consistent with our previous email you may have received, you will not be able to access your Castlight account until you contact our support team to verify your identity and reset your password. If you have not already done this, please contact the Castlight Support Center at 1-888-722-0483, weekdays 8 a.m. to 9 p.m. ET;
- Increased the sensitivity of security monitoring systems that block automated login attempts;

- Prevented certain types of suspicious international login attempts by blocking the internet protocol (IP) addresses behind these suspicious attempts; and
- Implemented security technology to proactively identify user accounts that recycle the same user name and password combinations available on the internet.

We believe we have taken appropriate steps to stop the suspicious activity.

What You Can Do.

We want to make sure you are informed of this incident to help protect your information. You should update your login information if you use the same email and password combination from your Castlight account across various websites or applications. We also recommend that you stay vigilant to incidents of fraud and identity theft by, among other things, reviewing account statements and monitoring free credit reports. We have provided more information on measures you may want to take to protect your identity in *Attachment A*.

Other Important Information.

Maintaining the integrity of your information is extremely important to us. We sincerely apologize for any inconvenience this incident may have caused you.

For More Information.

If you have any questions or would like to obtain additional information, please contact the Castlight Support Center at 1-888-722-0483, weekdays 8 a.m. to 9 p.m. ET or email privacy@castlighthealth.com.

Sincerely,

Jennifer Chaloemtiarana
General Counsel and Chief Privacy Officer
Castlight Health, Inc.

ATTACHMENT A: PROTECTIVE MEASURES YOU CAN TAKE

The following resources are available to help you protect your personal information and monitor your accounts for suspicious activity.

Free Credit Report

You are entitled to receive your credit report from each of the three national credit reporting agencies below once per year, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com, by calling 877-322-8228 or by mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

When you receive your credit report(s), please review them carefully. Look for any accounts you did not open, requests for your credit report from anyone that you did not apply for credit with, or inaccuracies regarding your personal identifying information, such as your home address or social security number. If you see anything you do not understand or that is incorrect, contact the appropriate credit reporting agency using the contact information on the credit report or listed below and ask them to have information relating to fraudulent transactions deleted:

Experian	**Equifax**	**TransUnion**
P.O. Box 9554	P.O. Box 740256	P.O. Box 6790
Allen, TX 75013	Atlanta, GA 30374	Fullerton, CA 92834
www.experian.com	www.equifax.com	www.transunion.com
888-397-3742	800-525-6285	800-680-7289

Flagging Your Credit Report

To further protect you from the possibility of identity theft, each of the national credit reporting agencies provides the ability to place a fraud alert or security freeze on your credit files. A fraud alert notifies any creditors that access your credit report that you may be the victim of fraud and encourages them to take additional steps to protect you from fraud. Placing a fraud alert is as simple as calling the numbers above for each or any of the credit reporting agencies and requesting that a fraud alert be placed on your credit file.

Whether or not you find any signs of fraud on your credit reports, we recommend that you closely monitor your banking and credit account statements for suspicious activity on your existing accounts. You should also remain vigilant over the next two years by attentively monitoring your credit reports and account statements for indications of fraud and/or theft, including identity theft.

Additional Resources

You can also obtain information from the Federal Trade Commission (www.ftc.gov) about taking steps to avoid identity theft, including fraud alerts and security freezes at: http://www.consumer.ftc.gov/features/feature-0014-identity-theft. You may also file a consumer complaint if you have been the victim of fraud, identity theft, or other unfair or deceptive

business practices by calling the FTC's Consumer Response Center at 1-877-FTC-HELP (1-877-382-4357).

For *Maryland* residents, you may also contact your Attorney General's office to learn about how you can take to avoid identity theft by calling 410-576-6491, writing Office of the Attorney General, Attn: Security Breach Notification, 200 St. Paul Place, Baltimore, MD 21202, or by visiting www.marylandattorneygeneral.gov/Pages/IdentityTheft/databreech.aspx.

For *Minnesota* residents, upon completion of our investigation of this incident, you have the right to receive a report on the facts and details of the investigation. If you would like a copy of the report, please contact Castlight Support Center at 1-888-722-0483, weekdays 8 a.m. to 9 p.m. ET or email privacy@castlighthealth.com to request delivery of the report via mail or email.

For *Missouri* residents, it is recommended that you report identity fraud to law enforcement, which includes the FTC and your Attorney General's Consumer Protection Hotline at 1-800-392-8222.

For *North Carolina* residents, you may also contact your Attorney General's consumer hotline at 1-877-566-7226 or visit www.ncdoj.gov for more information.