

2020

## Blackbaud's Breach: 3.4 Million Patients and Counting...



Dissent Doe

DataBreaches.net

September 13, 2020

- Blackbaud, a software firm that provides cloud-based donor management solutions for fund-raising purposes, experienced a ransomware attack that they discovered on May 7, 2020. On July 16, they notified clients of the attack. We are first beginning to see breach notifications by the clients.
- Based on currently available notifications, DataBreaches.net has tallied more than 3.4 million patients whose records may have been accessed or acquired by the attackers – and that is just for 14 of Blackbaud’s clients for whom we already have numbers involving patients.
- The Blackbaud breach is likely to be the biggest or one of the biggest breaches involving patient information in 2020. But we may never know the total number of patients whose data were caught up in this incident unless Congress or the U.S. Department of Health & Human Services starts demanding answers from Blackbaud, or information is revealed in discovery during any lawsuits.

In May, 2020, Charleston-based [Blackbaud](#) discovered that they had been the victim of a ransomware attack that had begun in February. The software firm, which describes itself as powering social good, found itself with numerous clients to notify – clients such as hospitals and non-profit foundations and organizations who used Blackbaud for fundraising and relationship management solutions.

On July 16, Blackbaud notified clients and posted a [breach disclosure](#) that was somewhat astonishing for both its spin and lack of transparency. The notification did not reveal what type of ransomware was deployed, nor how the attackers had managed to gain a foothold to their systems. Nor did Blackbaud reveal how many people had their personal information stolen (exfiltrated) by the hackers. What they did say was to pat themselves on their back for being able to expel the attackers before they had encrypted everything. They also disclosed that they had paid the ransom in exchange for assurances from the attackers that they would destroy all copies of any data they had exfiltrated and would not misuse it. They said both law enforcement and their consultants told them that they could rely on these criminals’ assurances.



*Law enforcement does not want victims to pay ransom. To dissuade them from paying, they tell them that threat actors cannot be trusted to keep their word and how they may come back and “double-dip” or attack the victim again.*

*Now we are to believe that law enforcement told Blackbaud that it could rely on the word of these threat actors?*

Based on their notifications, at least several entities are now re-evaluating their relationship with Blackbaud and have expressed concern that Blackbaud did not protect the security of data as well as they had expected. Others have expressed frustration at Blackbaud's refusal to answer their questions and provide additional details.

Of special concern to DataBreaches.net, many of these fundraising or relationship management clients not only targeted former patients or grateful patients as potential donors, but the files that they provided to Blackbaud revealed the named potential donors or contacts as current or former patients. For some of these entities, the only information might be their medical record number included in the files held by Blackbaud, but other entities provided more information such as the dates of service and treatment departments visited, or doctors seen.

As of September 13, DataBreaches.net has identified 38 entities whose incident disclosures mention some data type or types related to the named individual being or having been a patient. I expect that there will be many more disclosures in the next weeks or months, as it is somewhat less than 60 days since most clients of Blackbaud were notified.

Not all the entities that we already know about are covered entities under HIPAA, and we do not have numbers for all of the 38 entities that we do know about already.

You can see the list I compiled on the following pages. In some cases, DataBreaches.net has emailed entities to clarify whether any medically related or patient status information was involved at all.



*For the 14 entities who provided numbers, we have a total of **3,430,882** patients whose demographic information and status as patients was revealed, sometimes with additional details about their patient experiences.*

I am not sure whether I will be updating this list, as it is time-consuming, but it seems clear that the Blackbaud incident will rank as one of the largest, if not the largest, incident of 2020 involving patient data.

Any corrections to the list can also be sent to [breaches@databreaches.net](mailto:breaches@databreaches.net).

And if any firm or organization would like to throw some sponsorship at this site to support this site's efforts to shine the light on protecting patient data privacy and security, please contact me at [breaches@databreaches.net](mailto:breaches@databreaches.net).

Table 1. Blackbaud clients whose disclosures indicate patient status may have been accessed by threat actors

Entity	Notification or Media	Number Affected
Adventist Healthcare	<a href="https://www.adventisthealthcare.com/news/2020/informs-patients-affected-by-blackbaud-data-breach/">https://www.adventisthealthcare.com/news/2020/informs-patients-affected-by-blackbaud-data-breach/</a>	
Atrium Health	<a href="https://atriumhealth.org/-/media/chs/files/about-us/blackbaud-substitute-notice.pdf">https://atriumhealth.org/-/media/chs/files/about-us/blackbaud-substitute-notice.pdf</a>	165000
Augusta University (Georgia Health Sciences Foundation)	<a href="https://jagwire.augusta.edu/information-about-blackbaud-security-incident/">https://jagwire.augusta.edu/information-about-blackbaud-security-incident/</a>	
Catholic Health	<a href="https://buffalonews.com/news/local/local-hospitals-disclose-data-breach-blamed-on-national-software-company/article_61c999de-ed1e-11ea-995b-0799a158eae0.html">https://buffalonews.com/news/local/local-hospitals-disclose-data-breach-blamed-on-national-software-company/article_61c999de-ed1e-11ea-995b-0799a158eae0.html</a>	
Children's Minnesota	<a href="https://www.childrensmn.org/2020/09/11/blackbaud-security-incident/">https://www.childrensmn.org/2020/09/11/blackbaud-security-incident/</a>	
Community Medical Centers	<a href="https://www.communitymedical.org/Privacy/Notice-of-Vendor-Data-Security-Incident">https://www.communitymedical.org/Privacy/Notice-of-Vendor-Data-Security-Incident</a>	
Enloe Medical Center	<a href="https://www.enloe.org/media/file/BlackbaudDataPrivacyEvent.pdf">https://www.enloe.org/media/file/BlackbaudDataPrivacyEvent.pdf</a>	
Hebrew Senior Life	<a href="https://www.hebrewseniorlife.org/notice-data-incident">https://www.hebrewseniorlife.org/notice-data-incident</a>	
Holy Cross Health (Trinity Health)	<a href="https://www.holy-cross.com/about-us/ways-to-give/blackbaud-incident">https://www.holy-cross.com/about-us/ways-to-give/blackbaud-incident</a>	
Hydrocephalus Association	<a href="https://oag.ca.gov/system/files/Sample%20Notification%20Letter_6.pdf">https://oag.ca.gov/system/files/Sample%20Notification%20Letter_6.pdf</a>	
Inova Health	<a href="https://www.inova.org/about-inova/blackbaud-notice">https://www.inova.org/about-inova/blackbaud-notice</a>	1045270

LifeFlight Foundation	<a href="https://waldo.villagesoup.com/p/lifeflight-foundation-among-thousands-of-nonprofits-affected-by-software-security-event/1869293">https://waldo.villagesoup.com/p/lifeflight-foundation-among-thousands-of-nonprofits-affected-by-software-security-event/1869293</a>	
Main Line Health	<a href="https://www.mainlinehealth.org/news/2020/08/24/blackbaud">https://www.mainlinehealth.org/news/2020/08/24/blackbaud</a>	60595
Margaret Mary Health Foundation	<a href="https://www.mmhealth.org/wp-content/uploads/Blackbaud-FAQ.pdf">https://www.mmhealth.org/wp-content/uploads/Blackbaud-FAQ.pdf</a>	
Mercy Hospital & Medical Center (Trinity Health)	<a href="https://www.mercy-chicago.org/blackbaud-incident">https://www.mercy-chicago.org/blackbaud-incident</a>	
MercyOne Clinton Medical Center	<a href="https://www.mercyone.org/clinton/giving/blackbaud-incident#information">https://www.mercyone.org/clinton/giving/blackbaud-incident#information</a>	
MultiCare Health System	<a href="https://www.multicare.org/news/multicare-foundation-addresses-security-incident/">https://www.multicare.org/news/multicare-foundation-addresses-security-incident/</a>	179189
Northern Light Health Foundation	<a href="https://northernlighthealth.org/securityevent">https://northernlighthealth.org/securityevent</a>	657392
NorthShore University HealthSystem	<a href="https://www.chicagobusiness.com/health-care/northshore-data-hacked-348000-individuals-exposed">https://www.chicagobusiness.com/health-care/northshore-data-hacked-348000-individuals-exposed</a>	348000
Northwestern Memorial HealthCare	<a href="https://www.nm.org/patients-and-visitors/notice-of-privacy-incident">https://www.nm.org/patients-and-visitors/notice-of-privacy-incident</a>	55983
Nuvance Health	<a href="https://www.poughkeepsiejournal.com/story/news/local/2020/09/11/nuvance-health-announces-third-party-data-breach/3470232001/">https://www.poughkeepsiejournal.com/story/news/local/2020/09/11/nuvance-health-announces-third-party-data-breach/3470232001/</a>	
Piedmont Healthcare	<a href="https://www.piedmont.org/media/file/PHC-Notice-Privacy-Incident.pdf">https://www.piedmont.org/media/file/PHC-Notice-Privacy-Incident.pdf</a>	
Polycystic Kidney Disease Foundation	<a href="https://oag.ca.gov/system/files/PKD%20Foundation%20Data%20Security%20Breach%20Notice%20Letter.pdf">https://oag.ca.gov/system/files/PKD%20Foundation%20Data%20Security%20Breach%20Notice%20Letter.pdf</a>	
Regions Hospital	<a href="https://www.healthpartners.com/hospitals/regions/about/blackbaud/">https://www.healthpartners.com/hospitals/regions/about/blackbaud/</a>	
Richard J. Caron Foundation	<a href="https://www.caron.org/lp/COVID19-message">https://www.caron.org/lp/COVID19-message</a>	22718
Riverside Foundation	<a href="https://www.riversideonline.com/foundation/Blackbaud-Data-Security-Incident.cfm">https://www.riversideonline.com/foundation/Blackbaud-Data-Security-Incident.cfm</a>	
Roper St. Francis	<a href="https://www.live5news.com/2020/09/08/roopr-st-francis-sends-data-security-breach-warning-almost-k-patients/">https://www.live5news.com/2020/09/08/roopr-st-francis-sends-data-security-breach-warning-almost-k-patients/</a>	93000
Saint Luke's Foundation	<a href="https://www.saintlukeskc.org/saint-lukes-foundation/security-incident">https://www.saintlukeskc.org/saint-lukes-foundation/security-incident</a>	360212
SCL Health - St. Mary's	<a href="https://www.sclhealth.org/locations/st-marys-medical-center/about/notice-to-patients-blackbaud-security-incident/">https://www.sclhealth.org/locations/st-marys-medical-center/about/notice-to-patients-blackbaud-security-incident/</a>	

Skyland Trail	<a href="https://www.skylandtrail.org/news/blackbaud-data-security-breach/">https://www.skylandtrail.org/news/blackbaud-data-security-breach/</a>	
Spectrum Health	<a href="https://woodradio.iheart.com/content/2020-09-02-nationwide-data-breach-impacts-spectrum-health-foundation/">https://woodradio.iheart.com/content/2020-09-02-nationwide-data-breach-impacts-spectrum-health-foundation/</a>	52500
St. Mary's Health System (Covenant Health)	<a href="https://www.stmarysmaine.com/news/news-story?news=16">https://www.stmarysmaine.com/news/news-story?news=16</a>	
The Guthrie Clinic	<a href="https://www.guthrie.org/notice-our-patients-blackbaud-data-security-incident">https://www.guthrie.org/notice-our-patients-blackbaud-data-security-incident</a>	92064
University of Florida Health	<a href="https://ufhealth.org/news/2020/information-data-security-incident">https://ufhealth.org/news/2020/information-data-security-incident</a>	135959
University of Kentucky HealthCare	<a href="https://uknow.uky.edu/uk-healthcare/blackbaud-data-security-incident-affects-uk-healthcare">https://uknow.uky.edu/uk-healthcare/blackbaud-data-security-incident-affects-uk-healthcare</a>	163000
UT Health San Antonio	<a href="https://makelivesbetter.uthscsa.edu/blackbaud">https://makelivesbetter.uthscsa.edu/blackbaud</a>	
Virginia Mason	<a href="https://www.virginiamason.org/workfiles/VM%20_Substitute_Notice_9.4.20.pdf">https://www.virginiamason.org/workfiles/VM%20_Substitute_Notice_9.4.20.pdf</a>	
Waterbury Hospital	<a href="https://www.waterburyhospital.org/notice-of-a-privacy-incident/">https://www.waterburyhospital.org/notice-of-a-privacy-incident/</a>	

Subtotal as of September 13, 2020: 3,430,882