



Tennessee and North Mississippi

Elise Gibbons
Planned Parenthood of Tennessee and North Mississippi
2430 Poplar Avenue, Suite 100
Memphis, TN 38112

August 11, 2020

Office of the Attorney General
1125 Washington St SE
Olympia, WA 98504
SecurityBreach@atg.wa.gov

To Whom It May Concern:

I am writing on behalf of Planned Parenthood of Tennessee and North Mississippi (PPTNM) to inform you of a security incident experienced by Blackbaud, a vendor whose fundraising and donor engagement software is used by nonprofit organizations nationwide. Blackbaud identified a ransomware cyberattack affecting certain information stored on its servers. They responded to and contained the situation with the aid of law enforcement and cybersecurity and forensics experts. The attack began on February 7, 2020, and was stopped by May 20, 2020. Blackbaud informed us that some PPTNM data may have been impacted by this incident.

Unfortunately, the criminal was able to remove a portion of the data stored on the company's servers, which included some information about donors, such as street addresses, phone numbers, email addresses, and birthdate. Data such as social security numbers, credit card data, or bank account information was not affected. Blackbaud has obtained confirmation that the stolen data was destroyed and has no reason to believe the information was or will be misused or made publicly available.

Blackbaud informed us of the security incident on July 16. PPTNM provided notice to state residents who may have been affected by the incident beginning on August 10. 12 Washington residents were affected by this incident.

PPTNM's service agreements with Blackbaud require them to employ stringent security measures to protect the data of our supporters, and this breach has violated those agreements. We are conducting a close investigation to fully understand what measures Blackbaud is taking to remedy this situation and prevent further incidents.

A sample copy of the notice sent to individuals is attached. Please feel free to contact me if you have any questions or require additional information.

Sincerely,

Elise Gibbons
Senior Stewardship & Operations Manager
Pronouns: She, Her, Hers

Planned Parenthood of Tennessee and North Mississippi
Main Line: 866-711-1717
www.pptnm.org

August 10, 2020

Dear 

We're reaching out today to let you know that Planned Parenthood of Tennessee and North Mississippi (PPTNM) was recently notified of a data breach at Blackbaud, a vendor whose fundraising and donor engagement software is used by nonprofit organizations nationwide. Blackbaud identified a ransomware cyberattack affecting certain information stored on its servers. They responded to and contained the situation with the aid of law enforcement and cybersecurity and forensics experts. The attack began on February 7, 2020, and was stopped by May 20, 2020.

Unfortunately, the criminal was able to remove a portion of the data stored on the company's servers, which included some information about you and other donors, such as street addresses, phone numbers, email addresses, and birth dates. **Sensitive data — such as social security numbers, credit card data, or bank account information — was not affected.** Blackbaud has obtained confirmation that the stolen data was destroyed and has no reason to believe the information was or will be misused or made publicly available.

Blackbaud discovered and contained this attack in May of this year. Unfortunately, the company did not notify its clients — including PPTNM — until mid-July. To say the least, we find this delay unacceptable, and we are extremely dissatisfied with Blackbaud's lack of transparency around this incident. We are deeply committed to the privacy of our supporters and have been working diligently since we were notified to obtain substantial, accurate information to share with you.

PPTNM's service agreements with Blackbaud require them to employ stringent security measures to protect the data of our supporters, and this breach has violated those agreements. We are conducting a close investigation to fully understand what measures Blackbaud is taking to remedy this situation and prevent further incidents. Blackbaud's statement on this attack can be found on their website at <https://www.blackbaud.com/securityincident>.

While we are confident that no sensitive financial information was exposed in the Blackbaud breach, it is always good practice to monitor your credit to guard against identity theft. For your convenience, I have included, below my signature, contact information for the three major credit reporting agencies.

Thank you, as always, for your support. If you have any further questions about this incident, please don't hesitate to reach out to us at alewis@pptnm.org or 866-711-1717.

Best,



Aimee Lewis
Vice President of External Affairs
PPTNM
alewis@pptnm.org
866-711-1717

Experian

888-397-3742
Experian Security Freeze
PO Box 9554
Allen, TX 75013

Equifax

888-298-0045
Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348-5788

TransUnion

888-909-8872
TransUnion LLC
PO Box 2000
Chester, PA 19016