Planned Parenthood of Northern New England

FUNDRAISING DEPARTMENTS
784 Hercules Dr., Suite 110, Colchester, VT 05446 • 800-287-8188
443 Congress St., 3rd Floor, Portland, ME 04101 • 844-245-9388
18 Low Ave., Concord, NH 03301 • 844-250-7957

Via UPS

November 2, 2020

Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Dear Sir or Madam:

This letter is to provide the Office of the New Hampshire Attorney General with notice of a breach.

Notification of Breach: On July 16, 2020, Planned Parenthood of Northern New England ("PPNNE") received notice from one its vendors, Blackbaud, Inc. ("Blackbaud"), informing PPNNE of a ransomware attack involving some of PPNNE's data.

Date of Breach: According to Blackbaud, the attack began on February 7, 2020, and was stopped by May 20, 2020. Blackbaud discovered the ransomware attack in May 2020 (the "Blackbaud Security Breach")

Description of Breach: According to Blackbaud, a cybercriminal removed of a copy of a subset of data from Blackbaud's self-hosted environment, and the removed data included a copy of the backup of PPNNE's Blackbaud Financial Edge NXT and Blackbaud Raiser's Edge NXT (the "PPNNE Removed Data"). Blackbaud informed PPNNE that the PPNNE Removed Data "did not contain any credit card information. Further, the cybercriminal did not gain access to bank account information, usernames, passwords, or social security numbers stored in your database because they were encrypted." Blackbaud paid the cybercriminal's demand with confirmation that the removed file had been destroyed. According to Blackbaud:

> After discovering the attempted attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system….
> Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misuses; or will be disseminated or otherwise made available publicly….
> We have hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

PPNNE's Investigation: Despite Blackbaud's assurances, PPNNE conducted its own investigation. PPNNE engaged a consultant to investigate and assess its notification requirements. From the consultant's investigation, PPNNE learned that some records in the PPNNE removed file included attachments containing copies of checks that, although encrypted when transmitted to Blackbaud, were not encrypted when stored by Blackbaud. The consultant concluded that there is only a low probability that the impermissible acquisition, access, use or

disclosure of the removed data compromises the privacy and security of the removed data. Because some state laws require notification even when only a low probability exists, PPNNE is providing this notification, and PPNNE has provide consumer notification to the impacted individuals.

PPNNE is offering impacted consumers identity theft protection services as follows: 1 year of complimentary membership in Experian's IdentityWorks, which includes tri-bureau credit reporting, daily credit reports, identity theft insurance, and identity restoration

Consumer Notice: There were two (2) New Hampshire residents whose PII was in the removed files. PPNNE has provided each of them with notice, and a copy of the redacted communication is attached.

Yours truly,

Planned Parenthood of Northern New England

Meagan Gallagher
President & CEO

Attachment (redacted consumer notification)

Planned Parenthood of Northern New England

FUNDRAISING DEPARTMENTS
784 Hercules Dr., Suite 110, Colchester, VT 05446 • 800-287-8188
443 Congress St., 3rd Floor, Portland, ME 04101 • 844-245-9388
18 Low Ave., Concord, NH 03301 • 844-250-7957

Via UPS

November 2, 2020

[redacted]

Re: Notice of Data Breach – New Hampshire Residents

Dear [redacted]:

I am writing to let you know that one of Planned Parenthood of Northern New England's (PPNNE) software vendors, Blackbaud, Inc., experienced a security incident that involved some of your personally identifiable information ("PII"). At this time, we have no reason to believe that your PII has been used inappropriately. We take the protection and proper use of your information very seriously. We want to let you know what we know about this incident, what we are doing about it, and what you can do to protect your information.

Blackbaud's Security Incident. Blackbaud is a leading provider of fundraising and donor software, used by thousands of non-profits throughout the United States and internationally, including PPNNE. On July 16, 2020, Blackbaud informed us that information from PPNNE's Financial Edge NXT and Raiser's Edge NXT databases had been breached through a ransomware attack on Blackbaud's servers and that the data may have been accessed between February 7 and May 20, 2020. Blackbaud paid the cybercriminal's demand with confirmation that the stolen data had been destroyed.

What information was involved? The stolen data contained certain information that we had provided to Blackbaud through encrypted transmission but that was not encrypted when stored by Blackbaud. Your [redacted] were included in the stolen data. It also is possible that your [redacted] were included in the stolen data. No other personally identifiable information was included.

What PPNNE is doing. Once we learned of Blackbaud's security incident, we conducted our own investigation. Blackbaud has informed us that, as part of its ongoing efforts to help prevent something like this from happening in the future, it has implemented changes that will protect your data from any subsequent incidents. Blackbaud has confirmed through testing by multiple privacy and cybersecurity third parties that its fix withstands all known attack tactics. You can find Blackbaud's summary information on its website located at www.blackbaud.com/securityincident.

Blackbaud has informed us it has worked with law enforcement to investigate the security incident, and that there is currently no evidence that your information has been or will be misused, but we know this situation can cause concern and worry. That is why PPNNE is offering to purchase a one-year membership of Experian's® IdentityWorks℠ for you. This product is designed to help detect possible misuse of your personal information and provide you with identity protection services focused on immediate identification and resolution of identity theft. **For more information on identity theft prevention and IdentityWorks, including**

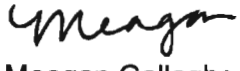
instructions on how to activate your complimentary one-year membership, please see the information provided at the end of this letter.

What You Can Do. We hope you will accept our offer to enroll in Experian's IdentityWorks for one year at no cost to you. Additionally, we recommend that you are vigilant regarding any suspicious activity, including questionable emails. If you observe any suspicious activity, please promptly report it to us as well as to the proper law enforcement authorities. We include at the end of this letter a list of additional steps you can take to help protect yourself.

PPNNE's Commitment to You. I am distressed to know that any information about you may have been accessed without permission. We hold dear to our commitment as a trusted, confidential health care provider. That ethic extends to the partnership we have with you, our supporter. Your privacy and the protection of your information is of the utmost importance to us.

If you have any questions about this matter, please do not hesitate to be in touch with Jennifer Long, Director of Development Operations, at 802-448-9735.

Sincerely,



Meagan Gallagher
President & CEO

Identity Theft Protection - Experian's® IdentityWorks℠

To help protect your identity, we are offering to purchase for your a one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft.

To Activate IdentityWorks:

1. ENROLL by **January 20, 2021** (your code will not work after this date)
2. VISIT the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
3. PROVIDE your Activation Code: [redacted]

If you have any questions about the Experian IdentityWorks product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877.890.9332** by **January 20, 2021**. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

Additional Information About Your Complimentary 12-Month Experian IdentityWorks Membership:

- You do not need a credit card to enroll in Experian IdentityWorks.
- You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:
    - **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
    - **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for indicators of fraud.
    - **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
    - **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
    - **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling .
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Steps You Can Take

As a precautionary measure, we recommend that you continue to be vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should be aware of any other suspicious activity, including questionable emails. If you

observe any suspicious activity, please promptly report it to the proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC") (see below for contact information).

1. **Review your bank, credit card, and debit card account statements** over the next twelve to twenty-four months and immediately report any suspicious activity to your bank or credit union.

2. **Monitor your credit reports** with the major credit reporting agencies.
   a. Equifax: 1-800-685-1111, P.O. Box 740241, Atlanta, GA 30374-0241, www.equifax.com
   b. Experian TransUnion: 1-888-397-3742, P.O. Box 2104, Allen, TX 75013, www.experian.com
   c. TransUnion: 1-800-916-8800, P.O. Box 2000, Chester, PA 19022, www.transunion.com

   Under some state laws (including Vermont), you may be entitled to a free copy of your credit report from those agencies every twelve months. Please contact the Attorney General's Office in your state.

   Call the credit reporting agency at the telephone number on the report if you find:
   - Accounts you did not open
   - Inquiries from creditors that you did not initiate
   - Inaccurate personal information, such as home address and Social Security number

3. If you do find suspicious activity on your credit reports or other account statements, **call your local police or sheriff's office** and **file a report of identity theft**. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records, and also to access some services that are free to identity theft victims.

4. If you find suspicious activity on your credit reports or on your other account statements, **consider placing a fraud alert** on your credit files so creditors will contact you before opening new accounts. Call any one of the three credit reporting agencies at the numbers below to place fraud alerts with all of the agencies.
   a. Equifax: 888-766-0008
   b. Experian: 888-397-3742
   c. TransUnion: 800-680-7289

5. You also may get information about **security freezes** by contacting the credit bureaus at the following addresses:
   a. Equifax: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
   b. Experian: http://www.experian.com/consumer/security_freeze.html
   c. TransUnion: http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/securityFreeze.page

   Vermont Residents who do not have internet access but would like to learn more about how to place a security freeze on their credit report can contact the Vermont

Attorney General's Office at 802-656-3183 or 800-649-2424 (toll free in Vermont only).

6. Even if you do not find suspicious activity on your credit report or your other account statements, it is important that you **check your credit report** for the next two years. Just call one of the numbers in section 2 above to order your reports or to keep a fraud alert in place.

7. You may wish to review the tips provided by **the FTC** on fraud alerts, security/credit freezes, and steps you can take to avoid identity theft. For more information and to contact the FTC:
    a. Visit www.ftc.gov/idtheft
    b. Call 1-877-ID-THEFT (1-877-438-4338)
    c. Write to the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580

8. Individuals interacting with credit reporting agencies have rights under **the Fair Credit Reporting Act**. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pgf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.