

## Appendix

This notification is being submitted by PeaceHealth, on behalf of its affiliated charitable foundations – Ketchikan Medical Center Foundation, St. Joseph Medical Center Foundation, San Juan Island Community Foundation, St. John Medical Center Foundation, Southwest Medical Center Foundation, Sacred Heart Medical Center Foundation, Cottage Grove Community Medical Center Foundation, Whatcom Hospice Foundation, and Peace Harbor Medical Center Foundation (the “Foundations”) – regarding a data security incident that occurred at one of its vendors, Blackbaud, Inc. (“Blackbaud”).

Blackbaud is a third-party vendor that provides cloud-based and data solution services relating to the fundraising activities conducted by the Foundations. Blackbaud notified PeaceHealth that an unauthorized individual gained access to the Blackbaud systems between February 7, 2020 and May 20, 2020. Blackbaud further advised that the unauthorized individual acquired backup copies of databases used by its customers, including a backup of the database the Foundations use for fundraising purposes.

After learning about the incident, PeaceHealth immediately took steps to understand the extent of the incident and the data involved. PeaceHealth underwent extended efforts to obtain a copy of the backup database that was acquired from Blackbaud. PeaceHealth received a copy of the backup on August 20, 2020 and worked diligently to restore the backup and review the database to determine what information it contained.

On November 2, 2020, PeaceHealth’s investigation and review of the database involved in the incident determined that it contained some information belonging to two (2) Maine residents including names and bank names, accounts numbers and routing numbers.

PeaceHealth mailed notification letters to the Maine residents on December 16, 2020, in accordance with Me. Rev. Stat. Tit. 10, §1348.<sup>1</sup> A copy of the notification letter is enclosed. To help prevent something like this from happening again, PeaceHealth is reviewing its relationship with Blackbaud and evaluating Blackbaud’s security safeguards.

---

<sup>1</sup> This report is not, and does not constitute, a waiver of PeaceHealth’s objection that Maine lacks personal jurisdiction over PeaceHealth regarding any claims related to this data security incident.



<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

The PeaceHealth affiliated foundations – Ketchikan Medical Center Foundation, St. Joseph Medical Center Foundation, San Juan Island Community Foundation, St. John Medical Center Foundation, Southwest Medical Center Foundation, Sacred Heart Medical Center Foundation, Cottage Grove Community Medical Center Foundation, Whatcom Hospice Foundation, and Peace Harbor Medical Center Foundation (the “Foundations”) – are committed to protecting the security and privacy of our donors, and all the individuals who support our Mission. Regrettably, we are writing to notify you of a recent incident that occurred at one of our vendors, Blackbaud, Inc. (“Blackbaud”), that may have involved some of your information.

**What Happened?**

Blackbaud is a third-party vendor that provides cloud-based and data solution services relating to the fundraising activities of the Foundations, as well as to many other organizations across the country. Blackbaud informed us it had discovered that an unauthorized individual gained access to its systems between February 7, 2020 and May 20, 2020. Blackbaud further advised that the unauthorized individual acquired backup copies of databases used by its customers, including a backup of the database that manages our donor information.

After learning about the incident, we immediately took steps to understand the extent of the incident and the data involved. We underwent extended efforts to obtain a copy of the backup database that was acquired from Blackbaud, and once we received it, we worked diligently to restore the backup and review the database to determine what information it contained.

**What Information Was Involved:**

On November 2, 2020, after a thorough investigation and review of the database, we determined that it contained some of your information, including your name, bank account number, bank name, and routing number.

**What You Can Do:**

Though we are not aware at this time of any misuse of information involved in the incident, out of an abundance of caution, we remind you to remain vigilant to the possibility of fraud by reviewing your financial statements for any unauthorized activity. You should immediately report any unauthorized activity to your financial institution. You may also review the following pages for more information about steps you can take in response to the incident.

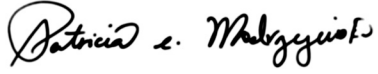
**What We Are Doing:**

We are notifying you of this incident because we take the privacy of your information very seriously. To help prevent something like this from happening again, we are reviewing our relationship with Blackbaud and evaluating its security safeguards.

**For More Information:**

We sincerely regret any concern or inconvenience this incident may cause you. Thank you for being a part of the PeaceHealth family. We hope that you and your loved ones stay safe as we enter this holiday season. Should you have any questions or concerns, please contact [1-800-424-2424](tel:1-800-424-2424), Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,



Patricia Modrzejewski  
Interim System Vice President/Chief Development Officer  
PeaceHealth



Tarra Carey  
System Privacy Officer  
PeaceHealth

## ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

### Fraud Alerts and Credit or Security Freezes:

**Fraud Alerts:** There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

**Credit or Security Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

*How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

**Additional information for residents of the following states:**

**North Carolina:** You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)