



August 14, 2020

Hunter O. Ferguson  
600 University Street, Suite 3600  
Seattle, WA 98101  
D. 206.386.7514  
hunter.ferguson@stoel.com

**VIA EMAIL SECURITYBREACH@ATG.WA.GOV**

Attorney General Bob Ferguson  
Office of the Attorney General  
1125 Washington Street SE  
PO Box 40100  
Olympia, WA 98504-0100

**Re: Notice of Data Security Incident**

Dear Attorney General Ferguson:

We are writing on behalf of our client, Portland Community College Foundation (“**PCC Foundation**”) to notify you of a security incident involving a service provider engaged by PCC Foundation – Blackbaud, Inc. (“**Blackbaud**”) – that involved the disclosure of personal information of Washington residents requiring notice under RCW 19.255.010(5), namely individuals’ names and dates of birth.

1. Nature of the Incident

As you are likely familiar, in light of the publicity of the Blackbaud incident and the notices that your office has already received about the underlying incident, Blackbaud is one of the largest donor management software companies serving non-profits, including the PCC Foundation. Blackbaud notified PCC Foundation on July 16, 2020 that it experienced a data breach between February 7, 2020 and May 20, 2020. This breach affected numerous non-profits like the PCC Foundation, nationally and internationally. As part of the breach, the cybercriminal accessed or might have been able to access a backup file (the “**accessed file**”) containing personal information of Washington residents that PCC Foundation had uploaded to the Blackbaud service.

2. Number of Affected Washington Residents and Types of Compromised Personal Information

After receiving notice of the incident, PCC Foundation investigated what information had been supplied to Blackbaud for processing and PCC Foundation determined that the accessed file included personal information of 17,908 Washington residents. The personal information

involved included the Washington resident's names, their relationship with the PCC Foundation, past donations, and demographic data, such as dates of birth and addresses. Additionally, the file contained financial account numbers and routing numbers for seven Washington residents who had made donations to PCC Foundation using paper checks.

Blackbaud informed PCC Foundation that it engaged forensic experts and law enforcement to assist in the investigation and containment of the breach. Blackbaud also informed PCC Foundation that it believes the cybercriminal destroyed the personal information and that Blackbaud has no reason to believe that the data will be misused further or that the cybercriminal shared the data before destroying it.

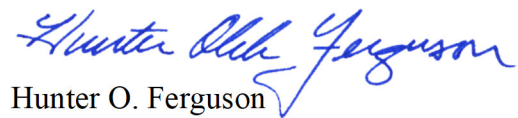
3. Actions PCC Is Taking

PCC Foundation, in coordination with the Portland Community College, sent on August 12, 2020, the enclosed notices of the incident to all Washington residents whose personal information was involved, both through email and U.S. Mail. This notice explains what happened in the incident, what personal information was involved, what further steps PCC Foundation took in response to the incident, what individuals can do to protect their information. PCCC Foundation has sent this same notice to non-Washington residents whose information was involved as well. For individuals whose financial account information was involved on paper checks, PCCC Foundation is offering complimentary credit monitoring and identity restoration services.

Although the breach involved Blackbaud's network, not the networks of PCC Foundation, PCC is taking this opportunity to evaluate security protocols and reinforce staff education about security.

For further information or if you have any questions regarding this notice, please contact me at 206.386.7514 or by email at [hunter.ferguson@stoel.com.com](mailto:hunter.ferguson@stoel.com.com)

Very truly yours,

  
Hunter O. Ferguson

Enclosure

---

**Data incident notification**

1 message

---

**Portland Community College Foundation** <pccfoundation@pcc.edu>

Thu, Aug 13, 2020 at 3:02 PM

Reply-To: pccfoundation@pcc.edu

To: "Christina J. Kline" &lt;christina.kline@pcc.edu&gt;



To Our Donors and Alumni:

We are writing to inform you of a recent cybersecurity incident that may have involved some of your personal information.

Earlier this year, criminals engineered a "ransomware attack" against Blackbaud – one of the largest software service providers that supports non-profits, including PCC Foundation. During this incident, criminals gained access to Blackbaud's systems and made many of its data files unusable. Fortunately, your financial account and credit/debit card information were not accessible in this incident, but there is a possibility that other information – such as names, contact information, and birthdays – was accessible. **Please click [here](#) to learn more and what you can do to protect your information.**

**Our network and systems were not affected by this incident, and we have not received any indication that any information regarding our friends, alumni or donors has been misused or was even actually accessed in the incident.** Nevertheless, out of an abundance of caution and in the interest of transparency, we are notifying you. To comply with applicable laws, we are also mailing this notice to individuals who live in North Dakota and Washington, using addresses we have on file.

We apologize for this incident. If you have any questions, please do not hesitate to contact us at [pccfoundation@pcc.edu](mailto:pccfoundation@pcc.edu) or 971-722-4382.

Sincerely,

Ann Prater  
Executive Director  
PCC Foundation

[Privacy Policy](#) | [Unsubscribe](#)

Portland Community College Foundation  
PO Box 19000, Portland, OR 97280-0990



Portland Community College Foundation  
12000 S.W. 49th Ave., Portland, OR 97219  
P.O. Box 19000, Portland, OR 97280-0990  
p. 971-722-4382 • f. 971-722-4960  
[www.pcc.edu/foundation](http://www.pcc.edu/foundation)

August 12, 2020

ADDRESSEE  
ADDRESS1  
ADDRESS2  
CITY, STATE ZIP

Dear SALUTATION,

We are writing to inform you of a cybersecurity incident at one of our service providers that may have involved your personal information. This notice explains what happened, what information of yours might have been affected, and what you can do to protect yourself. We take your privacy seriously and value your trust and ask that you take a moment to review this entire notice<sup>1</sup>. If you have any questions, please contact us.

**WHAT HAPPENED.** The incident occurred at a company known as Blackbaud, which is one of the largest donor management software companies serving non-profits, including the PCC Foundation. We use Blackbaud's services to process donations to the Foundation and manage related donor and alumni records. On July 16, 2020, Blackbaud notified us that it experienced a data breach between February 7 and May 20, 2020.

According to Blackbaud, it suffered a ransomware attack in which a cybercriminal gained access to its computer network and files and prevented Blackbaud from using its data files. Blackbaud informed us that, as part of this incident, the cybercriminal may have been able to access files that contained some of your personal information, although there is not a clear indication that an unauthorized user actually accessed your information. Blackbaud further informed us that the cybercriminal(s) who attacked its systems destroyed the data involved in the incident. Blackbaud has also reported that, based on the results of its investigation and investigations of forensic experts and law enforcement, there are no indications that your information was misused and that any misuse appears to be unlikely.

After Blackbaud notified us, we reviewed our records to confirm what categories of information had been shared with Blackbaud for processing so that we could notify our friends and donors.

**WHAT INFORMATION WAS INVOLVED.** Based on information from Blackbaud, none of your financial account or credit/debit card account information that we collected from you was affected. Blackbaud explained that this information was encrypted, so the cybercriminal was not able to access it. But there is a possibility that files containing the following categories of your personal information were accessed in the incident: name, address, date of birth, donation information (*i.e.*, date(s) and amount(s) of donations), and details about your relationship with the Foundation.

*continued on back*

<sup>1</sup> Residents of North Dakota and Washington may receive a copy of this notice both through email and through U.S. Mail, in line with applicable laws in these states.

**WHAT WE ARE DOING.** We are continuing to monitor reports and gather other information about the incident. The incident did not involve our systems, but we are examining our security and other ways to protect your data, such as evaluating how we collect and store personal information. Although we are not certain that the cybercriminal accessed your information in particular, we are contacting you to explain what happened and to provide you with steps you may wish to take to protect your personal information.

**WHAT YOU CAN DO TO PROTECT YOUR INFORMATION.** Please review the information below this letter ("**Steps You Can Take to Further Protect Your Information**") for further information on actions you can take to protect yourself.

We sincerely apologize for this incident and regret any inconvenience it may cause you. If you have questions or concerns regarding this matter, please do not hesitate to contact us at 971-722-4382 or [pccfoundation@pcc.edu](mailto:pccfoundation@pcc.edu).

Sincerely,

A handwritten signature in cursive script that reads "Ann Prater".

Ann Prater  
Executive Director  
PCC Foundation

August 12, 2020

To Our Donors and Alumni:

We are writing to inform you of a cybersecurity incident at one of our service providers that may have involved your personal information. This notice explains what happened, what information of yours might have been affected, and what you can do to protect yourself. We take your privacy seriously and value your trust and ask that you take a moment to review this entire notice<sup>1</sup>. If you have any questions, please contact us.

**WHAT HAPPENED.** The incident occurred at a company known as Blackbaud, which is one of the largest donor management software companies serving non-profits, including the PCC Foundation. We use Blackbaud's services to process donations to the Foundation and manage related donor and alumni records. On July 16, 2020, Blackbaud notified us that it experienced a data breach between February 7 and May 20, 2020.

According to Blackbaud, it suffered a ransomware attack in which a cybercriminal gained access to its computer network and files and prevented Blackbaud from using its data files. Blackbaud informed us that, as part of this incident, the cybercriminal may have been able to access files that contained some of your personal information, although there is not a clear indication that an unauthorized user actually accessed your information. Blackbaud further informed us that the cybercriminal(s) who attacked its systems destroyed the data involved in the incident. Blackbaud has also reported that, based on the results of its investigation and investigations of forensic experts and law enforcement, there are no indications that your information was misused and that any misuse appears to be unlikely.

After Blackbaud notified us, we reviewed our records to confirm what categories of information had been shared with Blackbaud for processing so that we could notify our friends and donors.

**WHAT INFORMATION WAS INVOLVED.** Based on information from Blackbaud, none of your financial account or credit/debit card account information that we collected from you was affected. Blackbaud explained that this information was encrypted, so the cybercriminal was not able to access it. But there is a possibility that files containing the following categories of your personal information were accessed in the incident: name, address, date of birth, donation information (*i.e.*, date(s) and amount(s) of donations), and details about your relationship with the Foundation.

**WHAT WE ARE DOING.** We are continuing to monitor reports and gather other information about the incident. The incident did not involve our systems, but we are examining our security and other ways to protect your data, such as evaluating how we collect and store personal information. Although we are not certain that the cybercriminal accessed your information in particular, we are contacting you to explain what happened and to provide you with steps you may wish to take to protect your personal information.

<sup>1</sup> Residents of North Dakota and Washington may receive a copy of this notice both through email and through U.S. Mail, in line with applicable laws in these states.

**WHAT YOU CAN DO TO PROTECT YOUR INFORMATION.** Please review the information below this letter (“**Steps You Can Take to Further Protect Your Information**”) for further information on actions you can take to protect yourself.

We sincerely apologize for this incident and regret any inconvenience it may cause you. If you have questions or concerns regarding this matter, please do not hesitate to contact us at 971-722-4382 or [pccfoundation@pcc.edu](mailto:pccfoundation@pcc.edu).

Sincerely,

A handwritten signature in cursive script that reads "Ann Prater".

Ann Prater  
Executive Director  
PCC Foundation

## **Steps You Can Take to Further Protect Your Information**

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and 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 promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to [IdentityTheft.gov](http://IdentityTheft.gov) or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Or you can purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax  
(800) 685-1111  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 740241  
Atlanta, GA 30374

Experian  
(888) 397-3742  
[www.experian.com](http://www.experian.com)  
P.O. Box 4500  
Allen, TX 75013

TransUnion  
(800) 888-4213  
[www.transunion.com](http://www.transunion.com)  
2 Baldwin Place  
P.O. Box 1000  
Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit [IdentityTheft.gov](http://IdentityTheft.gov) or call 1-877-ID-THEFT (877-438-4338). Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at <https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf>.

- **Security Freeze**

You have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check.

Contact the three credit reporting agencies listed above (Equifax, Experian and TransUnion) to request a security freeze. The credit reporting agencies' websites explain how to request a security freeze. *You must separately place a security freeze on your credit file with each credit reporting agency.*

To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement.

## **Steps You Can Take to Further Protect Your Information**

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and 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 promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to [IdentityTheft.gov](http://IdentityTheft.gov) or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Or you can purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax  
(800) 685-1111  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 740241  
Atlanta, GA 30374

Experian  
(888) 397-3742  
[www.experian.com](http://www.experian.com)  
P.O. Box 4500  
Allen, TX 75013

TransUnion  
(800) 888-4213  
[www.transunion.com](http://www.transunion.com)  
2 Baldwin Place  
P.O. Box 1000  
Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit [IdentityTheft.gov](http://IdentityTheft.gov) or call 1-877-ID-THEFT (877-438-4338). Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at <https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf>.

- **Security Freeze**

You have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check.

Contact the three credit reporting agencies listed above (Equifax, Experian and TransUnion) to request a security freeze. The credit reporting agencies' websites explain how to request a security freeze. *You must separately place a security freeze on your credit file with each credit reporting agency.*

To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement.