June 18, 2019

[redacted]
[redacted]
[redacted]

[redacted]:

This is to notify you of a security incident that was first raised on May 6, 2019 that may have compromised some of your personal identifiable information. On this date, an email was sent and reported by a staff member in School Services that appeared to come from their account but they had no knowledge or awareness of sending this email. This email was sent to a small number of Howard Center Staff with a survey request.

As the staff member stated they did not send this email, on May 8th, the Howard Center technical team engaged Champlain College's Leahy Center for Digital Investigation (LCDI) for digital forensic assistance to investigate. Howard Center has a contractual and confidential relationship with LCDI for security support and investigations. LCDI identified a few connections via a web browser version of email access (Outlook Web Client) and using a VPN (Strong VPN). As you know from the investigations, LCDI identified 2 staff members, including you, that had accounts attacked via this method. In each case, the exposure was accessed via a browser to a web email client and no activity was identified or discovered beyond the email mailbox exposure.

During the Howard Center technical staff and the LCDI investigation, it was identified that your email mailbox had an email that included your personally identifiable information.

In that email, there was information that included your banking information (Name, Address, Account Number and Routing Number) along with tax information from Fidelity (Account Number, Federal ID Number, Partial SSN).

At the recommendation, you changed your network password which terminated this exposure of your email account information. The LCDI and Howard Center staff continued the investigations for several weeks to assess any further compromise, reviewed the details of this potential exposure, and at this point have identified nothing further.

At this point, we have found no evidence or are aware that this information has been compromised but due to the sensitive nature of the information we are treating this as a potential breach and notifying you so that you are aware.

Below is a check list of suggestions from the Vermont Attorney General's Office of how you can best protect yourself.

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.

Equifax	Experian	TransUnion
1-800-685-1111	1-888-397-3742	1-800-916-8800
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Under Vermont law, you are entitled to a free copy of your credit report from those agencies every twelve months. Information on how to obtain a free credit report is available https://www.annualcreditreport.com/index.action

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 the local police or sheriff's office and **file a report of identity theft**. I recommend you obtain 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 number below to place fraud alerts with all of the agencies.
   - **Equifax** - 888-766-0008
   - **Experian** - 888-397-3742
   - **TransUnion** - 800-680-7289

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

   If you do not have Internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (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 paragraph above to order your reports or to keep a fraud alert in place.

Helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report is available on the Vermont Attorney General's website at http://ago.vermont.gov/. Another helpful source is the Federal Trade Commission website, available at https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

On behalf of the agency, I would like to apologize for this breach of your information and assure you that we do take privacy and security very seriously.

If you have any further questions, or there is anything we can do to assist you, please feel free to contact me.

Sincerely,

Bob Stetzel
HIPAA Security Office
Director of Information Technology
802-488-6985
877-217-7019 (Toll free)