

18702



STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

<<First Name>> <<Last Name>>
<<Address>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Dear <<First Name>>:

Stevens is following up on our July 2020 email regarding a data security incident involving Stevens' third-party vendor, Blackbaud, Inc. ("Blackbaud") to provide you with an update. As per the previous communication, Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals and other non-profits, including Stevens Institute of Technology.

Our investigation determined that the incident may have involved some of your information stored in Blackbaud, including your name and financial information (including account and routing numbers) for your bank account with Bank of America ending in 0339.

Although, to date, we are not aware of any misuse of your data, we are notifying you of this incident in accordance with Massachusetts' data breach notification law, which requires that we notify you of this incident, but prohibits us from providing additional details.¹

We recommend that you remain vigilant to the possibility of fraud by reviewing your financial account statements for any suspicious activity. You should immediately report any suspicious activity to your financial institution. For more information on additional steps you can take in response and to mitigate overall risk from any source, please see the additional information provided in the following pages.

We regret that this occurred and apologize for any inconvenience. To help prevent something like this from happening again, we are undertaking a review of how our information is stored with Blackbaud and evaluating Blackbaud's security safeguards.

Should you have any further questions or concerns regarding this matter, please do not hesitate to contact me at 201-216-5667.

Sincerely,

Kathy Schulz

¹ Under M.G.L.A. 93H § 3(b), "notice shall not include the nature of the breach of security or unauthorized acquisition or use, or the number of residents of the commonwealth affected by said breach of security or unauthorized access or use."

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. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit 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, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, 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

Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described below. You may contact and obtain information from your state attorney general at:

Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

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
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, 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.