HEWITT

Notice of Data Breach

November 5, 2020

Consumer Protection Bureau
Office of Attorney General
30 Capitol Street
Concord, NH 03301

VIA EMAIL: DOJ-CPB@doj.nh.gov

Dear Attorney General Gordon MacDonald,

The Hewitt School is an all girls independent K-12 school in New York City, New York. On September 29th, 2020, we received notification from Blackbaud, Inc., one of our service providers, of newly discovered information about a previous security incident. Blackbaud believes a ransomware attack on its systems began on February 7, 2020, and could have continued intermittently until May 20, 2020. Blackbaud informed us that, after discovering the attack in May 2020, it worked with experts and law enforcement to successfully prevent the cybercriminal from blocking its system access and fully encrypting files, and ultimately expelled the cybercriminal from its system. Prior to locking the cybercriminal out, the cybercriminal removed a copy of certain data, including data in a backup file that contained personal information of New Hampshire residents. Blackbaud paid the cybercriminal's demands and received confirmation that the copy had been destroyed.

On September 29th, 2020, Blackbaud advised us that based on new information regarding their investigation—contrary to what they had previously told us—certain social security numbers were included in the file that may have been accessed by the cybercriminal. As Blackbaud has advised us previously, the removed files may also have contained, in an unencrypted form, names and contact information, dates of birth, familial relationships, and philanthropic giving history.

On October 6th, 2020, we received a file from Blackbaud which contained the names of impacted individuals, but did not necessarily contain current contact information. On October 23rd, 2020, our team was able to match the contact information in the file received from Blackbaud with updated information from our records. Through this matching process, we also uncovered that information from New Hampshire residents had been impacted. **Approximately one New Hampshire resident was impacted by this breach. Residents will be notified on or about November 13, 2020.**

Blackbaud advised us that it will be making changes to protect data from any subsequent incidents. Further, Blackbaud advised us that they continue to monitor the dark web and have found no evidence of the compromised information being available. Hewitt will continue to work with Blackbaud to confirm they have taken the steps they have promised and identify any further steps

that might be taken to prevent a recurrence. As indicated in our notice to impacted residents, Blackbaud is offering them 24 months of credit monitoring services free of charge.

If you have any questions, do not hesitate to contact Chief Financial Officer Doug Odom at 212-994-2621 or by email at dodom@hewittschool.org or Director of Technology Jeremy Sambuca at 212-994-2568 or by email at jsambuca@hewittschool.org

Sincerely,

Doug Odom
Chief Financial Officer

Jeremy Sambuca
Director of Technology

NOTIFICATION TEMPLATE FOR INDIVIDUALS

HEWITT

Notice of Data Breach

November ___, 2020

[Insert Address]

Dear [Name],

On September 29th, 2020, we received notification from Blackbaud, Inc., one of our service providers, of newly discovered information about a previous security incident. Blackbaud is a large provider of cloud based data management services to The Hewitt School, as well as many other schools, colleges, universities, and other not-for-profit organizations.

What Happened

Blackbaud believes an attack on its systems began on February 7, 2020, and could have continued intermittently until May 20, 2020. Blackbaud informed us that, after discovering the attack in May 2020, it worked with experts and law enforcement to successfully prevent the cybercriminal from blocking its system access and fully encrypting files, and ultimately expelled the cybercriminal from its system. Prior to locking the cybercriminal out, the cybercriminal removed a copy of certain data from Blackbaud's environment, including data in a backup file that contained some of your personal information. Blackbaud paid the cybercriminal's demands and received confirmation that the copy had been destroyed.

What Information Was Involved

In its initial notice to us, provided in July 2020, Blackbaud communicated that the incident did not involve unencrypted credit card information, bank account information, or social security numbers, and the cybercriminal did not access any encryption key. Blackbaud's most recent notice advised us that based on new information regarding their investigation—contrary to what they had previously told us—certain social security numbers, including your social security number, were included in the file that may have been accessed by the cybercriminal. Based on our review of the information provided to us by Blackbaud, one of the removed files may also have contained, in an unencrypted form, names and contact information, dates of birth, familial relationships, and philanthropic giving history.

We are extremely disappointed by this new information, particularly given that it contradicts information Blackbaud previously provided to us. We have expressed our concern and dissatisfaction to Blackbaud.

Nevertheless, based on the nature of the incident, Blackbaud's research, and third party (including law enforcement) investigation, there continues to be no reason to believe that any data went beyond the cybercriminal, and no reason to believe that any of your data was or will be misused or will be disseminated or otherwise made available publicly.

What We and Blackbaud Are Doing

Blackbaud advised us that it will be making changes to protect your data from any subsequent incidents. Further, as a precautionary measure, Blackbaud advised us that they continue to monitor the dark web and have found no evidence of the compromised information being available. Hewitt will continue to work with Blackbaud to confirm they have taken the steps they have promised and identify any further steps that might be taken to prevent a recurrence.

What You Can Do

In addition, Blackbaud is providing you with access to **Single Bureau Credit Monitoring** services at no charge. Services are for 24 months from the date of enrollment. When changes occur to your Experian credit file, notification will be sent to you the same day the change or update takes place with the bureau. In addition, Blackbaud is providing you with proactive fraud assistance to help with any questions you might have through CyberScout. CyberScout will work with you on a one-on-one basis, answering any questions or concerns you may have. In the event you become a victim of fraud you will also have access to remediation support from a CyberScout Fraud Investigator. This service includes assistance with making telephone calls and preparing documentation to report the incident and reviewing credit reports for possible fraudulent activity, as well as assistance with credit file freezes, where available. Further information on these services can be obtained at https://www.cyberscouthq.com/.

Enrollment Instructions

To enroll in credit monitoring services at no charge to you, please navigate to:
https://www.cyberscouthq.com[redacted]

If prompted, please provide the following unique code to gain access to services:
[redacted]

Once registered, you can access monitoring services by selecting the "Use Now" link to fully authenticate your identity and activate your services. **Please ensure you take this step to receive your alerts**.

In order for you to receive the monitoring services described above, **you must enroll within 90 days from the date of this letter.**

More Information

We recommend that you remain vigilant by reviewing your account statements and report any suspected identity theft to law enforcement, including the Attorney General for your state of residence and the Federal Trade Commission. For additional assistance in monitoring your credit activity, including accessing information about fraud alerts and obtaining security freezes, please see below for the contact information for the three national credit reporting agencies and the Federal Trade Commission:

Equifax (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	TransUnion (800) 916-8800 www.transunion.com P.O. Box 6790 Fullerton, CA 92834	Federal Trade Commission 1-877-ID-THEFT (877-438-4338) www.ftc.gov/idtheft

We regret any inconvenience this incident may cause you. We deeply value your relationship with Hewitt, and the security of our constituents' personal information is of the utmost importance to us. Should you have any further questions or concerns regarding this matter, please do not hesitate to reach out to Doug Odom at doug.odom@hewittschool.org or Jeremy Sambuca at jeremy.sambuca@hewittschool.org.

Sincerely,

Doug Odom
Chief Financial Officer
The Hewitt School

Jeremy Sambuca
Director of Technology
The Hewitt School