

Morgan Lewis

Ezra D. Church

Partner
215.963.5710
ezra.church@morganlewis.com

STATE OF NH
DEPT OF JUSTICE
2020 SEP 11 PM 12:03

VIA US MAIL

September 4, 2020

State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Office of the Attorney General:

This Firm represents the Japan America Society of Greater Philadelphia ("JASGP") and we are writing to notify you regarding the nature and circumstances of a recent data security incident involving a ransomware attack suffered by one of JASGP's vendors. The data security incident potentially affects personal information of individual donors and prospective donors to JASGP.

On or about July 16, 2020, it came to JASGP's attention that in May 2020, Blackbaud, a vendor that supports JASGP's fundraising and engagement efforts, experienced a ransomware attack on systems that contained information of a number of its nonprofit clients. As a result, hackers obtained personally identifying information about Blackbaud's nonprofit clients' donors and prospective donors, including those of JASGP. JASGP initially believed that Blackbaud had sent or would send notifications to state authorities like your office, but it subsequently learned that was not the case. Therefore, out of an abundance of caution, we are sending this notice to you at this time.

After investigation, JASGP has determined that information on Blackbaud's systems at the time of the ransomware incident did not include credit card or bank account information because this information was not stored in the impacted database. Nor were social security numbers of constituents impacted, because JASGP does not collect this information and it is not in any of JASGP's systems. JASGP believes that impacted data may have contained constituents' contact information and a history of their relationship with JASGP, including a history of giving.

At this time, JASGP has no evidence that the personal information of its affected donors and prospective donors has been used inappropriately. JASGP's contracts with Blackbaud require Blackbaud to keep JASGP's donor information confidential and to have security procedures in place, and Blackbaud has indicated to JASGP that it has successfully retrieved the stolen data and prevented it from being used in an unauthorized way. Nevertheless, JASGP sent notifications by mail and email to affected donors and prospective donors to explain what happened, what information was involved, what JASGP has done and how affected donors and prospective donors can contact JASGP with questions.

State of New Hampshire
Office of the Attorney General
September 4, 2020
Page 2

Further information about what JASGP has done and is recommending to the individuals in question can be found in the enclosed notification that JASGP sent to 9 New Hampshire residents via mail and email on September 4, 2020.

If you have any questions, please do not hesitate to contact me.

Regards,

A handwritten signature in black ink, appearing to read "E.D.C.", with a stylized flourish above the letters.

Ezra D. Church

Enclosure



JAPAN AMERICA SOCIETY
OF GREATER PHILADELPHIA

September 4, 2020

Dear Members and Supporters of the Japan America Society of Greater Philadelphia,

We are writing to let you know that the Japan America Society of Greater Philadelphia (JASGP) was notified of a data security incident at one of our outside vendors, Blackbaud. We are contacting you as a precautionary measure to share what Blackbaud has told its clients about the incident. We believe that alerting you is the right thing to do in the interests of transparency and fairness that are at the heart of our organization.

Blackbaud works with many large and small nonprofits, including JASGP, to support fundraising and engagement efforts. Blackbaud recently notified us that it was the target of a ransomware attack that involved the information of a number of its clients. As a result, the hackers obtained some personally identifying information about Blackbaud's nonprofit clients' donors and prospective donors, including those of JASGP.

We believe your information may have been involved. According to Blackbaud, the cybercriminal did not access credit card or bank account information, as this is not stored in the impacted database. Additionally, your social security number was not impacted because we do not collect this, and it is not in any of our systems. Our understanding is that impacted data may have contained constituents' contact information and a history of their relationship with our organization.

Based on the nature of the incident, Blackbaud's research, and third party (including law enforcement) investigation, Blackbaud has stated that it has no reason to believe that any data went beyond the cybercriminal, was misused, or will be disseminated or otherwise made available publicly. Blackbaud has assured us that it has taken the necessary steps to protect its systems from any subsequent incidents. Our contracts with Blackbaud have always required them to keep our constituent information confidential and to have security procedures in place to minimize breaches. For more information from Blackbaud on the incident, visit: www.blackbaud.com/securityincident.

The privacy of donors and supporters like you is of the utmost importance, and we promise to do everything in our power to ensure your private information remains secure.

Please know that we are here for you to answer questions. Due to our office staff working remotely, please contact us via email at info@japanphilly.org with any questions. If you prefer to speak on the phone, please email us and we will call you back to discuss your questions.

Sincerely,

Kim Andrews
Executive Director
キム アンドリュース
専務理事