SOCIETY FOR SCIENCE & THE PUBLIC

September 9, 2020

Attorney General Wayne Stenehjem
Office of the Attorney General
Consumer Protection and Antitrust Division
1050 E. Interstate Avenue, Suite 200
Bismarck, ND 58503-5574

RE: Notice of Security Incident

Dear Attorney General Stenehjem:

I am writing on behalf of the Society for Science & the Public (the "Society"), pursuant to N.D. Cent. Code § 51-30-02, to inform you of a data security incident experienced by one of our third-party service providers, Blackbaud, Inc. ("Blackbaud"), that appears to have involved the names and birth dates of approximately 439 North Dakota residents.

The Society, like many other nonprofit organizations, uses Blackbaud to research and maintain information about our donors and prospective donors. On July 16, 2020, we were notified by Blackbaud of a security incident that occurred on its system beginning on February 7, 2020 and continuing through May 20, 2020. Blackbaud informed us that in May 2020, it detected and interrupted a ransomware attack. However, before Blackbaud was able to stop this ransomware attack, an unauthorized third party accessed and copied certain data from its system, some of which was unencrypted. Blackbaud advised that after detecting the attempted ransomware attack on May 14, 2020, its Cyber Security team, together with independent forensics experts and law enforcement, was able to expel the intruder from Blackbaud's system. Blackbaud reported to us that it paid a ransom in exchange for confirmation that any data that was accessed and copied by the unauthorized third party was destroyed and that it would not be used or disseminated. Blackbaud has told us that it is monitoring for any evidence that the data has been used or made available and has found no such evidence to date.

As a client of Blackbaud, we are not privy to all details of the intrusion or results of its investigation. Our understanding of this incident, the information impacted, and Blackbaud's efforts to contain it, is based entirely on information we have received from Blackbaud. Blackbaud has informed us that it has already made enhancements to further improve its data security, and that it continues to monitor the web, including the dark web, for any signs that the information accessed during this incident has been misused and to monitor its systems for any suspicious activity

Blackbaud has posted public information about this incident on its website at https://www.blackbaud.com/securityincident.

While all of the details regarding the incident are not available to the Society, based on information provided by Blackbaud we understand that as a result of this incident, some Society constituents'

names were disclosed in connection with dates of birth.

No other personal information that is defined as "personal information" under N.D. Cent. Code § 51-30-01(4) was included in the accessed data as far as we know at this time.

Concurrently with the filing of this letter, we are sending notifications to 439 affected North Dakota residents. They will be mailed by no later than September 11, 2020. A copy of the notification letter is attached here as Exhibit A.

Sincerely,

James C. Moore

Chief Technology Officer
Society for Science and the Public

SOCIETY FOR SCIENCE & THE PUBLIC

EXHIBIT A

Sample Notification Letter – North Dakota

September __, 2020

<Salutation 1>
<Salutation 2>
<Address line 1>
<Address line 2>
<Address line 3>

Dear [**Name**]

We are contacting you to inform you about a data security incident at Blackbaud, an outside vendor, that may have involved your name and date of birth.

What happened:

The Society for Science & the Public (SSP) utilizes Blackbaud, a leading donor relationship software provider, to house data of donors and prospective donors. On July 16, 2020 we received notification from Blackbaud informing us that cybercriminals gained access to their systems beginning on February 7, 2020 and had the capability of intermittent access until May 20, 2020. During this time, the cybercriminal was able to use ransomware malware to encrypt a portion of the files on Blackbaud's system and to exfiltrate a copy of our backup file located in Blackbaud's system containing certain of our files. Once the intrusion was discovered, Blackbaud advised that it stopped the ransomware attack and expelled the cybercriminals from their systems. SSP was one of a significant number of organizations whose data had been compromised.

Based on the nature of the incident and Blackbaud's investigation with law enforcement and third-party security experts, SSP has been assured by Blackbaud that the information has been destroyed — and that Blackbaud has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly. You can also view Blackbaud's statement on the incident here: https://www.blackbaud.com/securityincident.

What we are doing about it:

SSP takes data privacy and security very seriously. Blackbaud has assured us they have already implemented changes to further protect their system from breaches, including fixing the vulnerability that led to this breach. Out of an abundance of caution, Blackbaud advised it has also hired a security expert to monitor the dark web as an additional precautionary measure. We will continue monitoring any new developments.

SSP sincerely regrets any inconvenience or concern this incident may have caused. If you have any immediate concerns or questions, please contact us by phone at (202) 785-2255, by email at privacy@societyforscience.org, or by postal mail at 1719 N Street, N.W., Washington, D.C. 20036.

Sincerely,

James C. Moore

Chief Technology Officer
Society for Science and the Public