August 14, 2020

By Electronic Mail
securitybreach@atg.wa.gov

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

RE: Notice of Security Incident

Dear Attorney General Ferguson:

We are writing on behalf of the American Civil Liberties Union, Inc., American Civil Liberties Union Foundation, Inc., American Civil Liberties Union of Washington, Inc., and American Civil Liberties Union of Washington Foundation, Inc. (together, "ACLU"), pursuant to Wash. Rev. Code §§ 19.255.005–.040, to inform you of a data security incident experienced by one of our third-party service providers that appears to have involved the names and birth dates of approximately 86,269 Washington residents.

We were recently notified by one of our third-party service providers, Blackbaud, Inc. ("Blackbaud"), of a security incident that occurred on its system beginning on February 7, 2020 and continuing through May 20, 2020. The ACLU, like many other nonprofit organizations, uses Blackbaud to research and maintain information about our donors and prospective donors, including supporters of ACLU affiliates.

Specifically, Blackbaud informed us on July 16 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 has told us 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 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 ACLU, based on information provided by Blackbaud we understand that as a result of this incident, some ACLU constituents' names were disclosed in connection with dates of birth.

No other personal information that is defined as "personal information" under RCW 19.255.010 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 86,269 affected Washington residents. They will be mailed by no later than August 15, 2020. A copy of the notification letter is attached here as Exhibit A.

One of the ACLU's core values is ensuring the privacy rights of all individuals in our democracy. The ACLU remains committed to ensuring the security and privacy of its constituents' information. We are exploring our options to prevent this from happening again, including revisiting our relationship with Blackbaud.

Please do not hesitate to contact us if you have any questions.

Sincerely,

Terence Dougherty
Chief Operating Officer and General Counsel
American Civil Liberties Union, Inc.
American Civil Liberties Union Foundation, Inc.
125 Broad Street, 18th Floor
New York, NY 10004

Michele Storms
Executive Director
American Civil Liberties Union of Washington, Inc.
American Civil Liberties Union of Washington Foundation, Inc.
P.O. Box 2728
Seattle, WA 98111-2728

EXHIBIT A – SAMPLE NOTIFICATION

Re: Notice of Blackbaud Data Security Incident August __, 2020

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

Dear ACLU Supporter,

We are writing on behalf of the American Civil Liberties Union, the American Civil Liberties Union Foundation, the American Civil Liberties Union of Washington, and the American Civil Liberties Union of Washington Foundation (collectively "ACLU") to let you know about a data security incident experienced by one of our third-party service providers that involved your personal information. (More details are below, but please note that no credit card data, bank account information or social security numbers were accessed in this incident). Pursuant to Washington State law, Wash. Rev. Code §§ 19.255.005–.040, notice is required in the event that certain non-public personal information about Washington residents, including name together with date of birth, is compromised. We are grateful for your support of the ACLU, and we provide this notice to you to explain what happened and how you can protect yourself.

What Happened?

We were recently notified that Blackbaud, Inc., a provider of data management software and services to the ACLU and many other nonprofit organizations, experienced a ransomware attack earlier this year. As a client of Blackbaud, we are not privy to all details of the intrusion or the results of Blackbaud's 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 over the course of numerous communications.

We understand from Blackbaud that the incident began on February 7, 2020, and is believed to have continued through May 20, 2020, after Blackbaud detected and expelled an unauthorized intruder from its systems. The intruder accessed and copied a subset of data stored on Blackbaud's systems and demanded a ransom payment in exchange for destroying that information. This data included certain information that the ACLU maintains on a Blackbaud platform regarding our supporters. Blackbaud has advised us that it paid a ransom in exchange for confirmation from the intruder that any data that was accessed and copied has been destroyed. Additionally, Blackbaud reports that it is actively monitoring via third party experts and has found no trace of the data being available. We have no reason to believe at this point that your information was actually used by, or will be disseminated by, the intruder.

(Over, please)

What Information Was Involved?

There was no unauthorized access to your credit card data or bank account information as part of this incident. We do not use Blackbaud to process financial transactions, and Blackbaud has confirmed that no credit card data, bank account information, usernames, passwords, or social security numbers were accessed from its clients. However, we have determined, based on information provided by Blackbaud, that the data which was copied contained certain information about you, including your name and date of birth.

What Are We Doing?

The ACLU takes the protection and proper use of your personal information very seriously. Blackbaud has informed us that the ransomware attack has been fully contained and that its system has been secured. Blackbaud has also told us that it has already made enhancements to further improve its data security, and that it continues to monitor the web for any signs that the information accessed during this incident has been misused and to monitor its systems for any suspicious activity. We have communicated our disappointment regarding this incident to Blackbaud, and we continue to investigate to confirm and better understand what occurred. We are exploring all options to prevent this from happening again, including revisiting our relationship with Blackbaud.

What You Can Do to Protect Personal Information

Although we currently have no evidence that your personal information has been or will be misused as a result of this incident, we encourage you to remain vigilant and promptly report to your credit agencies, financial institutions, and the proper law enforcement authorities if you notice any suspicious activity or suspected misuse of your personal information. As a general practice, we recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. Contact information for the major credit reporting agencies is included here:

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30374-0256	Allen, TX 75013	Chester, PA 19016
(866) 349-5191	(888) 397-3742	(855) 681-3196
www.equifax.com	www.experian.com	www.transunion.com

(Next page, please)

For More Information

We appreciate your support of our work, and we regret any inconvenience this may cause you. Should you have any further questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact us at 1-888-567-ACLU (2258).

One of the ACLU's core values is ensuring the privacy rights of all individuals in our democracy. The privacy rights of our supporters are of critical concern, and we promise to do everything in our power to live up to the trust you have placed in us.

Sincerely,

Terence Dougherty
Chief Operating Officer & General Counsel
American Civil Liberties Union, Inc.
American Civil Liberties Union Foundation, Inc.
125 Broad Street, 18th Floor
New York, NY 10004

Mark Wier
Chief Development Officer
American Civil Liberties Union, Inc.
American Civil Liberties Union Foundation, Inc.
125 Broad Street, 18th Floor
New York, NY 10004

Michele Storms
Executive Director
American Civil Liberties Union of Washington, Inc.
American Civil Liberties Union of Washington Foundation, Inc.
P.O. Box 2728
Seattle, WA 98111-2728