601 E Street NW
Washington, DC 20049
www.aarp.org

September 14, 2020

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, Washington 98504

RE: Notice of Data Security Incident

Dear Mr. Ferguson,

I am writing this letter on behalf of AARP, Inc. and AARP Foundation (together, "AARP"), pursuant to RCW 19.255.010(7)(b), to provide notice to the Washington Office of Attorney General (the "Attorney General") that some AARP members were affected by the Blackbaud data security incident.

On July 16, 2020, Blackbaud, Inc. ("Blackbaud"), our donor management service provider, notified AARP of a security incident that began on Blackbaud's systems on February 6, 2020. According to Blackbaud, during the security incident, AARP donor information provided to Blackbaud was accessible to the intruder, and the intruder copied a significant amount of this information, although the most sensitive information was stored in encrypted form. As a result, the full name and date of birth for 248,615AARP donors who are Washington residents appear to have been acquired by the hacker. However, no other more sensitive information was acquired in unencrypted form.

Per what Blackbaud has told us, Blackbaud did not discover the breach until May 14, 2020, and Blackbaud then negotiated with the intruder and paid a ransom to him or her in exchange for a promise to delete the data. Only after these negotiations concluded did Blackbaud notify us on July 16, 2020, and, despite AARP's repeated inquiries to Blackbaud, it was not until August 14, 2020 that Blackbaud provided us full information about the AARP donor information affected by the breach.

We note that Blackbaud has publicly stated that it paid the attacker in exchange for destruction of all the information obtained by the hacker. Blackbaud believes that, as of May 20, 2020, the attacker destroyed all of the obtained information and did not share this information with anyone else. Blackbaud has also told us that it has engaged several services to search the Internet for anyone posting or offering to sell information obtained from its breach, and these services have found no such evidence.

AARP did not at any time approve of, or know about, Blackbaud's response to the breach until we were informed of this incident on July 16, 2020.

601 E Street NW
Washington, DC 20049
www.aarp.org

AARP has discontinued its engagement of Blackbaud for certain advocacy activities, and we are currently evaluating Blackbaud's security program and safeguards for other Blackbaud services and products we currently use.

We notified the affected Washington residents regarding this matter as of September 14, 2020, and a copy of such notice is attached.

If you have questions or need additional information regarding this matter, please contact me at ajean@aarp.org or (202) 434-2378.

Sincerely,

Audrey Jean
SVP, Privacy Officer and Senior Associate General Counsel

Attachment

[NAME]
[ADDRESS]

September 14, 2020

RE: Service Provider Data Breach

As a valued donor to AARP Foundation, we hope this letter finds you and yours well and healthy during this time of crisis. Your financial support of our work has been an important reason we have been able to respond to this crisis and support those in need. We are writing to share that we were told that your name and date of birth were obtained by an unauthorized person.

What Happened: On February 6, 2020, Blackbaud, Inc., our donor management vendor, experienced a security intrusion. In this intrusion, information provided to Blackbaud by its many customers, including AARP, was accessible to the intruder and the intruder copied a significant amount of this information, although the most sensitive information was stored in encrypted form. Blackbaud did not discover its breach until May 14, 2020. Blackbaud negotiated with the intruder and paid a ransom to them in exchange for a promise to delete the data. Only after these negotiations concluded did Blackbaud notify us, on July 16, 2020. Blackbaud only provided us full information about the AARP donor information affected by the breach on August 14, 2020.

Please be aware that this incident was not the result of any security failure of AARP. We believe your name and date of birth, but no other AARP information that gives rise to a breach notice requirement, were obtained in unencrypted form from Blackbaud's systems by the attacker. In addition, Blackbaud holds other information in its systems about donors that could have been affected in the incident.

Blackbaud has publicly stated that it paid the attacker in exchange for destruction of all the information obtained by the hacker. Blackbaud believes that, as of May 20, 2020, the attacker destroyed all the obtained information and did not share this information with anyone else. Neither AARP nor AARP Foundation approved of, or knew about, Blackbaud's response to the breach until we were informed of this on July 16, 2020.

Personal Information Involved: Your name and date of birth as they were provided as part of your prior donation to AARP Foundation.

What We Are Doing: AARP Foundation had used Blackbaud to help evaluate donor capacity. AARP Foundation no longer uses Blackbaud for the donor evaluation work. We are evaluating Blackbaud's security program and safeguards for other Blackbaud services and products used by AARP and AARP Foundation, as well as our relationship with them overall.

What You Can Do: We believe that the risk associated with this incident is very low, but as always, we encourage you to always use good security practices in protecting your digital

information. You may always seek more information from AARP's fraud resource center, the AARP Fraud Watch Network, on www.aarp.org/fraudwatchnetwork.

In particular, the AARP Fraud Watch Team recommends the following tips:

- To protect against someone opening an account in your name, put a "credit freeze" on your credit accounts with each of the three credit monitoring agencies.
- Contact one of the three credit agencies to request a "fraud alert" be placed on your credit.
- Check your credit reports to monitor for suspicious activity.
- Be sure to use strong passwords — not the same one for every account — and consider using a password manager.
- Obtain more information from AARP's free Fraud Watch Network Helpline at 877-908-3360 to speak with volunteers trained in fraud counseling

Although we do not believe that there is any heightened risk of identity theft due to this incident, we are required to provide you contact information for the major credit bureaus. Should you have a need for the contact information for the major credit reporting bureaus, please see the following:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Additional Questions: If you have additional questions not addressed in this notice letter, you may contact an AARP representative at 1-888-OUR-AARP (1-888-687-2277).

Sincerely,

Audrey Jean
SVP, Privacy Officer and Senior Associate General Counsel