Locke Lord LLP
Attorneys & Counselors

600 Travis Street, Suite 2800
Houston, Texas 77002
Telephone: 713-226-1200
Fax: 713-223-3717
www.lockelord.com

Laura L. Ferguson
Direct Telephone: 713-226-1590
Direct Fax: 713-229-2553
lferguson@lockelord.com

July 31, 2020

Via Email and Certified Mail
(securitybreach@atg.wa.gov)

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

Re: Notice of Security Incident

Dear Attorney General Ferguson:

Our Firm is writing you on behalf of our client, George W. Bush Presidential Center (the "Center"), to notify you of a recent security incident that affected the personal information of some Washington residents as a result of a service provider's breach.

On July 16, 2020, we were notified by Blackbaud, a large provider of cloud-based data management services to the Center and many educational institutions and other not-for-profit organizations, that it had discovered and stopped a ransomware attack that occurred in May 2020. Blackbaud's systems that were affected by the attack included databases containing certain information about the Center's donors and other contacts. Blackbaud, with independent forensics experts and law enforcement, successfully prevented the cybercriminals from blocking system access and fully encrypting files; and ultimately expelled them from Blackbaud's system. Prior to locking the cybercriminals out, the cybercriminals removed a copy of the Center's data (some unencrypted, some encrypted) from Blackbaud's self-hosted environment; however, the encrypted data was the most sensitive - Social Security numbers, credit card information, or bank account information, and the cyber criminals did not access the encryption key.

According to Blackbaud, any Social Security numbers or payment card information contained in the affected systems were encrypted and the decryption keys were not compromised in connection with this incident. Other unencrypted, less sensitive information concerning the Center's donors and other contacts, however, was acquired by the attackers such as name, birth date, physical and email addresses, telephone numbers, gender and giving history. In addition, Blackbaud informed us that it paid a ransom to the attackers and obtained confirmation that the compromised information has been destroyed.

According to Blackbaud, and as far as we know, there is no indication that any of the compromised information is subject to further disclosure or misuse, and given the intent of the criminals to obtain the payment of the ransom, the Center does not believe there is a high risk that the unencrypted information would be used for other purposes. Blackbaud has also assured us that they are enhancing their safeguards to mitigate the risk of future attacks, including paying a third party service to periodically review the dark web to confirm whether any of the Center's information is for sale.

The names and dates of birth of 6,797 Washington residents were accessed by the intruders. Even though we do not believe any Washington residents will be subject to harm as a result of this incident, out of an abundance of caution, we wanted to advise you of this incident. In addition, the Center is preparing notification letters to mail to these Washington residents on or about July 29, 2020 to inform them of this incident as well. A copy of the form of notification letter is attached.

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

Sincerely,

Laura Ferguson
For the Firm

LLF:cs
Enclosure

GEORGE W. BUSH
PRESIDENTIAL CENTER

July 29, 2020

Inserted: Addressee
Inserted: Address Line
Inserted: City, ST Zip

RE: Important Security and Protection Notification – Please read this entire letter.

On July 16, 2020, we were notified by one of our service providers, Blackbaud, a large provider of cloud-based data management services to the George W. Bush Presidential Center (the "Bush Center") and many educational institutions and other not-for-profit organizations, that it had discovered and stopped a ransomware attack that occurred in May 2020. Blackbaud's systems that were affected by the attack included databases containing certain information about our donors and other contacts. Blackbaud, with independent forensics experts and law enforcement, successfully prevented the cybercriminals from blocking system access and fully encrypting our files; and ultimately expelled the criminals from Blackbaud's system. However, prior to locking the cybercriminals out, the cybercriminals removed a copy of some of the Bush Center's data from Blackbaud's self-hosted environment.

According to Blackbaud, any Social Security numbers, credit card information, or bank account information contained in the affected systems were encrypted and the decryption keys were not compromised in connection with this incident. Other unencrypted, less sensitive information concerning the Bush Center's donors and other contacts, however, was acquired by the attackers, such as name, physical and email addresses, telephone numbers, gender, date of birth, and giving history. In addition, Blackbaud informed us that it paid a ransom to the attackers in exchange for confirmation that the compromised unencrypted information has been destroyed.

According to Blackbaud, and as far as we know, there is no indication that any of the compromised information is subject to further disclosure or misuse, and given the intent of the criminals to obtain the payment of the ransom, the Bush Center does not believe there is a high risk that your unencrypted information would be used for other purposes. Blackbaud has also assured us that they are enhancing their safeguards to mitigate the risk of future attacks, including paying a third-party service to periodically review the dark web to confirm whether any of our information is for sale.

Even though we do not believe your personal information has been subjected to misuse or further unauthorized access due to this incident, out of an abundance of caution, we wanted to advise you of this incident. Please contact donorservices@bushcenter.org if you have any questions or particular concerns.

Sincerely,

Michael McMahan
Vice President, Corporate Planning & Development

ADDITIONAL GUIDANCE, AND DISCLOSURES FOR RESIDENTS OF CERTAIN STATES:

Your taking steps to protect yourself may include contacting credit reporting agencies as further described below.

PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

An **initial 90 day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax	**Experian**	**TransUnion**
PO Box 740241	PO Box 2104	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www. transunion.com

You can renew a fraud alert after 90 days. Note that a fraud alert in your file can protect you, but also may delay you when you seek to obtain credit.

PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. The cost to place and lift a freeze depends on state law. Find your state Attorney General's office at naag.org to learn more.

You may obtain additional information about fraud alerts and security freezes from the Federal Trade Commission, or the consumer reporting agencies. You may contact the FTC at 1-877-ID-THEFT (877-438-4338) or visit the FTC website at www.identitytheft.gov. Contact information is provided above for the consumer reporting agencies.