October 2, 2020

Kevin M. Scott
Direct: 312/602-5074
Fax: 312/698-7474
kevin.scott@bryancave.com

BRYAN CAVE LEIGHTON PAISNER LLP
161 North Clark Street Suite 4300
Chicago IL 60601 3315
T: +1 312 602 5000
F: +1 312 602 5050
www.bclplaw.com

Attorney General Wayne Stenehjem

Office of the Attorney General
Consumer Protection and Antitrust Division
1050 E Interstate Avenue, Suite 200
Bismarck, ND 58503
NDAG@ND.GOV

Dear Attorney General Stenehjem,

We represent the the Supreme Council, 33°, of the Ancient and Accepted Scottish Rite of Free Masonry, Southern Jurisdiction of United States of America ("SC"), a private fraternal organization, located in Washington, DC, and its charitable affiliates, the House of the Temple Historic Preservation Foundation, Inc. ("HOT") and the Scottish Rite Foundation, Southern Jurisdiction, USA, Inc. (SRF) with respect to a data security incident described in more detail below. SC and its charitable affiliates take the security and privacy of the information in their control very seriously and is notifying our constituents who may have been impacted by this incident so they can take steps to protect themselves.

On July 16, 2020 Blackbaud sent notice to HOT that Blackbaud had experience a data security incident. It was investigating the incident to ascertain the scope and to repair any system shortcomings. On September 9, 2020, HOT was notified by Blackbaud that following its investigation it had determined that the data security incident had exposed some of HOT's members' personal information. The incident involved a ransomware attack, which was successfully defeated. However, prior to being expelled from Blackbaud's system, the attacker removed the backup data files of hundreds of organizations worldwide. With the assistance of law enforcement and forensic investigators, Blackbaud was able to receive confirmation that the backup data was destroyed and has confirmed that it has not been found anywhere on the internet at this time.

HOT has received assurances that the data has not gone beyond the attacker, was not or will not be misused, disseminated or otherwise made publicly available. The information within the data files may have contained contact information and dates of birth of HOT and SRF donors and SC members. The attacker did not access credit card information, bank account information, or Social Security numbers.

Five hundred, ninety-one (591) North Dakota residents' personal information was contained within the data file. Notification letters to the individuals will be mailed by first class mail on October 6, 2020. A sample copy of the notification letter is included with this letter.

Blackbaud has already implemented several changes that will protect the data from any subsequent incidents. First, Blackbaud's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the attacker, and took swift action to fix it. Blackbaud has confirmed through testing by multiple third parties, including the appropriate platform vendors, that its fix withstands all known attack tactics. Additionally, they are accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

HOT, SRF and SC remain dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me.

Very truly yours,

Kevin M. Scott

KMS:llh
Attachment

THE
SCOTTISH RITE OF FREEMASONRY
SUPREME COUNCIL, 33° ✠ SOUTHERN JURISDICTION, USA

<<MemberFirstName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year)

Dear <<MemberFirstName>> <<MemberLastName>>

We are contacting you to make you aware of an issue recently brought to our attention by our third-party software vendor, Blackbaud. Blackbaud is one of the world's largest providers of customer relationship management systems for not-for-profit organizations. We take the security of your personal information very seriously, and we sincerely apologize for any concern this incident may cause.

What happened?
On July 16, 2020, we were notified by Blackbaud of a data security incident. The incident involved a ransomware attack, which was successfully defeated. However, the attacker removed the backup data files of hundreds of organizations worldwide. Blackbaud stated that a computer forensic team was investigating the matter to determine the scope of the breach. On September 9, 2020, we received notice from Blackbaud that its investigation indicated that our data was accessed by the perpetrator of the ransomware attack. With the assistance of law enforcement and forensic investigators, Blackbaud was able to receive confirmation that the backup data was destroyed and has confirmed that it has not been found anywhere on the internet at this time.

What information was involved?
We have received assurances that the data has not gone beyond the attacker and was not or will not be misused, disseminated or otherwise made publicly available. It is important to note that your information was contained in those data files, and *may* have contained your contact information and date of birth. **The attacker did not access your credit card information, bank account information, or Social Security number**.

What we are doing.
Please know that we take this incident and the security of your personal information very seriously. Ensuring the safety of our constituents' data is of the utmost to us. In order to prevent a reoccurrence, Blackbaud has already implemented several changes that will protect your data from any subsequent incidents.

First, Blackbaud's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the attacker, and took swift action to fix it. Blackbaud has confirmed through testing by multiple third parties, including the appropriate platform vendors, that its fix withstands all known attack tactics. Additionally, they are accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

What you can do.
We recommend that you review the additional information enclosed, which contains important steps you can take to further protect your personal information.

For more information.
We very much regret any inconvenience this incident may cause you. Should you have any further questions or concerns regarding this matter, please contact me at blackbaudbreachinfo@scottishrite.org.

Sincerely

Matthew T. Szramoski
Director of Development

Additional Important Information

You can obtain information from the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identitytheft.gov

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (https://www.experian.com/fraud/center.html), or Transunion (https://www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
www.experian.com/freeze/center.html
888-397-3742

TransUnion (FVAD)
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.