IfrahLaw
Hands-on Counsel, Gloves-off Litigation
ifrahlaw.com
(202) 524-4140
1717 Pennsylvania Ave, N.W., Suite 650, Washington, D.C. 20006

August 12, 2020

Via Electronic Mail
ndag@nd.gov

Attorney General Wayne Stenehjem
Office of the Attorney General
600 E. Boulevard Avenue, Dept. 125
Bismarck, ND 58505

Re: Notice of Security Incident

Dear Attorney General Stenehjem:

We are writing you on behalf of our client, National Fallen Firefighters Foundation ("NFFF"), to notify you of a recent security incident that affected the personal information of five North Dakota residents whose personal information NFFF maintained. The incident, of which you have been notified by other impacted organizations, took place at a service provider with which NFFF contracts services, Blackbaud, Inc. ("Blackbaud").

NFFF is a 501(c)(3) organization created to honor fallen firefighters, to support their families, and to work to reduce death and injuries in the fire service community. NFFF works nationwide and receives funding through private donations and grants. NFFF contracted with Blackbaud to facilitate donations through Blackbaud's fundraising and donor management software.

On July 16, 2020, Blackbaud notified its customers, including NFFF, of a ransomware attack perpetrated by cybercriminals between February and May 2020. Blackbaud stated in its notice that the company coordinated with independent forensic experts and law enforcement and "ultimately expelled [the cybercriminals] from their system." However, the cybercriminals had removed a copy of Blackbaud's backup file, which contained personal information, including certain information of NFFF's donors. Blackbaud informed its customers that it paid a ransom to the cybercriminals in exchange for confirmation that the compromised data was destroyed. Blackbaud further stated that there is no indication that any of the compromised data will be subject to further misuse. Blackbaud is also undertaking additional measures to secure data on its systems and to mitigate against exposure, including paying a third-party

service to review the dark web to confirm whether the compromised data appears for sale. Further information on the incident, as provided by Blackbaud, is in the company's statement regarding the security incident at https://www.blackbaud.com/securityincident.

When NFFF was made aware of the incident, it promptly notified counsel and sought support on what measures it should undertake. It also sought further detail from Blackbaud on what NFFF donor data was in fact compromised. Given the information provided by Blackbaud, NFFF has been unable to isolate specific and exact details on what data may have been accessed by the cybercriminal. However, it is likely that the personal information, as defined in N.D. Cent. Code. Section 51-30-01(4)(a), of five North Dakota residents may have been exposed during the incident. That personal information included donors' names, addresses, email address, phone numbers, and dates of birth. According to Blackbaud, any Social Security numbers, credit card information, or bank account information contained in the affected file were encrypted and therefore not impacted by the incident.

We do not believe the personal information of our North Dakota donors has been misused or that they will be subject to harm as a result of the incident. However, we have prepared letters to notify the impacted residents to inform them. A copy of the notification letter is attached.

If you have any questions, please do not hesitate to contact me at michelle@ifrahlaw.com or (202) 524-4144.

Sincerely,

Michelle W. Cohen

Enclosure

August 13, 2020

RE: Notice of Data Breach

Dear :

We are writing to let you know about a data security incident that may have involved your personal information. National Fallen Firefighters Foundation ("NFFF") takes the protection and proper use of your information very seriously. We are therefore contacting you to explain the incident and provide you with steps you can take to protect yourself.

What Happened

We were recently notified by one of our third-party service providers, Blackbaud, of a security incident. At this time, we understand they discovered and stopped a ransomware attack. The company, together with law enforcement, was able to lock out the cybercriminal. However, before doing so, the cybercriminal removed a backup file. That backup file contained personal information of individuals from across Blackbaud's customers. For NFFF, that means it contained certain of your personal information, as Blackbaud provides NFFF a constituent management software.

According to the notice that we received from Blackbaud on July 16, 2020, the breach occurred at some point beginning on February 7, 2020 and could have been in there intermittently until May 20, 2020.

Blackbaud paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, their research, and third party (including law enforcement) investigation, we have 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.

What Information Was Involved

It's important to note that the *cybercriminal did not access your credit card information, bank account information, or social security number*. However, we have determined that the file removed may have contained your contact information, including your name, address, phone or email; demographic information, including your birthdate; and a history of your relationship with our organization, such as donation dates and amounts.

What We Are Doing

We are notifying you so that you can take immediate action to protect yourself. Ensuring the safety of our constituents' data is of the utmost importance to us. As part of their ongoing efforts to help prevent something like this from happening in the future, Blackbaud has already implemented several changes that will protect your data from any subsequent incidents. We are monitoring their response and will continue to do so to ensure that where our constituent data is housed follows or exceeds industry standards on data security and protection.

What You Can Do

As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities. Please review the attached "Additional Information" that may be helpful to you.

For More Information

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you like to review further information about the Blackbaud incident, please see https://www.blackbaud.com/securityincident. You may also contact Rebecca Nusbaum, Director of Development, at (410) 721-6212 or bnusbaum@FireHero.org.

Sincerely,

Ronald J. Siarnicki
Executive Director
National Fallen Firefighters Foundation
16825 South Seton Avenue
Emmitsburg, MD 21727

ADDITIONAL INFORMATION

Contact information for the three nationwide credit reporting companies is as follows:

1. Equifax, P.O. Box 105788, Atlanta, GA 30348, 1-877-478-7625, www.equifax.com
2. Experian, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com
3. TransUnion, P.O. Box 2000, Chester, PA 19016, 1-800-680-7289, www.transunion.com

The following information reflects recommendations from the Federal Trade Commission regarding identity theft protection.

Free Credit Report. It is always a good practice to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, Georgia 30348-5281.

Fraud Alert. You may place a fraud alert on your credit file by calling one of the three nationwide credit reporting agencies above. 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. Pursuant to federal and state laws, you may place a fraud alert on your credit file free of charge.

Security Freeze. You have the right to put a security freeze on your credit file, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. If you place a security freeze on your credit file, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. *Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting agency.* Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze.

The following information must be included when requesting a security freeze (note that if you are requesting a security freeze for your spouse, this information must be provided for your spouse 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 (5) years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a

copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Federal Trade Commission and North Dakota Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the North Dakota Attorney General's office. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580, www.ftc.gov/bcp/edu/microsites/idtheft, 1-877-IDTHEFT (438-4338).

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.