McGuireWoods LLP
Gateway Plaza
800 East Canal Street
Richmond, VA 23219-3916
Phone: 804.775.1000
Fax: 804.775.1061
www.mcguirewoods.com

Janet Peyton
Direct: 804.775.1166

McGUIREWOODS

jpeyton@mcguirewoods.com
Fax: 804.698.2230

September 18, 2020

VIA FEDERAL EXPRESS
The Honorable Gordon MacDonald
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Notice of Data Breach

Dear Attorney General MacDonald:

I am writing on behalf of The FUND for Lake George, a non-profit organization with an address of P.O. Box 352, Lake George, New York 12845 ("The FUND") to provide a report of a recent data breach. Like many non-profit organizations, The FUND has historically used a software vendor called Blackbaud as a platform for its development activities. On July 16, 2020, The FUND was informed by Blackbaud that Blackbaud had been the subject of a "ransomware" attack on their systems between February 7 and May 20, 2020, during which time unauthorized individuals accessed and extracted some of Blackbaud's client files, including some files that were property of The FUND.

Although Blackbaud initially advised The FUND that no credit card, bank account information, social security numbers, or user login credentials and passwords were compromised or accessed, on July 22, 2020, Blackbaud informed us that some media files, which included images of donors' checks, were breached. These included the donor's full name and address, and possibly other contact information (phone number, e-mail address) together with the donor's bank account number and routing number. The group of impacted donors included eight (8) New Hampshire residents. As such, The FUND sent notification letters to these eight individuals on September 4, 2020, pursuant to N.H. Rev. Stat. § 359-C:20 (I)(b).

In response to this incident, The FUND has terminated its contract with Blackbaud and is implementing a number of steps, both internally and with vendors who will have access to our data in the future, to ensure that all of our data is processed and stored securely.

A copy of the notification letter that was sent to affected individuals on September 4, 2020 is enclosed. As you will see, among other things, the letter describes various steps that affected individuals can take to protect themselves, provides contact information for consumer reporting agencies and relevant governmental agencies (including your office), and provides information about enrolling in one year of credit monitoring services that will be provided to the individual by The FUND at no cost.

If you have questions about this incident, please feel free to contact me at the email or phone numbers listed above.

Sincerely,

Janet P. Peyton

Enclosure: Template Notification Letter

cc: Eric Siy, Executive Director, The FUND for Lake George (w/encl.)

McGuireWoods LLP
Gateway Plaza
800 East Canal Street
Richmond, VA 23219-3916
Phone: 804.775.1000
Fax: 804.775.1061
www.mcguirewoods.com

Janet Peyton
Direct: 804.775.1166

McGUIREWOODS

jpeyton@mcguirewoods.com
Fax: 804.698.2230

September 18, 2020

VIA FEDERAL EXPRESS
The Honorable Gordon MacDonald
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Notice of Data Breach

Dear Attorney General MacDonald:

I am writing on behalf of The FUND for Lake George, a non-profit organization with an address of P.O. Box 352, Lake George, New York 12845 ("The FUND") to provide a report of a recent data breach. Like many non-profit organizations, The FUND has historically used a software vendor called Blackbaud as a platform for its development activities. On July 16, 2020, The FUND was informed by Blackbaud that Blackbaud had been the subject of a "ransomware" attack on their systems between February 7 and May 20, 2020, during which time unauthorized individuals accessed and extracted some of Blackbaud's client files, including some files that were property of The FUND.

Although Blackbaud initially advised The FUND that no credit card, bank account information, social security numbers, or user login credentials and passwords were compromised or accessed, on July 22, 2020, Blackbaud informed us that some media files, which included images of donors' checks, were breached. These included the donor's full name and address, and possibly other contact information (phone number, e-mail address) together with the donor's bank account number and routing number. The group of impacted donors included eight (8) New Hampshire residents. As such, The FUND sent notification letters to these eight individuals on September 4, 2020, pursuant to N.H. Rev. Stat. § 359-C:20 (I)(b).

In response to this incident, The FUND has terminated its contract with Blackbaud and is implementing a number of steps, both internally and with vendors who will have access to our data in the future, to ensure that all of our data is processed and stored securely.

A copy of the notification letter that was sent to affected individuals on September 4, 2020 is enclosed. As you will see, among other things, the letter describes various steps that affected individuals can take to protect themselves, provides contact information for consumer reporting agencies and relevant governmental agencies (including your office), and provides information about enrolling in one year of credit monitoring services that will be provided to the individual by The FUND at no cost.

If you have questions about this incident, please feel free to contact me at the email or phone numbers listed above.

Sincerely,

Janet P. Peyton

Enclosure: Template Notification Letter

cc: Eric Siy, Executive Director, The FUND for Lake George (w/encl.)

THE FUND for LAKE GEORGE

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

September 4, 2020

F7656-L01-0000027 P001 T00001 **********MIXED AADC 159

[redacted]
NH

RE: Notice of Data Breach

Dear [redacted]:

I am writing to you on behalf of The FUND for Lake George with important information about a data security incident at our donor software provider that may have involved your personal information ("PI"). The FUND for Lake George takes the protection and proper use of your information very seriously. We are, therefore, contacting you to explain the incident and provide you with next steps and new security measures we are taking, as well as those you can take to further protect yourself.

What Happened: On July 16, 2020, The FUND for Lake George was informed of the cyber breach at Blackbaud, Inc., which provides software services to 35,000 nonprofit fundraising entities worldwide, including The FUND for Lake George. Blackbaud indicated the incident involved a "ransomware" attack on its systems between February 7 and May 20, 2020, during which time unauthorized individuals accessed and extracted some of Blackbaud's client files, including some files that were property of The FUND for Lake George. These individuals attacked Blackbaud in exchange for financial gain.

What Information Was Involved: Blackbaud initially advised us that no credit card, bank account information, social security numbers, or user login credentials and passwords were compromised or accessed. However, on July 22, 2020, Blackbaud informed us that some media files were breached, including: your full name and address, and possibly other contact information (phone number, e-mail address) together with an image of your donation(s) by check including bank account number and routing number.

What We Are Doing: We understand Blackbaud has taken action to mitigate the breach, including notifying law enforcement, successfully locking out the unauthorized users from Blackbaud's system, paying a financial demand in exchange for confirmation that the extracted files were destroyed and hiring a monitoring service to monitor the dark web to ensure there is no future use of the data. Blackbaud has also heightened its security efforts to protect against future ransomware attacks. That said, we are deeply disappointed in their handling of this incident and have lost faith in them as a vendor. As such, The FUND for Lake George has terminated its contract with Blackbaud and is implementing a number of steps, both internally and with vendors who will have access to our data in the future, to ensure that all of our data is held securely.

What You Can Do: We want to make you aware of other steps you may take to guard against identity theft or fraud. Please review the information provided below for steps you can take to protect your personal information, including toll-free numbers and addresses for each of the three credit reporting agencies (Equifax, Experian and TransUnion), and the Federal Trade Commission ("FTC"). You can obtain additional information from these sources about steps to avoid identity theft.

As previously stated, we take the privacy and security of our donors very seriously. Therefore, to help protect your identity, we are offering a complimentary 12-month membership of Experian's IdentityWorks^{SM}. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure you enroll by November 30, 2020 (your code will not work after this date)
- Visit the Experian IdentityWorks^{SM} website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: [redacted]

Information regarding your 12-month EXPERIAN IDENTITYWORKS^{SM} Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks^{SM}. You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks using the unique code provided in your letter:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks^{SM} membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (855) 387-4540. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site. If you wish to enroll in credit monitoring, please follow the instructions in the letter you received.

We recommend that you consider placing a fraud alert on your credit files and/or an alert with ChexSystems in light of the check information that was involved in this breach. The applicable numbers for the credit reporting agencies and ChexSystems are provided in the enclosure. It is important that you remain vigilant over the next 12 to 24 months by reviewing your account statements and monitoring your credit reports for suspicious activity. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the FTC.

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks^{SM} online, please contact Experian's customer care team at (855) 387-4540 by November 30, 2020. Be prepared to provide Engagement Number [redacted] as proof of eligibility for the identity restoration services by Experian.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

For More Information: Please refer to the information on obtaining credit reports, credit freezes and security alerts below. The FUND for Lake George is committed to protecting the personal and financial information provided to our organization. We deeply value your relationship and commitment to our mission, and sincerely apologize for this incident involving our former software provider.

Sincerely,

Dede Potter

Dede Potter
Director of Finance and Administration

Information on Obtaining Credit Reports, Credit Freezes and Security Alerts

Obtain a Free Credit Report:

You may obtain a free copy of your credit report from each of the three nationwide consumer reporting agencies by calling 1-877-322-8228 or going online to www.annualcreditreport.com. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies.

Credit Freezes & Fraud Alerts:

You may contact the fraud departments of the three nationwide credit reporting agencies to discuss your options. You have the right to place a free 90-day fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. It also may delay your ability to obtain credit. To place a fraud alert on your credit report contact the three credit reporting agencies below.

To place a security freeze on your credit report, you must contact **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below, or in some cases their websites provide alternate methods:

Experian	**Equifax**	**TransUnion**
Experian Security Freeze P.O. Box 9554 Allen, TX 75013 (888) 397-3742 https://www.experian.com/freeze/center.html	Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788 (877) 298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/	TransUnion Credit Freeze P.O. Box 160 Woodland, PA 19094 (888) 909-8872 https://www.transunion.com/credit-freeze

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

Security Alert with ChexSystems:

You may place an alert with ChexSystems. Chex Systems, Inc. is a consumer-reporting agency governed by the FCRA and other laws (the Federal Trade Commission enforces the FCRA) which provides account verification

services to its financial institution members to aid them in identifying account applicants who may have a history of account mishandling (for example, people whose accounts were overdrawn and then closed by them or their bank). In short, ChexSystems is like the credit reporting agencies (Equifax, Experian, TransUnion) but specific to checking/savings history instead of credit/loan history. ChexSystems has two protections available:

- **Consumer Report Security Alert**. This puts a flag on your consumer file stating the banking institution needs to take additional steps to confirm it is you who is initiating the action (much like placing a fraud alert with the credit reporting agencies). You may request a 90-day alert, which is the default, though you may extend it to 7 years if you complete the ChexSystems ID Theft affidavit form (available online), have the affidavit notarized, and send the notarized affidavit to ChexSystems. To set the Consumer Report Security Alert, call (888) 478-6536 or online by visiting https://www.chexsystems.com.

- **Consumer Report Security Freeze**. This will prohibit ChexSystems from releasing any information in your consumer file without your express authorization, meaning you have to contact ChexSystems and lift the freeze in order for your information to be released (much like placing a freeze with the credit reporting agencies). You should be aware that taking advantage of this right may delay or prevent timely approval from any user of your consumer report that you wish to do business with. The third party will receive a message indicating that you have blocked your information. To set the Consumer Report Security Freeze, call (800) 887-7652 or online by visiting https://www.chexsystems.com.

To learn more about fraud alerts, security freezes, and protecting yourself from identity theft and to report incidents of identity theft, you can visit the Federal Trade Commission's website at www.consumer.gov/idtheft, or www.ftc.gov/credit, or call 1-877-IDTHEFT (1-877-438-4338). You may also receive information from the Federal Trade Commission by writing to:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580.

You have a variety of rights under the federal Fair Credit Reporting Act (FCRA). For more information on your FCRA rights, visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf

- For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

- For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

- For residents of New York: You may also obtain information about preventing and avoiding identity theft from the New York Division of Consumer Protection, consumer hotline 800-697-1220 or https://www.dos.ny.gov/consumerprotection/security_breach/data_security_breach.htm

- For residents of Washington DC: You may also obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at: https://oag.dc.gov/