



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

MAR 15 2021

CONSUMER PROTECTION

Julie Siebert-Johnson
Office: (267) 930-4005
Fax: (267) 930-4771
Email: jsjohnson@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 11, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of the Blackbaud Data Event

Dear Sir or Madam:

We represent Fayetteville Public Library Foundation (“FPLF”) located at 401 West Mountain Street, Fayetteville, AR 72701, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, FPLF does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 16, 2020, FPLF received notification of a cyber incident from one of its third-party vendors, Blackbaud, Inc. (“Blackbaud”). Blackbaud is a cloud computing provider that provides database services tools to organizations, including FPLF. Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. While Blackbaud discovered this activity in May 2020, it was not until July 16, 2020 that Blackbaud notified FPLF that an unknown actor may have accessed or acquired certain Blackbaud customer data.

Upon receiving notice of the cyber incident, FPLF commenced an investigation to better understand the nature and scope of the incident and any impact on FPLF data. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident and to assess the risk to any FPLF data stored on impacted systems. On December 14, 2020, FPLF received further information from Blackbaud about this incident and the scope of the impact to FPLF data. On February 9, 2021, after a thorough review process, FPLF confirmed the population of potentially impacted individuals. FPLF thereafter worked to provide notice to potentially impacted individuals as quickly as possible.

The information that could have been subject to unauthorized access includes information as defined by New Hampshire law including name and financial account information.

Notice to New Hampshire Resident

On or about March 11, 2021, FPLF provided written notice of this incident to affected individuals, which includes one (1) New Hampshire resident. Written notice was provided in substantially the same form as the letter attached hereto as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, FPLF moved quickly to investigate and respond to the incident, assess the security of FPLF systems, and notify potentially affected individuals. FPLF is working to review and revise existing policies and procedures and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. Further, FPLF is providing access to monitoring services for twelve (12) months through Kroll Inc. to eligible individuals whose personal information was potentially affected by this incident, at no cost to these individuals. To date, FPLF has not received any information from Blackbaud that any FPLF information was specifically accessed or acquired as a result of this event.

Additionally, FPLF is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. FPLF is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. FPLF will also be notifying other state regulators as required.

Office of the Attorney General
March 11, 2021
Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4005.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Julie Siebert-Johnson', written in a cursive style.

Julie Siebert-Johnson of
MULLEN COUGHLIN LLC

JSJ/mep

EXHIBIT A



Fayetteville
Public Library
Foundation

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: <<b2b_text_1(SubjectLine)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Fayetteville Public Library Foundation (“FPLF”) writes to inform you of a recent incident involving one of its third-party vendors, Blackbaud, Inc. (“Blackbaud”), that may affect the privacy of some of your information. While we have no evidence of any actual or attempted misuse of any information as a result of this incident, this notice provides information about the Blackbaud incident, our response and efforts to obtain additional information from Blackbaud, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On July 16, 2020, FPLF received notification from Blackbaud of a cyber incident on its network. Blackbaud is a cloud computing provider that provides database services tools to organizations, including FPLF. Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. While Blackbaud discovered this activity in May 2020, it was not until July 16, 2020 that Blackbaud notified FPLF that an unknown actor may have accessed or acquired certain Blackbaud customer data.

Upon receiving notice of the cyber incident, FPLF commenced an investigation to better understand the nature and scope of the incident and any impact on FPLF data. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident and to assess the risk to any FPLF data stored on impacted systems. On December 14, 2020, FPLF received further information from Blackbaud about this incident and the scope of the impact to FPLF data which aided our internal analysis. On February 9, 2021, after a thorough review process, FPLF confirmed the population of potentially impacted individuals. We thereafter worked to provide notice to potentially impacted individuals as quickly as possible.

What Information is Involved? Our investigation determined that the involved Blackbaud systems contained your name and financial account information, and therefore this information may have been impacted. Please note that, to date, we have not received confirmation from Blackbaud that your specific information was accessed or acquired by the unknown actor.

What Are We Doing? The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review and revise our existing policies and procedures and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. We will also be notifying state regulators, as required.

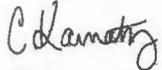
Further, although FPLF is unaware of any actual or attempted misuse of your information as a result of this incident, as an added precaution, and at no cost to you, we are providing you with access to monitoring services for twelve (12) months through Kroll in this matter. The offered monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Please review the enclosed *Steps You Can Take to Help Protect Your Information* for additional information and enrollment instructions. Please note that you must complete the activation process yourself, as we are not permitted to activate these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and credit reports for suspicious charges. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find general information on what you can do to help protect your personal information, as well as information on how to activate the monitoring services being offered.

For More Information. We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-498-2035, which is available Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Additionally, you may also write to FPLF at Fayetteville Public Library Foundation, Attention: Christina Karnatz, Director of Development and Marketing & Communications, 401 West Mountain Street Fayetteville, AR 72701-5819.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,



Christina Karnatz
Director, Development and Marketing & Communications
Fayetteville Public Library Foundation

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Offered Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. To activate:

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

*You have until **June 11, 2021** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

ADDITIONAL DETAIL REGARDING YOUR 12 MONTH COMPLIMENTARY MONITORING SERVICES

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); and

7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

| Equifax | Experian | TransUnion |
|---|---|---|
| https://www.equifax.com/personal/ | https://www.experian.com/help/ | https://www.transunion.com/credit-help |
| 888-298-0045 | 1-888-397-3742 | 833-395-6938 |
| Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 | Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 | TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 |
| Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788 | Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013 | TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094 |

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. FPLF is located at 401 West Mountain Street Fayetteville, AR 72701-5819.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.