



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

DEC 21 2020

CONSUMER PROTECTION

M. Alexandra Belton
Office: 267-930-4773
Fax: 267-930-4771
Email: abelton@mullen.law

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

December 11, 2020

VIA U.S. MAIL

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

Re: Notice of Blackbaud Cyber Incident

Dear Sir or Madam:

We represent The National WWII Museum (“The Museum”) located at 945 Magazine Street, New Orleans, LA, 70130, and write to notify your office of an incident that may affect the security of some personal information relating to two (2) New Hampshire residents. The Museum reserves the right to supplement this notice with any new significant facts learned subsequent to its submission. By providing this notice, The Museum 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, The Museum received notification from one of its third-party vendors, Blackbaud, Inc. (“Blackbaud”), of a cyber incident. Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud advised that it reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, and two months after the incident, Blackbaud notified its customers, including The Museum, that an unknown actor may have accessed or acquired certain Blackbaud customer data at some point before Blackbaud locked the actor out of its environment on May 20, 2020. According to Blackbaud, it detected the first indicator of compromise on May 14, 2020 and that unauthorized activity was contained and stopped by May 20, 2020.

Upon learning of the Blackbaud incident, The Museum commenced an investigation to determine what, if any, sensitive Museum data was potentially involved. On or about September 29, 2020, The Museum received additional information from Blackbaud on the incident. Because Blackbaud failed to provide a list of the potentially affected Museum data, The Museum undertook a comprehensive analysis of the information Blackbaud provided and the data stored on the systems identified by Blackbaud to confirm what records could have been accessible to the threat actor and to identify the individuals associated with the records. On or about November 10, 2020, The Museum completed its investigation and confirmed that

personal information, as defined by N.H. RSA § 359-C:19, could have been subject to unauthorized access or acquisition including name and financial account information.

Notice to New Hampshire Residents

On December 10, 2020, The Museum provided written notice of the Blackbaud incident to two (2) New Hampshire residents. Written notice was provided in substantially the same form as the letter attached here as *Exhibit A*. To date, The Museum has not received any information from Blackbaud that any The Museum information was specifically accessed or acquired by the unknown actor.

Other Steps Taken and To Be Taken

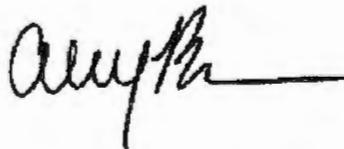
Upon discovering the event, The Museum moved quickly to obtain information from Blackbaud regarding their incident. The Museum then provided notice to potentially affected individuals associated with The Museum. That notice provided information about the Blackbaud incident, The Museum's response thereto, and resources available to help protect personal information from possible misuse. The Museum's response included attempts to coordinate with Blackbaud to confirm what information could have been potentially affected that may have contained personal information. The Museum is working to review existing policies and procedures regarding third-party vendors and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

Additionally, The Museum is providing notified individuals with guidance on how to better protect against identity theft and fraud. The Museum is providing individuals with 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. The Museum will also be notifying other state regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4773.

Very truly yours,



M. Alexandra Belton of
MULLEN COUGHLIN LLC

MAB/amw
Enclosure

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notice of Data Breach

Dear <<Name 1>>:

The National WWII Museum writes to inform you of a recent incident that may affect the privacy of some of your information. The Museum received notification from one of its third-party vendors, Blackbaud, Inc., of a cyber incident. Blackbaud is one of the world's largest cloud computing providers that offers donor management and financial services tools to hundreds of organizations, including The National WWII Museum. This notice provides information about the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? In July 2020, Blackbaud reported that it experienced a ransomware incident in May 2020 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 at some point before Blackbaud locked the actor out of the environment on May 20, 2020. Blackbaud believes the data was destroyed by the actor and was not spread beyond the actor.

Upon receiving notice of the cyber incident, the Museum immediately commenced an investigation to better understand the nature and scope of the incident. On September 29, 2020, we received further information from Blackbaud that the scope of affected information was wider than originally reported. Since learning of this incident, the Museum team has worked diligently to receive the information necessary from Blackbaud to conduct a full audit of its systems to confirm what information related to our institution may have been impacted. Through these efforts, on or around November 10, 2020, The National WWII Museum determined the scope of personal information that may have been affected. Our team then worked to provide those individuals with notice of the incident and put in place resources to assist them in protecting their personal information from potential misuse. You are receiving this notice because our investigation determined your information was present on the impacted Blackbaud systems.

What Information was Involved? Our investigation determined that the involved Blackbaud systems contained your name and <<Breach Elements>>. 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 We Are 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 our existing policies and procedures regarding our third-party vendors, 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 regulators, as required.

In response to the incident, we are offering you identity protection services provided by TransUnion for 12 months at no cost to you. Please review the enclosed *Steps You Can Take to Protect Your Information* for additional information and enrollment instructions.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity and to detect errors. Please 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 enroll in the credit 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 800-447-1082, Monday through Friday, 9am to 9pm Eastern Time.

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

Sincerely,



Stephen J. Watson
President & CEO
The National WWII Museum



Activation Code: <<Activation Code>>

Complimentary One-Year *myTrueIdentity* Credit Monitoring Service

Enroll in Identity Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,[®] one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Monitor Accounts

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

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
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.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 agencies listed on the next page:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can 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.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; www.oag.state.md.us.

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.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act ("FCRA"). Those rights include but are not limited to 1) the right to be told if information in your credit file has been used against you; 2) the right to know what is in your credit file 3) the right to ask for your credit score; and 4) and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting agencies must 1) correct or delete inaccurate, incomplete, or unverifiable information; and 2) limit access to your file; and 3) get your consent for credit reports to be provided to employers. Additionally, consumer reporting agencies may 1) not report outdated negative information; and 2) limit "prescreened" offers of credit and insurance you receive based on information in your credit report. You may also seek damages from violators. 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 <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.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 Attorney General can be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For District of Columbia residents, the District of Columbia Attorney General can be contacted at 441 4th St. NW #1100 Washington, D.C. 20001; by phone at 202-727-3400; and by email at oag@dc.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.