



**MULLEN
COUGHLIN_{LLC}**
ATTORNEYS AT LAW

RECEIVED
MAR 15 2021
CONSUMER PROTECTION

Vincent F. Regan
Office: (267) 930-4842
Fax: (267) 930-4771
Email: vregan@mullen.law

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

March 10, 2021

VIA FIRST-CLASS MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent The Museum of the American Revolution (“The Museum”), located at 101 S. 3rd St., Philadelphia, PA 19106, and are writing to notify your office of an incident that may affect the security of personal information relating to approximately two (2) New Hampshire residents. This notice may be supplemented if new significant facts are 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 or personal jurisdiction.

Nature of the Data Event

The Museum recently learned of unusual activity related to one Museum email account. Upon learning of the suspicious activity, we immediately took steps to secure the email account and began working with a third-party computer forensic specialist to determine the nature and scope of the event. The investigation confirmed that a Museum email account was accessed by an unknown actor between September 22, 2020 and October 13, 2020.

The investigation was unable to determine what emails, if any, were accessed by the unauthorized actor. In an abundance of caution, The Museum worked with third party specialists to perform a comprehensive review of all information stored in the email account at the time of unauthorized access to confirm the identities of the individuals whose information may have been accessible to the unauthorized actor. The Museum then conducted a manual review of its records to determine the identities and contact information for potentially impacted individuals. This review concluded on February 25, 2021.

Mullen.law

The personal information impacted by this event for New Hampshire residents varies by individual but includes the following: name and financial account information. There is no evidence that information specifically relating to New Hampshire residents was actually accessed by an unauthorized actor, but that activity cannot be ruled out with certainty. The Museum is providing notice in an abundance of caution.

Notice to New Hampshire Residents

On March 10, 2021, The Museum began providing written notice of this incident to potentially affected individuals, which includes two (2) New Hampshire residents. Written notice was provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the potential unauthorized access to the contents of the email account, The Museum moved to identify those that may be affected, put in place resources to assist them, and provide them with notice of this incident. The Museum is also working to implement additional safeguards to protect the security of information in its system.

The Museum is providing written notice to those individuals who may be affected by this incident. This notice includes an offer of complimentary access to credit monitoring and identity restoration services through IDEXperts, and the contact information for a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, The Museum is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, 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, 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 is also providing written notice of this incident to other regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4842.

Very truly yours,



Vince Regan of
MULLEN COUGHLIN LLC

EXHIBIT A



C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
(833) 903-3648
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code:
<<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

March 10, 2021

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

It is an unfortunate reality that in today's world, cyber threats are an endemic problem that require constant vigilance. I regret to inform you of an event that may impact the security of some of your personal information. While we are unaware of any attempted or actual misuse of your information, we want to alert you regarding this event, our response, and actions you may want to take to protect yourself against the possibility of identity theft and fraud should you feel it is necessary to do so.

What Happened? Last fall, the Museum learned of unusual activity related to an individual Museum email account. The Museum took immediate action to secure the email account and to engage a third-party computer forensic specialist to determine the nature and scope of the suspicious activity.

The investigation confirmed that an unknown actor accessed the email account of one employee between September 22, 2020 and October 13, 2020 but was unable to determine how the compromise occurred. This event was limited to a single email account and there was no impact to our donor fundraising database, financial reporting database, or our payroll systems.

In an abundance of caution, we worked with third-party specialists to perform a comprehensive review of all information stored in the email account at the time of unauthorized access to identify the individuals whose information may have been accessible to the unauthorized actor. We then conducted a thorough manual review of our records to determine contact information for potentially impacted individuals. On or around February 25, 2021, we completed our internal review.

What Information Was Involved? The investigation was unable to confirm precisely what emails, if any, were accessed by the unauthorized actor. However, it was determined that the following type(s) of information relating to you were present in the impacted email account and potentially accessible to the unknown actor during this incident: name and <<variable text>>. The investigators uncovered no evidence that this personal information was actually accessed or misused by the unknown actor, nor was there any evidence that the information in the account was downloaded for future access.

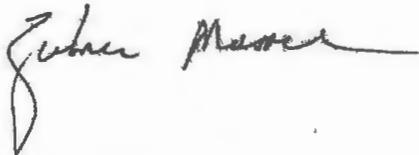
What We Are Doing. We deeply regret that this incident occurred. The security of your personal information is of paramount importance to us. As part of our ongoing commitment to the privacy of personal information in our care, we have reviewed and enhanced our policies and procedures with additional safeguards to further secure the information in our systems. We also notified state regulators, as required. While we are unaware of any misuse of your personal information because of this incident, we are offering you <<12 or 24>> months of complimentary credit monitoring and identity restoration services through IDX. Please note the deadline for enrollment is June 10, 2021.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Protect Your Information*. 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. You may also enroll in the complimentary credit monitoring services described above. Enrollment instructions are attached to this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at (833) 903-3648, Monday through Friday (excluding U.S. holidays), during the hours of 9:00 a.m. to 9:00 p.m., Eastern Time. You may also write to the Museum at 101 S. 3rd St., Philadelphia, PA 19106.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

A handwritten signature in black ink, appearing to read "ZeeAnn Mason". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

ZeeAnn Mason
Chief Operating Officer
Museum of The American Revolution

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Credit Monitoring Instructions.

- 1. Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided here <<Enrollment Code>>.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at (833) 903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts.

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. 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 2000
Chester, PA 19016
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 below:

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

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); 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 Maryland residents: The Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; and www.oag.state.md.us.

For North Carolina residents: The Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and 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, 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 agencies 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 Rhode Island residents: The Rhode Island Attorney General may be contacted at: 150 South Main Street, Providence, Rhode Island 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 3 Rhode Island residents impacted by this incident.

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

For Washington, D.C. residents: The Attorney General may be contacted at Office of the Attorney General, 441 4th Street, NW, Washington, DC 20001; (202) 727-3400; and www.oag@dc.gov.