MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

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

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

November 25, 2020

VIA U.S. MAIL

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

Re: Supplemental Notice of Data Event

Dear Sir or Madam:

We represent New-York Historical Society ("N-YHS") located at 170 Central Park West, New York, New York 10024, and write to supplement our October 5, 2020 notice of data event, which is attached here as ***Exhibit A***. By providing this notice, N-YHS 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

In July, 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. Blackbaud reported that certain data was acquired by the threat actor at some point before Blackbaud locked the threat actor out of the system on May 20, 2020.

Blackbaud initially reported that credit card information, financial account information, and Social Security numbers were not affected by the ransomware event; however, on September 29, 2020, Blackbaud notified N-YHS that its previous statement was incorrect and some such data was potentially affected by the incident. N-YHS immediately took steps and worked with Blackbaud to obtain additional information surrounding this data. On October 27, 2020, Blackbaud provided N-YHS with information that allowed the N-YHS team to determine what specific data was

potentially affected. N-YHS then worked diligently to identify those individuals and their appropriate contact information in order to provide notice of this incident. The information that could have been subject to unauthorized access includes name, address, and Social Security number.

Notice to New Hampshire Residents

Based on the additional information received from Blackbaud, on November 25, 2020, N-YHS will provide notice of this incident to the individuals identified following Blackbaud's September 29, 2020 notice, including approximately two (2) New Hampshire residents. Written notice is being provided on November 25, 2020 in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering the event, N-YHS moved quickly to investigate and respond to the incident, including working with Blackbaud to learn more about the incident and determine what N-YHS data may be involved. N-YHS then worked diligently to identify and notify those individual whose information may have been affected. N-YHS is also providing potentially impacted individuals with access to credit monitoring and identity services provided by Blackbaud through Cyberscout for two (2) years.

N-YHS is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including providing individuals with 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, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

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

MABB/smm

EXHIBIT A

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

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

October 5, 2020

VIA U.S. 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 New-York Historical Society ("N-YHS") located at 170 Central Park West, New York, New York 10024, and write to notify your office of an incident that may affect the security of some personal information relating to approximately three (3) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, N-YHS 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, N-YHS received notification from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident. 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. Blackbaud reported that data may have been accessed or exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, N-YHS immediately commenced an investigation to determine what, if any, sensitive N-YHS data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident, as well as undertake diligent efforts to assess what N-YHS data was present in the Blackbaud system. On or

about August 21, 2020, N-YHS received further information from Blackbaud that allowed it to determine the information potentially affected may have contained personal information. On September 11, 2020, after a thorough review process, N-YHS confirmed the population of potentially impacted individuals, which includes three (3) New Hampshire residents. The information that could have been subject to unauthorized access includes name, address, financial account information, and payment card information.

Notice to New Hampshire Residents

On or about October 5, 2020, N-YHS will provide written notice of this incident to affected individuals, which includes three (3) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, N-YHS moved quickly to investigate and respond to the incident, including working with Blackbaud to learn more about the incident and determine what N-YHS data may be involved. N-YHS then worked diligently to identify and notify those individual whose information may have been affected. N-YHS is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including providing individuals with 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, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

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

MABB/ken

EXHIBIT A

To the October 5, 2020 Notice of Data Event

NEW-YORK HISTORICAL SOCIETY
MUSEUM & LIBRARY

<<b2b_text_1(Extra2)>>
<<b2b_text_2(Extra5)>>
<<b2b_text_3(Extra6)>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

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

<<b2b_text_4(Extra1)>>

Dear <<b2b_Text_5(Extra3)>>:

New-York Historical Society ("N-YHS") writes to inform you of a recent incident that may affect the privacy of some of your information. On July 16, 2020, N-YHS received notification from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including N-YHS. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on N-YHS data. 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? 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. 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. Upon learning of the Blackbaud incident, N-YHS immediately commenced an investigation to determine what, if any, sensitive N-YHS data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On or about August 21, 2020, N-YHS received further information from Blackbaud that allowed it to determine the information potentially affected may have contained personal information. On September 11, 2020, after a thorough review process, N-YHS confirmed the population of potentially impacted individuals.

What information was Involved? Our investigation determined that the involved Blackbaud systems contained your name and <<b2b_Text_6(Extra4)>>. 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 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 state regulators, as required.

What Can You 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.

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-###-###-#### between the hours of 9:00 am and 6:30 pm Eastern Time. You may also write to New-York Historical Society at 170 Central Park West, New York, NY 10024.

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

Sincerely,

Matthew Bregman
Vice President for Development
New-York Historical Society

Steps You Can Take to Help Protect Your Information

Monitor Accounts

Under U.S. law you are entitled to one (1) free credit report annually from each of the three (3) 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 listed below 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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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 one (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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/ fraud-alerts	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); 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 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 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. 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 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 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 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 Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island residents impacted by this incident.

For District of Columbia residents, the District of Columbia Attorney General can be reached 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.

EXHIBIT B

NEW-YORK HISTORICAL SOCIETY
MUSEUM & LIBRARY

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

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

<<Date>>

<<Variable Heading>>

Dear <<Name 1>>:

New-York Historical Society ("N-YHS") writes to inform you of a recent incident that may affect the privacy of some of your information. N-YHS recently received a notification from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident that may have affected N-YHS information. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including N-YHS. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on N-YHS data. 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, 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. Blackbaud reported that certain data was acquired by the threat actor at some point before Blackbaud locked the threat actor out of the system on May 20, 2020.

Blackbaud initially reported that credit card information, financial account information, and Social Security numbers were not affected by the ransomware event; however, on September 29, 2020, Blackbaud notified us that its previous statement was incorrect and some such data was potentially affected by the incident. N-YHS immediately took steps and worked with Blackbaud to obtain additional information surrounding this data. On October 27, 2020, Blackbaud provided us with information that allowed us to determine what specific N-YHS data was potentially affected. We then worked diligently to identify those individuals and their appropriate contact information in order to provide notice of this incident.

What Information Was Involved? Our investigation determined that the involved Blackbaud systems contained your name and Social Security number. 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 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 state regulators, as required.

As an added precaution, we are also offering you complimentary access to twenty-four (24) months of credit monitoring and identity theft restoration services provided by Blackbaud, through CyberScout. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you. Please review the instructions contained in the attached *Steps You Can Take to Protect Your Information* for additional information on these services.

What Can You 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. You may also enroll to receive the identity protection services we are making available to you. There is no charge to you for this service; however, you will need to enroll yourself in this service.

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 855-914-4711 between the hours of 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday. You may also write to New-York Historical Society at 170 Central Park West, New York, NY 10024.

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

Sincerely,

Richard Shein
Chief Financial Officer
New-York Historical Society

Steps You Can Take to Protect Your Information

Complimentary Credit Monitoring Services

We are providing you with access to **Single Bureau Credit Monitoring** services at no charge. Services are for 24 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please navigate to [redacted] and, when prompted, please provide the following unique code to gain access to services: [redacted] Once registered, you can access Monitoring Services by selecting the "Use Now" link to fully authenticate your identity and activate your services. Please ensure you take this step to receive your alerts.

Monitor Accounts

Under U.S. law, you are entitled to one (1) free credit report annually from each of the three (3) 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 listed below 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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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 one (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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/ fraud-alerts	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); 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 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 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. 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 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 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 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 Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this incident.

For District of Columbia residents, the District of Columbia Attorney General can be reached 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.