MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Edward J. Finn
Office: (267) 930-4776
Fax: (267) 930-4771
Email: efinn@mullen.law

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

April 9, 2021

VIA FIRST-CLASS 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 American College of Emergency Physicians ("ACEP") located at 4950 W. Royal Lane, Irving, TX 75063-2524. ACEP writes to supplement its Notice of Data Event from November 17, 2020 to your office, which is attached as ***Exhibit A***. By providing this supplemental notice, ACEP 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 Additional Discovery

ACEP is a professional organization that not only provides services to its own members, customers, and/or donors, but also provides management services to other similar professional organization clients and their members, customers, and/or donors, including the Emergency Medicine Foundation ("EMF"), the Emergency Medicine Residents' Association ("EMRA") and the Society for Emergency Medicine Physician Assistants ("SEMPA") (collectively, "Related Organizations").

Since providing initial notice, ACEP's investigation into the event continued. During the course of the investigation, it was determined that credentials to ACEP's separate SQL database servers were stored on a server that was compromised by the unauthorized actor. While there is no evidence the SQL servers were subject to unauthorized access or acquisition, because it cannot be ruled out, ACEP notified the Related Organizations in an abundance of caution and offered to

provide notice to their impacted members, customers, and/or donors. The information was at risk between the dates of April 8, 2020 and September 21, 2020.

ACEP has since determined the SQL database servers contained information relating to twelve (12) New Hampshire residents. The information that could have been subject to unauthorized access now includes the member/customer/donor name, address, Social Security number, financial account information, date of birth, tax identification number, and a username or email address and hashed password. Most of the information impacted was limited to names and usernames/email addresses with hashed passwords. While ACEP has not determined any of the information in the SQL databases was accessed or taken, ACEP takes the security of the member, customer, and/or donor information in its possession seriously and is notifying those individuals and your office in an abundance of caution.

Notice to New Hampshire Residents

On or about April 8th, 2021 ACEP began providing written notice of this incident to potentially affected individuals, which includes twelve (12) New Hampshire residents. Written (and e-mail, where permitted) notice is being provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering the event, ACEP moved quickly to investigate and respond to the incident, assess the security of ACEP systems, and notify potentially affected individuals. While there is no evidence the SQL servers were subject to unauthorized access or acquisition, ACEP commenced a large-scale review of its SQL database servers containing this information. As an added precaution, ACEP is providing access to credit monitoring services for twelve (12) months, from TransUnion (through Epiq), to individuals whose Social Security number and/or tax identification number was potentially affected by this incident, at no cost to these individuals.

Additionally, ACEP is providing all potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals whose impacted information includes an email or online username and hashed password to promptly change their password/security question and answer, as well as any password/security question and answer that is the same or similar for other accounts. ACEP is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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. ACEP is notifying the credit reporting agencies and 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) 930-4776.

Very truly yours,

Edward J. Finn of
MULLEN COUGHLIN LLC

EJF/nsj

EXHIBIT A

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Edward J. Finn
Office: (267) 930-4776
Fax: (267) 930-4771
Email: efinn@mullen.law

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

November 17, 2020

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 American College of Emergency Physicians ("ACEP") located at 4950 W. Royal Lane, Irving, Texas 75063-2524, and write to notify your office of an incident that may affect the security of certain payment card information relating to ten (10) New Hampshire residents. By providing this notice, ACEP 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 September 7, 2020, ACEP discovered unusual activity on its e-commerce site. Upon discovery, ACEP commenced an immediate investigation that involved working with computer forensic specialists to determine the full scope of the activity. On September 24, 2020, the investigation confirmed that payment card information used for a subset of purchases on its e-commerce site between May 21, 2020 and September 22, 2020 was potentially subject to unauthorized acquisition. Once ACEP confirmed the scope of the incident, it took steps to identify which ACEP customers may have been impacted and identified address information so that notice could be provided. The information that could have been subject to unauthorized access includes their name, address, payment card account number, expiration date, card security code, and zip code.

Notice to New Hampshire Residents

On or about November 16, 2020 ACEP provided written notice of this incident to affected individuals, which includes ten (10) 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, ACEP moved quickly to investigate and respond to the incident, assess the security of ACEP systems, and notify potentially affected individuals. Specifically, ACEP disabled payment card transactions and rebuilt its e-commerce servers in a secure environment. ACEP also provided notice to the payment card brands, its payment card processor, and is notifying the impacted cardholders.

ACEP is advising the impacted individuals to remain vigilant for fraudulent charges or misuse by monitoring their payment card accounts and encouraging cardholders to promptly report unauthorized or suspicious activity to their bank, credit union, or credit card company. ACEP is providing individuals with information, generally, 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. ACEP is also notifying the consumer reporting agencies and other state 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) 930-4776.

Very truly yours,

Edward J. Finn of
MULLEN COUGHLIN LLC

EJF/nsj

EXHIBIT A

(To the November 17th, 2020 Submission)

American College of
Emergency Physicians®
ADVANCING EMERGENCY CARE
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

November 16, 2020

F9714-L01-0000001 T00017 P003 *********ALL FOR AADC 123
SAMPLE A SAMPLE, LICENSURES - L01 US
APT B
123 ANY ST
ANYTOWN, US 12345-6789

Re: Notice of Data [Extra1]

Dear Sample A Sample:

The American College of Emergency Physicians ("ACEP") writes to notify you of an incident that may affect the security of your payment card information. ACEP takes this incident very seriously and is providing you with details about the incident, our response, and steps you can take to better protect your payment card information, should you feel it appropriate to do so.

What Happened? On September 7, 2020, ACEP discovered unusual activity on its e-commerce site. Upon discovery, we commenced an immediate investigation that involved working with computer forensic specialists to determine the full scope of the activity. On September 24, 2020, the investigation confirmed that payment card information used for a subset of purchases on our e-commerce site between May 21, 2020 and September 22, 2020 was potentially subject to unauthorized acquisition. Once we confirmed the scope of the incident, we took steps to identify which ACEP customers may have been impacted and identified address information so that notice could be provided.

What Information Was Involved? Our investigation determined that your name, address, [Extra2] payment card account number, expiration date, card security code, and zip code may have been subject to unauthorized acquisition.

What ACEP is Doing. ACEP takes the security of your payment card information seriously. We note that it appears this incident only impacted a subset of pages in our e-commerce environment. Upon notice of the suspicious activity, we immediately disabled payment card transactions for the impacted pages. We rebuilt our e-commerce servers in a secure environment and notified our payment card processor to put the payment card brands on notice of the incident.

What You Can Do. We encourage you to remain vigilant for instances of fraudulent charges or misuse by monitoring your payment card accounts and reviewing the enclosed *Steps You Can Take to Protect Personal Information* for additional guidance on how to protect against payment card fraud from any source.

For More Information. If you have additional questions that are not addressed in this letter, please call our toll-free assistance hotline at (833) 796-8640, available between Monday through Friday, 8:00 a.m. and 10:00 p.m., Central Time and Saturday & Sunday, 10:00 a.m. and 7:00 p.m. Central Time. Be prepared to provide engagement # B006515 for assistance.

We sincerely regret any inconvenience this incident may cause you and we remain committed to safeguarding your information within our care.

Sincerely,

Leslie Moore

Leslie Patterson Moore
Chief Counsel and Chief Legal Officer
American College of Emergency Physicians ("ACEP")

Steps You Can Take To Protect Personal Information

Monitor Your Accounts

We encourage you to remain vigilant against incidents of payment card fraud or misuse, to review your payment card account statements, and to monitor your credit reports for suspicious activity. If you see any unauthorized or suspicious activity, promptly contact your bank, credit union, or credit card company.

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.

Place a Security Freeze

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.); and
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.

Place a Fraud Alert

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-alerts**	**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 the 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); or 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 District of Columbia residents, the Attorney General for the District of Columbia may be contacted at 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; (202) 727-3400; and https://oag.dc.gov. *For Maryland residents*, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 410-528-8663; and 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 1-919-716-6400; and www.ncdoj.gov. *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 a 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 Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; 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; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are fifteen (15) Rhode Island residents impacted by this incident.

MULLEN
COUGHLIN

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

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

EXHIBIT B

American College of Emergency Physicians
ADVANCING EMERGENCY CARE

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>>

Re: Notice of Data <<Extra 1>>

Dear <<Name 1>>:

The American College of Emergency Physicians ("ACEP") writes to notify you of an event that may affect some of your information. ACEP has your information and is notifying you because it not only provides professional organization services to its own members, but also provides management services to other similar professional organizations in the industry, including the Emergency Medicine Foundation ("EMF"), the Emergency Medicine Residents' Association ("EMRA") and the Society for Emergency Medicine Physician Assistants ("SEMPA"). You are receiving this notice because you are (or were) a member of, made a purchase from, or donated to, one or more of these entities.

While ACEP has no indication your information has been misused, ACEP takes this event very seriously and is sharing details about the event, our response, and steps you can take to better protect your information, should you feel it appropriate to do so.

What Happened? On September 7, 2020, ACEP discovered unusual activity on its systems. Upon discovery, we commenced an investigation to determine the full scope of the activity. During the course of the investigation, it was determined that credentials to ACEP's separate SQL database servers were stored on a server that was compromised by an unauthorized actor. While there is no evidence the SQL servers were subject to unauthorized access or acquisition, because it cannot be ruled out, ACEP notified its partners in an abundance of caution and is providing this notice to you. The information was at risk between the dates of April 8, 2020 and September 21, 2020.

What Information Was Involved? A review of our SQL database servers indicated that your name, <<Notice Data Elements>> were stored on an ACEP SQL server at the time of the incident. Again, we have not determined that your information was viewed or taken but are providing this notice out of an abundance of caution because the information was accessible during the time of the incident.

What ACEP is Doing. ACEP takes the security of member and customer information seriously. Upon notice of the potential for unauthorized activity, we commenced an investigation, rebuilt the impacted server, changed passwords, and implemented additional technical safeguards.

ACEP has also secured the services of Epiq to provide you with credit monitoring and identity restoration services for twelve (12) months, at no cost to you. More information on how to take advantage of these services can be found in the enclosed *Steps You Can Take to Protect Personal Information.*

What You Can Do. We encourage you to remain vigilant for instances of fraud or misuse of your information from any source and to review the enclosed *Steps You Can Take to Protect Personal Information* for the resources you can take advantage of to better protect your information, should you feel it appropriate to do so. **If your impacted information includes an email or online username, password, and/or security question and answer, you should promptly change your password/security question and answer, as well as any password/security question and answer that is the same or similar for other accounts.**

For More Information. If you have additional questions that are not addressed in this letter, please call our toll-free assistance hotline at 877-792-0488, available between Monday through Friday, 8:00 a.m. and 8:00 p.m., Central Time.

We sincerely regret any inconvenience this event may cause you and we remain committed to safeguarding the information within our care.

Sincerely,

Leslie Patterson Moore, J.D.

Leslie Patterson Moore, J.D.
General Counsel and Chief Legal Officer
American College of Emergency Physicians ("ACEP")

Steps You Can Take to Protect Personal Information

Enroll in Credit Monitoring and Utilize Identity Restoration, if Necessary
As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for twelve (12) months 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 *my*TrueIdentity 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 TWELVE (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 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/credit-report-services/	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 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. ACEP is located at 4950 W. Royal Lane, Irving, TX 75063-2524.

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 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 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 North Carolina 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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 613 Rhode Island residents impacted by this incident.