Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

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

May 23, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent The Peddie School ("Peddie") located at 201 S Main St, Hightstown, NJ 08520, and are writing to notify your office of an incident that may affect the security of certain personal information relating to fifteen (15) Maryland 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, Peddie does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On December 22, 2023, Peddie discovered suspicious activity in its computer network and determined that certain systems were encrypted and inaccessible. Peddie immediately commenced an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the unauthorized activity. Peddie also worked to securely restore impacted system operations. The investigation found that Peddie systems were accessed by an unknown actor between October 30, 2023, and December 22, 2023, and during this time certain files were copied.

In general, Peddie stores sensitive data off network with third-party providers and the investigation did not identify any evidence of lateral movement outside of the Peddie environment. Furthermore, the initial investigation did not reveal any evidence of access to sensitive data on Peddie's network. Out of an abundance of caution Peddie reviewed the involved Peddie systems further for personal information and in late February the investigation determined that certain personal information may have been stored on the systems outside of the ordinary course of business. Therefore, Peddie engaged in further review of the systems to determine what specific information could have been present at the time of the event. Although this review is ongoing, the initial review concluded on April 21, 2024. Peddie then took steps to further validate and enrich the data for purpose of providing notice.

Peddie's investigation determined that the involved systems may have contained personal information as defined by Maryland law including name, Social Security number, and taxpayer identification number.

Notice to Maryland Residents

On or about May 23, 2024, Peddie provided written notice of this incident to fifteen (15) Maryland 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, Peddie moved quickly to investigate and respond to the incident, assess the security of Peddie systems, and identify potentially affected individuals. Peddie also notified federal law enforcement regarding the event. Peddie has implemented additional technical safeguards and is revising its policies and procedures related to the handling of data. Peddie is providing access to credit monitoring services for one (1) year through Experian to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Peddie is providing individuals with guidance on how to better protect against identity theft and fraud. Peddie is 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.

Peddie is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,

Sian M Schafle

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/cml
Enclosure

EXHIBIT A

PEDDIE
201 SOUTH MAIN STREET
HIGHTSTOWN, NJ 08520
(609) 944-7500
PEDDIE.ORG

Return Mail Processing
PO Box 999
Suwanee, GA 30024

1 1 1 ********************AUTO**MIXED AADC 300
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

May 23, 2024

[Extra1]

Dear Sample A. Sample:

The Peddie School is committed to protecting the privacy of its community. As part of this commitment, we are writing to inform you of an incident that may involve some of your information. Below is information concerning the incident along with some resources that can help you protect against the possibility of misuse of your information.

What Happened?

We became aware of suspicious activity involving our computer network and immediately began an investigation. The investigation determined that Peddie's systems were accessed by an unknown actor between October 30, 2023 and December 22, 2023, and during this time certain files were copied. We reviewed the systems to identify their contents and to determine if they contain information belonging to individuals. On April 21, 2024, we completed our initial review.

What Information Was Involved?

The information identified in the involved systems includes your name and Social Security number or taxpayer identification number.

What We Are Doing?

Peddie takes this incident and the security of the information in our care very seriously. Upon discovering the incident, we took steps to assess and secure our network and we worked with third-party cybersecurity specialists to determine what happened. We also reported the incident to the Federal Bureau of Investigation.

Peddie also has implemented additional security measures within the network and is reviewing and revising its policies and procedures to reduce the risk of a similar incident occurring in the future.

As an added precaution, Peddie is offering you access to credit monitoring services for [Extra2] months at no cost. Information on the credit monitoring services and instructions on how to activate it may be found in the attachment to this letter. Please note, due to privacy restrictions, we are unable to automatically enroll you in the complimentary monitoring services.

What You Can Do?

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. Please also review the information contained in the enclosed *Steps You Can Take to Protect Personal Information*.

For More Information

If you have additional questions or concerns, please contact us at 833-918-1723 Monday through Friday from 8am to 8pm Central Time, excluding major U.S. holidays. Be prepared to provide engagement number [Engagement Number]. You may also write to Peddie at 201 S Main St, Hightstown, NJ 08520.

Sincerely,

Sanjeev Puri
Assistant Head of Finance and Operations

Steps You Can Take To Protect Personal Information

<u>Enroll in Monitoring Services</u>

To help protect your identity, we are offering a complimentary [Extra1]-month membership of Experian's IdentityWorks^{SM}. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **August 30, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-918-1723 by **August 30, 2024.** Be prepared to provide engagement number **[Engagement Number]** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your [Extra1]-month Experian IdentityWorks Membership

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

[1]Offline members will be eligible to call for additional reports quarterly after enrolling.
[2]The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 one-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a fraud alert or a 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
1-888-298-0045	1-888-397-3742	1-800-916-8800
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

As a best practice, consumers should change all passwords to their personal accounts on a regular basis, use strong passwords, and refrain from using the same password for multiple accounts. Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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, individuals have the right to obtain any police report filed in regard to this event. There are approximately 6 Rhode Island residents that may be impacted by this event.

Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

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

March 25, 2025

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent The Peddie School ("Peddie") located at 201 S Main St, Hightstown, NJ 08520. We are supplementing Peddie's previous notice to your office on May 23, 2024 and July 5, 2024. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Peddie does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

As detailed in our prior notice to your office, Peddie began providing written notice of this event to fifteen (15) Maryland residents on May 23, 2024. Subsequently, as additional information became available, Peddie provided written notice to an additional one (1) Maryland resident on July 5, 2024. Peddie's review of the potentially at-risk data was completed on December 24, 2024, and Peddie thereafter worked to validate the data and identify and confirm contact information to notify the remaining population.

On or about March 25, 2025, Peddie provided written notice of this event to forty-three (43) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Peddie also provided substitute notice in accordance with relevant state laws.

Peddie's investigation determined that the involved systems may have contained personal information as defined by Maryland law including name, Social Security number or individual taxpayer identification number, driver's license or state identification number, passport number, US military or other government-issued identification number, health insurance information, medical information.

Contact Information

Should you have any questions regarding this notification or other aspects of the event, please contact us at (267) 930-4799.

Very truly yours,

Sian M Schafle

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/azd
Enclosure

EXHIBIT A

PEDDIE

Return Mail Processing
PO Box 999
Suwanee, GA 30024

20 1 4248 ************************************SNGLP
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

March 25, 2025

[Extra1]

Dear Sample A. Sample:

The Peddie School ("Peddie") is committed to protecting the privacy of its community. As part of this commitment, we are writing to inform you of an incident that may involve some of your information. Below is information concerning the incident along with some resources that can help you protect against the possibility of misuse of your information.

What Happened?

We became aware of suspicious activity involving our computer network and immediately began an investigation. The investigation determined that Peddie's systems were accessed by an unknown actor between October 30, 2023 and December 22, 2023, and during this time certain files were copied. We reviewed the systems to identify their contents and to determine if they contain information belonging to individuals. This comprehensive review was completed on or around December 24, 2024. Upon completion of the review, Peddie worked to provide notice to potentially impacted individuals as quickly as possible.

What Information Was Involved?

The information identified in the involved systems includes your [Extra2] and name.

What We Are Doing.

Peddie takes this incident and the security of the information in our care very seriously. Upon learning of the suspicious activity, we took steps to assess and secure our network and we worked with third-party cybersecurity specialists to determine what happened. We notified individuals as information became available. We also reported the incident to the Federal Bureau of Investigation.

Peddie has implemented additional security measures within the network and completed a review of our policies and procedures to mitigate reoccurrence of this type of incident.

As an added precaution, Peddie is offering you access to credit monitoring services for [Extra3] months at no cost. Information on the credit monitoring services and instructions on how to activate it may be found in the attachment to this letter. Please note, due to privacy restrictions, we are unable to automatically enroll you in the complimentary monitoring services.

What You Can Do.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. Please also review the information contained in the enclosed *Steps You Can Take to Protect Personal Information*.

For More Information

If you have additional questions or concerns, please contact us at 1-833-918-9466 Monday through Friday from 9am to 9pm Eastern Time, excluding major U.S. holidays. Be prepared to provide engagement number [Engagement Number]. You may also write to Peddie at 201 S Main St, Hightstown, NJ 08520.

Sincerely,

Sanjeev Puri
Assistant Head of Finance and Operations

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

To help protect your identity, we are offering a complimentary [Extra3]-month membership of Experian's IdentityWorks^{SM}. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **June 30, 2025** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-9466 by **June 30, 2025.** Be prepared to provide engagement number **[Engagement Number]** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your [Extra3]-month Experian IdentityWorks Membership

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.
[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 one-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a fraud alert or a 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/get-credit-report https://www.transunion.com/credit-freeze https://www.transunion.com/fraud-alerts
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, P.O. Box 160, Woodlyn, PA 19094

Additional Information

As a best practice, consumers should change all passwords to their personal accounts on a regular basis, use strong passwords, and refrain from using the same password for multiple accounts. Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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, individuals have the right to obtain any police report filed in regard to this event. There are approximately 8 Rhode Island residents that may be impacted by this event.