JOHN F. WEAVER
Direct Dial: 781.904.2685
Email: john.weaver@mclane.com
Admitted in MA and NH
900 Elm Street, P.O. Box 326
Manchester, NH 03105-0326
T 603.625.6464
F 603.625.5650

MCLANE MIDDLETON

July 23, 2021

Office of the Attorney General
State of New Hampshire
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03302

Re: Data Security Breach

To whom it may concern,

McLane Middleton, P.A. represents Electronic Environments Co. LLC ("EEC" or "Company"), which is located at 410 Forest Street, Marlborough, MA 01752. We are writing to inform you about a data security breach that affects 43 individuals who are residents of New Hampshire.

What Happened: EEC experienced a ransomware event that occurred between May 10 and May 11, 2021. The Company's advanced threat detection system alerted the Company to the situation and the Company promptly shut down the network as the IT team assessed how to safely restore the affected servers. In response to the security incident, EEC contacted law enforcement and hired outside computer forensic experts to investigate and help determine how the incident occurred and what data, if any, was affected.

Out of an abundance of caution, the Company informed all employees about the ransomware event and the ongoing investigation on June 11, 2021. On June 22, 2021, the Company received preliminary information from their forensic expert that files containing information about some of the Company's current and former employees and their dependents may have been compromised in the incident. The Company thereafter confirmed that this group of affected individuals may include 43 New Hampshire residents.

What Information Was Involved: The files that EEC believes may have been compromised contained the following types of information about some of the Company's current and former employees and their dependents: name; address; telephone number; email address; full dates of birth of employee and dependent(s); driver's license number of employee; certain medical information; health insurance information, including policy numbers; Health Savings Account numbers; and social security numbers of employee and dependent(s). While there is no indication to date that this information has been used for fraudulent or unlawful purposes, the Company has taken the following measures to address this matter.

What EEC Is Doing: In addition to sending the enclosed notification to affected individuals on July 8, 2021, and addressing any questions or concerns they have, the Company is providing affected individuals with a free, two-year membership in an Experian identity theft and fraud prevention program. The Company has also taken measures to ensure that this type of incident does not reoccur. For example, the Company is increasing its users' password requirements, moving parts of its IT infrastructure to a protected cloud environment, and evaluating further technical monitoring options. The Company will continue to work with its outside forensic expert and cybersecurity attorney to ensure that the Company has taken all additional reasonable and appropriate measures designed to safeguard the confidentiality of its employees' and their dependents' information.

Thank you for your attention to this matter. Please contact us if you have any questions or we can be of any assistance with this matter.

Very truly yours,

John F. Weaver

cc: Electronic Environments Co. LLC

Electronic Environments
Infrastructure Solutions

Return Mail Processing
PO Box 999
Suwanee, GA 30024

4 1 904 **********AUTO**ALL FOR AADC 015
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

July 8, 2021

Re: Notice of Data Breach

Dear Sample A. Sample:

We are writing to inform you about a data security breach experienced by Electronic Environments Co. LLC ("EEC" or "Company") affecting some of our current and former employees and their dependents. We are notifying you because the incident may have involved personally identifiable information ("PII"), in the form of social security numbers and driver's license numbers. While we are not aware of any improper use of your PII, we are nonetheless notifying you of the incident and providing you and your dependents with two years of complimentary Experian IdentityWorks identity and credit protection services. We encourage you to review this letter, promptly enroll in the IdentityWorks program, and call 508-229-1431 or send an email to HRInfo@eecnet.com if you have any questions about this matter.

What Happened? EEC experienced a ransomware event that occurred between May 10 and May 11, 2021. The Company's advanced threat detection system alerted us to the situation and we promptly shut down our network as our IT team assessed how to safely restore the affected servers. In response to the security incident, EEC contacted law enforcement and hired outside computer forensic experts to investigate and help determine how the incident occurred and what data, if any, was affected.

On June 11, 2021, the Company informed all of our employees about the ransomware event and the ongoing investigation. Based on the results of the forensic investigation, EEC believes that files containing information about some of our employees and their dependents may have been compromised in the incident. Please note that the Company is not aware of any actual misuse of your PII. Nonetheless, because we value your privacy and security, we are offering and encouraging you to enroll yourself and your dependents in the identity and credit protection services described below.

What Information Was Affected? The files that EEC believes may have been compromised contained the following types of information about some of our current and former employees and their dependents: name; address; telephone number; email address; full dates of birth of employee and dependent(s); driver's license number of employee; certain medical information;

health insurance information, including policy numbers; Health Savings Account numbers; and social security numbers of employee and dependent(s).

What Should You Do? Protecting yourself and your family's credit and identity is important, no matter whether you know that you have been affected by a security incident or not. An identity and credit protection program is one of the tools you can and should use to do so.

EEC is offering you and your dependents complimentary two-year memberships in Experian's IdentityWorks program. This program affords you and your dependents both identity and credit monitoring as well as services to resolve any identity or credit fraud that may occur. To activate your memberships please follow these steps:

- Enroll by **January 31, 2022**. Your code will not work after that date.
- Visit the Experian IdentityWorks website: https://www.experianidworks.com/credit
- Provide the information requested and the following activation code:

If you have questions about this service, or need assistance with identity or credit fraud restoration, please contact Experian at (877) 890-9332 by no later than **January 31, 2022**. Please be prepared to provide Engagement Number as proof of eligibility for the IdentityWorks identity and credit monitoring and restoration services.

You will not need to provide a credit card to enroll in Experian IdentityWorks. You can contact Experian ***immediately*** to enroll or discuss any identity or credit fraud issues, and you will have access to the following features once you enroll in 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 specialists 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.
- **$1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

EEC strongly encourages you to promptly use the foregoing information to enroll yourself and your dependents in these credit identity protection services.

What Else Could You Do? In addition to enrolling in IdentityWorks, we also encourage you to review the information in the below "*Steps You Can Take To Help Protect Your Information.*"

---

[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.

To the extent you feel that any such measures are necessary to protect your identity or credit, we encourage you take them.

We are cooperating with law enforcement regarding this matter. Under certain state laws, you may have a right to obtain a copy of such a report, if any exists. Also, if you feel that you have experienced identity or credit fraud or otherwise want to contact law enforcement about this matter, we encourage you to contact your state or local police department.

What Is EEC Doing? In addition to providing complimentary identity and credit protection services, EEC has taken measures to ensure that this type of incident does not reoccur. For example, the Company is increasing its users' password requirements, moving parts of its IT infrastructure to a protected cloud environment, and evaluating further technical monitoring options. The Company is working with its outside forensic expert and cybersecurity attorney to ensure that we have taken all additional reasonable and appropriate measures designed to safeguard the confidentiality of your information.

For More Information. If you have any questions, please call 508-229-1431 or send an email to HRInfo@eecnet.com. We apologize for any concern or inconvenience this situation may cause, and thank you for your continued service and loyalty to EEC.

Sincerely,

James Lundrigan

James Lundrigan,
President and CEO

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Accounts

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

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**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 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 19016	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-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. **Colorado Residents:** You can obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes using the contact information provided above. **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. You may contact the Maryland Attorney General's Office and the Federal Trade Commission to obtain information about preventing identity theft. **Massachusetts Residents:** Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. **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. You can 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. **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/. **North Carolina Residents:** Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC). You may contact the North Carolina Attorney General's Office and the Federal Trade Commission to obtain information about preventing identity theft. **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. You may report suspected identity theft to law enforcement, including the Attorney General and Federal Trade Commission. **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 23 Rhode Island residents impacted by this incident. **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Return Mail Processing
PO Box 999
Suwanee, GA 30024

41 903 **********AUTO**ALL FOR AADC 015
SAMPLE A. SAMPLE - L02
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

July 8, 2021

Re: Notice of Data Breach

Dear Sample A. Sample:

We are writing to inform you about a data security breach experienced by Electronic Environments Co. LLC ("EEC" or "Company") affecting some of our current and former employees and their dependents. We are notifying you because the incident may have involved personally identifiable information ("PII"), in the form of social security numbers and driver's license numbers. While we are not aware of any improper use of your PII, we are nonetheless notifying you of the incident and providing you with two years of complimentary Experian IdentityWorks identity and credit protection services. We encourage you to review this letter, promptly enroll in the IdentityWorks program, and call 508-229-1431 or send an email to HRInfo@eecnet.com if you have any questions about this matter.

What Happened? EEC experienced a ransomware event that occurred between May 10 and May 11, 2021. The Company's advanced threat detection system alerted us to the situation and we promptly shut down our network as our IT team assessed how to safely restore the affected servers. In response to the security incident, EEC contacted law enforcement and hired outside computer forensic experts to investigate and help determine how the incident occurred and what data, if any, was affected.

On June 11, 2021, the Company informed all of our employees about the ransomware event and the ongoing investigation. Based on the results of the forensic investigation, EEC believes that files containing information about some of our employees and their dependents may have been compromised in the incident. Please note that the Company is not aware of any actual misuse of your PII. Nonetheless, because we value your privacy and security, we are offering and encouraging you to enroll yourself in the identity and credit protection services described below.

What Information Was Affected? The files that EEC believes may have been compromised contained the following types of information about some of our current and former employees and their dependents: name; address; telephone number; email address; full dates of birth of employee and dependent(s); driver's license number of employee; certain medical information; health insurance information, including policy numbers; Health Savings Account numbers; and social security numbers of employee and dependent(s).

What Should You Do? Protecting your credit and identity is important, no matter whether you know that you have been affected by a security incident or not. An identity and credit protection program is one of the tools you can and should use to do so.

EEC is offering you a complimentary two-year membership in Experian's IdentityWorks program. This program affords you both identity and credit monitoring as well as services to resolve any identity or credit fraud that may occur. To activate your memberships please follow these steps:

- Enroll by **January 31, 2022**. Your code will not work after that date.
- Visit the Experian IdentityWorks website: https://www.experianidworks.com/credit
- Provide the information requested and the following activation code:

If you have questions about this service, or need assistance with identity or credit fraud restoration, please contact Experian at (877) 890-9332 by no later than **January 31, 2022**. Please be prepared to provide Engagement Number as proof of eligibility for the IdentityWorks identity and credit monitoring and restoration services.

You will not need to provide a credit card to enroll in Experian IdentityWorks. You can contact Experian ***immediately*** to enroll or discuss any identity or credit fraud issues, and you will have access to the following features once you enroll in 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 specialists 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.
- **$1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

EEC strongly encourages you to promptly use the foregoing information to enroll yourself in these credit identity protection services.

What Else Could You Do? In addition to enrolling in IdentityWorks, we also encourage you to review the information in the below "*Steps You Can Take To Help Protect Your Information.*" To the extent you feel that any such measures are necessary to protect your identity or credit, we encourage you take them.

---

[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.

We are cooperating with law enforcement regarding this matter. Under certain state laws, you may have a right to obtain a copy of such a report, if any exists. Also, if you feel that you have experienced identity or credit fraud or otherwise want to contact law enforcement about this matter, we encourage you to contact your state or local police department.

What Is EEC Doing? In addition to providing complimentary identity and credit protection services, EEC has taken measures to ensure that this type of incident does not reoccur. For example, the Company is increasing its users' password requirements, moving parts of its IT infrastructure to a protected cloud environment, and evaluating further technical monitoring options. The Company is working with its outside forensic expert and cybersecurity attorney to ensure that we have taken all additional reasonable and appropriate measures designed to safeguard the confidentiality of your information.

For More Information. If you have any questions, please call 508-229-1431 or send an email to HRInfo@eecnet.com. We apologize for any concern or inconvenience this situation may cause, and thank you for your continued service and loyalty to EEC.

Sincerely,

James Lundrigan

James Lundrigan,
President and CEO

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Accounts

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

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**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 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 19016	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-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. **Colorado Residents:** You can obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes using the contact information provided above. **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. You may contact the Maryland Attorney General's Office and the Federal Trade Commission to obtain information about preventing identity theft. **Massachusetts Residents:** Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. **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. You can 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. **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/. **North Carolina Residents:** Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC). You may contact the North Carolina Attorney General's Office and the Federal Trade Commission to obtain information about preventing identity theft. **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. You may report suspected identity theft to law enforcement, including the Attorney General and Federal Trade Commission. **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 23 Rhode Island residents impacted by this incident. **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.