DAY PITNEY LLP

Boston | Connecticut | Florida | New Jersey | New York | Providence | Washington, DC

WILLIAM J. ROBERTS
Attorney at Law

Goodwin Square
225 Asylum Street
Hartford, Connecticut 06103
T: (860) 275-0184 F: (860) 881-2431
wroberts@daypitney.com

September 23, 2025

VIA EMAIL (DOJ-CPB@doj.nh.gov)

Office of the Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Notice of Security Breach - All States Materials Group

Dear Office of the Attorney General:

Pursuant to N.H. Rev. Stat. Ann. § 359-C:20, Day Pitney LLP, as acting counsel, is providing notice on behalf of its client, All States Materials Group, Inc. ("ASMG"), of a breach of the security of its computer systems which may have affected the personal information of forty-four (44) New Hampshire residents.

On the morning of August 25, 2025, ASMG identified suspicious activity within its network. ASMG's internal IT team immediately isolated affected systems and engaged its independent cybersecurity vendor, Blue Mantis, to investigate and contain the activity. The investigation determined that a cybercriminal gained unauthorized access to limited portions of ASMG's computer systems beginning on August 22, 2025. The malicious activity was contained by 11:00 AM on August 25, 2025. The cybercriminal has been identified as the "Play" ransomware group.

The investigation revealed that the cybercriminal's access was limited to certain file directories containing employee and vendor related information. The cybercriminal did not gain access to ASMG's email system, Microsoft Teams, or ERP system (which housed the bulk of ASMG's human resources, operational, and financial information). Because Blue Mantis was unable to determine with certainty which files in the affected directories were in fact accessed, ASMG is, out of an abundance of caution, notifying all individuals and vendors with identifiable information in the file directories.

The New Hampshire residents affected by this incident included employees and vendors of ASMG, who we believe used their personal Social Security number as a tax ID. The information of these individuals affected by this incident is name, Social Security number, bank account numbers, medical information, and contact information. There is no evidence at this time that the data has been misused.

ASMG has since implemented a range of additional security measures, including:

- Deployment of a 24/7 Security Operations Center monitoring solution;
- Review and strengthening of firewall configurations and M365 security settings; and
- Engagement of third-party cybersecurity experts to conduct ongoing testing and review of ASMG's IT infrastructure.

ASMG is notifying all affected individuals directly and is offering 24 months of complimentary identity theft protection services, including credit monitoring and recovery services, through IDX, a ZeroFox company. Template copies of the notices provided to the New Hampshire residents are attached.

Please let me know if the Attorney General's Office has any questions or requires additional information.

Sincerely,

William J. Roberts

All States Materials Group®

Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: December 23, 2025

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

September 23, 2025

RE: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

We recently discovered that All States Materials Group ("ASMG," "we," "us") was the victim of a cyberattack that may have involved a small amount of the information we hold about you. While we have no evidence that your specific information was in fact viewed or used by an unauthorized party, we are, nonetheless, writing to explain what happened, how we have responded, and what you can do to protect your information.

1. **Here is What Happened:**

During the early morning of August 25, 2025, ASMG identified suspicious behavior indicating unauthorized activity was occurring on our network. ASMG immediately contacted Blue Mantis, ASMG's independent cybersecurity investigation and recovery vendor, to provide assistance. Blue Mantis was able to quickly secure our servers from further unauthorized activity and then began an independent cybersecurity analysis to determine what had occurred.

Blue Mantis's investigation determined that the cyberattack began during the evening of August 22, 2025, when the cybercriminal leveraged a vulnerability to gain access to certain portions of our computer systems. Blue Mantis's investigation further revealed that the cyberattack ended at approximately 11:00AM on August 25, 2025 (only mere hours after discovery), when Blue Mantis confirmed ASMG had successfully isolated all compromised servers, and there was no evidence of further malicious activity. According to Blue Mantis's investigation, the cybercriminal was able to gain access to certain file directories maintained on our network. Fortunately, the cybercriminal did not gain access to ASMG's email system, Microsoft Teams, or our ERP system.

2. **How We Responded:**

Once Blue Mantis had concluded its investigation and determined the scope of the cybercriminal's potential access to our files, we reviewed the affected file directories for inclusion of identifiable information. Regrettably, on September 5, 2025, we learned that a small number of the directory files potentially accessed by the cybercriminal contained such information.

We are notifying relevant state authorities of this cyberattack. Further, while no business can be 100% secure, ASMG has implemented a series of security hardening measures, including the use of a fully monitored 24/7 SOC security solution, reviewing and updating security configurations on all firewalls and having a full review of M365 security settings performed by an outside firm. ASMG will continue to review all access controls, internal policies, security practices and IT infrastructure configurations in a campaign to improve IT security and to that end has engaged with 3rd party security

experts to perform ongoing reviews and testing of all IT infrastructure to ensure continued protection and adherence to industry best practices.

3. **Types of Information Involved:**

Based upon Blue Mantis's investigation, the cybercriminal's potential access to identifiable data included certain files containing vendor account information. While the types of information affected will vary by vendor, the information maintained in the affected files generally included the following: vendor name, bank account information, Social Security number, and contact information.

4. **Protection of Your Information:**

We are providing written notice to all vendors that we have identified as having information potentially affected by this incident. We encourage vendors to monitor bank account activity closely, notify your bank of any suspect or unusual activity, and be aware of scams. Importantly, ASMG has not changed its bank account information or its payment processes.

We are also making available a variety of support services at no cost or expense. Included with this notice is a "Reference Guide", which provides useful information regarding how to protect your identity, including obtaining copies of your credit report and implementing credit freezes. We encourage you to review the Reference Guide closely.

In addition, we are offering you twenty-four (24) months of identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan® monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-788-9712, going to https://app.idx.us/account-creation/protect, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6am - 6pm Pacific Time. Please note the deadline to enroll is December 23, 2025.

5. **For more information:**

ASMG takes its obligation to protect the privacy and confidentiality of our vendor information very seriously and we deeply regret that this breach occurred. If you have any questions, you may contact IDX or Lisa Marden (Office Manager for West Springfield) by phone at 413-665-7021 x1001.

Sincerely,

Seth Hankowski
Chief Executive Officer

Reference Guide

Review Your Account Statements. We encourage you to remain vigilant by reviewing your account statements. If you believe there is an unauthorized charge on your card, please contact your financial institution or card issuer immediately. The payment card brands' policies provide that cardholders have zero liability for unauthorized charges that are reported in a timely manner. Please contact your card brand or issuing bank for more information about the policy that applies to you.

Order A Free Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and about fraud alerts and security freezes:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 2002 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

Equifax	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	1-800-349-9960	www.equifax.com/personal/credit-report-services/
Experian	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/freeze/center.html
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-888-909-8872	www.transunion.com/credit-freeze

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)
- Social Security Card, pay stub, or W2
- 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.

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.marylandattorneygeneral.gov

For Massachusetts Residents. 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. You may also place a security freeze on your credit reports, free of charge. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
https://ag.ny.gov

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/resources/individuals/consumer-issues/technology

For North Carolina Residents.

You can also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (Toll-free within North Carolina)
919-716-6000
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to law enforcement and the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401)-274-4400
www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
(202)-727-3400
www.oag.dc.gov

All States Materials Group®

Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: December 23, 2025

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

September 23, 2025

RE: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

We recently discovered that All States Materials Group ("ASMG," "we," "us") was the victim of a cyberattack that may have involved a small amount of the personal information we hold about you. While we have no evidence that your specific personal information was in fact viewed or used by an unauthorized party, we are, nonetheless, writing to explain what happened, how we have responded, and what you can do to protect your personal information.

1. **Here is What Happened:**

During the early morning of August 25, 2025, ASMG identified suspicious behavior indicating unauthorized activity was occurring on our network. ASMG immediately contacted Blue Mantis, ASMG's independent cybersecurity investigation and recovery vendor, to provide assistance. Blue Mantis was able to quickly secure our servers from further unauthorized activity and then began an independent cybersecurity analysis to determine what had occurred.

Blue Mantis's investigation determined that the cyberattack began during the evening of August 22, 2025, when the cybercriminal leveraged a vulnerability to gain access to certain portions of our computer systems. Blue Mantis's investigation further revealed that the cyberattack ended at approximately 11:00AM on August 25, 2025 (only mere hours after discovery), when Blue Mantis confirmed ASMG had successfully isolated all compromised servers, and there was no evidence of further malicious activity. According to Blue Mantis's investigation, the cybercriminal was able to gain access to certain file directories maintained on our network. Fortunately, the cybercriminal did not gain access to ASMG's email system, Microsoft Teams, or the Viewpoint/Vista system.

2. **How We Responded:**

Once Blue Mantis had concluded its investigation and determined the scope of the cybercriminal's potential access to our files, we reviewed the affected file directories for inclusion of personally identifiable information. Regrettably, on September 5, 2025, we learned that a small number of the directory files potentially accessed by the cybercriminal contained personal information.

We are notifying relevant state authorities of this cyberattack. Further, while no business can be 100% secure, ASMG has implemented a series of security hardening measures, including the use of a fully monitored 24/7 SOC security solution, reviewing and updating security configurations on all firewalls and having a full review of M365 security settings performed by an outside firm. ASMG will continue to review all access controls, internal policies, security practices and IT infrastructure configurations in a campaign to improve IT security and to that end has engaged with 3rd party security

experts to perform ongoing reviews and testing of all IT infrastructure to ensure continued protection and adherence to industry best practices.

3. **Types of Information Involved:**

Based upon Blue Mantis's investigation, the cybercriminal's potential access to identifiable data was limited to certain files containing payroll and other employment-related information. While the types of information affected will vary by person, the personal information maintained in the affected files generally included the following: names, Social Security Numbers, bank account numbers, home address and contact information, and certain safety and medical information.

4. **Protection of Your Information:**

We are providing written notice to all individuals that we have identified as having information potentially affected by this incident. Included with this notice is a "Reference Guide", which provides useful information regarding how to protect your identity, including obtaining copies of your credit report and implementing credit freezes. We encourage you to review the Reference Guide closely.

In addition, we are offering you twenty-four (24) months of identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan® monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-788-9712, going to https://app.idx.us/account-creation/protect, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6am - 6pm Pacific Time. Please note the deadline to enroll is December 23, 2025.

5. **For More Information:**

ASMG takes its obligation to protect the privacy and confidentiality of our employees' personal information very seriously and we deeply regret that this breach occurred. If you have any questions, you may contact IDX or Lisa Marden (Office Manager for West Springfield) by phone at 413-665-7021 x1001.

Sincerely,

Seth Hankowski
Chief Executive Officer

Reference Guide

Review Your Account Statements. We encourage you to remain vigilant by reviewing your account statements. If you believe there is an unauthorized charge on your card, please contact your financial institution or card issuer immediately. The payment card brands' policies provide that cardholders have zero liability for unauthorized charges that are reported in a timely manner. Please contact your card brand or issuing bank for more information about the policy that applies to you.

Order A Free Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and about fraud alerts and security freezes:

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided

below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 2002 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

Equifax	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	1-800-349-9960	www.equifax.com/personal/credit-report-services/
Experian	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/freeze/center.html
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-888-909-8872	www.transunion.com/credit-freeze

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)
- Social Security Card, pay stub, or W2
- 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.

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.marylandattorneygeneral.gov

For Massachusetts Residents. 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. You may also place a security freeze on your credit reports, free of charge. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
https://ag.ny.gov

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/resources/individuals/consumer-issues/technology

For North Carolina Residents. You can also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (Toll-free within North Carolina)
919-716-6000
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to law enforcement and the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401)-274-4400
www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
(202)-727-3400
www.oag.dc.gov