Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

January 2, 2025

Via Email: Idtheft@oag.state.md.us

Maryland Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Security Incident

Dear Office of the Attorney General:

Wilson Elser Moskowitz Edelman and Dicker, LLP ("Wilson Elser") represents Excelsior Orthopaedics, LLP ("Excelsior"), a healthcare company that specializes in orthopaedic treatment located at 3925 Sheridan Drive, Amherst, NY 14226, and Buffalo Surgery Center ("BSC"), a healthcare company located at 3921 Sheridan Drive, Amherst, NY 14226. Excelsior discovered a data security incident on June 23, 2024 (hereinafter, the "incident"). Excelsior takes the security and privacy of the information within its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that Excelsior and BSC have taken in response to the incident. We have also enclosed hereto a sample of the notices mailed to impacted individuals. Each notification letter includes an offer of free credit monitoring services.

1. Nature of the Incident

On June 23, 2024, Excelsior detected unusual activity on its network and discovered that it was the victim of a data security incident. Upon discovery of this incident, Excelsior immediately took steps to contain the intrusion and engage a specialized third-party cybersecurity firm to help secure the environment and conduct a comprehensive forensic investigation into the nature and scope of the incident. Initial results of the forensic investigation indicated that the incident resulted in the compromise of data relating to current and former patients and employees of Excelsior and its related entities, including the Buffalo Surgery Center and Northtowns Orthopaedics.

In light of those findings, Excelsior engaged outside data mining experts to conduct a thorough analysis of the compromised data and identify affected individuals. In August of 2024, with the data mining process ongoing, Excelsior mailed an initial wave of notices to a small population of affected individuals and reported the incident to the U.S. Department of Health and Human Services and the Office for Civil Rights ("HHS/OCR"). The bulk of data mining was completed in December 2024, which identified additional individuals for purposes of notification. Excelsior mailed a second wave of notices to patients on December 31, 2024. Efforts to identify affected individuals is ongoing, and any remaining affected individuals will be notified via first class mail as they are identified.

2. Number of Maryland Residents Affected.

Based upon the investigation, Excelsior identified and notified eighteen (18) residents whose information was impacted as a result of the incident. Notices were mailed to these individuals beginning on December 31, 2024. Sample notification letters are enclosed hereto as **Exhibit A** and **Exhibit B**.

3. Steps taken in Response to the Incident.

Excelsior is committed to ensuring the security and privacy of all personal information in its control and is taking steps to prevent a similar incident from occurring in the future. After discovering the incident, we immediately took steps to contain the intrusion and secure our environment, including disconnecting all external access to the network, isolating suspect equipment, and changing credentials across the organization to safeguard user and administrative system accounts. After securing our environment, Excelsior has taken several steps enhance existing security measures and prevent similar incidents from occurring in the future, including deployment of new security tools, redesign of key system and business processes, and implementation of internal security awareness campaigns and enhanced system alerts. Excelsior has and will continue to take steps to mitigate the risk of future harm. Finally, Excelsior has reported this incident to the FBI and cooperated with law enforcement investigations.

Excelsior is also offering twelve (12) months of complimentary credit monitoring and identity theft restoration services through CyberScout, a TransUnion company, to all affected state residents to help protect their identity. Additionally, Excelsior provided guidance on how to better protect against identity theft and fraud, including providing 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 the contact details for the Federal Trade Commission.

4. Contact information

Excelsior remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A

Excelsior Orthopaedics, LLP
c/o Cyberscout
PO Box 179
Manchester, NH 03105

P
[redacted]

July 25, 2024

Re: Data Security Incident Involving Excelsior Orthopaedics, LLP

Dear [redacted]

Excelsior Orthopaedics, LLP ("Excelsior") is writing to inform you of a recent data security incident that may have resulted in an unauthorized access of your sensitive personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On June 23, 2024, Excelsior detected unusual activity on its network and discovered that it was the victim of a data security incident. Upon discovery of this incident, Excelsior immediately disconnected all external access to the network, isolated suspect equipment, and changed all network credentials. In addition, Excelsior promptly engaged a specialized third-party cybersecurity firm to help secure the environment and conduct a comprehensive forensic investigation into the nature and scope of the incident. Efforts to secure and restore Excelsior's environment are ongoing. Initial results of the ongoing investigation indicate that the incident may have resulted in the compromise of employee information stored on Excelsior servers. Compromised data may include information about employees of the Buffalo Surgery Center, a related entity. At this time, Excelsior is not aware of the misuse of any employee information. Nonetheless, out of an abundance of caution, Excelsior is notifying its employees so that they can take steps to protect themselves as outlined in this letter.

What Information Was Involved?

Although Excelsior is unaware of any fraudulent misuse of information, the following types of employee information may have been impacted as a result of the incident: An individual's full name, address, date of birth, Social Security Number, Driver's License number, non-driver identification card number, and biometric information. Please note that impacted data will vary depending on the individual.

What We Are Doing

Excelsior is committed to ensuring the security and privacy of all personal information in its control and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the incident, Excelsior moved quickly to respond and investigate the incident, assess the security of its systems, and identify potentially affected individuals. Specifically, Excelsior engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident and assist in efforts to remediate. Excelsior's information technology ("IT") team responded quickly to contain the situation by isolating impacted machines, shutting down external system access, and safeguarding user and administrative system accounts. Before bringing systems back online, Excelsior's IT team also restored the data to offline servers to verify the integrity of backups and detect malware. Excelsior has also provided the FBI with information about the incident and intends to cooperate with any investigation by law enforcement.

000010103G0500

P

In addition, Excelsior has taken steps to enhance existing security measures and prevent similar events from occurring in the future. Following the incident, Excelsior deployed new security tools to augment its security platform, redesigned key system and business processes, increased internal security awareness campaigns designed to improve employees' ability to detect phishing, and implemented enhanced system alerts to reduce response times. An increase in employee education of cybersecurity threats through expanded course content on internal and external training platforms will also be implemented. Excelsior is also in the process of migrating the bulk of its data to the cloud for additional protection. Excelsior has and will continue to take steps to mitigate the risk of future harm.

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by CyberScout, a TransUnion company, specializing in fraud assistance and remediation services. Details on how to enroll in these complimentary services can be found below.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to [redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

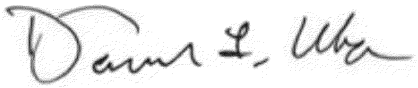
We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call 1-833-531-2298 (toll free) Monday through Friday, during the hours of 8 a.m. and 8 p.m. Eastern Standard Time (excluding U.S. national holidays).

Excelsior sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,



David Uba
Chief Executive Officer
Excelsior Orthopaedics, LLP

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

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	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

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	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

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

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a 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.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at 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 residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of *Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island:* You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General - Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-999-5630**;** www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division**:** 200 St. Paul Place**,** 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division**:** 9001 Mail Service Center, Raleigh, NC 27699**;** 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903**;**

1-401-274-4400**;** www.riag.ri.gov

EXHIBIT B

Excelsior Orthopaedics, LLP
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Via First-Class Mail

P [redacted]

December 31, 2024

Re: Notice of Data Security Incident

Dear [redacted]

Excelsior Orthopaedics, LLP ("Excelsior") is writing to inform you of a recent data security incident that resulted in unauthorized access of your personal information. In an abundance of caution, we are offering free credit monitoring and identity theft protection services to affected individuals. This letter provides instructions on how to enroll in those services as well as details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On June 23, 2024, Excelsior detected unusual activity on its network and discovered that it was the victim of a data security incident. Upon discovery of this incident, Excelsior immediately took steps to contain the intrusion and engage a specialized third-party cybersecurity firm to help secure the environment and conduct a comprehensive forensic investigation into the nature and scope of the incident. Initial findings from the forensic investigation indicated that the incident resulted in the compromise of data relating to current and former patients and employees of Excelsior and its related entities, including Buffalo Surgery Center and Northtowns Orthopaedics. In light of those findings, Excelsior engaged outside data mining experts to conduct a thorough analysis of the compromised data and identify affected individuals.

In August 2024, with the data mining process ongoing, Excelsior mailed an initial wave of notices to a small population of affected individuals and reported the incident to the U.S. Department of Health and Human Services and the Office for Civil Rights. The bulk of data mining was completed in December 2024, which identified additional individuals for purposes of notification.

What Information Was Involved?

Based on the data mining results, the following information related to you was impacted as a result of this incident: full name, Date of Birth, Medical Record Number, Diagnosis, Diagnosis Code, Treatment Location, Procedure Type, Provider Name, Treatment Cost, Medical Date of Service, Health Insurance Information, Subscriber Member Number and Patient Account Number. Note, impacted data varies based on the individual.

What We Are Doing

Excelsior is committed to ensuring the security and privacy of all personal information in its control and is taking steps to prevent a similar incident from occurring in the future.

0000101102G0500

P

After discovering the incident, we immediately took steps to contain the intrusion and secure our environment, including disconnecting all external access to the network, isolating suspect equipment, and changing credentials across the organization to safeguard user and administrative system accounts. After securing our environment, Excelsior has taken several steps to enhance existing security measures and prevent similar incidents from occurring in the future, including but not limited to, deploying new security tools, redesigning key system and business processes, partnering with a first-in-class managed security service provider, and implementing enhanced internal security awareness campaigns and system alerts. Finally, Excelsior has reported this incident to the FBI and cooperated with law enforcement investigations. Excelsior has and will continue to take steps to mitigate the risk of future harm.

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by CyberScout, a TransUnion company, specializing in fraud assistance and remediation services. Details on enrolling in these complementary services can be found below.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

To enroll in Credit Monitoring services at no charge, please log on to [redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

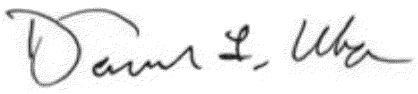
In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity. We encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call 1-**833-531-2298** (toll free) Monday through Friday, during the hours of 8 a.m. and 8 p.m. Eastern Standard Time (excluding U.S. national holidays).

Excelsior sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,



David Uba
Chief Executive Officer
Excelsior Orthopaedics, LLP

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

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	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

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	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

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

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a 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.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at 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 residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of *Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island:* You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General - Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-999-5630**;** www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division**:** 200 St. Paul Place**,** 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division**:** 9001 Mail Service Center, Raleigh, NC 27699**;** 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903**;** 1-401-274-4400**;** www.riag.ri.gov