March 7, 2024

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

Via Email:

Attorney General Brian Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Re: Preliminary Notice of Cybersecurity Incident Involving Antunovich Associates

Dear Attorney General Frosh:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Antunovich Associates ("AA"), a civil architecture firm headquartered in Illinois, with respect to a recent cybersecurity incident that was first discovered by AA on January 22, 2024 (hereinafter, the "Incident"). AA takes the security and privacy of the information in 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, and the steps that AA has taken in response to the Incident. At this time, we are still investigating the matter and confirming individuals that have been impacted, but we wanted to notify you in an abundance of caution. We have also enclosed hereto a sample of the substitute notification made while we confirm the potentially impacted individuals.

1. Nature of the Incident

On January 22, 2024, AA discovered unauthorized activity within its network. Upon discovery of this incident, AA promptly engaged a specialized third-party cybersecurity firm to secure the network and conduct a comprehensive forensic investigation to determine the nature and scope of the incident. On February 22, 2024, the forensic investigation confirmed unauthorized activity within AA's network and identified possibly affected systems. Based on these findings, AA is reviewing the affected systems to identify the specific individuals and types of information that may have been compromised. Due to the possibility of incomplete contact information for affected individuals, AA also posted preliminary substitute notice on its website while the investigation is finalized.

It is possible that the affected systems may contain data belonging to an unknown number of Maryland residents. AA is providing preliminary notice to your agency for full transparency and will supplement this notice upon completion of the review of affected systems and identified impacted personal information.

As of March 7, 2024, AA has not received any reports of fraudulent misuse of the information.

2. Number of Maryland residents affected.

We are still in the process of confirming the individuals impacted as a result of the Incident. However, out of an abundance of caution, AA has posted a preliminary substitute notice on their website. A copy of the preliminary substitute notice is attached as Exhibit A. Once the impacted individuals are confirmed, notification letters will be sent to these individuals by first class mail.

3. Steps taken in response to the Incident.

Data privacy and security is among AA's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon discovery of the Incident, AA moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, AA engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, AA took the following steps, including, but not limited to: implementing new technical safeguards; revised policies and procedures; enhanced monitoring detection and reporting, and took steps and will continue to take steps to mitigate the risk of future harm.

4. Contact information

AA 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

ANTUNOVICH ASSOCIATES
ARCHITECTURE · PLANNING · INTERIOR DESIGN
Chicago • Washington DC • Los Angeles • Austin

Notice of Data Breach

Chicago, IL – March 7, 2024 – Antunovich Associates is writing to inform you of a recent data security incident that may have resulted in unauthorized access to some individuals' sensitive personal information. This notice is intended to provide details about the incident, steps we are taking in response, and resources available to help protect against the potential misuse of sensitive personal information. At this time, we have not received any reports of related misuse of personal information since the date of the Incident.

What Happened? On January 22, 2024, Antunovich Associates discovered unauthorized activity within its network. Upon discovery of this incident, Antunovich Associates promptly engaged a specialized third-party cybersecurity firm to secure the network and conduct a comprehensive forensic investigation to determine the nature and scope of the incident. On February 22, 2024, the forensic investigation confirmed unauthorized activity within Antunovich Associates' network.

Based on these findings, Antunovich Associates began reviewing the affected systems to identify the specific individuals and types of information that may have been compromised. While this process remains ongoing, it has been determined that the affected information was limited to individuals who were current or former employees. Antunovich Associates will notify affected individuals by First Class Mail with an offer of complimentary credit monitoring and identity theft protections services as the information becomes available. Due to the possibility of incomplete contact information for affected individuals, Antunovich Associates is also posting preliminary substitute notice on its website while we finalize the investigation.

To date, Antunovich Associates has not received any reports of fraudulent misuse of the information.

What Information Was Involved? While the review of affected systems is ongoing, but the following information related to potentially impacted individuals may have been subject to unauthorized access: name;

employees. Antunovich Associates will notify affected individuals by First Class Mail with an offer of complimentary credit monitoring and identity theft protection services as [illegible] becomes available. Due to the possibility of incomplete contact information for affected individuals, Antunovich Associates is also posting preliminary substitute notice on its website while we finalize the investigation.

To date, Antunovich Associates has not received any reports of fraudulent misuse of the information.

What Information Was Involved? While the review of affected systems is ongoing, but the following information related to potentially impacted individuals may have been subject to unauthorized access: name; address; date of birth; Social Security Number; driver's license/state identification number; financial account information; health insurance information; and limited health information. Please note that the information above varies for each potentially impacted individual. Affected individuals will be notified by mail of information that was impacted. Please note there is no evidence at this time that any personal information has been misused as a result of this incident.

What We Are Doing? Data privacy and security is among Antunovich Associates' highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon discovery of the Incident, Antunovich Associates moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, Antunovich Associates engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, Antunovich Associates took the following steps, including, but not limited to: implementing new technical safeguards; revised policies and procedures; enhanced monitoring detection and reporting, and took steps and will continue to take steps to mitigate the risk of future harm. The review of affected systems is still ongoing.

Upon completion of the review of affected systems, Antunovich Associates will review all impacted information, if any, to determine whether personally identifiable information was accessed by an unauthorized user. Notice letters will be mailed to the affected individuals via First Class Mail along with an offer of complimentary credit monitoring and identity theft protection services.

291712630v.1

291712630v.1

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.

Other Important Information:

We recognize that you may have questions not addressed in this notice. If you have any questions or concerns, please call 1-800-405-6108 Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

Antunovich Associates 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,

Charles Kennedy
President
Antunovich Associates

291712630v.1

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 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),

291712630v.1

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 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

291712630v.1

WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

May 9, 2024

Joseph M. Fusz
312.821.6141 (direct)
Joseph.Fusz@wilsonelser.com

Via E-Mail: Idtheft@oag.state.md.us

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

Re: Notice of Cybersecurity Incident

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Antunovich Associates ("AA"), an architecture firm located at 224 West Huron Street, Suite 7E, Chicago, Illinois, 60654, with respect to a recent cybersecurity incident that was first discovered by AA on January 22, 2024 (hereinafter, the "Incident"). AA takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve as an addendum to previous preliminary notice sent to you on March 7, 2024, and to inform you of the nature of the Incident, what information may have been compromised, the number of residents being notified, and the steps that AA has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On January 22, 2024, AA discovered unauthorized activity within its network. Upon discovery of this incident, AA promptly engaged a specialized third-party cybersecurity firm to secure the network and conduct a comprehensive forensic investigation to determine the nature and scope of the incident. On February 22, 2024, the forensic investigation confirmed unauthorized activity within AA's network. Based on these findings, AA began reviewing the affected systems to identify the specific individuals and types of information that may have been compromised. AA determined that the incident involved personally identifiable information (PII) and worked to identify the persons impacted. While AA investigated the specific individuals who may have been affected, AA posted a public notice of the incident on their website on March 7, 2024.

The identified PII included individuals' full name; address; date of birth; Social Security Number; driver's license/state identification number; passport number; financial account information; account information; health insurance information; and limited health information. The information impacted varies by individual. The notice list was finalized on May 2, 2024, and notice was mailed to impacted persons on May 9, 2024, via First Class Mail.

2. Number of Maryland residents affected.

AA identified fifteen (15) Maryland residents whose information was potentially affected by this Incident. Notification letters to these individuals were mailed on May 9, 2024. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

AA 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, AA moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, AA engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, AA took the following steps, including, but not limited to: implementing new technical safeguards; revised policies and procedures; enhanced monitoring detection and reporting, and took steps and will continue to take steps to mitigate the risk of future harm. AA takes the protection and proper use of personal information very seriously.

AA also offered twelve (12) months of complimentary credit monitoring and identity theft restoration services through CyberScout to all individuals to help protect their identity. Additionally, AA 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

AA 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 Joseph.Fusz@WilsonElser.com or 312-821-6141.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Joseph M. Fusz

Enc.

EXHIBIT A

Antunovich Associates Inc.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-08617

ANTUNOVICH ASSOCIATES
ARCHITECTURE · PLANNING · INTERIOR DESIGN
Chicago • Washington DC • Los Angeles • Austin

Via First-Class Mail

[redacted]

[redacted]

Re: Notice of Data Security Incident

Dear [redacted]:

Antunovich Associates ("AA") is writing to inform you of a recent data security incident that may have resulted in an unauthorized access to your sensitive personal information. We take our data responsibilities and protection of your data very seriously and we are sorry for any worry and inconvenience this news will cause. Out of abundance of caution, 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 January 22, 2024, AA discovered unauthorized activity within its network. Upon discovery of this incident, AA promptly engaged a specialized third-party cybersecurity firm to secure the network and conduct a comprehensive forensic investigation to determine the nature and scope of the incident. On February 22, 2024, the forensic investigation confirmed unauthorized activity within AA's network.

Based on these findings, AA began reviewing the affected systems to identify the specific individuals and types of information that may have been compromised. This review identified that some of your personal information may have been impacted by this incident. On May 2, 2024, AA finalized the list of individuals to notify.

What Information Was Involved?

Based on the investigation, the following information related to you may have been subject to unauthorized access: name; address; date of birth; Social Security Number; driver's license/state identification number; passport number; financial account information; account information; health insurance information; and limited health information. This does not mean that your personal information from AA has been misused as a result of this incident. We would like to reassure you that we have taken all efforts possible to mitigate any further exposure of your personal information and we are committed to supporting you.

What We Are Doing

Data privacy and security is among AA's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon discovery of the Incident, AA moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, AA engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, AA took the following steps, including, but not limited to: implementing new technical safeguards; revised policies and procedures; enhanced monitoring detection and reporting, and took steps 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 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.

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 https://bfs.cyberscout.com/activate 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.

Other Important Information:

We recognize that you may have questions not addressed in this notice. If you have any questions or concerns, please call 1-800-405-6108 Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

Antunovich Associates 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,

Charles S. Kennedy

Charles Kennedy
President
Antunovich Associates

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