



February 7, 2023

Via electronic-mail: [DOJ-CPB@doj.nh.gov](mailto:DOJ-CPB@doj.nh.gov); [AttorneyGeneral@doj.nh.gov](mailto:AttorneyGeneral@doj.nh.gov)

**Attorney General John M. Formella**

Consumer Protection Bureau

Office of the Attorney General

33 Capitol Street

Concord, NH 03302

**Re: Our Client : Mount Saint Mary College**  
**Matter : Data Security Incident**

---

Dear Attorney General Formella:

We represent Mount Saint Mary College (hereinafter “MSMC”), located in Newburgh, New York, with respect to a data security incident described in more detail below. MSMC takes the security and privacy of the information in its control 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 security breach, the number of New Hampshire residents being notified, what information has been compromised, and the steps that MSMC is taking to restore the integrity of its systems. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On December 20, 2022, MSMC was the target of a cybersecurity incident. An unauthorized third infiltrated MSMC’s network. This incident may have resulted in the exposure of student and faculty personal information that was located on MSMC’s systems, including: full name, Social Security number, passport number, and/or email address or username with password.

MSMC is not aware of any evidence that information has been misused and has not received any reports of related identity theft since the date of the incident.

2. Number of New Hampshire Residents Affected

A total of twenty (20) residents of New Hampshire were potentially affected by this security incident. Notification letters to these individuals are being mailed today February 7, 2023, by first class mail, and should be received by individuals promptly. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Upon learning of this incident, MSMC moved quickly to institute a response plan, which included conducting an investigation with the assistance of third-party forensic specialists and engaging in steps to confirm the security of any relevant systems. MSMC is reviewing and enhancing its technical safeguards and policies relating to the security of its systems and servers.

4. Contact Information

MSMC 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

Very truly yours,

Lewis Brisbois Bisgaard & Smith LLP

Rachel C. Pitts, Esq.

Copy: Robert F. Walker, Esq. (Lewis Brisbois Bisgaard & Smith LLP)

Enclosure: *Sample Notification Letter*

Mount Saint Mary College  
c/o Cyberscout  
38120 Amrhein Road  
Livonia, MI 48150  
Via First-Class Mail



February 7, 2023

Notice of Data Security Incident

Dear [REDACTED],

You are receiving this letter because you are a current or former student or employee of Mount Saint Mary College ("MSMC") in Newburgh, New York. We are writing to inform you of an incident that may have exposed your personal information. MSMC takes the privacy of personal information seriously and wants to provide you with information and resources you can use to protect your information.

What Happened and What Information Was Involved:

On December 20, 2022, we detected and stopped a network security incident in which an unauthorized third party accessed and disabled some of our systems. We immediately engaged third-party forensic specialists to assist us with securing the network environment and investigating the extent of any unauthorized activity. Our investigation determined an unauthorized third party may have accessed certain individual personal information during this incident.

We found no evidence that your information has been specifically misused; however, it is possible that the following personal information could have been accessed by an unauthorized third party: first and last name; Social Security number; passport number; email address or username with password.

What We Are Doing:

Data security is one of our highest priorities. Upon detecting this incident we moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of our network environment. We notified law enforcement. We are wiping and rebuilding affected systems and taking steps to bolster our network security, as well as reviewing our policies, procedures, and network security software relating to the security of our systems and how we store and manage data.

We are offering access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services through Cyberscout, a Transunion company and a leading identity protection technology company. Cyberscout services include: twelve (12) months of credit monitoring and fully managed identity theft recovery services. With this protection, Cyberscout will help you resolve issues if your identity is compromised.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/msmc> and follow the instructions provided. When prompted please provide the following unique code to receive services:

000010102G0500

P

. Cyberscout is available Monday through Friday, 8:00 a.m. to 8:00 p.m. EST. Please note 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 this service offering. Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call 1-833-570-2891, Monday through Friday, 8:00 a.m. to 8:00 p.m. EST.

We value the security of the personal data that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused.

Sincerely,

Jason Adsit  
President  
Mount Saint Mary College

### Additional 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](http://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.



**Security Freeze:** You also 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:

00001020280000

P

<b>Equifax Security Freeze</b>	<b>Experian Security Freeze</b>	<b>TransUnion Security Freeze</b>
P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 <a href="https://www.equifax.com/personal/credit-report-services/credit-freeze/">https://www.equifax.com/personal/credit-report-services/credit-freeze/</a>	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a>	P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 <a href="http://www.transunion.com/credit-freeze">www.transunion.com/credit-freeze</a>

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax ([https://assets.equifax.com/assets/personal/Fraud\\_Alert\\_Request\\_Form.pdf](https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf));
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

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. The phone numbers for all three credit bureaus are at listed above.

**Monitoring:** You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

**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](http://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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

**For Maryland residents,** the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and [www.oag.state.md.us](http://www.oag.state.md.us).

**For New Mexico residents,** you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from 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 by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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 North Carolina residents,** the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and [www.ncdoj.gov](http://www.ncdoj.gov).

**For New York residents,** the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and <https://ag.ny.gov/>.

**For Rhode Island residents,** the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

Mount Saint Mary College  
c/o Cyberscout  
38120 Amrhein Road  
Livonia, MI 48150  
Via First-Class Mail



February 7, 2023

Notice of Data Security Incident

Dear Family of [REDACTED],

You are receiving this letter because your family member was a current or former student or employee of Mount Saint Mary College ("MSMC") in Newburgh, New York. We are writing to inform you of an incident that may have exposed your family member's personal information. MSMC takes the privacy of personal information seriously and wants to provide you with information and resources you can use to protect your family member's information.

What Happened and What Information Was Involved:

On December 20, 2022, we detected and stopped a network security incident in which an unauthorized third party accessed and disabled some of our systems. We immediately engaged third-party forensic specialists to assist us with securing the network environment and investigating the extent of any unauthorized activity. Our investigation determined an unauthorized third party may have accessed certain individual personal information during this incident.

We found no evidence that your family member's information has been specifically misused; however, it is possible that the following personal information could have been accessed by an unauthorized third party: first and last name; Social Security number; passport number; email address or username with password.

What We Are Doing:

Data security is one of our highest priorities. Upon detecting this incident we moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of our network environment. We notified law enforcement. We are wiping and rebuilding affected systems and taking steps to bolster our network security, as well as reviewing our policies, procedures, and network security software relating to the security of our systems and how we store and manage data.

To assist you in protecting your family member's information, we are providing you with access to Cyber Monitoring services for your deceased family member at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment. Cyber monitoring will look out for your family member's personal data on the dark web and alert you if their personally identifiable information is found online. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

000010102G0500

P



What You Can Do:

To enroll your family member in monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/msmc> and follow the instructions provided. When prompted please provide the following unique code to receive services: . Cyberscout is available Monday through Friday, 8:00 a.m. to 8:00 p.m. EST. Please note 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.

Enclosed you will find additional information regarding the resources available to you and the steps that you can take to further protect your family member's personal information. If you choose not to use these services, we strongly urge you to contact the credit bureaus and ensure that no active credit file exists in the name of your family member.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call 1-833-570-2891, Monday through Friday, 8:00 a.m. to 8:00 p.m. EST.

We value the security of the personal data that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused.

Sincerely,

Jason Adsit  
President  
Mount Saint Mary College



### **Additional 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](http://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.



**Security Freeze:** You also 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:

00001020280000

P

<b>Equifax Security Freeze</b> P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 <a href="https://www.equifax.com/personal/credit-report-services/credit-freeze/">https://www.equifax.com/personal/credit-report-services/credit-freeze/</a>	<b>Experian Security Freeze</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a>	<b>TransUnion Security Freeze</b> P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 <a href="http://www.transunion.com/credit-freeze">www.transunion.com/credit-freeze</a>
---	---	--

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax ([https://assets.equifax.com/assets/personal/Fraud Alert Request Form.pdf](https://assets.equifax.com/assets/personal/Fraud%20Alert%20Request%20Form.pdf));
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

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. The phone numbers for all three credit bureaus are at listed above.

**Monitoring:** You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

**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](http://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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

**For Maryland residents,** the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and [www.oag.state.md.us](http://www.oag.state.md.us).

**For New Mexico residents,** you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from 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 by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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 North Carolina residents,** the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and [www.ncdoj.gov](http://www.ncdoj.gov).

**For New York residents,** the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and <https://ag.ny.gov/>.

**For Rhode Island residents,** the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

Mount Saint Mary College  
c/o Cyberscout  
38120 Amrhein Road  
Livonia, MI 48150  
Via First-Class Mail



February 7, 2023

Notice of Data Security Incident

Dear Parent or Guardian of [REDACTED],

You are receiving this letter because your minor child is a current or former student or employee of Mount Saint Mary College ("MSMC") in Newburgh, New York. We are writing to inform you of an incident that may have exposed your minor child's personal information. MSMC takes the privacy of personal information seriously and wants to provide you with information and resources you can use to protect your minor child's information.

What Happened and What Information Was Involved:

On December 20, 2022, we detected and stopped a network security incident in which an unauthorized third party accessed and disabled some of our systems. We immediately engaged third-party forensic specialists to assist us with securing the network environment and investigating the extent of any unauthorized activity. Our investigation determined an unauthorized third party may have accessed certain individual personal information during this incident.

We found no evidence that your minor child's information has been specifically misused; however, it is possible that the following personal information could have been accessed by an unauthorized third party: first and last name; Social Security number; passport number; email address or username with password.

What We Are Doing:

Data security is one of our highest priorities. Upon detecting this incident we moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of our network environment. We notified law enforcement. We are wiping and rebuilding affected systems and taking steps to bolster our network security, as well as reviewing our policies, procedures, and network security software relating to the security of our systems and how we store and manage data.

We are providing the parents of impacted minor dependents with access to **Cyber Monitoring** services for you and your minor child for twelve (12) months at no charge. Cyber Monitoring will look out for your and your child's personal data on the dark web and alert you if your personally identifiable information or your child's is found online. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

000010102G0500

P

### What You Can Do:

To enroll in cyber monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/msmc> and follow the instructions provided. When prompted please provide the following unique code to receive services:

. Cyberscout is available Monday through Friday, 8:00 a.m. to 8:00 p.m. EST. Please note, 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 will require enrollment by parent or guardian first. 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. Once you have enrolled yourself, click on your name in the top right of your dashboard and select "Manage Family Protection" then "Add Family Member" to enroll your child. We encourage you to take full advantage of this service offering.

Enclosed you will find additional information regarding the resources available to you and the steps that you can take to further protect your minor child's personal information. If you choose not to use these services, we are strongly urging all parents to contact the credit bureaus and ensure that no credit file exists in the name of your minor child.

### For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call 1-833-570-2891, Monday through Friday, 8:00 a.m. to 8:00 p.m. EST.

We value the security of the personal data that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused.

Sincerely,

Jason Adsit  
President  
Mount Saint Mary College

## **Additional 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](http://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.



**Security Freeze:** You also 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:

<b>Equifax Security Freeze</b> P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 <a href="https://www.equifax.com/personal/credit-report-services/credit-freeze/">https://www.equifax.com/personal/credit-report-services/credit-freeze/</a>	<b>Experian Security Freeze</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a>	<b>TransUnion Security Freeze</b> P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 <a href="http://www.transunion.com/credit-freeze">www.transunion.com/credit-freeze</a>
---	---	--

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax ([https://assets.equifax.com/assets/personal/Fraud Alert Request Form.pdf](https://assets.equifax.com/assets/personal/Fraud%20Alert%20Request%20Form.pdf));
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

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. The phone numbers for all three credit bureaus are at listed above.

**Monitoring:** You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

**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](http://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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

**For Maryland residents,** the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and [www.oag.state.md.us](http://www.oag.state.md.us).

**For New Mexico residents,** you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from 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 by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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 North Carolina residents,** the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and [www.ncdoj.gov](http://www.ncdoj.gov).

**For New York residents,** the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and <https://ag.ny.gov/>.

**For Rhode Island residents,** the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.