MD PIGA Breach Assessment

To be used by Units Subject to MD. State Government Code Ann. §§ 10-1301-1308

Form Purpose:

Use this form to determine whether an incident is a breach that requires notification. Any unauthorized use or disclosure of Personal Information may be a breach that requires notification under the Maryland Protection of Information by Government Agencies (MD. State Government Code Ann. § 10-1305), also referred to as MD PIGA. The factors in the following assessment help with the breach determination. Determinations should be made on a case-by-case basis based on the facts of a particular incident.

Notification Requirements:

If notice is required, it must be sent to the impacted individual(s) within a reasonable amount of time after the investigation into the incident is conducted. The law allows for some delays of notification. *See Section 7.* Details about how to provide notice are included in MD. State Government Code Ann. § 10-1305.

Determination Record:

If an agency determines, after the investigation, that notification is not required under MD PIGA, the unit shall maintain records that reflect its determination for 3 years after the determination is made.

Section 1 – Investigation Details		
REFERENCE NUMBER: SIR0051435, SIR0051498, SIR0051595, SIR0051692, SIR0051484, SIR0051450, SIR0051589, SIR0051569, SIR0051744, SIR0051502, SIR0052303, SIR0052529.	DATE FORM COMPLETED: March 28, 2025	NUMBER OF INDIVIDUALS AFFECTED: Students 155,452 records Teachers 22,206 records
DATE DISCOVERED: December 28, 2024	DATE(S) OF INCIDENT: December 19-28, 2024	
FORM COMPLETED BY: Cecilia Barajas	TITLE: Maryland State Department of Education- Chief Privacy Officer	
OTHERS CONSULTED: MD-SOC, DoIT, MD Chief Privacy Officer, MSDE CIO, MSDE CISSO.	NAME AND CONTACT INFORMATION, IF THIRD PARTY INCIDENT:	

FINAL DETERMINATION

X	Breach occurred; provide notification as required by MD. State Government Code Ann. § 10-1305
	Not a breach; notification may be provided but is not required by MD. State Government Code Ann. § 10-1305

Section 2 – Incident Summary
DESCRIBE THE INCIDENT AND THE NATURE OF INFORMATION THAT WAS POTENTIALLY COMPROMISED OR EXPOSED. **PowerSchools SIS** 12/19/2024—A threat actor was able to access the Admin level (Username and Password) of PowerSchool's PS PowerSource Portal. Caused by a lack of a VPN and MFA. 12/22/2024—Data was exfiltrated from PS SIS systems. Two tables containing Student and Teacher Private Information sets were accessed through the compromised PS SIS portal. This impacted ~ 4,000 schools nationwide. This affected both On-site and Cloud-based systems. 12/28/2025-- PS Became Aware of Compromise/Data Exfiltration. CyberSteward was engaged and offered assurance that the data was deleted by the mal-actor, and that no copies exist. The incident was contained, no malware evident. New administrative policies were instituted to secure the system-strengthening passwords, block access to PowerSource.

01/07/2025—Impacted schools Districts were notified. For the State of Maryland of the 25 School Districts, nine Districts were notified that they were affected, of the nine, seven are using the PowerSchool Student Information System (PS SIS) including on Premises and Cloud systems. Two Districts were in the initiation phase of migrating current information systems to PS SIS. These two contained only test data and no student records were affected (see below list and notes). The remaining seven contained PII (Names, Addresses, SSN, EIN, and even some PHI information). Only one district used alternative IDs for the SSN fields. All nine districts have been advised to report directly to MD PIGA or use MSDE as the report compiler, five (*) have accepted this consolidated report method. All affected districts have accepted PowerSchool's role in reporting this incident to all the regulatory agencies, as well setting up notification to the impacted individuals, along with credit monitoring and identity protection.

MSDE is taking on this reporting role as part of our duty of care to our constituents and to assist our Local Education Agencies (LEA) with this reporting requirement.

In short here are the impacted Maryland Schools.

- Frederick County Public Schools—**No SSN**, contains other PII, does not want to join this joint report
- Dorchester County Public Schools—Contained SSN and other PII
- Kent County Public Schools*—Contained SSN and other PII
- Cecil County Public Schools*---Contained SSN and other PII
- Talbot County Public Schools—Contained SSN and other PII
- Allegany County Public Schools—No PII contained only test data
- Somerset County Public Schools*-- PS SIS is not in production in this district
- Caroline County Public Schools*--Contained SSN and other PII
- Worcester County Public Schools*--Contained SSN and other PII

All the schools have reported the incident to Maryland's SOC and the tickets listed above have now been closed.

Section 3 – ENCRYPTION OR OTHER SECURITY		
Was the information secured by encryption or redacted; and the encryption key was not compromised or disclosed? If unsure, contact an information technology professional to determine if information was secure.		
	Yes	MD PIGA only applies to information that is not secured. Completing the rest of the assessment is optional.
X	**No**	Continue Assessment.

Section 4 - Was the information affected Personal Information? What Data elements were potentially compromised? Mark the elements involved in your incident.	
Yes	First name (or first initial) and last name, personal mark, or unique biometric or genetic print or image
In combination with any one or more of the following:	
Yes	a Social Security Number

Yes	a driver's license number, state identification card number, or other individual identification number issued by a unit
No	a passport number or other identification number issued by the United States government;
Yes	an Individual Taxpayer Identification Number
No	a financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account
	Other information involved:

Section 4.a		
Did you mark the name and at least one other data element?		
X	**Yes**	The information is Personal Information. Continue to Section 5.
	No	The information is not Personal Information. Continuing is optional.

Section 5 – Exception for Good Faith Acquisition	
Is the person who received or accessed the information:	
• An employee or agent of the unit	• Acting in good faith;
• Within the scope of work; and	• **With no further use or disclosure.**
If all four are satisfied, the incident does not require notification under MD PIGA, continuing is optional. Please create and retain an internal memo regarding the incident, detailed analysis, and determination.	

Section 6 – Risk Assessment	
An unauthorized use or disclosure is presumed to be a breach that requires notification. That presumption can be overcome if there is a low risk that the incident will create a risk of harm. Use the factors below to determine whether, on balance, there is a low risk that the incident creates a risk of harm.	
1. Nature and extent of Personal Information involved, including types of identifiers and ability to identify individual:	
LOW	Information is unlikely or unable to be usable to identify a person or commit identity theft
MODERATE	Information could be used to identify individual but is not sensitive or specially protected.
HIGH	Information includes elements that could be used for identity theft, or records that are highly sensitive or personal, and are protected by heightened confidentiality laws.
2. Nature of person who acquired, accessed, used or received the Personal Information:	
LOW	Limited or no risk of re-disclosure of information by recipient. *Examples*: Employee of another agency or trusted contractor; recipient required by law to maintain confidentiality such as attorney or law enforcement; recipient subject to confidentiality laws and confirmed did not access data or returned data intact and did not retain copy.
MODERATE	Moderate or unknown risk of disclosure. *Examples*: Unclear or unknown whether recipient accessed or retained data; recipient returned information; recipient not subject to confidentiality laws but acting in good faith.
HIGH	Severe risk of disclosure and recipient likely to re-disclose, sell or transfer data or is known to have used Personal Information for malicious purposes. *Examples*: Acquisition was because of a criminal act including theft or hacking or information was obtained by a person with dishonest motives.
3. Risk that Personal Information was actually accessed or acquired or viewed by unauthorized individual:	
LOW	No proof of access or acquisition of Personal Information. Would be difficult or unable to access Personal Information without sophisticated or extreme measures and individual had limited opportunity or ability to do so, or able to demonstrate lack of access through technical assessment.
MODERATE	Unknown whether access to Personal Information was acquired or Personal Information was acquired by a known individual in a manner that could be replicated. Technical assessment of access shows limited access or is inconclusive. Means to access data commonly known or available.
HIGH	Known or reported that access to Personal Information was acquired, used, sold, or further disclosed for malicious purposes.
4. Mitigation steps taken and remaining risk to Personal Information after implementation of mitigation steps. (See Section 7 for examples of mitigation that an agency may choose to take to address an incident.)**	
LOW	All corrective actions have been taken and risk of future occurrences has been removed or reduced to acceptable level.
MODERATE	Some corrective actions have been taken but other reasonable steps cannot be implemented due to cost or other factors.
HIGH	Significant risk of continuing compromise of Personal Information remains despite mitigation.

Section 7 – Final Determination and Explanation	
	Incident has not resulted in or is unlikely to result in the misuse of the information. Notification is optional and is not required under MD. State Government Code Ann. § 10-1305
X	Incident has resulted or is likely to result in the misuse of the information. Proceed with notification required by MD. State Government Code Ann. § 10-1305

Finding and Explanation:

According to PowerSchools this is what happen and status.

On January 7, 2025, we proactively communicated this incident to the PowerSchool SIS customers affected by this incident. From January 17-[23/24], 2025, PowerSchool shared next steps with those same SIS customers. Districts and schools that do not utilize PowerSchool SIS were not affected.

As soon as we learned of the incident, we immediately engaged our cybersecurity response protocols and mobilized a cross-functional response team, including senior leadership and third-party cybersecurity experts. Since then, over the last few weeks, we have been focused on assessing the scope of data involved, making further enhancements to our cybersecurity defenses, and developing a plan to help you and our shared community. We take our responsibility to protect student, family, and educator data privacy extremely seriously, and we are committed to providing customers, families, and educators with resources and support as we work through this together.

Notification may be delayed:

- *if a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security; or*
- *to determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system.*

Examples of Mitigation Actions:

Adopt encryption technologies	Change or strengthen password requirements	Create/perform new/updated risk management plan or risk analysis.
Implement new technical safeguards	Implement periodic technical and nontechnical evaluations	Improve physical security
Train or retrain workforce members	Provide contractor with additional training on security requirements	Provide free credit monitoring
Revise contract terms	Revise policies and procedures	Sanction workforce members involved (including up to termination)

MD PIGA Notification Assessment

To be used by Units Subject to MD. State Government Code Ann. §§ 10-1301-1308 and are required to send notifications to affected individuals.

Form Purpose:

Use this form to ensure that you meet all of the notification requirements as outlined within the Maryland Protection of Information by Government Agencies (MD. State Government Code Ann. § 10-1305), also referred to as MD PIGA. The factors in the following assessment help determine the notification requirements for an agency given the facts of a particular incident.

Section 1 – Methods for Notification	
Notifications can be sent by any one of the following methods:	
	1) by written notice sent to the most recent address of the individual in the records of the unit;
	2) by electronic mail to the most recent electronic mail address of the individual in the records of the unit if: (i) the individual has expressly consented to receive electronic notice; or (ii) the unit conducts its duties primarily through Internet account transactions or the Internet;
	3) by telephonic notice, to the most recent telephone number of the individual in the records of the unit.

Section 2 – Substitute Notice Qualification		
Can the unit demonstrate that the cost of providing notice would exceed $ 100,000 or that the affected class of individuals to be notified exceeds 175,000?		
	Yes	Substitute Notice may be provided. *See Section 3 for further details.*
	No	Traditional methods of notification are required as outlined in *Section 1*.
Does the unit lack sufficient contact information to give notice in accordance with item (1), (2), or (3) of *Section 1*?		
	Yes	Substitute Notice may be provided. *See Section 3 for further details.*
	No	Traditional methods of notification are required as outlined in *Section 1*.

Section 3 – Substitute Notice Requirements	
Substitute Notice must consist of all three of the following methods:	
	Electronically mailing the notice to an individual entitled to notification under Section 1 if the unit has an electronic mail address for the individual to be notified;
	Conspicuous posting of the notice on the Web site of the unit if the unit maintains a Web site; and
	Notification to appropriate media.

Section 4 - Content of Notification Is all the following information included within your notification letter?	
	A description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired;
	Contact information for the unit making the notification, including the unit's address, telephone number, and toll-free telephone number if one is maintained;
	The toll-free telephone numbers and addresses for the major consumer reporting agencies;
	The toll-free telephone numbers, addresses, and Web site addresses for: 1) the Federal Trade Commission; and 2) the Office of the Attorney General; and a) a statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft

Section 5 - Notice of Breach to Other Departments Units are required to notify certain departments upon the occurrence of an incident and before sending out notification letters.	
Yes	Have you notified the Department of Information Technology of the breach of security? ● Email summary of the incident to the Department of Information Technology by using the following email address: ○ SOC@maryland.gov ● This notification must be provided even if you determine the incident is non-reportable
	Before giving the notification required to affected individuals, a unit shall provide notice of the breach of the security of a system to the Office of the Attorney General via one of the options below. ● By U.S. Mail: Office of the Attorney General Attn: Security Breach Notification 200 St. Paul Place Baltimore, MD 21202 ● By Fax: Attn: Security Breach Notification (410) 576-6566 ● By Email: Idtheft@oag.state.md.us

Note: PowerSchool SIS has started sending Notifications to Affected Parties and has used the attached templates to notify regulatory agencies, credit bureaus and according to PowerSchools State Attorney General.

PowerSchool Fact Sheet on Next Steps.p

Section 6 - Additional Notice to Credit Reporting Agencies **If a Unit is required to notify 1,000 or more affected individuals, the Unit is required to notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis.**	
YES	Was notification given to the consumer reporting agencies regarding the timing, distribution, and content of the notices? ● *Names and other identifying information of the recipients are **not required** to be included.* ● *Addresses for the Major Credit Reporting Agencies are outlined below:* ○ Experian Security Assistance Post Office Box 9554 Allen, Texas 75013 ● Equifax Information Services, LLC ○ Post Office Box 105069 ○ Atlanta, Georgia 30348-5069 ● TransUnion ○ Fraud Victim Assistance Department Post Office Box 2000 Chester, Pennsylvania 19022

**** Compliance with MD PIGA does not relieve a Unit from its duties under federal law or other compliance regulations and standards applicable to the Unit. Please consult with your Assistant Attorney General to determine other compliance requirements applicable to your incident.**

PowerSchool
Personalized Education for Every Journey

PowerSchool Fact Sheet on Next Steps

Identity Protection and Credit Monitoring Services: PowerSchool will be offering two years of complimentary identity protection services for all students and educators whose information was exfiltrated from your PowerSchool SIS, which will also include two years of complimentary credit monitoring services for all adult students and educators whose information was involved, regardless of whether an individual's Social Security number was exfiltrated.

Experian, a trusted credit reporting agency, will be helping us to provide these services. Details on how to enroll will be included as part of individual notifications. As the offer is specific to this incident, the details contained in the forthcoming enrollment notification will be required to enroll, and cannot be obtained directly from Experian.

Credit monitoring agencies do not offer credit monitoring services for individuals under the age of 18. If a parent / guardian enrolls an individual under the age of 18 in the offered identity protection services, the individual, upon turning 18, will have the opportunity to enroll in credit monitoring services for the duration of the two-year coverage period.

Notifications: You may have notification obligations to key stakeholders in our shared community. To reduce the burden of these notifications on you and your institution, PowerSchool will be handling notification to individuals and state attorney general offices on your behalf.

- **Community:** In coordination with Experian, PowerSchool will provide notice on your behalf to students (or their parents / guardians for students under 18) and educators whose information was exfiltrated from your PowerSchool SIS.
    - PowerSchool will publish the notice on its website, circulate the notice to local media, and send the notice to email addresses, where available, of involved individuals.
    - The notice received by each individual will include a description of the categories of personal information that were exfiltrated and the identity protection and credit monitoring services offered (as applicable).
    - We will also provide you a link to the notification if you would like to share with your community.
    - Experian will also provide a call center to answer questions from the community.

- **Regulatory:** PowerSchool will provide notification on your behalf to relevant state attorney general offices. You may also have notification requirements with your state's Department of Education. Since many customers have already notified and are in close contact with their state's Department of Education, PowerSchool will defer to you on these notifications.

- For involved students and educators, the types of information exfiltrated in the incident may have included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, Social Security Number (SSN), and other related information. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base.

- **Timing:** PowerSchool intends to begin the notification process for relevant students, parents / guardians of students, educators, and state attorney general offices (as applicable) in the next few weeks. If your institution does not want PowerSchool to notify individuals or state attorney general offices on your behalf,

please contact PowerSchool Customer Support or your designated CSM, or log a customer support ticket, by no later than January 24, 2025.

- If you are an on-premise PowerSchool SIS customer who would like PowerSchool to complete these notification processes on your behalf, please contact PowerSchool Customer Support or your designated CSM by no later than January 24, 2025. Otherwise, we will provide you a link and a relevant communication in the coming weeks that you can use to notify involved individuals.

We have also posted additional FAQs in the PowerSchool Community Portal.

PowerSchool
Personalized Education for Every Journey

Proposed Update Communications

READY FOR DISTRIBUTION TO FAMILIES AND EDUCATORS
(PLEASE FEEL FREE TO CUSTOMIZE TO YOUR PREFERENCE)

TO: Our Community
FROM: [INSERT SCHOOL DISTRICT]
SUBJECT: An Update from [INSERT SCHOOL DISTRICT] on the PowerSchool Cybersecurity Incident

Email Body:

Dear families and educators of the [INSERT] community—

[As you may be aware / as we previously communicated], PowerSchool – a cloud-based software vendor used by [INSERT SCHOOL DISTRICT] – recently experienced a cybersecurity incident involving unauthorized access to certain information in the PowerSchool Student Information System (SIS).

We are reaching out to share more information and next steps that we recently received directly from PowerSchool:

- **Identity Protection and Credit Monitoring Services:** PowerSchool has engaged Experian, a trusted credit reporting agency, to offer **two years of complimentary identity protection services for all students and educators whose information from our PowerSchool SIS was involved. This offer will also include two years of complimentary credit monitoring services for all adult students and educators whose information was involved.**

- **Notification to Individuals Involved:** Starting in the next few weeks, in collaboration with Experian, PowerSchool will provide notice to students (or their parents / guardians if the student is under 18) and educators whose information was involved, as well as a phone number to answer any questions you may have about the incident. The notice will include the identity protection and credit monitoring services offer (as applicable).

- As soon as PowerSchool learned of the incident, they engaged cybersecurity response protocols and mobilized senior leadership and third-party cybersecurity experts to conduct a forensic investigation of the scope of the incident and to monitor for signs of information misuse. PowerSchool is not aware of any identity theft attributable to this incident.

In the meantime, I encourage you to visit https://www.powerschool.com/security/sis-incident/ for up-to-date information on the cybersecurity incident. We care deeply about the welfare of our [INSERT SCHOOL DISTRICT] families and will continue to do everything we can to support you. Thank you for the important role you play in our community and your shared commitment to putting our students first.

Sincerely,
[INSERT NAME]
[INSERT TITLE], [INSERT SCHOOL DISTRICT]

PowerSchool
Personalized Education for Every Journey

Form Individual Notification Template

DRAFT (VERISON NOT FOR DISTRIBUTION)
[Date of email notification]

DRAFT Notice of Data Breach

Dear PowerSchool User or Parent / Guardian of User:

As you may know, PowerSchool provides software and services to your current or former school or the current or former school of a person to whom you are a parent or guardian. We are writing to share with you some important information regarding a recent cybersecurity incident involving personal information belonging to you or to a person to whom you are a parent or guardian (the "individual").

What Happened? On December 28, 2024, PowerSchool became aware of a cybersecurity incident involving unauthorized exportation of certain personal information from PowerSchool Student Information System (SIS) environments through one of our community-focused customer support portals, PowerSource.

What Information Was Involved? The types of information involved in this incident included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, and other related information. [The individual's Social Security number was also involved.] / [At this time, we do not have evidence that the individual's Social Security number was involved.]

What Are We Doing? PowerSchool is offering two years of complimentary identity protection services to students and educators whose information was involved. For adult students and educators, this offer will also include two years of complimentary credit monitoring services. If you are interested in enrolling, please sign up via [AAAAA] using the following code: [XXXXX] (if the individual is a minor) or [YYYY] (if the individual is an adult).

As soon as PowerSchool learned of the incident, we engaged cybersecurity response protocols and mobilized senior leadership and third-party cybersecurity experts to conduct a forensic investigation of the scope of the incident and to monitor for signs of information misuse. We are not aware of any identity theft attributable to this incident.

What Can You Do? You are encouraged to remain vigilant against incidents of identity theft and fraud by reviewing account statements for suspicious activity. PowerSchool will never contact you by phone or email to request your personal or account information. The enclosed "General Information About Identity Theft Protection" provides further information about what steps you can take.

Other Important Information. If you have any questions or concerns about this notice, please call [toll-free contact number], Monday through Friday between the hours of [9:00 am to 9:00 pm ET, excluding holidays].

Sincerely,
The PowerSchool Team

PowerSchool
Personalized Education for Every Journey

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

It is always advisable to regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service. P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below:

- **Equifax**, P.O. Box 740241, Atlanta, GA 30374-0241. 1.800.685.1111. www.equifax.com
- **Experian**, P.O. Box 9532, Allen, TX 75013. 1.888.397.3742. www.experian.com
- **TransUnion**, Consumer Disclosure Center, P.O. Box 1000, Chester, PA 19016. 1.800.888.4213. www.transunion.com

Fraud Alert: You may contact the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:	Report Fraud:	1.888.378.4329
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.680.7289

Security Freeze for Credit Reporting Agencies: You may request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. It is free to place, lift or remove a security freeze. You must separately place a security freeze on your credit report at each credit bureau. To do so, you must contact the credit bureaus by phone, mail, or secure electronic means:

- **Equifax:** P.O. Box 105788, Atlanta, GA 30348, 1.888.298.0045, www.Equifax.com
- **Experian:** P.O. Box 9554, Allen, TX 75013, 1.888.397.3742, www.Experian.com
- **TransUnion:** P.O. Box 160, Woodlyn, PA 19094, 1.800.916.8800, www.TransUnion.com

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

If you request a freeze online or by phone, the agency must place the freeze within one business day. The credit bureaus have three business days after receiving a request by mail to place a security freeze on your credit report, and they must also send confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must contact the credit reporting agencies and include (1) proper identification; (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available.

You also have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit http://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf or http://www.ftc.gov.

Steps You Can Take if You Are a Victim of Identity Theft

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at http://www.ftc.gov/idtheft; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.
- Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is helpful to log conversations with creditors, law enforcement officials, and other relevant parties.

Additional Steps to Avoid Identity Theft: The FTC has further information about steps to take to avoid identity theft at: http://www.ftc.gov/idtheft; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

State Specific Information

District of Columbia residents can obtain information from the District of Columbia's Attorney General's Office regarding steps to take to avoid identity theft. This office can be reached by visiting the website at https://oag.dc.gov/, calling (202) 727-3400, or visiting 400 6th Street NW Washington, D.C. 20001.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to its honoring your request.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at www.marylandattorneygeneral.gov, calling the Identity Theft Unit at 1.410.576.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.
New York residents can learn more about preventing identity theft from the North York Office of the Attorney General, by visiting their web site at https://ag.ny.gov/resources/individuals/credit-lending/identity-theft, calling 1.800.771.77755 or requesting more information from the New York Attorney General's Office, 28 Liberty St, New York, NY 10005.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at https://ncdoj.gov/protecting-consumers/identity-theft/, calling 1.877.566.7226 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.401.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

South Carolina residents may access educational resources and the availability of consumer assistance from the South Caroline Department of Consumer Affairs. This office can be reached by visiting the website at https://consumer.sc.gov/, calling (803) 734-4200, or visiting 293 Greystone Boulevard, Ste. 400 Columbia, SC 29210.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at http://www.atg.state.vt.us.