



SIDLEY AUSTIN LLP
ONE SOUTH DEARBORN STREET
CHICAGO, IL 60603
+1 312 853 7000
+1 312 853 7036 FAX

AMERICA • ASIA PACIFIC • EUROPE

+1 312 853 7766
KATHRYN.ALLEN@SIDLEY.COM

VIA EMAIL: IDTheft@oag.state.md.us

August 8, 2022

NOTICE OF DATA BREACH

Dear Attorney General Frosh:

On behalf of our client, Abrams & Bayliss LLP ("A&B"), we are writing to notify you about a data security incident involving personal information of one (1) Maryland resident that was maintained by A&B.

As explained in the enclosed notice to potentially impacted individuals, on March 17, 2022, A&B was alerted to a compromise of its internal data systems, which was a result of a ransomware attack.

A&B will send the enclosed notice via US mail to the one Maryland resident whose personal information was made available as a result of the security incident. The impacted information includes name, address, email address, date of birth, financial account information, driver's license, passport and social security number.

Since learning of the incident, A&B adopted several new security measures to strengthen the security of its network, internal systems, and applications. A&B is also offering all potentially impacted individuals two years of complimentary credit monitoring.

A&B will continue to monitor the dark web and will also work with our employees to make sure cyber security is top of mind. If you have any questions, please contact us.

Sincerely,

Kathryn R. Allen
Managing Associate

ABRAMS & BAYLISS LLP
20 MONTCHANIN ROAD, SUITE 200
WILMINGTON, DE 19807
MAIN: 302-778-1000
FAX: 302-778-1001

NOTICE OF DATA SECURITY INCIDENT

[Date]

[FIRST NAME] [LAST NAME]
[ADDRESS 1]
[ADDRESS 2]
[CITY] [STATE], [ZIP]

Dear [FIRSTNAME]:

As you know, Abrams & Bayliss LLP (“A&B”) suffered a cyber-attack on its internal data systems. Between March 17 and 28, 2022, you and other members of the A&B team pulled together to help restore our systems, with little to no disruption to our business operations or clients. Since that time, we have been conducting an extensive investigation about the attack, in conjunction with forensic and legal advisors, and informed the FBI. We also implemented further substantial data security measures.

I write to you today to advise how your personal information may have been impacted by the attack. Our investigation determined that the threat actor obtained data from at least one A&B internal data system between February 4 and March 17, 2022. The threat actor then deployed encryption across A&B’s internal data systems. The encryption prevented us from determining whether data on all systems were accessed, rather than just encrypted. Thus, we are reviewing the files on all those systems.

In our investigation, we learned that your name, address, e-mail address, social security number, date of birth, passport, driver’s license, and information about your benefits and employment may have been exposed. In some instances, limited health information provided for employment operation purposes, may be been exposed as well.

We are providing you with information about steps you can take to help protect your personal information and, as an added precaution, we are offering identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 24 months of Single Bureau Credit and CyberScan monitoring, a \$1,000,000 insurance

Page 3

reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

To Enroll, Please Visit: <https://app.idx.us/account-creation/protect>

Or Enroll by Phone: 1-800-939-4170

Enrollment Deadline: December 5, 2022

Enrollment Code: <<XXXXXXXX>>

Again, we're sorry about this development and regret the inconvenience. Should you have questions or concerns, please contact me at (302) 778-1152.

Sincerely,

/s/ **DRAFT**

John M. Seaman

Important Notice

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some we suggest you consider:

Reviewing Your Accounts and Credit Reports

Federal regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax 1-800-525-6285 Equifax.com	Experian 1-888-397-3742 Experian.com	TransUnion 1-800-680-7289 Transunion.com
---	---	---

You can obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report 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. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft

If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

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. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at www.IdentityTheft.gov. You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of *Identity Theft: A Recovery Plan*, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Special Information for Residents of Maryland and North Carolina

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <http://www.oag.state.md.us/idtheft/index.htm>, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

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 <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, calling 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.



SIDLEY AUSTIN LLP
ONE SOUTH DEARBORN STREET
CHICAGO, IL 60603
+1 312 853 7000
+1 312 853 7036 FAX

AMERICA • ASIA PACIFIC • EUROPE

+1 312 853 7766
KATHRYN.ALLEN@SIDLEY.COM

VIA EMAIL: IDTheft@oag.state.md.us

August 31, 2022

SUPPLEMENTAL NOTICE OF DATA BREACH

Dear Attorney General Frosh:

On behalf of our client, Abrams & Bayliss LLP ("A&B"), we write to provide supplemental notice about a data security incident. We first notified you about this incident on August 8, 2022, which at that time impacted one (1) Maryland resident. On August 10, 2022, we discovered that one (1) additional Maryland resident was impacted, bringing the number of Maryland residents impacted to two (2).

As explained in the enclosed notice to potentially impacted individuals, on March 17, 2022, A&B was alerted to a compromise of its internal data systems, which was a result of a ransomware attack.

On or about September 1, 2022, A&B will send the enclosed notice via U.S. mail to the one (1) additional Maryland resident whose personal information was made available as a result of the security incident. The impacted information includes name, address, email address, date of birth, financial account information, driver's license, passport and social security number.

Since learning of the incident, A&B adopted several new security measures to strengthen the security of its network, internal systems, and applications. A&B is also offering all potentially impacted individuals two years of complimentary credit monitoring.

A&B will continue to monitor the dark web and will also work with our employees to make sure cyber security is top of mind. If you have any questions, please contact us.

Sincerely,

Kathryn R. Allen
Managing Associate

Enc. – 9/1/2022 Notice letter

ABRAMS & BAYLISS LLP
20 MONTCHANIN ROAD, SUITE 200
WILMINGTON, DE 19807
MAIN: 302-778-1000
FAX: 302-778-1001

September 1, 2022

<<FIRST_NAME_LAST_NAME>>
<<ADDRESS 1>>
<<ADDRESS 2>>
<<CITY_STATE_ZIP>>

Notice of Data Breach

Dear <<first name>>:

As a current or former vendor and service provider to Abrams & Bayliss LLP (“A&B”), we write to provide you information about a cyber-attack on A&B’s internal data systems, and how it may have impacted your personal information.

What Happened? Between February 4, 2022, and March 17, 2022, an unauthorized party gained access to certain A&B internal data systems. The unauthorized party obtained data from at least one such system during this timeframe, before being detected, deploying encryption, and being removed from the systems. A&B thereafter launched an investigation, retained legal and forensic advisors, and informed the FBI. The encryption prevented us from determining whether data on all of A&B’s internal systems were accessed, rather than just encrypted. Thus, we are undertaking a review of the files on all those systems. In our investigation, we learned on or about August 10, 2022, that certain personal information of yours was on A&B’s systems and hence potentially accessed by the unauthorized party. We found no evidence that your personal information was misused or even accessed. But out of an abundance of caution, we are notifying you about this incident.

What Information was Involved? Personal information of yours that may have been accessed include name, address, e-mail address, and social security number.

What We Are Doing? Upon identifying the unauthorized access to our systems, we immediately assessed and remediated the unauthorized system access. We have strengthened A&B’s security posture, installed several additional network security applications, updated intrusion detection and prevention policies, and now change critical passwords daily. Additionally, we have obtained complimentary two-year credit monitoring for all potentially affected individuals. We encourage you to take advantage of the free credit monitoring services, which includes fully managed identity recovery and \$1,000,000 in identity theft insurance. Details about this complimentary credit monitoring service are enclosed.

What You Can Do. We recommend that you remain vigilant to the possibility of fraud by reviewing your financial account statements for any suspicious activity. If you identify any suspicious activity, you should immediately report it to your financial institution. You may also review some additional steps you can take to protect your information in the pages that follow this letter.

For More Information. Again, we’re sorry about this development and regret the inconvenience. Should you have questions or concerns, please contact me at (302) 778-1152.

Sincerely,

John M. Seaman

ENCLOSURE

Important Notice

We are offering identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 24 months of Single Bureau Credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

To Enroll, Please Visit: <https://app.idx.us/account-creation/protect>

Or Enroll by Phone: 1-800-939-4170

Enrollment Deadline: December 5, 2022

Enrollment Code: <<insert>>

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some we suggest you consider:

Reviewing Your Accounts and Credit Reports

Federal regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax 1-800-525-6285 Equifax.com	Experian 1-888-397-3742 Experian.com	TransUnion 1-800-680-7289 Transunion.com
---	---	---

You can obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report 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. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft

If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

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. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at www.IdentityTheft.gov. You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of *Identity Theft: A Recovery Plan*, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Special Information for Residents of Maryland and North Carolina

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <http://www.oag.state.md.us/idtheft/index.htm>, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

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 <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, calling 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.



SIDLEY AUSTIN LLP
ONE SOUTH DEARBORN STREET
CHICAGO, IL 60603
+1 312 853 7000
+1 312 853 7036 FAX

AMERICA • ASIA PACIFIC • EUROPE

+1 312 853 7594
TCUNNINGHAM@SIDLEY.COM

VIA EMAIL: IDTheft@oag.state.md.us

January 5, 2023

SUPPLEMENTAL NOTICE OF DATA BREACH

Dear Attorney General Brown:

On behalf of our client, Abrams & Bayliss LLP ("A&B"), we write to provide supplemental notice about a data security incident. We previously notified you about this incident on August 8 and 31, 2022, which then impacted two Maryland residents. On December 9, 2022, A&B discovered that four additional residents were impacted, bringing the total number of Maryland residents impacted to six (6).

On or about January 6, 2023, A&B will send the enclosed notice via U.S. mail to the four additional Maryland residents whose personal information were made available as a result of the security incident. The impacted information includes name, address, email address, date of birth, financial account information, driver's license, passport and social security number.

Since learning of the incident, A&B adopted several new security measures to strengthen the security of its network, internal systems, and applications. A&B is also offering all potentially impacted individuals two years of complimentary credit monitoring.

A&B will continue to monitor the dark web and will also work with our employees to make sure cyber security is top of mind. If you have any questions, please contact us.

Sincerely,

Thomas D. Cunningham

Enc.

ABRAMS & BAYLISS LLP
20 MONTCHANIN ROAD, SUITE 200
WILMINGTON, DE 19807
MAIN: 302-778-1000
FAX: 302-778-1001

NOTICE OF DATA SECURITY INCIDENT

January [REDACTED], 2023

[FIRST NAME] [LAST NAME]
[ADDRESS 1]
[ADDRESS 2]
[CITY] [STATE], [ZIP]

Dear [FIRST NAME]:

Abrams & Bayliss LLP (“A&B”) is writing to inform you of a data security incident that may have affected your personal information. A&B is a full-service law firm in Wilmington, Delaware that provides legal services to clients in a wide variety of industries and business sectors and we hold relevant data to serve our clients. In 2019, A&B participated in routine document exchanges on behalf of one of its clients involved in opioid litigation filed by the State of Delaware. As a result of these exchanges, A&B came into possession of certain documents containing several individuals’ prescription information and other personal information deemed to be Protected Health Information (“PHI”). At this time, we have no indication of fraud or misuse of your information as a result of this incident. Nevertheless, we are notifying you to explain the circumstances and to make you aware of the steps we have taken in response to the incident and the resources that we are making available to you, including complimentary credit monitoring.

What Happened?

On March 17, 2022 we detected a ransomware cyberattack on our local systems. We immediately took measures to control the incident, launched an investigation, and retained a prominent forensics firm and nationally recognized outside counsel to assist. We also notified the FBI and cooperated with them. We fully recovered through our backup systems.

During our review of the data that may have been impacted by this incident, we determined on December 9, 2022 that some of your personal information was on the servers impacted by the incident.

What Information May Have Been Involved?

Our servers contained PHI in connection with routine document exchanges between A&B and the State of Delaware in a civil action captioned *State of Delaware v. Purdue Pharma L.P. et al.*, Civil Action No. N18C-01-223 MMJ CCLD (“*Purdue*”). Your personal information that may have been impacted included certain PHI, such as your full name, date of birth, social security number, health insurance member identification number, prescription medication details, ESI member ID, home address, and other certain protected health information provided to us by the State of Delaware in the *Purdue* case.

What We Are Doing

The safety of your personal information is important to us. We adopted several new security measures to strengthen the security of A&B's network, internal systems, and applications. We will continue to evaluate additional steps that may be taken to further increase A&B's defense going forward.

As an added precaution to help protect your identity, we are offering a complimentary two-year membership through IDX, a data breach and recovery services expert. IDX identity protection services include: 24 months of Single Bureau Credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

To activate your membership and start monitoring your personal information please follow the steps below:

- To Enroll, Please Visit: <https://app.idx.us/account-creation/protect>
- Or Enroll by Phone: 1-800-939-4170
Call Center Hours: Mon-Fri | 6am – 6pm Pacific Time
- Enrollment Deadline: April 20, 2023
- Enrollment Code: [XXXXXX]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in this identify theft product, please contact IDX. Be prepared to provide your Enrollment Code as proof of eligibility for the identity restoration services.

What You Can Do

While we do not have indication of fraud as a result of this incident, in addition to enrolling in the identity theft protection services described above we encourage you to remain vigilant with regards to your personal accounts.

In addition to credit monitoring, we encourage you to review and monitor your account for suspicious activity. Federal regulatory agencies recommend that you remain vigilant for the next 12 to 24 months and report any suspected incidents of fraud to us or the relevant financial institution. We would also encourage you to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information.

Please refer to the enclosure entitled “Additional Ways to Protect Your Identity” for additional actions you should consider taking to protect yourself against fraud and identity theft.

For More Information

We take the security of your information very seriously and sincerely regret any inconvenience or concern. Our customers have always been our first concern and highest priority, and we are

January __, 2023
Page 3

committed to protecting your information and maintaining your trust and confidence. Should you have questions or concerns, please do not hesitate to contact us at (302) 778-1000.

Sincerely,

/s/ *Draft*

John M. Seaman

Important Notice

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some we suggest you consider:

Reviewing Your Accounts and Credit Reports

Federal regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax 1-800-525-6285 Equifax.com	Experian 1-888-397-3742 Experian.com	TransUnion 1-800-680-7289 Transunion.com
---	---	---

You can obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report 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. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft

If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

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. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at www.IdentityTheft.gov. You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of *Identity Theft: A Recovery Plan*, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Special Information for Residents of Iowa, Maryland, Massachusetts, New Mexico, North Carolina, Oregon, Rhode Island, and Vermont

District of Columbia residents may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, (202) 442-9828, <http://www.oag.dc.gov>.

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.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <http://www.oag.state.md.us/idtheft/index.htm>, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

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.

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 may contact the New York Department of State Division of Consumer Protection,

One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, (518) 474-8583 / (800) 697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <http://ag.ny.gov>.

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 <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, calling 1.919.716.6400 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 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

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>.