



2049 Century Park East, Suite 2900, Los Angeles, CA 90067 • (310) 229-1335

March 19, 2024

Pasha A. Sternberg
310-229-1335
psterberg@polsinelli.com

VIA E-MAIL (IDTheft@oag.state.md.us)

Office of Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: Notification of Data Security Incident

To Whom It May Concern:

We represent McMillan Pazdan Smith Architecture (“MPS”), which has a mailing address of 400 Augusta St., Suite 200, Greenville, SC 29601 in connection with a recent incident that involved the personal information of two (2) Maryland residents. We provide this notice on behalf of MPS pursuant to MD. Code. Ann., Com. Law §14-3504 (h).

This notice will be supplemented, if necessary, with any new, significant facts discovered subsequent to its submission. While MPS is notifying you of this incident, MPS does not waive any rights or defenses relating to the incident, this notice, or the applicability of Maryland law on personal jurisdiction.

BACKGROUND OF THE INCIDENT

On January 24, 2024, MPS learned that an unauthorized party gained access to its computer network. Upon discovering this, MPS promptly began an internal investigation and engaged a leading computer forensics firm to further examine its network and confirm the security of its systems. Through that investigation, MPS learned that, between January 8, 2024, and January 24, 2024, the unauthorized party accessed files on the MPS network. MPS reviewed those files to determine what, if any, personal information they contained.

On February 9, 2024, MPS determined that the files contained personal information pertaining to certain individuals. Upon learning this, MPS began compiling a list of the individuals involved and locating current contact information with which to notify the individuals. Once this process was complete, MPS began taking steps to notify the involved individuals. This included drafting notification letters, arranging for complimentary credit monitoring and identify theft protection services, and setting up a call center to assist in timely answering questions from letter recipients.

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Seattle Washington, D.C. Wilmington
Polsinelli PC, Polsinelli LLP in California



March 19, 2024

Page 2

Although MPS is not aware of any instances of identity theft stemming from this event, MPS is notifying these individuals and is offering them complimentary credit monitoring.

NUMBER OF MARYLAND RESIDENTS NOTIFIED

MPS determined that the involved files contained personal information pertaining to two (2) Maryland residents. The involved personal information consisted of name along with Social Security number, health insurance information, and/or health insurance claim information, but may have also included a driver's license number, passport number, bank account information, credit card information, and/or other medical information.

MPS mailed the notification letters to the involved individuals on March 19, 2024. Enclosed is a sample of the notice that is being sent to the individuals via first-class United States mail. As shown in the sample, the notification letter includes an offer for one (1) year of complimentary credit monitoring and identity theft protection services.

STEPS TAKEN RELATING TO THE INCIDENT

As mentioned, MPS identified individuals whose personal information was involved in the incident and is notifying them of the incident via letters that provide information on ways to protect against potential fraud and identity theft, as well as complimentary credit monitoring. Additionally, MPS is taking steps to reduce the risk of this type of incident occurring in the future, including reviewing its technical security measures.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

A handwritten signature in dark ink, appearing to read 'Pasha A. Sternberg'.

Pasha A. Sternberg

Enclosure



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

McMillan Pazdan Smith ("MPS") values and respects your privacy, which is why we are writing to let you know about a recent incident that may have involved some of your personal information. We also wanted to explain the steps that we have taken since discovering the incident and to provide you with information on steps you can take to protect yourself, if you feel that is appropriate.

What Happened? On January 24, 2024, MPS observed evidence of unauthorized access to its network. MPS's investigation found evidence that the unauthorized third party acquired a number of files from MPS's network. MPS has since reviewed these files and confirmed that they contained personal information for a limited number of individuals.

What Information Was Involved? MPS reviewed the contents of the files and on February 9, 2024, determined that they may have contained your name along with your social security number, health insurance information, and/or health insurance claim information. For a limited number of individuals, the information may have also included a driver's license number, passport number, bank account information, credit card information, tax documentation, and/or other medical information.

What We Are Doing. Upon learning about the incident, MPS brought in outside experts to investigate the incident and confirm the security of our environment. We also notified law enforcement of the issue. We take this kind of incident very seriously and are exploring additional security controls to help reduce the risk of this type of incident from occurring in the future. Finally, although we are not aware of any instances of fraud or identity theft, we are offering a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

What You Can Do. You can find more information on steps to protect yourself against potential fraud in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your information seriously, and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call (866) 495-4381 from 8:00 a.m. – 5:30 p.m. Central Time, Monday through Friday, excluding major US holidays.

Sincerely,

A handwritten signature in black ink that reads 'Chad Cousins'.

Chad Cousins, CEO

400 augusta street, suite 200, greenville, sc 29601
o. 864 242 2033 f. 864 242 2034

mcmillanpazdansmith.com

ELN-21372

ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<b2b_text_6(activation deadline)>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: <<activation code s_n>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332. Be prepared to provide engagement number <<b2b_text_1(engagement number from Experian)>> as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 12-MONTH EXPERIAN IDENTITYWORKS credit 3b Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-890-9332 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-890-9332.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: By law, you may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies. The three national credit reporting agencies have also agreed to provide free weekly online credit reports. You can obtain your free credit report by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>. Alternatively, you may elect to purchase a copy of your credit report by contacting the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 1000
Chester, PA 19016

Fraud Alerts: By law, you have the right to place a fraud alert on your credit report if you believe you have been, or are about to become, a victim of fraud or related crime. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com/protectYourIdentity.action.

Credit and Security Freezes: By law, you have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742 <https://www.experian.com/freeze/center.html>
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
<https://www.transunion.com/credit-freeze>
P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Oregon Residents: Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 503-378-4400; <https://www.doj.state.or.us/>.



2049 Century Park East, Suite 2900, Los Angeles, CA 90067 • (310) 229-1335

May 1, 2024

Pasha A. Sternberg
310-229-1335
psterberg@polsinelli.com

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General
Attn: Jeff Karberg, Administrator of the Identity Theft Program
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Supplemental Notification of Data Security Incident

Dear Mr. Karberg:

We represent McMillan Pazdan Smith Architecture (“MPS”), which has a mailing address of 400 Augusta St., Suite 200, Greenville, SC 29601 in connection with a recent incident that involved the personal information of four (4) Maryland residents. We provide this notice on behalf of MPS pursuant to MD. Code. Ann., Com. Law §14-3504 (h). This notice supplements a letter previously sent to your office.

This notice will be supplemented, if necessary, with any new, significant facts discovered subsequent to its submission. While MPS is notifying you of this incident, MPS does not waive any rights or defenses relating to the incident, this notice, or the applicability of Maryland law on personal jurisdiction.

BACKGROUND OF THE INCIDENT

As previously disclosed, on January 24, 2024, MPS learned that an unauthorized party gained access to its computer network. Upon discovering this, MPS promptly began an internal investigation and engaged a leading computer forensics firm to further examine its network and confirm the security of its systems. Through that investigation, MPS learned that, between January 8, 2024, and January 24, 2024, the unauthorized party accessed files on the MPS network. MPS reviewed those files to determine what, if any, personal information they contained.

On February 9, 2024, MPS determined that the files contained personal information pertaining to certain individuals. Upon learning this, MPS began compiling a list of the individuals involved and locating current contact information with which to notify the individuals. Once this process

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Seattle Washington, D.C. Wilmington
Polsinelli PC, Polsinelli LLP in California

May 1, 2024

Page 2

was complete, on March 19, 2024, MPS began taking steps to notify the involved individuals. This included drafting notification letters, arranging for complimentary credit monitoring and identify theft protection services, and setting up a call center to assist in timely answering questions from letter recipients.

On April 12, 2024, MPS identified additional individuals that may have been impacted by the event, including two (2) additional Maryland residents, that had not been notified previously. Therefore, MPS began preparing to notify the additional individuals.

MPS is not aware of any instances of identity theft stemming from this event.

NUMBER OF MARYLAND RESIDENTS NOTIFIED

On March 19, 2024, MPS began mailing notification letters to impacted individuals and provided them with an offer for complimentary credit monitoring. MPS mailed notification letters to the additional individuals identified on May 1, 2024, including two (2) Maryland residents. To date, MPS has notified four (4) Maryland residents of the incident.

The involved personal information consisted of name along with Social Security number, health insurance information, and/or health insurance claim information, but may have also included a driver's license number, passport number, bank account information, credit card information, and/or other medical information. Enclosed is a sample of the notice that is being sent to the individuals via first-class United States mail. As shown in the sample, the notification letter includes an offer for one (1) year of complimentary credit monitoring and identity theft protection services.

STEPS TAKEN RELATING TO THE INCIDENT

As mentioned, MPS identified individuals whose personal information was involved in the incident and is notifying them of the incident via letters that provide information on ways to protect against potential fraud and identity theft, as well as complimentary credit monitoring. Additionally, MPS is taking steps to reduce the risk of this type of incident occurring in the future, including reviewing its technical security measures.



May 1, 2024
Page 3

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Pasha A. Sternberg

Enclosure



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

McMillan Pazdan Smith ("MPS") values and respects your privacy, which is why we are writing to let you know about a recent incident that may have involved some of your personal information. We also wanted to explain the steps that we have taken since discovering the incident and to provide you with information on steps you can take to protect yourself, if you feel that is appropriate.

What Happened? On January 24, 2024, MPS observed evidence of unauthorized access to its network. MPS's investigation found evidence that the unauthorized third party acquired a number of files from MPS's network. MPS has since reviewed these files and confirmed that they contained personal information for a limited number of individuals.

What Information Was Involved? MPS reviewed the contents of the files and on February 9, 2024, determined that they may have contained your name along with your social security number, health insurance information, and/or health insurance claim information. For a limited number of individuals, the information may have also included a driver's license number, passport number, bank account information, credit card information, tax documentation, and/or other medical information.

What We Are Doing. Upon learning about the incident, MPS brought in outside experts to investigate the incident and confirm the security of our environment. We also notified law enforcement of the issue. We take this kind of incident very seriously and are exploring additional security controls to help reduce the risk of this type of incident from occurring in the future. Finally, although we are not aware of any instances of fraud or identity theft, we are offering a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

What You Can Do. You can find more information on steps to protect yourself against potential fraud in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your information seriously, and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call (866) 495-4381 from 8:00 a.m. – 5:30 p.m. Central Time, Monday through Friday, excluding major US holidays.

Sincerely,

A handwritten signature in black ink that reads 'Chad Cousins'.

Chad Cousins, CEO

400 augusta street, suite 200, greenville, sc 29601
o. 864 242 2033 f. 864 242 2034

mcmillanpazdansmith.com

ELN-21372

ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<b2b_text_6(activation deadline)>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: <<activation code s_n>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332. Be prepared to provide engagement number <<b2b_text_1(engagement number from Experian)>> as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 12-MONTH EXPERIAN IDENTITYWORKS credit 3b Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-890-9332 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-890-9332.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: By law, you may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies. The three national credit reporting agencies have also agreed to provide free weekly online credit reports. You can obtain your free credit report by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>. Alternatively, you may elect to purchase a copy of your credit report by contacting the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 1000
Chester, PA 19016

Fraud Alerts: By law, you have the right to place a fraud alert on your credit report if you believe you have been, or are about to become, a victim of fraud or related crime. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com/protectYourIdentity.action.

Credit and Security Freezes: By law, you have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742 <https://www.experian.com/freeze/center.html>
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
<https://www.transunion.com/credit-freeze>
P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Oregon Residents: Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 503-378-4400; <https://www.doj.state.or.us/>.