
Good afternoon,

I am writing to you today on behalf of Philips Respironics International Colorado, Inc. (RICO), a supplier of durable medical equipment. RICO's parent company, Philips Respironics, was notified on June 5, 2023 of a security vulnerability in a data transfer tool it uses known as MOVEit. RICO uses the MOVEit Transfer tool in its management of therapy data for medical devices. The MOVEit security vulnerability had a significant global impact, affecting hundreds of organizations worldwide. RICO and Philips Respironics took steps to investigate and respond to the security incident. On November 2, 2023, Philips' ongoing investigation confirmed that an unauthorized party exploited the MOVEit software vulnerability and extracted files on May 31, 2023. After further analysis, on December 1, 2023, Philips determined which individuals' information potentially was involved in this incident.

Based on the investigation, the breach incident occurred on May 31, 2023 and was contained on June 5, 2023. The breach was discovered by Philips on December 1, 2023.

RICO further determined that 7,869 Maryland residents were affected by the breach. The breach affected the following data elements: name, address, date of birth, e-mail address, phone number, patient ID, facility ID, device serial number, modem serial number, physician, and device usage.

RICO and Philips Respironics promptly suspended their use of MOVEit and resumed use after installation of a patch. RICO and Philips Respironics also continue to strengthen their security protocols through measures such as enhanced encryption, aiming to minimize the risk of any future incidents. RICO is working closely with Philips Respironics to notify all impacted parties, including Maryland residents. To help protect the identity of Maryland residents, RICO is offering a complimentary one-year membership to Experian's Identity Works services, which include credit monitoring and identity restoration services.

Please see a copy of the notice that will be provided to Maryland residents attached. The notice will be provided today, January 11, 2024.

Please do not hesitate to contact Reece Hirsch should you have any questions. Reece can most easily be reached at reece.hirsch@morganlewis.com or 415.442.1422.

Thank you.

Sydney Reed Swanson

Morgan, Lewis & Bockius LLP

1000 Louisiana Street, Suite 4000 | Houston, TX 77002-5005

Direct: +1.713.890.5105 | Main: +1.713.890.5000 | Fax: +1.713.890.5001
sydney.swanson@morganlewis.com | www.morganlewis.com



150 YEARS OF RAISING THE BAR

Learn More



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

Important Security Notification. Please read this entire letter.

Dear <<Name 1>>,

Subject: Notice of Data Breach

Philips Respironics International Colorado, Inc. (“Respironics Colorado, Inc., a Philips company”), a supplier of durable medical equipment, is writing to inform you of a security incident potentially involving your personal data. We place a high value on maintaining the privacy and security of the information we maintain for our customers. This message is to inform you of the situation, the steps taken in response, and what you can do.

What Happened

RICO’s parent company, Philips Respironics, was notified on June 5, 2023 of a security vulnerability in a data transfer tool it uses known as MOVEit. RICO uses the MOVEit Transfer tool in its management of therapy data for medical devices. The MOVEit security vulnerability had a significant global impact, affecting hundreds of organizations worldwide. RICO and Philips Respironics took steps to investigate and respond to the security incident.

On November 2, 2023, our ongoing investigation confirmed that an unauthorized party exploited the MOVEit software vulnerability and extracted files on May 31, 2023. After further analysis, on December 1, 2023, we determined that some of your information potentially was involved in this incident. This data may include your name, address, date of birth, e-mail address, phone number, patient ID, facility ID, device serial number, modem serial number, physician, and device usage. <<This incident affected 30,002 Texas residents.>>

What We Are Doing

We are working closely with Philips Respironics to notify all impacted parties. RICO and Philips Respironics temporarily suspended their use of MOVEit as a proactive measure which is part of an effort to strengthen their security protocols such as enhanced encryption, aiming to minimize the risk of any future incidents.

Further, to help protect your identity, RICO is offering a complimentary one-year membership to Experian’s Identity Works services, which include credit monitoring and identity restoration services. You can enroll in these complimentary services by following the enrollment instructions contained in this letter.

What You Can Do

Please be on the lookout for any scams that ask you to provide your personal information in connection with this incident. We will NOT call you or send you any email messages asking for your personal information or credit card information in relation to this incident or send you any email messages asking you to “click” on any links to activate identity protection services. You should not provide information in response to any such calls or email messages, and you should not click on any links within any such email messages.

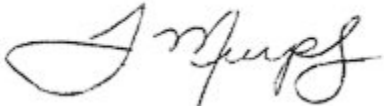
You will find additional details in the enclosed “General Information About Identity Theft Protection” document.

For More Information

We sincerely apologize for the inconvenience and concern this incident may cause you. If you have any questions regarding this incident, please call 888-541-3407, Monday through Friday, 9:00 AM to 9:00 PM Eastern Time.

Thank you for your understanding and support in this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Tim Murphy". The signature is fluid and cursive, with the first name "Tim" being more prominent than the last name "Murphy".

Tim Murphy
Business Leader
Sleep & Respiratory Care

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: <<enrollment deadline>> Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [URL]
3. PROVIDE the **Activation Code**: <<Activation Code>>

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 [PHONE NUMBER]. Be prepared to provide engagement number <<ENGAGEMENT NUMBER>> 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 file 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 [URL]
or call [PHONE NUMBER] 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 [PHONE NUMBER].

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annualreport-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact the nationwide credit reporting agencies at:

Equifax

1-866-640-2273

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

1-855-681-3196

www.transunion.com

P.O. Box 2000

Chester, PA 19016

Fraud Alerts. You may place a fraud alert on your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put 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 a 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. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *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 indicated above. You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the respective address indicated above.

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and proof of current residential address (e.g., a copy of a utility bill, bank or insurance statement). Each copy should be legible, display your name and current mailing address, and the date of issue. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, the agency cannot charge you to place, lift or remove a security freeze. In all other cases, the credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

If you are a Connecticut resident, you may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

If you are a District of Columbia resident, you may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov. **If you are an Iowa resident,** state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

If you are a Kentucky resident, for more information on steps you may take to avoid identity theft, you may contact the Office of the Kentucky Attorney General at: 700 Capital Avenue, Suite 118, Frankfort, KY 40601-3449, <https://www.ag.ky.gov/Pages/default.aspx>, 1-888-432-9257.

If you are a Maryland resident, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement or to the FTC. You can contact the Oregon Attorney General at: 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, 1-877 877-9392.

If you are a Rhode Island resident, you have the right to obtain a police report. You also have the right to request a security freeze, as described above. You can also contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov/>, (401) 274-4400 or file a police report by contacting (401) 444-1000.

If you are a West Virginia resident, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

Important Security Notification. Please read this entire letter.

Dear <<Name 1>>,

Subject: Notice of Data Breach

Philips Respironics International Colorado, Inc. (“Respironics Colorado, Inc., a Philips company”), a supplier of durable medical equipment, is writing to inform you of a security incident potentially involving your personal data. We place a high value on maintaining the privacy and security of the information we maintain for our customers. This message is to inform you of the situation, the steps taken in response, and what you can do.

What Happened

RICO’s parent company, Philips Respironics, was notified on June 5, 2023 of a security vulnerability in a data transfer tool it uses known as MOVEit. RICO uses the MOVEit Transfer tool in its management of therapy data for medical devices. The MOVEit security vulnerability had a significant global impact, affecting hundreds of organizations worldwide. RICO and Philips Respironics took steps to investigate and respond to the security incident.

On November 2, 2023, our ongoing investigation confirmed that an unauthorized party exploited the MOVEit software vulnerability and extracted files on May 31, 2023. After further analysis, on December 1, 2023, we determined that some of your information potentially was involved in this incident. This data may include your name, address, date of birth, e-mail address, phone number, patient ID, facility ID, device serial number, modem serial number, physician, and device usage. <<This incident affected 30,002 Texas residents.>>

What We Are Doing

We are working closely with Philips Respironics to notify all impacted parties. RICO and Philips Respironics temporarily suspended their use of MOVEit as a proactive measure which is part of an effort to strengthen their security protocols such as enhanced encryption, aiming to minimize the risk of any future incidents.

Further, to help protect your identity, RICO is offering a complimentary one-year membership to Experian’s Identity Works services, which include credit monitoring and identity restoration services. You can enroll in these complimentary services by following the enrollment instructions contained in this letter.

What You Can Do

Please be on the lookout for any scams that ask you to provide your personal information in connection with this incident. We will NOT call you or send you any email messages asking for your personal information or credit card information in relation to this incident or send you any email messages asking you to “click” on any links to activate identity protection services. You should not provide information in response to any such calls or email messages, and you should not click on any links within any such email messages.

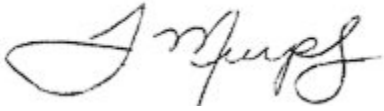
You will find additional details in the enclosed “General Information About Identity Theft Protection” document.

For More Information

We sincerely apologize for the inconvenience and concern this incident may cause you. If you have any questions regarding this incident, please call 888-541-3407, Monday through Friday, 9:00 AM to 9:00 PM Eastern Time.

Thank you for your understanding and support in this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Tim Murphy". The signature is fluid and cursive, with the first name "Tim" being more prominent than the last name "Murphy".

Tim Murphy
Business Leader
Sleep & Respiratory Care

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: <<enrollment deadline>> Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [\[URL\]](#)
3. PROVIDE the **Activation Code**: <<Activation Code>>

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 [\[PHONE NUMBER\]](#). Be prepared to provide engagement number <<ENGAGEMENT NUMBER>> 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 file 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 [\[URL\]](#)
or call [\[PHONE NUMBER\]](#) 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 [\[PHONE NUMBER\]](#).

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annualreport-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact the nationwide credit reporting agencies at:

Equifax

1-866-640-2273

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

1-855-681-3196

www.transunion.com

P.O. Box 2000

Chester, PA 19016

Fraud Alerts. You may place a fraud alert on your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put 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 a 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. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *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 indicated above. You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the respective address indicated above.

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and proof of current residential address (e.g., a copy of a utility bill, bank or insurance statement). Each copy should be legible, display your name and current mailing address, and the date of issue. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, the agency cannot charge you to place, lift or remove a security freeze. In all other cases, the credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

If you are a Connecticut resident, you may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

If you are a District of Columbia resident, you may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov. **If you are an Iowa resident,** state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

If you are a Kentucky resident, for more information on steps you may take to avoid identity theft, you may contact the Office of the Kentucky Attorney General at: 700 Capital Avenue, Suite 118, Frankfort, KY 40601-3449, <https://www.ag.ky.gov/Pages/default.aspx>, 1-888-432-9257.

If you are a Maryland resident, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement or to the FTC. You can contact the Oregon Attorney General at: 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, 1-877 877-9392.

If you are a Rhode Island resident, you have the right to obtain a police report. You also have the right to request a security freeze, as described above. You can also contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov/>, (401) 274-4400 or file a police report by contacting (401) 444-1000.

If you are a West Virginia resident, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.