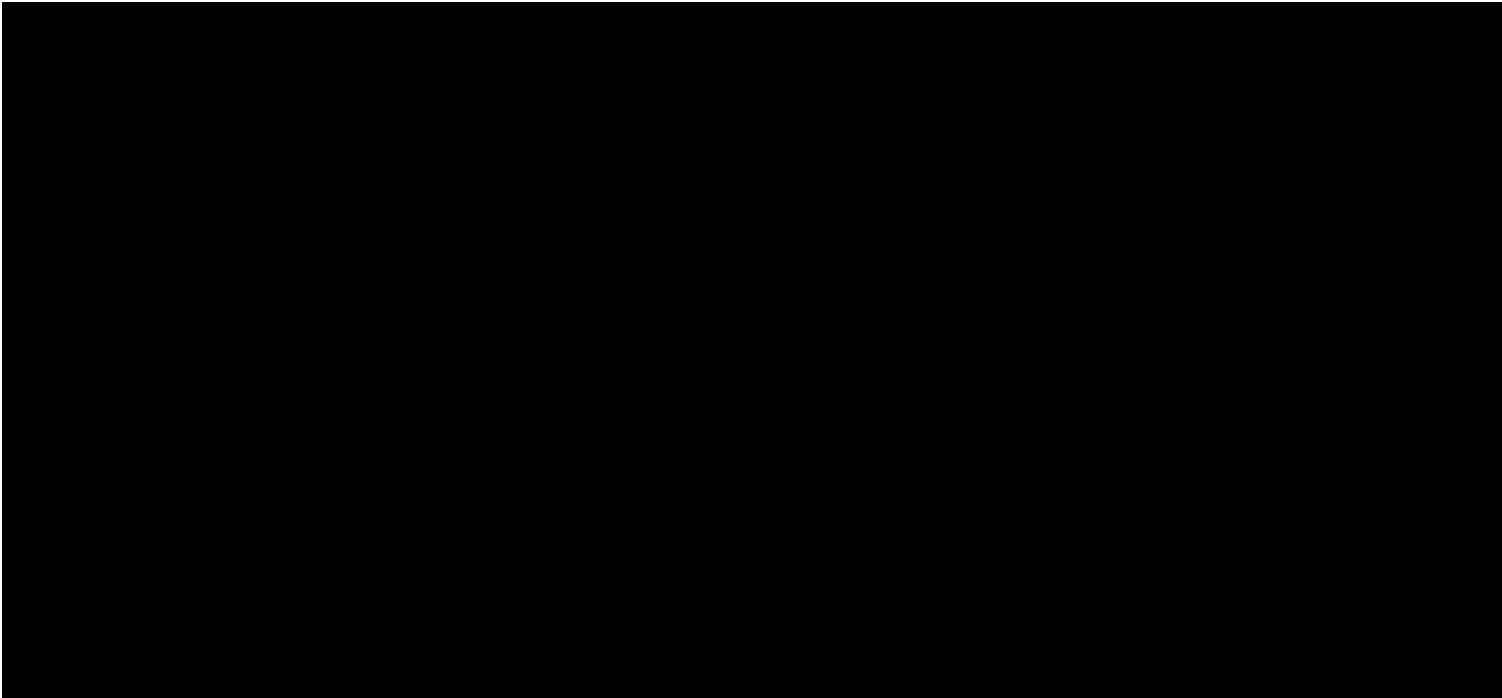




Dear Sir/Ma'am:

This firm represents Urology of Greater Atlanta ("UGA"), and is providing this notice pursuant to the Maryland Personal Information Protection Act.

On August 29, 2021 UGA discovered suspicious activity on its system. The system was immediately taken off-line and the practice's cyber carrier was contacted. The cyber carrier contacted counsel and forensic investigators (Unit 42 of Palo Alto Network) were immediately hired. The forensic investigation determined that unauthorized access to the system had occurred via remote desk protocol on several occasions during the period August 8 to August 29, 2021. Forensic investigation further determined that 42,316 files had been downloaded from UGA's file servers on August 8, but that no files were accessed or downloaded during any subsequent intrusion to the system. Forensic investigation further confirmed that there had been no intrusion to UGA's medical records data base or billing and practice management system; rather, a substantial portion of the stolen files contained data that was largely "legacy" data and was many (at least 10) years old. Remedial steps were taken by UGA's IT vendor in consultation with Unit 42, including scans of existing practice data, re-installing software and replacing the system's firewall. UGA also has revised its remote desk protocol procedures.

Because the stolen files consisted largely of scans or "printed" documents, manual review was necessary to determine the personal information (if any) that may have been contained in these documents. A third-party vendor was therefore hired to data mine and review these documents, and identify the personal information contained therein. In addition, because much of this information was at least 10 years old and often was incomplete, the results of the data mining and review was then manually compared against UGA's current data to update and obtain complete data (such as mailing addresses). This process was lengthy and extensive, and ultimately determined that the Protected Health Information ("PHI") as defined by federal law of over 70,000 patients had been compromised, including the personal information (Social Security number, driver's license number, account information and/or health information) of 44 residents of Maryland.

Following this incident, UGA replaced its firewall (which was determined to be the likely source of the unauthorized entry) and revised its remote access protocol (which now is by VPN); UGA also re-installed software and confirmed the security of its data.

UGA will be sending notification to affected persons by First-class mail and making substitute notice including website and media announcements on Monday, November 28. Copies of the form of notification are attached hereto; please note that credit monitoring/identity protection services are being provided to all affected persons. Notifications already have been made to the three major credit bureaus, Experian, Equifax and Transunion.

If you have any questions or require any additional information, please contact Ms. Cambre, whose is copied here and whose contact information is shown in the signature block below.

John Dalbey



Brittany M. Cambre | Partner

CHILIVIS GRUBMAN

1834 Independence Square | Atlanta, Georgia 30338

Main: 404.233.4171 | **Direct:** 404.262.6502 | **E:** bcambre@cglawfirm.com

Confidentiality Notice

This message is being sent by or on behalf of a lawyer. It is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged or confidential, or otherwise legally protected from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by return e-mail and delete all copies of the message.



P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-896-7100

Or Visit:

<https://app.idx.us/account-creation/protect>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>

<<ADDRESS1>>

<<ADDRESS2>>

<<CITY>>, <<STATE>> <<ZIP>>

<<Country>>

November 28, 2022

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

You are receiving this letter from us at Urology of Greater Atlanta because you have been a patient, or a loved one or a caretaker of a patient receiving care from one of our physician locations or our affiliate Surgical Center for Urology. Urology of Greater Atlanta sincerely appreciates that you have entrusted us with your care and the confidentiality of your information. As such, we want to notify you of a data security event.

What Happened

On August 29, 2021, Urology of Greater Atlanta learned that an unauthorized user had accessed portions of our computer system during the period from August 8 to August 29, 2021. Upon learning of this illegal access, we immediately blocked such access and hired third-party computer security experts to investigate and to assist us.

The investigation and review were lengthy and detailed, and ultimately determined that while the unauthorized user did not access our electronic medical record database or billing and practice management systems, the unauthorized user was able to access and/or acquire files containing certain personal information. There is no evidence that any of the accessed information has been improperly used. Nevertheless, we are notifying you of this event and providing you with free identity theft protection and credit monitoring.

What Information Was Involved

The files that were accessed held documents containing protected health information that may have included full name, address, date of birth, age, <<Variable Text 3>> date of service, patient account number, diagnoses and treatment, and medical history. **Fortunately, after extensive investigation, we do NOT believe any bank account, credit card number or other financial information, or Social Security number, was contained in the affected documents containing your information.**

What We Are Doing

Since this event, we have worked extensively with our outside security consultants to implement additional safeguards to further protect and secure our patient information. These additional safeguards include replacing certain components of our computer system and changing the remote access protocols for our systems.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-896-7100 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 28, 2023.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives are knowledgeable about the incident and can answer questions or concerns you may have regarding protection of your personal information.

You will find detailed instructions for enrollment in the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-896-7100 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read "J Libby MD".

James M. Libby, MD, FACS
Managing Director
Urology of Greater Atlanta

(Enclosure)



Recommended Steps to Help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-896-7100 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-896-7100

Or Visit:

<https://app.idx.us/account-creation/protect>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>

<<ADDRESS1>>

<<ADDRESS2>>

<<CITY>>, <<STATE>> <<ZIP>>

<<Country>>

November 28, 2022

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

You are receiving this letter from us at Urology of Greater Atlanta because you have been a patient, or a loved one or a caretaker of a patient receiving care from one of our physician locations or our affiliate Surgical Center for Urology. Urology of Greater Atlanta sincerely appreciates that you have entrusted us with your care and the confidentiality of your information. As such, we want to notify you of a data security event.

What Happened

On August 29, 2021, Urology of Greater Atlanta learned that an unauthorized user had accessed portions of our computer system during the period from August 8 to August 29, 2021. Upon learning of this illegal access, we immediately blocked such access and hired third-party computer security experts to investigate and to assist us.

The investigation and review were lengthy and detailed, and ultimately determined that while the unauthorized user did not access our electronic medical record database or billing and practice management systems, the unauthorized user was able to access and/or acquire files containing certain personal information. There is no evidence that any of the accessed information has been improperly used. Nevertheless, we are notifying you of this event and providing you with free identity theft protection and credit monitoring.

What Information Was Involved

The files that were accessed held documents containing protected health information that may have included full name, address, date of birth, age, <<Variable Text 3>> date of service, patient account number, diagnoses and treatment, medical history, and social security number. **Fortunately, after extensive investigation, we do NOT believe any bank account, credit card number or other financial information was contained in the affected documents containing your information.**

What We Are Doing

Since this event, we have worked extensively with our outside security consultants to implement additional safeguards to further protect and secure our patient information. These additional safeguards include replacing certain components of our computer system and changing the remote access protocols for our systems.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-896-7100 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 28, 2023.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives are knowledgeable about the incident and can answer questions or concerns you may have regarding protection of your personal information.

You will find detailed instructions for enrollment in the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-896-7100 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read "J Libby MD".

James M. Libby, MD, FACS
Managing Director
Urology of Greater Atlanta

(Enclosure)



Recommended Steps to Help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-896-7100 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-896-7100

Or Visit:

<https://app.idx.us/account-creation/protect>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>

<<ADDRESS1>>

<<ADDRESS2>>

<<CITY>>, <<STATE>> <<ZIP>>

<<Country>>

November 28, 2022

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

You are receiving this letter from us at Urology of Greater Atlanta because you have been a patient, or a loved one or a caretaker of a patient receiving care from one of our physician locations or our affiliate Surgical Center for Urology. Urology of Greater Atlanta sincerely appreciates that you have entrusted us with your care and the confidentiality of your information. As such, we want to notify you of a data security event.

What Happened

On August 29, 2021, Urology of Greater Atlanta learned that an unauthorized user had accessed portions of our computer system during the period from August 8 to August 29, 2021. Upon learning of this illegal access, we immediately blocked such access and hired third-party computer security experts to investigate and to assist us.

The investigation and review were lengthy and detailed, and ultimately determined that while the unauthorized user did not access our electronic medical record database or billing and practice management systems, the unauthorized user was able to access and/or acquire files containing certain personal information. There is no evidence that any of the accessed information has been improperly used. Nevertheless, we are notifying you of this event and providing you with free identity theft protection and credit monitoring.

What Information Was Involved

The files that were accessed held documents containing protected health information that may have included full name, address, date of birth, age, <<Variable Text 3>> date of service, patient account number, diagnoses and treatment, medical history, and financial account number. **Fortunately, after extensive investigation, we do NOT believe your social security number was contained in the affected documents.**

What We Are Doing

Since this event, we have worked extensively with our outside security consultants to implement additional safeguards to further protect and secure our patient information. These additional safeguards include replacing certain components of our computer system and changing the remote access protocols for our systems.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-896-7100 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 28, 2023.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives are knowledgeable about the incident and can answer questions or concerns you may have regarding protection of your personal information.

You will find detailed instructions for enrollment in the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-896-7100 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read "J Libby MD".

James M. Libby, MD, FACS
Managing Director
Urology of Greater Atlanta

(Enclosure)



Recommended Steps to Help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-896-7100 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-896-7100

Or Visit:

<https://app.idx.us/account-creation/protect>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>

<<ADDRESS1>>

<<ADDRESS2>>

<<CITY>>, <<STATE>> <<ZIP>>

<<Country>>

November 28, 2022

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

You are receiving this letter from us at Urology of Greater Atlanta because you have been a patient, or a loved one or a caretaker of a patient receiving care from one of our physician locations or our affiliate Surgical Center for Urology. Urology of Greater Atlanta sincerely appreciates that you have entrusted us with your care and the confidentiality of your information. As such, we want to notify you of a data security event.

What Happened

On August 29, 2021, Urology of Greater Atlanta learned that an unauthorized user had accessed portions of our computer system during the period from August 8 to August 29, 2021. Upon learning of this illegal access, we immediately blocked such access and hired third-party computer security experts to investigate and to assist us.

The investigation and review were lengthy and detailed, and ultimately determined that while the unauthorized user did not access our electronic medical record database or billing and practice management systems, the unauthorized user was able to access and/or acquire files containing certain personal information. There is no evidence that any of the accessed information has been improperly used. Nevertheless, we are notifying you of this event and providing you with free identity theft protection and credit monitoring.

What Information Was Involved

The files that were accessed held documents containing protected health information that may have included full name, address, date of birth, age, <<Variable Text 3>> date of service, patient account number, diagnoses and treatment, medical history, social security number, and financial account number.

What We Are Doing

Since this event, we have worked extensively with our outside security consultants to implement additional safeguards to further protect and secure our patient information. These additional safeguards include replacing certain components of our computer system and changing the remote access protocols for our systems.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-896-7100 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 28, 2023.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives are knowledgeable about the incident and can answer questions or concerns you may have regarding protection of your personal information.

You will find detailed instructions for enrollment in the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-896-7100 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read "J Libby MD".

James M. Libby, MD, FACS
Managing Director
Urology of Greater Atlanta

(Enclosure)



Recommended Steps to Help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-896-7100 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-896-7100

Or Visit:

<https://app.idx.us/account-creation/protect>
Enrollment Code: <<ENROLLMENT>>

c/o Parent/Legal Guardian

<<FIRST NAME>> <<LAST NAME>>

<<ADDRESS1>>

<<ADDRESS2>>

<<CITY>>, <<STATE>> <<ZIP>>

<<Country>>

November 28, 2022

Notice of Data Breach

Dear Parent or Legal Guardian of <<FIRST NAME>> <<LAST NAME>>,

You are receiving this letter from us at Urology of Greater Atlanta because your minor may have been a patient of one of our physician locations or our affiliate Surgical Center for Urology. Urology of Greater Atlanta sincerely appreciates that you have entrusted us with your minor's care and the confidentiality of your minor's information. As such, we want to notify you of a data security event.

What Happened

On August 29, 2021, Urology of Greater Atlanta learned that an unauthorized user had accessed portions of our computer system during the period from August 8 to August 29, 2021. Upon learning of this illegal access, we immediately blocked such access and hired third-party computer security experts to investigate and to assist us.

The investigation and review were lengthy and detailed, and ultimately determined that while the unauthorized user did not access our electronic medical record database or billing and practice management systems, the unauthorized user was able to access and/or acquire files containing certain personal information. There is no evidence that any of the accessed information has been improperly used. Nevertheless, we are notifying you of this event and providing you with free identity theft protection.

What Information Was Involved

The files that were accessed held documents containing protected health information that may have included your minor's full name, address, date of birth, age, <<Variable Text 3>> date of service, patient account number, diagnoses and treatment, and medical history. **Fortunately, after extensive investigation, we do NOT believe any bank account, credit card number or other financial information, or Social Security number, was contained in the affected documents containing your minor's information.**

What We Are Doing

Since this event, we have worked extensively with our outside security consultants to implement additional safeguards to further protect and secure our patient information. These additional safeguards include replacing certain components of our computer system and changing the remote access protocols for our systems.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include <<12/24>> months of CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your minor's identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll your minor in the free identity protection services by calling 1-833-896-7100 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 28, 2023.

Again, at this time, there is no evidence that your minor's information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives are knowledgeable about the incident and can answer questions or concerns you may have regarding protection of your minor's personal information.

You will find detailed instructions for enrollment in the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-896-7100 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read "J Libby MD".

James M. Libby, MD, FACS
Managing Director
Urology of Greater Atlanta

(Enclosure)



Recommended Steps to Help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Telephone. Contact IDX at 1-833-896-7100 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

3. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

5. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.