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

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

RE: Notice of Data Privacy Event

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Loudoun Medical Group d/b/a Comprehensive Sleep Care Center ("CSCC") writes to notify you of a recent event that may affect the security of some of your personal information. While, to date, we have no evidence that your information has been misused, we are making you aware of the event, so you may take steps to better protect your information, should you feel it appropriate to do so.

***What Happened?*** On or around June 19, 2019, the Loudoun Medical Group Information Technology (LMG IT) Department became aware of unusual activity related to a CSCC employee's email account. LMG IT immediately took steps to respond to and investigate this activity and change the user's password. Based on this review, LMG IT determined that an unauthorized individual may have gained access to the employee's email account. LMG IT immediately commenced a comprehensive investigation to determine the nature and scope of the incident. Through the investigation, which included working with third party forensic investigators, LMG IT determined that an unauthorized actor(s) gained access to a single CSCC employee email account between June 15, 2019 and June 19, 2019. CSCC then commenced a detailed and diligent review of all data present in the account to determine what records were present, to whom that data related, and contact information for those individuals. This process was completed on or around October 17, 2019. While, to date, the investigation has found no evidence of actual or attempted misuse of data, we did determine that the email account affected by this incident contained certain personal information.

***What Information Was Involved?*** Our investigation determined that the following information related to you was present in the email account at the time of the incident: <<ClientDef1(Impacted Data)>><<ClientDef(Impacted Data)>>.

***What We Are Doing.*** CSCC places the highest priority on the confidentiality, privacy and security of the personal information in our care. Upon learning of unusual activity in an employee email account, we immediately commenced an investigation to confirm the nature and scope of the event and identify what personal information may have been present in the affected emails. With the assistance of third-party forensic investigators, we have been working to identify and put in place resources to assist potentially affected individuals and are implementing additional safeguards to further protect the security of information in our systems. We will also be reporting this incident to the U.S. Department of Health and Human Services and state regulators, as appropriate.

As an added precaution, we are offering you access to one year of identity monitoring and fraud consultation and restoration services for twelve (12) months at no cost to you. The cost of these services will be paid for by CSCC. More information on these services, as well as instructions about how to activate your services, may be found in the enclosed "Privacy Safeguards." Please note that you must complete the activation process, as we are not able to activate these services on your behalf.

***What You Can Do.*** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity and to detect errors. You may also find more information in the enclosed "Privacy Safeguards," as well as detail on how to activate to receive the identity monitoring, fraud consultation and identity theft restoration services we are offering at no cost to you.

***For More Information.*** We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-946-0125, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Loudoun Medical Group d/g/a Comprehensive Sleep Care Center

Kroll | A Division of DUFF&PHELPS

## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

### Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

### Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## PRIVACY SAFEGUARDS

### Activate Your Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

*You have until **February 3, 2020** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

### Monitor Accounts

Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

### Security Freeze

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

| **Experian** | **TransUnion** | **Equifax** |
|---|---|---|
| PO Box 9554 | PO Box 160 | PO Box 105788 |
| Allen, TX 75013 | Woodlyn, PA 19094 | Atlanta, GA 30348-5788 |
| 1-888-397-3742 | 1-888-909-8872 | 1-800-349-9960 |
| www.experian.com/freeze/center.html | www.transunion.com/credit-freeze | www.equifax.com/personal/credit-report-services |

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

### Fraud Alert

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

| **Experian** | **TransUnion** | **Equifax** |
|---|---|---|
| P.O. Box 2002 | P.O. Box 2000 | P.O. Box 105069 |
| Allen, TX 75013 | Chester, PA 19106 | Atlanta, GA 30348 |
| 1-888-397-3742 | 1-800-680-7289 | 1-800-525-6285 |
| www.experian.com/fraud/center.html | www.transunion.com/fraud-victim-resource/place-fraud-alert | www.equifax.com/personal/credit-report-services |

**Additional Information**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); or TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

*For Maryland residents,* the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; or www.oag.state.md.us. Loudoun is located at 1718 Patterson Street, Nashville, TN 37203.

*For 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 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. We encourage you to 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.

*For North Carolina residents,* the North Carolina Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6000; and www.ncdoj.gov.

*For Rhode Island residents,* the Rhode Island Attorney General can be contacted at: 150 South Main Street, Providence, RI 02903; (401) 274-4400; or www.riag.ri.gov. A total of three (3) Rhode Island residents are potentially impacted by this incident. You have the right to file and obtain a police report if you ever experience identity theft or fraud. Please note that, in order to file a crime report or incident report with law enforcement for identity theft, you may be asked to provide some kind of proof that you have been a victim.

*For 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/.

## NOTICE OF DATA INCIDENT

### ABOUT THE DATA PRIVACY EVENT

Loudoun Medical Group d/b/a Comprehensive Sleep Care Center (CSCC) recently learned of an incident that may affect the privacy of certain information. Loudoun Medical Group d/b/a CSCC is providing notice of the event so potentially affected individuals may take steps to better protect their personal information, should they feel it appropriate to do so.

### FREQUENTLY ASKED QUESTIONS

***What Happened?*** On or around June 19, 2019, the Loudoun Medical Group Information Technology (LMG IT) Department became aware of unusual activity related to a CSCC employee's email account. LMG IT immediately took steps to respond to and investigate this activity and change the user's password. Based on this review, LMG IT determined that an unauthorized individual may have gained access to the employee's email account. LMG IT immediately commenced a comprehensive investigation to determine the nature and scope of the incident. Through the investigation, which included working with third party forensic investigators, LMG IT determined that an unauthorized actor(s) gained access to a single Loudoun employee email account between June 15, 2019 and June 19, 2019. CSCC then commenced a detailed and diligent review of all data present in the account to determine what records were present, to whom that data related, and contact information for those individuals. This process was completed on or around October 17, 2019. While, to date, the investigation has found no evidence of actual or attempted misuse of data, we did determine that the email account affected by this incident contained certain personal information.

***What Information Was Involved?*** The information present in the emails varies by individual, but may include patient name, date of birth, Social Security number, driver's license number, passport number, medical record number, patient account number, payment card information, financial account information, medical history, health insurance information, treatment information and/or date(s) of service.

***What is Loudoun Doing?*** CSCC places the highest priority on the confidentiality, privacy and security of the personal information in our care. Upon learning of unusual activity in an employee email account, we immediately commenced an investigation to confirm the nature and scope of the event and identify what personal information may have been present in the affected emails. With the assistance of third-party forensic investigators, we have been working to identify and put in place resources to assist potentially affected individuals and are implementing additional safeguards to further protect the security of information in our systems. We will also be reporting this incident to the U.S. Department of Health and Human Services and state regulators, as appropriate.

***What Can You Do?*** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity and to detect errors. CSCC also encourages individuals to review and consider the information and resources outlined in the below "Steps You May Take To Protect Personal Information."

***For More Information.*** If you have additional questions, please call our dedicated assistance line at 1-855-946-0125, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

## STEPS YOU MAY TAKE TO PROTECT PERSONAL INFORMATION

**Monitor Accounts**

Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

**Security Freeze**

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

| **Experian** | **TransUnion** | **Equifax** |
|---|---|---|
| PO Box 9554 | P.O. Box 2000 | PO Box 105788 |
| Allen, TX 75013 | Chester, PA 19016 | Atlanta, GA 30348-5788 |
| 1-888-397-3742 | 1-888-909-8872 | 1-800-685-1111 |
| www.experian.com/freeze/center.html | www.transunion.com/credit-freeze | www.equifax.com/personal/credit-report-services |

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

**Fraud Alert**

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

| **Experian** | **TransUnion** | **Equifax** |
|---|---|---|
| P.O. Box 2002 | P.O. Box 2000 | P.O. Box 105069 |

| | | |
|---|---|---|
| Allen, TX 75013<br>1-888-397-3742<br>www.experian.com/fraud/center.html | Chester, PA 19106<br>1-800-680-7289<br>www.transunion.com/fraud-victim-resource/place-fraud-alert | Atlanta, GA 30348<br>1-888-766-0008<br>www.equifax.com/personal/credit-report-services |

**Additional Information**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); or TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

*For Maryland residents*, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; or www.oag.state.md.us. Loudoun is located at 1718 Patterson Street, Nashville, TN 37203.

*For 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 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. We encourage you to 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.

*For North Carolina residents*, the North Carolina Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and www.ncdoj.gov.

*For Rhode Island residents*, the Rhode Island Attorney General can be contacted at: 150 South Main Street, Providence, RI 02903; (401) 274-4400; or www.riag.ri.gov. A total of three (3) Rhode Island residents are potentially impacted by this incident. You have the right to file and obtain a police report if you ever experience identity theft or fraud. Please note that, in order to file a crime report or incident report with law enforcement for identity theft, you may be asked to provide some kind of proof that you have been a victim.

*For 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/.