

Appendix

Compumedics USA, Inc. (“Compumedics”) develops diagnostic and research technologies and devices for sleep disorders and provides technology services and devices used by health care providers in sleep study clinics.

Compumedics recently completed its investigation of, and data analysis for, the incident that disrupted the operations of its Information Technology (“IT”) systems. After initially identifying the incident, Compumedics immediately took steps to secure its systems and contain the incident. Compumedics also began an investigation with the assistance of third-party forensic experts and notified law enforcement. The investigation determined that an unauthorized party accessed certain Compumedics systems between February 15, 2025, and March 23, 2025, and reviewed or copied some files.

On May 13, 2025, Compumedics’ review determined the files contained Social Security numbers for a total of 11 Nebraska residents, who are patients of its healthcare provider customers. Compumedics began notifying its health care provider customers whose patient information was involved on April 29, 2025 and is providing notification on their behalf.

On June 27, 2025, Compumedics mailed notification letters via First Class mail to the Nebraska residents whose information may have been involved in accordance with Neb. Rev. Stat. § 87-803 and HIPAA (45 CFR §§ 160.103 and 164.400 *et seq.*). Compumedics is offering them 12 months of complimentary identity and credit monitoring services through Experian. Compumedics has also established a dedicated, toll-free incident response line where residents can obtain more information regarding the incident.

To prevent similar incidents in the future, Compumedics is implementing additional measures to enhance the security of its network and continues training employees concerning data security.



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

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>,

Compumedics USA Inc. ("Compumedics") recognizes the importance of protecting the information we maintain. Compumedics provides diagnostic and research technologies for sleep disorders, which are used by your provider, <<Variable Data 1>>, for the administration of sleep studies. We are writing to notify you about a data security incident involving some of your information we received in connection with a sleep study you underwent. This letter explains the incident, measures we have taken in response, and additional steps you can take in response.

What Happened? On May 13, 2025, we completed our investigation of, and data analysis for, an incident that disrupted the operations of our information technology systems. After we initially identified the incident on March 22, 2025, we immediately took steps to secure our systems and contain the incident. We also began an investigation with the assistance of third-party forensic experts and notified law enforcement. The investigation determined that an unauthorized party accessed some of our systems between February 15, 2025, and March 23, 2025, and may have reviewed or copied some files. We then conducted a review and analysis of those files to determine what information they contained.

What Information Was Involved? Our review determined that some of those files contained your information, which may include some or all of the following: your name, date of birth, demographic information, Social Security number, medical record number, health insurance information, treatment and diagnosis information, date(s) of treatment, provider name(s), and/or sleep study results.

What We Are Doing: We want to assure you that we take this incident very seriously and sincerely regret any concern this may cause. We have secured the services of Experian® to offer you a complimentary membership to Experian's IdentityWorksSM. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is completely free and enrolling in this program will not hurt your credit score. In addition, to help prevent a similar incident from occurring in the future, we are implementing additional measures to enhance the security of our network and are continuing to train our employees concerning data security.

What You Can Do: We sincerely regret the concern and inconvenience this may cause, and we encourage you to enroll in the complimentary credit and identity monitoring services we are offering you. **For more information on IdentityWorks, including instructions on how to activate your complimentary membership, as well as some additional steps you can take in response to the incident, please see the pages that follow this letter.** We also recommend you review the statements you receive from your healthcare providers and insurers. If you see services that you did not receive, please contact the issuer of the statement immediately.

For More Information: Should you have questions, please contact 877-841-3302, Monday through Friday, between 8:00 a.m. and 8:00 p.m. Central Time.

Sincerely,

Song Yu
Customer Care Manager
Compumedics USA Inc.

Activate IdentityWorks 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: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the Activation Code: <<Activation Code>>

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-5931. Be prepared to provide engagement number <<Engagement #>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

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

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.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit>
or call 833-918-5931 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 833-918-5931.

* 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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com/get-credit-report, 1-833-799-5355

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit. *How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com/credit-freeze
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which

credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Compumedics USA Inc. is located at 5015 West WT Harris Blvd, Suite E, Charlotte, NC 28269, and can be reached via telephone at 877-717-3975.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.marylandattorneygeneral.gov/

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves <<RI#>> individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: 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.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.