



April 2, 2021

[Name]  
[Address]  
[City, State zip]

Re: Notice of Data Security Incident

Dear [Name]:

We are writing to notify you that Cardiva Medical, Inc. ("Cardiva") recently experienced a data security incident that we confirmed on March 23, 2021 to have involved your personal information from when you were a Cardiva employee. We have no reason to believe that the personal information has been used for any fraudulent purpose as a result of this incident and have taken steps to prevent that from happening. But, out of an abundance of caution, we are sharing details about what happened, what personal information was involved, what we are doing to address it, the steps you can take, and resources that we are making available to you. We take the privacy and security of your personal information very seriously and apologize for the concern and disruption caused by this incident.

### **What Happened**

Cardiva experienced a data security incident that affected the company's computer systems. The incident resulted in some information being taken from our systems. That information has not been disclosed publicly or on the Internet and we believe that will not occur as a result of this incident. We will continue to monitor for any such disclosure and will promptly notify you if it happens.

This recent incident is unrelated to the recent acquisition of Cardiva, which was completed on March 1, 2021.

### **What Information Was Involved**

We have confirmed that employee personal information provided to or collected by Cardiva during the tenure of your employment at Cardiva, such as name, address, social security number, bank account information used for direct deposit, compensation and benefit information was among the information taken. If you provided a copy of your driver's license to Cardiva, it was also taken. There is no evidence, however, that any information was made available on the Internet or has otherwise been publicly disclosed, or that any information was or will be misused for fraudulent purposes as a result of this incident.

### **What We Are Doing**

Since learning of this situation, we have been taking steps to further strengthen the security of the company's computer systems and protect your personal information. We also immediately engaged third-party cyber experts to partner with our team to launch an investigation to better understand what happened and to prevent a similar incident in the future.

We are also making resources available to those individuals whose information was involved. While we have no reason to believe that your information has been used for any fraudulent purpose as a result of this incident, we are offering complimentary access to Experian IdentityWorks<sup>SM</sup> for two years.

## What You Can Do

The enclosed Reference Guide describes steps you can take to protect your identity, credit and personal information, including enrolling in the credit monitoring services being provided through Experian IdentityWorks<sup>SM</sup> at no cost to you. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** June 30, 2021 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [[Enrollment URL](#)]
- Provide your **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 1-877-890-9332 by June 30, 2021. Be prepared to provide engagement number [[DB#####](#)] as proof of eligibility for the Identity Restoration services by Experian. In addition, it is always a good idea to monitor your regular account statements from banks, credit card companies and others for any activity that is suspicious or that you do not recognize. If you find any such activity, contact the institution that issued the statement immediately.

## For More Information

We are committed to maintaining the security and privacy of personal information you entrusted to us and apologize for this inconvenience. Theft of data and similar incidents are difficult to prevent in all instances, however, we want you to be assured that we are taking steps to minimize the chances of a similar occurrence happening again. If you have questions, please contact Cardiva by calling 1-866-602-6099 or emailing [customerservice@cardivamedical.com](mailto:customerservice@cardivamedical.com).

Sincerely,

**Justin Ballotta, Chief Operation Officer**

## REFERENCE GUIDE

**To Order Your Free Credit Report.** Visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at [www.ftc.gov](http://www.ftc.gov) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281 to obtain your free credit report. Do not contact the credit bureaus individually.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or [www.ftc.gov](http://www.ftc.gov)

**Place a Fraud Alert on Your Credit File:** To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

**Place a Security Freeze on Your Credit File.** You have the right to place a “security freeze” on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	P.O. Box 9554 Allen, Texas 75013	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	<a href="http://www.transunion.com">www.transunion.com</a>

The credit bureaus may require that you provide proper identification prior to honoring your request. 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 law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

**Contact the U.S. Federal Trade Commission.** If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**For District of Columbia Residents:** You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 200001, 202-727-3400, [www.oag.dc.gov](http://www.oag.dc.gov)

**For Iowa Residents:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

**For Maryland Residents:** You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland

Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023,  
[www.oag.state.md.us](http://www.oag.state.md.us)

**For Massachusetts Residents:** You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

**For New York Residents:** You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office  
Bureau of Internet and Technology  
(212) 416-8433

NYS Department of State's Division of  
Consumer Protection  
(800) 697-1220

<https://ag.ny.gov/internet/resource-center>

<https://www.dos.ny.gov/consumerprotection>

**For North Carolina Residents:** You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)

**For Oregon Residents:** State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, [www.doj.state.or.us](http://www.doj.state.or.us)

**For Rhode Island Residents:** You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, [www.riag.ri.gov](http://www.riag.ri.gov). As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.