

NOTICE OF DATA PRIVACY EVENT

April 26, 2024 – Designed Receivable Solutions, Inc. (“DRSI”) is providing notice of an event that may affect the privacy of certain individuals’ information. DRSI takes this incident very seriously and is providing information about the incident, our response to it, and resources available to individuals to help protect their information, should they feel it appropriate to do so.

What Happened? On January 22, 2024, DRSI detected suspicious activity in its network environment. Upon discovery of this incident, DRSI promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, DRSI learned that an unauthorized actor accessed certain files and data stored within our network. DRSI also conducted an examination of its systems and networks using all information available to determine the potential impact and the security of data housed on its servers. DRSI continued to investigate this issue using the assistance of third-party cybersecurity specialists. The investigation determined an unauthorized actor exfiltrated certain data from servers. DRSI subsequently undertook a time-consuming and detailed review of the data stored on the servers at the time of this incident to understand the contents of that data and to whom that data relates. On March 8, 2024, we completed this extensive review process and identified that information pertaining to certain current and former clients’ patients was present in the affected files. Since then, we have been coordinating efforts with our clients to review and verify the affected information as well as locate address information in order to provide direct notice to as many impacted individuals as possible.

What Information Was Involved? While we have no evidence that any of your information has been misused, we are notifying you and providing information and resources to help protect your personal information. The following types of information may have been impacted: name, address, date of birth, Social Security number, health insurance information, and medical information (dates of service). The type of information at issue varies for each person

What We Are Doing. DRSI takes this event and the security of personal information in its care very seriously. Upon learning of this event, DRSI moved quickly to investigate and respond to the event and notify potentially affected individuals. As part of its ongoing commitment to the security of information, DRSI is reviewing and enhancing its existing policies and procedures related to data privacy to reduce the likelihood of a similar future event. DRSI is notifying impacted individuals for whom DRSI has a valid mailing address via U.S. mail and offering them credit monitoring and identity protection services. DRSI is also notifying applicable regulators.

How Will Individuals Know If They Are Affected By This Incident? DRSI is mailing a notice letter to individuals whose information was determined to be in the affected files, for whom a valid mailing address is available. If an individual does not receive a letter but would like to know if they are affected, they may call DRSI’s dedicated assistance line, detailed below. We are providing notice to impacted individuals on behalf of the following organizations: Cedars-Sinai Medical Center, Redlands Community Hospital, Sycamore Physicians, LLC, Core Orthopaedics Medical Center, Valkyrie Clinical Trials, Inc, AMG Healthcare Management Services, Air Methods, OptumCare Management, LLC, CAN Emergency Physicians, GEM Physicians Group, CHA Hollywood Presbyterian Medical Center, L.P., Marshall Medical Center, USC Arcadia Hospital, formerly known as Methodist Hospital of Southern California, Ridgecrest Regional Hospital, South Coast ER Medical Group, Southland Medical Corporation, and Springhill Emergency Physicians.

Whom Should Individuals Contact For More Information? If individuals have questions or would like additional information, they may call DRSI’s dedicated assistance line at 1(833) 961-7183, between the hours of 6:00 a.m. to 8:00 p.m. Pacific time, Monday through Friday. This excludes all major U.S. holidays.

What You Can Do. We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

Consumers have the right to place an initial or extended “fraud alert” on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

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

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

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 24 Rhode Island residents impacted by this event.