The Georgia Institute for Plastic Surgery ("GIPS") has always prioritized providing high-quality care and services, which includes privacy and securing information entrusted to us.

You, a family member, or one of your loved ones may have received a recent letter from GIPS regarding a cyber security incident. On or about February 22, 2024, GIPS discovered that an unauthorized user accessed its network server and may have acquired certain personal information stored on that specific server on December 30, 2023. Upon discovering unusual activity on its networks, GIPS began an investigation which involved the assistance of cybersecurity experts. GIPS also engaged a forensic security firm to confirm the security of its network, analyze the incident, and determine the extent of the personal information that may have been accessed or acquired by the unauthorized user. The investigation determined that an intrusion into GIPS network occurred after an unauthorized user used a remote desktop to gain access to the system. It was further determined that some files accessed during the intrusion may have included patients' full name, address, date of birth, phone number, diagnosis code, procedure code, and/or patient account number.

On or about April 24, 2024, GIPS began sending written notification to patients whose personal information may have been accessed by the unauthorized user. Patients should refer to the notice they will or have received in the mail regarding steps they can take to protect themselves. No social security numbers or financial information were compromised, and there is no indication of any identity theft or fraud occurring as a result of this incident. However, as a precautionary measure, potentially affected patients should remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing their account statements and monitoring credit reports closely.

If individuals detect any suspicious activity on an account, they should promptly notify the financial institution or company with which the account is maintained. They should also promptly report any fraudulent activity or any suspected identity theft to proper law enforcement authorities, including the police and their state's attorney general. Individuals may also wish to review the tips provided by the Federal Trade Commission ("FTC") on fraud alerts, security/ credit freezes, and steps that they can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). Individuals may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

GIPS is providing a dedicated confidential, **toll-free inquiry line at 1-888-451-8338**, Monday through Friday from 9 am - 9 pm Eastern Time, for potentially affected patients looking for additional information. We ask that you and/or your family member use the foregoing number for all inquiries and please allow GIPS' staff to prioritize patient care, appointment setting, and follow-ups. The Georgia Institute for Plastic Surgery deeply regrets any concern or inconvenience this incident may cause.

Recommended Steps to help Protect your Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements, changing account passwords, implementing two-factor authentication, 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 from one of the three credit bureaus every four months.
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.

2. 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 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.

3. 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.

4. 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.