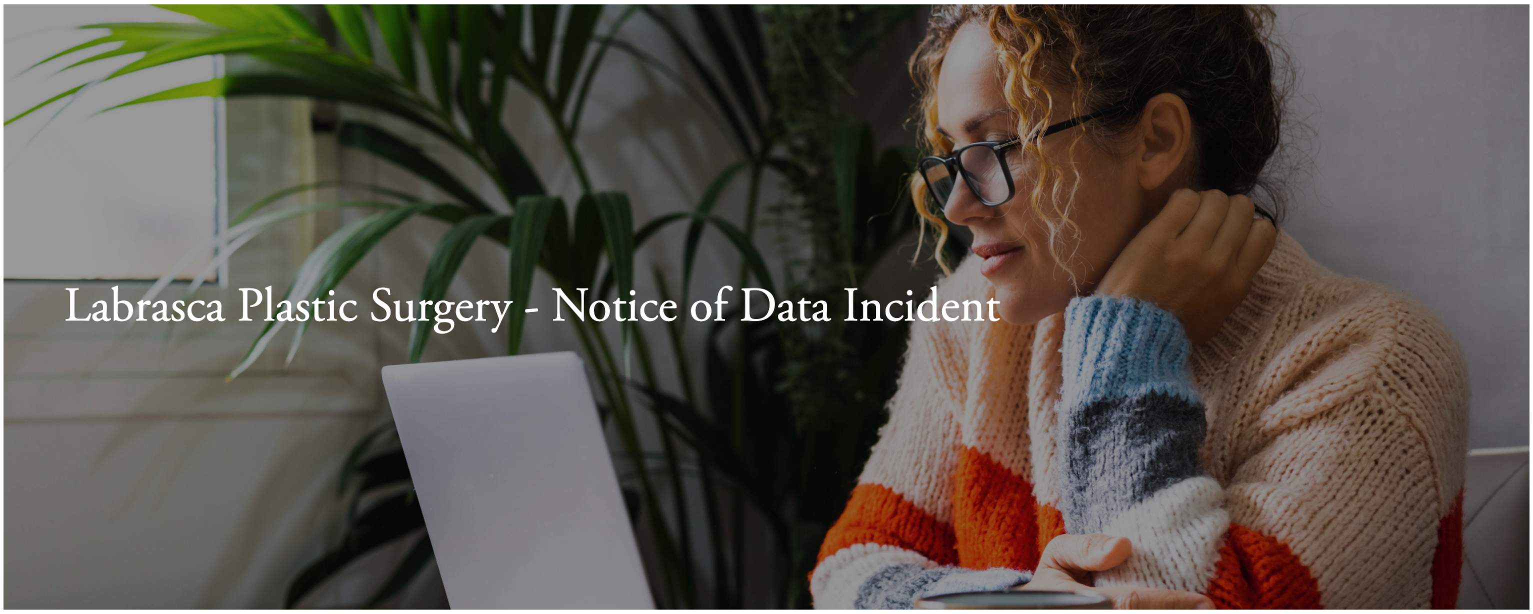

Labrasca Plastic Surgery - Notice of Data Incident

Notice of Data Incident

March 27, 2025 – LaBrasca Plastic Surgery is ("LPS") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to individual personal information. While this incident did not significantly impact LPS's ability to serve its patients, this notice is intended to provide details about the incident, steps LPS is taking in response, and resources available to help protect against the potential misuse of personal information.

What Happened? On January 26, 2025, LPS experienced a network disruption that impacted the functionality and access of its systems (the "Incident"). Upon discovery of this Incident, LPS immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the Incident. The investigation found evidence to suggest some LPS data has been accessed by an unauthorized individual. Please note that LPS's web-based systems, including Electronic Medical Record ("EMR"), human resource, and payroll systems were not impacted by the underlying incident.

Based on these findings, LPS began reviewing the affected systems to identify the specific individuals and the types of information that may have been impacted. While this process remains ongoing, LPS will notify affected individuals by U.S. First Class Mail as the information becomes available.

What Information Was Involved? Based on the investigation, the following information related to potentially impacted individuals may have been subject to unauthorized access: name, date of birth, driver's license, username and passwords, medical information, and health insurance information.

Please note that the information above varies for each potentially impacted individual. Affected individuals will be notified by U.S. First Class Mail as to what information, if any, was impacted.

What We Are Doing? Data privacy and security is among LPS's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon discovery of the Incident, LPS quickly took the following steps, including, but not limited to: disconnecting all access to the network; implementing an organization-wide credential reset of all users; and adding additional security tools. Additionally, LPS engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the Incident. Further, since the Incident, LPS has implemented additional security measures to prevent a similar incident from occurring in the future.

In light of the incident, LPS will be providing affected individuals with complimentary credit monitoring and identity theft restoration services. Any individuals whose information was impacted will be notified by U.S. First Class Mail with enrollment information.

What You Can Do: While we have not received any reports of related misuse of personal information relating to the Incident, we nevertheless 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 or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Additional Resources to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

Other Important Information: We recognize that you may have questions not addressed in this notice. If you have any questions or concerns, please call 855-549-2612 (toll free) Monday through Friday, during the hours of 9:00 a.m. and 9:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

LPS sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative, you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see “Contact Information” below). The agency you contact will then contact the other credit agencies.

Contact Information Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TranUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 Experian Fraud Center	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 Experian Freeze Center
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 Equifax Fraud Alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 Equifax Credit Freeze
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 TransUnion Fraud Alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 TransUnion Credit Freeze

Federal Trade Commission For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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 should also report instances of known or suspected identity theft to local law enforcement and the Attorney General’s office in your home state and you have the right to file a police report and obtain a copy of your police report.

