

Facial Surgery Group Provides Notice of Data Security Incident

Overland Park, Kansas – September 16, 2026 – Facial Surgery Group PC (“FSG”) experienced a data security incident that may have resulted in unauthorized access to certain individuals’ personal information. This notice is intended to provide details about the incident, steps that FSG is taking in response, and resources available to help protect against the potential misuse of personal information.

What Happened? On November 24, 2025, FSG detected suspicious activity within its email environment. Upon discovery of the incident, FSG promptly engaged a specialized third-party cybersecurity firm and IT personnel to conduct a comprehensive forensic investigation to determine the nature and the scope of the incident. The forensic investigation determined that there was potential access to some limited personal information contained in an employee email account.

FSG worked with a third-party data mining vendor to identify whose information and the type of information impacted. This process was completed on or about September 9, 2026. On **October 9, 2026**, FSG notified affected individuals by U.S. First Class Mail.

What Information Was Involved? The individual notices specify the type of information that may have been impacted for each person. The type of information may have included one or more of the following: Name, date of birth, Social Security number, demographic information, financial account number, and/or health information. If you received a letter, you can find the information potentially impacted under the *“What Information Was Involved”* section of the letter you received from FSG.

What Are We Doing? Data privacy and security are among FSG’s highest priorities, and it is committed to doing everything it can to protect the privacy and security of personal information within its care. Upon discovery of the incident, FSG immediately disabled the affected email account, changed the account password, active sessions were terminated, and promptly engaged a specialized third-party cybersecurity firm to conduct a forensic investigation. Finally, FSG is providing affected individuals with complimentary credit monitoring and identity theft restoration services.

What You Can Do: While FSG has not received any reports of related misuse of personal information relating to the Incident, FSG nevertheless encourages impacted individuals 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 impacted individuals contact their 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 attached *Additional Resources to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

Other Important Information: FSG recognizes that you may have questions not addressed in this notice. If you have any questions or would like to confirm whether your information may have been impacted by the incident, please call **888-214-6125** Monday through Friday, during the hours of 8:00 a.m. and 5:30 p.m. Central Standard Time (excluding U.S. national holidays).

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