Notice of Data Security Incident

Proliance Surgeons, Inc. ("Proliance") recently detected a data security incident affecting its corporate website. We immediately worked to contain the incident, launched an investigation, and engaged an industry leading digital forensics firm to assist. The investigation determined that payment card information may have been exposed for customers who made payments through Proliance's online payment platform between November 13, 2019 and June 24, 2020. The information involved in this incident may have included cardholder name, payment card account number, expiration date, and zip code. Only payments made online were at risk; in-person or phone payments were not affected.

Patient health care information was not affected by this incident. Aside from payment card information, no sensitive personal information or protected health information was exposed.

At Proliance, we take information privacy and security very seriously. That is why we are providing this information and offering free resources to help our customers protect their payment card information.

In coordination with our digital forensics firm, we have identified the source of the incident and ensured that our online payment platform has been secured. We have also launched a brand new website and payment platform with enhanced security measures to prevent similar incidents in the future.

We encourage our customers to carefully review and monitor their payment card account statements. If you believe your payment card may have been affected, you should immediately contact your bank or card issuer. We have notified payment card networks so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used during the identified timeframe. Additional information about steps you can take to protect your personal information is provided below.

We take your trust in us seriously and we deeply regret any worry or inconvenience that this may cause you.

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following national credit reporting agencies:

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
transunion.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
experian.com

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-525-6285
equifax.com

Free Annual Report
P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
consumer.ftc.gov
ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main St.
Providence, RI 02903
riag.ri.gov
401-274-4400

Federal Trade Commission
600 Pennsylvania Ave NW
Washington, DC 20580
consumer.ftc.gov
ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
riag.ri.gov
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit: http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf

Personal Information of a Minor: You can request that each of the national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft.

Residents of Massachusetts: Under Massachusetts law, state residents have the right to obtain any police report filed in regard to 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.