

Paul F. Schmeltzer
T (213) 417-5163
F +121348811
Email:pschmeltzer@ClarkHill.com

Clark Hill LLP
555 South Flower Street, 24th Floor
Los Angeles, CA 90071
T (213) 891-9100
F +12134881178

September 20, 2023

Via Electronic Mail

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

We represent Elevate Patient Financial Solutions (“ElevatePFS”), which is a business partner providing services to SSM Health, with respect to a data security incident involving the potential exposure of limited personally identifiable information (“PII”) described in more detail below. ElevatePFS is committed to answering any questions you may have about the data security incident its response and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On July 20, 2023, ElevatePFS learned that a limited number of SSM Health patients and individuals responsible for the charges of a SSM Health patient received contact letters sent through United States Postal Service from ElevatePFS with their Social Security number listed next to their name on the letter. The name, Social Security number, and address on the letter, when folded, was visible through the window of the envelope. Although ElevatePFS has no evidence of misuse of information as a result of this incident, out of an abundance of caution, they have engaged in a thorough review to determine the cause of the incident and to whom the information related. ElevatePFS determined that the problem was due to an internal mapping error in the processing of referral files. This mapping error caused a person’s Social Security number to be combined into the same field as their name in ElevatePFS’ records. On August 4, 2023, ElevatePFS determined that when an intended recipient was sent a contact letter this error in ElevatePFS’ records caused the intended recipient’s Social Security number to be listed visibly next to their name, above their address, in the envelope window.

2. Number of residents affected.

One (1) Maryland resident may have been affected and was notified of the incident. A notification letter was sent to the potentially affected individual on September 20, 2023 (a copy of the template letter is enclosed as Exhibit A).

3. Steps taken or plan to take relating to the incident.

Upon discovering this incident, ElevatePFS immediately began an investigation and took steps to prevent this type of issue from occurring again including correcting the mapping error, and putting additional validation controls in place within the referral processing module to ensure that no letter is mailed with numerals in the intended recipient's name without prior manual review and approval. ElevatePFS has also instituted increased auditing of mapping within the inbound processing of referral files.

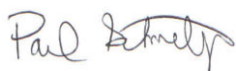
In addition, the potentially impacted individual can enroll in 12 months of complimentary credit monitoring and identity restoration services provided by IDX.

4. Contact information.

ElevatePFS takes the security of information in its control seriously and is committed to ensuring this information is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at pschmeltzer@clarkhill.com or (323) 497-4493.

Sincerely,

CLARK HILL



Paul F. Schmeltzer
Attorney

Enclosure

Elevate Patient Financial Solutions

P.O. Box 989728

West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

<<Country>>

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

September 20, 2023

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

Elevate Patient Financial Solutions (“ElevatePFS”) which is a business partner providing services to SSM Health, is writing to inform you of an incident that may have impacted your personal information described in more detail below. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What Happened?

On July 20, 2023, ElevatePFS learned that a limited number of SSM Health patients and individuals responsible for the charges of a SSM Health patient received contact letter(s) sent through the United States Postal Service from ElevatePFS with their Social Security number listed next to their name on the letter. The name, Social Security number, and address on the contact letter, when folded, was visible through the window of the envelope. Although ElevatePFS have no evidence of misuse of information as a result of this incident, out of an abundance of caution, they engaged in a thorough review to determine the cause of the incident and to whom the information related. ElevatePFS determined that the problem was due to an internal mapping error in the processing of referral files. This mapping error caused a person’s Social Security number to be combined into the same field as their name in ElevatePFS’ records. On August 4, 2023, ElevatePFS determined that when an intended recipient was sent a contact letter this error in ElevatePFS’ records caused the intended recipient’s Social Security number to be listed visibly next to their name, above their address, in the envelope window.

What Information Was Involved?

Your name, Social Security number, and address were exposed in the window of the letter envelope.

What We Are Doing:

Upon discovering this incident, ElevatePFS immediately began an investigation and took steps to prevent this type of issue from occurring again. ElevatePFS’ IT Department corrected the mapping error. ElevatePFS also put additional validation controls in place to ensure that no letter is mailed with numerals in the name, without prior manual review and approval. ElevatePFS has also instituted increased auditing of mapping within the processing of referral files.

Although there is no evidence your information has been misused, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed

identity theft recovery services at no cost to you. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-888-743-4798 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 a.m to 8 p.m Central Time. Please note the deadline to enroll is December 20, 2023.

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

We encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the event and can answer questions or concerns you may have regarding protection of your personal information.

Please monitor your financial statements and credit reports, and immediately report any suspicious activity.

For More Information:

You should contact IDX at the number provided above if you have any questions on protecting your identity or how to enroll in the services provided. If you have any questions or concerns, please call 1-888-743-4798 Monday through Friday from 8 a.m. to 8 p.m. Central. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Elevate Patient Financial Solutions, LLC

Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR code or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-888-743-4798 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements 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 by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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.

5. 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 also 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.

6. 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.

7. 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.

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: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. A total of 0 Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.