

July 3, 2019

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

VIA E-MAIL

Attorney General Gordon MacDonald

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
(603) 271-3643
DOJ-CPB@doj.nh.gov

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent FlexCare Medical Staffing (“FlexCare”), located in Roseville, California, with respect to a potential data security incident described in more detail below. FlexCare takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

On March 26, 2019, a FlexCare employee was the victim of a phishing email scam. The employee reported that she was unable to send or receive email to the IT department after her account was prevented from sending or receiving emails. The IT department took swift action and had the employee’s account credentials changed to prevent any further unauthorized access to the account. FlexCare also engaged independent computer forensics experts to determine how the incident occurred and whether any information had been accessed by the unauthorized intruder. On June 3, 2019, the investigation concluded. The investigation revealed that it was possible that the entire email account was potentially compromised and a review of the material in the account revealed that it contained individuals’ personal information, including name, date of birth, Social Security number and health information collected pursuant to employment with FlexCare.

2. Number of New Hampshire residents affected.

A total of sixty-six (66) residents of New Hampshire were potentially affected by this security incident. Notification letters were mailed on July 3, 2019, by first class mail. A sample copy of the notification letter is included with this letter.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

3. Steps taken.


FlexCare has taken steps to prevent a similar event from occurring in the future, and to protect the privacy and security of potentially impacted individuals' information. Those steps include strengthening our cybersecurity posture by forcing password changes for all employees and implementing multifactor authentication for all email users. FlexCare is also providing potentially impacted individuals with identity theft restoration and credit monitoring services for a period of twelve (12) months, at its own expense, through CyberScout.

4. Contact information.

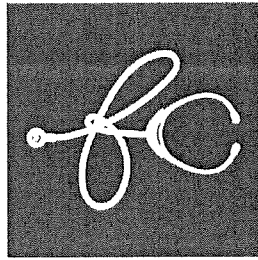
FlexCare remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@wilsonelser.com or (312) 821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP


Anjali C. Das *DHP*

Enclosure



flexcare

July 3, 2019

<First Name>><<Last Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

Dear [First Name][Last Name],

We are writing to inform you of a data security incident involving Flexcare, LLC that may have resulted in unauthorized access to some of your personal information. We take the privacy and protection of your personal information very seriously. We apologize and regret any inconvenience this may cause. This letter contains information about what happened, steps we have taken and resources we are making available to you to help protect your identity.

One of our employee's email accounts was recently accessed by an unauthorized party after the employee received a phishing email. Soon after receiving the phishing email the employee's email account was shutdown automatically by security features we have in place. We immediately changed the password to the account and conducted an internal investigation. Our internal investigation revealed evidence suggesting that the email account may have been accessed by an unauthorized party.

We then retained computer forensic professionals to conduct a thorough investigation to determine whether or not an unauthorized party accessed the employee's account. It was confirmed that the unauthorized party did access the employee's account and we discovered evidence to suggest that it was possible that the material contained within the email account was accessible to the unauthorized party.

We then conducted a full and thorough search of all the material accessible within the affected email account, and on June 3, 2019 discovered that information including your name and one or more of the following personal attributes: driver's license number, Social Security number, date of birth, address, and/or medical information, such as your drug test results, vaccination history or annual health questionnaire, were accessible from within the affected email account. None of our other systems, including our benefits systems, were accessed. The access was limited to a single employee's email account. At this time we have no evidence that anyone's personal information has been misused as a consequence of this incident.

In an abundance of caution, we are offering services to help protect your identity through CyberScout for a period of twelve (12) months. The services include credit monitoring, a copy of your credit report and identity fraud and theft restoration services with remediation up to

\$1,000,000 for certain out-of-pocket expenses arising from an occurrence of identity theft. Please review the included attachment for additional information regarding steps you can take to further protect your identity.

To activate your monitoring services please visit www.myservices.equifax.com/silver and use your unique activation code <XXXXXXXX> before [REDACTED]

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. Additional information describing your services is included with this letter.

We take the security of all information in our systems very seriously and want to assure you that we are taking steps to prevent a similar event from occurring in the future. Those steps include changing passwords, providing users with increased training on network security, implementing multi-factor authentication, and reporting the incident to government regulators.

We sincerely regret any inconvenience that this matter may cause you, and remain dedicated to protecting your information. If you have any questions, please call the CyberScout help line at 888-312-6920 Monday through Friday, 8:00 a.m. to 5:00 p.m., Mountain Standard Time.

Sincerely,



Travis Mannon, CEO

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

**Maryland Office of the
Attorney General**

Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

**Rhode Island Office of the
Attorney General**

Consumer Protection
150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

**North Carolina Office of the
Attorney General**

Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax ([https://assets.equifax.com/assets/personal/Fraud Alert Request Form.pdf](https://assets.equifax.com/assets/personal/Fraud%20Alert%20Request%20Form.pdf)); TransUnion (<https://www.transunion.com/fraud-alerts>) or Experian (<https://www.experian.com/fraud/center.html>). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

Enrollment Instructions

To sign up online for online delivery go to www.myservices.equifax.com/silver

- 1. Welcome Page:** Enter the Activation Code provided in the letter above and click the "Submit" button.
- 2. Register:** Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
- 3. Create Account:** Complete the form with your email address, create a User Name and Password, review the Terms of Use and then check the box to accept and click the "Continue" button.
- 4. Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
- 5. Order Confirmation:** This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.