

FLEXCARE LOGO

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

<<DATE>>

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, including your name and one or more of the following: your driver's license number, date of birth and/or medical information, such as your drug screening results, vaccination history and/or annual health questionnaire. 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 she 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 identity theft protection services through CyberScout. 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.

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.

FLEXCARE LOGO

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 (888) 312-6920 Monday through Friday, 9:00 a.m. to 6:00 p.m., Central Time.

Sincerely,

Travis Mannon, CEO