



Lindsay B. Nickle, Partner & Vice Chair
Cybersecurity & Data Privacy Team
1201 Elm Street, Suite 2550
Dallas, Texas 75270
LNickle@constangy.com

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

May 9, 2024

VIA EMAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: ldtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents FEI.com, Inc. dba FEI Systems ("FEI") in connection with a recent data security incident described in greater detail below.

1. Nature of the Security Incident

FEI currently contracts with HHSC to provide a critical incident management system which captures critical incident reportable events for persons receiving services from health care providers in Texas ("Texas CIMS"). Among other things, Texas CIMS provides reports permitting health care providers to access certain personal information of individuals for whom they provide services. The reporting tools in Texas CIMS are configured such that health care providers are able to view personal information only for those individuals that they serve. Between May 1, 2023 and August 4, 2023, however, one of the reports in the system was not so configured, and, as a result, up to 17 administrators for various Texas health care providers may have viewed information in the report that did not belong to the individuals served by their respective providers.

2. Number of Maryland Residents Affected

FEI notified one (1) Maryland resident of this incident via first class U.S. mail on May 9, 2024. The information potentially impacted in connection with this incident varies by individual but may include name, Social Security number, date of birth, Care ID and/or Medicaid ID.

A sample copy of the notification letter is included with this correspondence.

3. Steps Taken Relating to the Incident

FEI conducted a thorough review of the reasons why the information may have been viewable and has now remedied the issue such that provider administrators who access the report can only see information about the individuals directly served by their respective health care providers. It is important to note that this was not a hacking incident. Instead, each of the provider administrators who may have accessed the report between May 1 and August 4, 2023 was authorized by HHSC to access Texas CIMS to view the confidential information of their health care providers and are trained to properly protect personal information, and each administrator attests upon signing on to Texas CIMS to protect the information that they see. FEI has no reason to believe the administrators that accessed Texas CIMS or the report at issue have misused any personal or sensitive information.

FEI has established a toll-free call center through Cyberscout, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. In addition, while FEI is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, FEI is also providing complimentary credit and identity protection services to notified individuals.

4. Contact Information

FEI remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Constangy.

Best regards,

A handwritten signature in cursive script, appearing to read "LB Nickle".

Lindsay B. Nickle
Vice Chair
Constangy, Brooks, Smith & Prophete, LLP

Enc.: Sample Notification Letter



May 9, 2024

Re: Notice of Data Security Incident

Dear [REDACTED]:

The Texas Health and Human Service Commission ("HHSC") respects the privacy of your information, which is why, as a precautionary measure, FEI.com, Inc. dba FEI Systems ("FEI") is writing to let you know about a data security incident that may have involved your personal information.

WHAT HAPPENED?

FEI currently contracts with HHSC to provide a critical incident management system which captures critical incident reportable events for persons receiving services from health care providers in Texas ("Texas CIMS"). Among other things, Texas CIMS provides reports permitting health care providers to access certain personal information of individuals for whom they provide services. The reporting tools in Texas CIMS are configured such that health care providers are able to view personal information only for those individuals that they serve. Between May 1, 2023 and August 4, 2023, however, one of the reports in the system was not so configured, and, as a result, up to 17 administrators for various Texas health care providers may have viewed information in the report that did not belong to the individuals served by their respective providers.

WHAT INFORMATION WAS INVOLVED?

The information involved may have included your first name, last name, date of birth, Social Security number, Care ID, or Medicaid ID.

WHAT WE HAVE DONE

FEI conducted a thorough review of the reasons why the information may have been viewable and has now remedied the issue such that provider administrators who access the report can only see information about the individuals directly served by their respective health care providers. It is important to note that this was not a hacking incident. Instead, each of the provider administrators who may have accessed the report between May 1 and August 4, 2023 was authorized by HHSC to access Texas CIMS to view the confidential information of their health care providers and are trained to properly protect personal information, and each administrator attests upon signing on to Texas CIMS to protect the information that they see. FEI has no reason to believe the administrators that accessed Texas CIMS or the report at issue have misused your personal or sensitive information.

Also, in response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you

might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

WHAT YOU CAN DO

Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information about steps you can take to protect your information. In addition, to enroll in Credit Monitoring services at no charge, please log on to **<https://bfs.cyberscout.com/activate>** and follow the instructions provided. When prompted please provide the following unique code to receive services:

[REDACTED]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

FOR MORE INFORMATION

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-844-710-1716 and supply your unique code listed above.

While representatives should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with FEI regarding this incident. If so, please call contact the undersigned at 703-947-7025 or scott.morrow@feisystems.com.

Sincerely,



Scott Morrow
General Counsel
FEI.com, Inc. dba FEI Systems
9755 Patuxent Woods Drive, Suite 300
Columbia, Maryland 21046

Steps You Can Take to Protect Your Personal 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 <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Steps Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

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

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.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 one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor 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 <http://www.annualcreditreport.com>.

Security Freeze: 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.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

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
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

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 other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09.pdf.