BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Patrick H. Haggerty
direct dial: 513.929.3412
phaggerty@bakerlaw.com

May 26, 2017

VIA OVERNIGHT MAIL

Joseph Foster
Office of the Attorney General
33 Capitol St
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Foster:

We are writing on behalf of our client, FastHealth, to notify you of a security incident involving New Hampshire residents.

FastHealth develops and maintains operational platforms for a variety of business processes, including online bill payment and donation forms, on behalf of health care providers. On December 21, 2016, FastHealth discovered suspicious code on a server. Upon learning of this, FastHealth began an investigation and hired a leading computer security firm to assist. On January 24, 2017, the computer security firm determined that an unauthorized third party altered code on FastHealth's web server that was designed to capture payment card information as it was being entered on FastHealth clients' online bill-pay platforms from January 14, 2016 to December 20, 2016.

FastHealth completed the forensic investigation on March 25, 2017, and subsequently began the process of identifying the affected individuals. On May 9, 2017, FastHealth began notifying affected health care providers. FastHealth did not have contact information for some of the affected individuals and requested that information from certain health care providers. On May 26, 2017, FastHealth began notifying affected individuals.

The information that may have been affected includes patients' names, billing addresses, email addresses, phone numbers, payment card numbers, expiration dates and security codes (CVV), and any comments or messages included with the payment.

FastHealth has established a dedicated call center to assist individuals with any questions they may have. FastHealth is also recommending that potentially affected individuals remain vigilant to the possibility of fraud by reviewing their account statements and credit reports for unauthorized activity.

To help prevent something like this from happening in the future, FastHealth has removed the malicious code and continues to take steps to strengthen the security of its network.

FastHealth is notifying 3 New Hampshire residents in substantially the same form as the letters attached hereto, with written notification commencing today, May 26, 2017.[1]

Notification is being provided in the most expedient time possible pursuant to the investigation described above, which was necessary to determine the scope of the incident; restore the reasonable integrity of the data system; and identify the individuals potentially affected. *See* N.H. Rev. Stat. § 359-C:20(I)(a).

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Patrick H. Haggerty
Partner

Enclosure

[1] This report is not, and does not constitute, a waiver of personal jurisdiction.

FAST HEALTH®
Interactive Healthcare

May XX, 2017

[First Name][Last Name]
[Street Address]
[City], [State] [Zip Code]

Dear [First Name] [Last Name]:

FastHealth is a contracted vendor of [Healthcare provider]. We provide healthcare clients with operational and website services, including online bill-pay platforms. We are committed to protecting the security and confidentiality of our clients' and their patients' information. Regrettably, we are writing to inform you about an incident involving some of that information.

On December 21, 2016, FastHealth discovered suspicious code on a server. Upon learning of this, we immediately began an investigation and hired a leading computer security firm to assist. On January 24, 2017, the computer security firm determined that an unauthorized third party altered code on FastHealth's web server that was designed to capture payment card information as it was being entered on FastHealth's online bill-pay platforms from January 14, 2016 to December 20, 2016.

FastHealth's forensic investigation concluded on March 25, 2017, and we subsequently determined the information that may have been affected includes your name, billing address, email address, invoice number if provided, credit card type, payment card number, expiration date and security code (CVV), and any comments or messages you included with your payment.

We encourage that you remain vigilant to the possibility of fraud and identity theft by reviewing your financial statements for any unauthorized activity. You should immediately report any unauthorized charges to your financial institution because the major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported. The phone number to call is usually on the back of your payment card. You should also review the additional information on the following page on ways to protect yourself.

We sincerely apologize for any inconvenience or concern this may cause you. To help prevent something like this from happening in the future, we have removed the malicious code and continue to take steps to strengthen the security of our network. If you have any questions, please call 1-844-534-0814, Monday through Friday, from 9 a.m. to 9 p.m. ET (closed on U.S. observed holidays).

Sincerely,

Kevin A. Foote
Founder & CEO

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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