BakerHostetler

Baker&Hostetler LLP

45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com

Theodore J. Kobus III
direct dial: 212.271.1504
tkobus@bakerlaw.com

August 3, 2016

VIA FEDERAL EXPRESS

Office of the Attorney General
Consumer Protection Division
Hoover State Office Building
1305 E. Walnut St.
Des Moines, IA 50319

Re: Incident Notification

Dear Sir or Madam:

Our client, Banner Health ("Banner"), recognizes the importance of protecting personal information. On July 13, 2016, Banner learned that cyber attackers may have gained unauthorized access to patient information stored on a limited number of Banner computer servers. The investigation revealed that the attack was initiated on June 17, 2016. The servers contained information for Banner patients, providers, and health plan members and beneficiaries. For patients, affected information may have included patients' names, birthdates, addresses, physicians' names, dates of service, clinical information, health insurance information, and Social Security numbers. For providers, the affected server contained information including names, addresses, dates of birth, DEA (Drug Enforcement Agency) numbers, NPI (National Provider Identifier), or Social Security numbers. For health plan members, the affected server contained health insurance information including member names, birthdates, addresses, physicians' names, dates of service, clinical information, possibly health insurance information and Social Security numbers.

Beginning August 3, 2016, Banner is mailing notifications to approximately 3,038 Iowa residents[1] pursuant to the requirements of the Health Insurance Portability and Accountability Act ("HIPAA"), 45 C.F.R. §§ 164.400-414 and Iowa Code § 715C.2 in substantially the same

[1] Notwithstanding Iowa's exception to reporting HIPAA incidents, we are providing you with Iowa resident counts related to the HIPAA notices being sent as a courtesy so you have information to respond to inquiries from Iowa residents.

form as the document enclosed herewith.[2] In addition, pursuant to HIPAA and Iowa Code § 715C.2 and commencing August 3, 2016, Banner is providing substitute notification to Iowa residents by posting a statement on its website and issuing a press release in substantially the same form as the documents enclosed herewith. Banner is offering affected individuals a free one-year membership in credit monitoring and fraud monitoring protection services through Kroll. Notice is being provided in the most expeditious manner possible and without unreasonable delay.

Banner has established a dedicated call center that potentially affected individuals can contact with questions. Banner worked quickly to block the attackers and enhance the security of its systems in order to help prevent this from happening in the future. Banner is also working closely with the payment card networks to identify potentially affected cards so that the card issuers can be made aware and initiate heightened monitoring of those accounts.

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

Sincerely,

Theodore J. Kobus III
Partner

Enclosures

[2] As Banner does not conduct business in Iowa, this letter is not, and does not constitute, a waiver of personal jurisdiction.

Banner Health®

2901 North Central Ave., Suite 160
Phoenix, Arizona 85012
www.BannerHealth.com

<<MemberFirstName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

August 3, 2016

Dear <<MemberFirstName>> <<MemberLastName>>,

Banner Health is committed to maintaining the privacy and security of our patients' information. Regrettably, we are writing to inform you of a cyber attack involving your information.

What Happened

On July 13, 2016, we discovered that cyber attackers may have gained unauthorized access to information stored on a limited number of Banner Health computer servers. We immediately launched an investigation, hired a leading forensics firm, took steps to block the cyber attackers, and contacted law enforcement. The investigation revealed that the attack was initiated on June 17, 2016.

What Information Was Involved

The information may have included your name, birthdate, address, physician's name(s), date(s) of service, clinical information, possibly health insurance information, and social security number if you provided one to us. Your medical care will not be affected.

What You Can Do

As a precaution, we have secured the services of Kroll to provide credit and identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring powered by TransUnion, Web Watcher, Fraud Consultation, and Fraud Restoration. Visit **krollbreach.idmonitoringservice.com** to enroll and take advantage of your identity monitoring services. You must activate your identity monitoring services by no later than December 11, 2016. Membership Number: <<Member ID>>. Additional information describing your services is included with this letter. We also recommend that you review the explanation of benefits statements that you receive from your health insurer. If you see services that you did not receive, please contact your insurer immediately.

What We Are Doing

In addition to offering these free services and taking steps to block the cyber attack, we are further enhancing the security of our systems to help prevent something like this from happening again.

For More Information

We deeply regret any inconvenience or concern this may cause you. Should you have any questions, please call 1-855-223-4412, from 7 a.m. to 7 p.m. Pacific Time, seven days a week.

Sincerely,

Peter S. Fine
President and Chief Executive Officer

Kroll.

TAKE ADVANTAGE OF YOUR FRAUD MONITORING SERVICES FROM KROLL

Credit Monitoring through TransUnion: You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of fraud activity.

Web Watcher: Web Watcher monitors internet sites where criminals buy, sell, and trade personal information. You'll be promptly notified if evidence of your personal information being traded or sold is discovered.

Fraud Consultation: You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Fraud Restoration: If you become a victim of fraud, an experienced licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your investigator can dig deep to uncover all aspects of the fraud, and then work to resolve it.

Even if you choose not to take advantage of this free credit monitoring service, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge, once every twelve months, please visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 2002	PO Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-685-1111	1-888-397-3742	1-800-916-8800

If you believe that you are the victim of identity theft or have reason to believe that your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
1-877-438-4338

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.

* Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Banner Health®

For Immediate Release

Contact: Public Relations
media@bannerhealth.com

Banner Health Identifies Cyber Attack

PHOENIX (August 3, 2016) - Banner Health announced today that it is mailing letters to approximately 3.7 million patients, health plan members and beneficiaries, food and beverage customers and physicians and healthcare providers related to a cyber attack. Banner Health immediately launched an investigation, hired a leading forensics firm, took steps to block the cyber attackers and contacted law enforcement.

On July 7, 2016, Banner Health discovered that cyber attackers may have gained unauthorized access to computer systems that process payment card data at food and beverage outlets at some Banner Health locations. The attackers targeted payment card data, including cardholder name, card number, expiration date and internal verification code, as the data was being routed through affected payment processing systems. Payment cards used at food and beverage outlets at certain Banner Health locations during the two-week period between June 23, 2016 and July 7, 2016 may have been affected. A list of the outlets that were affected can be found at www.BannerSupports.com. The investigation revealed that the attack did not affect payment card payments used to pay for medical services.

On July 13, 2016, Banner Health learned that the cyber attackers may have gained unauthorized access to patient information, health plan member and beneficiary information, as well as information about physician and healthcare providers. The patient and health plan information may have included names, birthdates, addresses, physicians' names, dates of service, claims information, and possibly health insurance information and social security numbers, if provided to Banner Health. The physician and provider information may have included names, addresses, dates of birth, social security numbers and other identifiers they may use. The investigation also revealed that the attack was initiated on June 17, 2016.

This incident did not affect all Banner Health patients.

Banner Health worked quickly to block the attackers and is working to enhance the security of its systems in order to help prevent this from happening in the future. Banner Health is also working with the payment card networks so banks that issue payment cards can be made aware and initiate heightened monitoring on the affected cards. Customers should be assured that they can confidently use payment cards at Banner Health food and beverage outlets.

Banner Health is offering a free one-year membership in monitoring services to patients, health plan members, health plan beneficiaries, physicians and healthcare providers, and food and beverage customers who were affected by this incident.

Banner Health encourages its food and beverage customers to remain vigilant to the possibility of fraud by reviewing their payment card statements for any unauthorized activity. These customers should immediately report any unauthorized charges to their card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The telephone number to call is usually on the back of the payment card. Banner Health also recommends that patients review the explanation of benefits statements they receive from their health insurer. If they see any services they did not receive, the patient should contact the insurer immediately.

Banner Health deeply regrets any inconvenience this may have caused. Customers with questions can call 1-855-223-4412, from 7 a.m. to 7 p.m. Pacific Time, seven days a week.

About Banner

Headquartered in Arizona, Banner Health is one of the largest nonprofit health care systems in the country. The system owns and operates 29 acute-care hospitals, Banner Health Network, Banner – University Medicine, Banner Medical Group, long-term care centers, outpatient surgery centers and an array of other services, including family clinics, home care and hospice services, pharmacies and a nursing registry. Banner Health is in seven states: Alaska, Arizona, California, Colorado, Nebraska, Nevada and Wyoming. For more information, visit www.BannerHealth.com.

###

Banner Health®

2901 North Central Ave., Suite 160
Phoenix, Arizona 85012
www.BannerHealth.com

<<MemberFirstName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year)

Dear <<MemberFirstName>> <<MemberLastName>>,

Banner Health is committed to maintaining the privacy and security of our providers' information. Regrettably, we are writing to inform you of a cyber attack involving your information.

What Happened

On July 13, 2016, we discovered that cyber attackers may have gained unauthorized access to information stored on a limited number of Banner Health computer servers. We immediately launched an investigation, hired a leading forensics firm, took steps to block the cyber attackers, and contacted law enforcement. The investigation revealed that the attack was initiated on June 17, 2016.

What Information Was Involved

The information may have included your name, address, date of birth, DEA (Drug Enforcement Agency) number, TIN (Tax Identification Number), NPI (National Provider Identification) number, or social security number.

What You Can Do

As a precaution, we have secured the services of Kroll to provide credit and identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring powered by TransUnion, Web Watcher, Fraud Consultation, and Fraud Restoration. Visit **krollbreach.idmonitoringservice.com** to enroll and take advantage of your identity monitoring services. Membership Number: <<Member ID>>. You must activate your identity monitoring services by no later than December 11, 2016. Additional information describing your services is included with this letter.

What We Are Doing

In addition to taking steps to block the cyber attack and giving a courtesy notification to the DEA and Licensing Boards, we are further enhancing the security of our systems to help prevent something like this from happening again. If you are licensed in Arizona, you can also monitor the Prescription Monitoring Program (PMP) at www.azrxreporting.com to detect possible fraudulent use of your DEA number. If you detect any unauthorized activity, please call the number below.

For More Information

We deeply regret any inconvenience or concern this may cause you. Should you have any questions, please call 1-855-223-4412, from 7 a.m. to 7 p.m. Pacific Time, seven days a week.

Sincerely,

John Hensing, M.D.
Executive Vice President/Chief Medical Officer

TAKE ADVANTAGE OF YOUR FRAUD MONITORING SERVICES FROM KROLL*

Credit Monitoring through TransUnion: You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of fraud activity.

Web Watcher: Web Watcher monitors internet sites where criminals buy, sell, and trade personal information. You'll be promptly notified if evidence of your personal information being traded or sold is discovered.

Fraud Consultation: You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Fraud Restoration: If you become a victim of fraud, an experienced licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your investigator can dig deep to uncover all aspects of the fraud, and then work to resolve it.

Even if you choose not to take advantage of this free credit monitoring service, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge, once every twelve months, please visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 2002	PO Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-685-1111	1-888-397-3742	1-800-916-8800

If you believe that you are the victim of identity theft or have reason to believe that your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
1-877-438-4338

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.

* Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Notice to Our Patients

Banner Health is committed to maintaining the privacy and security of our patients' information. Regrettably, this notice is to inform our patients of a cyber attack involving some of that information.

What Happened
On July 13, 2016, we discovered that cyber attackers may have gained unauthorized access to information stored on a limited number of Banner Health computer servers. We immediately launched an investigation, hired a leading forensics firm, took steps to block the cyber attackers, and contacted law enforcement. The investigation revealed that the attack was initiated on June 17, 2016.

What Information Was Involved
The information may have included patients' names, birthdates, addresses, physicians' names, dates of service, clinical information, possibly health insurance information, and social security numbers if one was provided to Banner Health. Patients' medical care will not be affected.

What You Can Do
As a precaution, we have secured the services of Kroll to provide credit and identity monitoring at no cost to the affected patients for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. We also recommend that patients review the explanation of benefits statements that they receive from their health insurer. If they see services that they did not receive, please contact the insurer immediately.

What We Are Doing
In addition to offering these free services and taking steps to block the cyber attack, we are further enhancing the security of our systems to help prevent something like this from happening again. We began mailing letters to affected patients on August 3, 2016. We have established a dedicated call center for patients to call with any questions. If you believe you are affected but do not receive a letter before September 9, 2016, please call 1-855-223-4412 from 7 a.m. to 7 p.m. Pacific Time, seven days a week.

FedEx®
Express

B
8978
08.04
1
10:30
RT 615
FZ B01

PS|Ship - FedEx Label

XH DSMA

IA-US
DSM
50319
ASR
PRIORITY OVERNIGHT
THU - 04 AUG 10:30A

TRK# 7837 3822 8978
0201

FedEx Express

PO
INV
(713) 276-1610
DEPT
REF 04593 00001310895

DES MOINES IA 50319

TO OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION
1305 E WALNUT ST

544J1/137D/14EB

ORIGIN ID:EKXA
SUCHISMITA PAHI
(713) 751-1600
BAKER HOSTETLER LLP
811 MAIN STREET
SUITE 1100
HOUSTON, TX 77002
UNITED STATES US

SHIP DATE: 03AUG16
ACTWGT: 0.50 LB
CAD: 10326920/WSX12750

BILL SENDER

Extremely Urgent

Page 1 of 2

◄ Insert shipping document here.