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 EMAIL (SECURITYBREACH@ATG.WA.GOV)
AND FEDERAL EXPRESS

Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Attorney General Ferguson:

Our client, Banner Health ("Banner"), recognizes the importance of protecting personal information. On July 7, 2016, Banner discovered that cyber attackers may have gained unauthorized access to computer systems that process payment card data at the food and beverage outlets at some of its locations. Banner immediately launched an investigation, hired a leading forensics firm, took steps to block the cyber attackers, and contacted law enforcement. 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 cards used to pay for medical services.

Through its continuing investigation, on July 13, 2016, Banner learned that cyber attackers may have gained unauthorized access to 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, birthdates, 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 7,916 Washington residents pursuant to the requirements of the Health Insurance Portability and Accountability Act ("HIPAA"), 45 C.F.R. §§ 164.400-414 and Wash. Rev. Code § 19.255.010 in substantially the same form as the document enclosed herewith.[1] In addition, pursuant to the requirements of HIPAA and Wash. Rev. Code § 19.255.010 and commencing August 3, 2016, Banner is providing substitute notification to Washington 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 expedient time 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

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

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

Banner Health®

<<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.

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

Banner Health®

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

August 3, 2016

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

Banner Health understands the importance of protecting the payment card information we handle at our food and beverage outlets. Regrettably, we are writing to inform you of a cyber attack involving your information.

What Happened

On July 7, 2016, we discovered that cyber attackers may have gained unauthorized access to computer systems that process payment card data at the food and beverage outlets at some of our Banner Health locations. 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 did not affect payment card payments used to pay for medical services.

What Information Was Involved

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 BannerSupports.com/customers/affected-locations. You used a payment card ending in <<ClientDef1 (Card Number)>> at an affected location during the at-risk window.

What You Can Do

We encourage you to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. You should also review the additional information on ways to protect yourself enclosed with this letter. Additionally, we have secured the services of Kroll to provide one year of Web Watcher services at no cost to you. 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. 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.

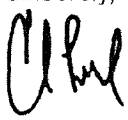
What We Are Doing

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

For More Information

We deeply regret any inconvenience and 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, Monday through Friday.

Sincerely,



Chuck Lehn
Executive Vice President
Banner Health

Kroll.

TAKE ADVANTAGE OF YOUR FRAUD MONITORING SERVICES from Kroll:*

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 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 2000
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.

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

Banner Health®

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

3 de agosto de 2016

Estimado(a) <<MemberFirstName>> <<MemberLastName>>,

Banner Health entiende la importancia de proteger la información de las tarjetas de pago que manejamos en nuestros puntos de venta de comida y bebidas. Lamentablemente, le escribimos para informarle que hubo un ataque cibernético que involucró su información.

Lo que sucedió

El 7 de julio de 2016, descubrimos que es posible que unos atacantes cibernéticos tuvieron acceso sin autorización a la información en los servidores que procesan la información de las tarjetas de pago en los puntos de venta de comida y bebidas de algunas de nuestras instalaciones de Banner Health. Inmediatamente iniciamos una investigación, contratamos una compañía líder de investigación forense, tomamos los pasos necesarios para bloquear el ataque cibernético y contactamos a las autoridades. La investigación reveló que el ataque empezó el 17 de junio de 2016 y que no afectó los pagos con tarjeta recibidos por servicios médicos.

¿Qué información estuvo involucrada?

Los atacantes se enfocaron en la información de las tarjetas de pago, incluidos el nombre del titular de la tarjeta, fecha de expiración y el código de verificación interna, debido a que la información estaba siendo enviada por los sistemas de procesamiento de pago afectados, las tarjetas de pago que se usaron en los puntos de venta de comida y bebidas en algunas de las instalaciones de Banner Health durante el período de 2 semanas entre el 23 de junio de 2016 y el 7 de julio de 2016 pueden haber sido afectadas. Puede encontrar la lista de los centros afectados en BannerSupports.com/customers/affected-locations. Usted usó su tarjeta terminada en <<OtherDef1 (Card Number)>> en uno de los centros afectados durante el periodo de riesgo.

¿Qué puede hacer usted?

Le animamos a que se mantenga vigilante ante la posibilidad de fraude, revise los estados de cuenta de su tarjeta de pago para detectar cualquier actividad que no ha sido autorizada. Debe reportar inmediatamente cualquier cargo no autorizado al emisor de la tarjeta; ya que, por lo general, los tarjetahabientes no son responsables por los cargos no autorizados que se reporten de manera oportuna. El teléfono donde puede hacer el reporte está por lo general al reverso de su tarjeta de pago. También debe revisar la información adicional de las formas en las que puede protegerse adjuntas a esta carta. Además, contratamos los servicios de Kroll para brindarle servicios de monitoreo de internet Web Watcher sin ningún costo para usted. Kroll es líder mundial en mitigación de riesgos y respuesta, y su equipo tiene una amplia experiencia en ayudar a las personas que han sufrido una exposición involuntaria de su información confidencial. Vaya a **krollbreach.idmonitoringservice.com** para inscribirse y pueda aprovechar los servicios de monitoreo de identidad. Número de membresía: <<Member ID>>. Debe activar su servicio de monitoreo de identidad a más tardar el 11 de diciembre de 2016. Adjunta a esta carta se encuentra más información que describe sus servicios.

¿Qué estamos haciendo?

Trabajamos rápidamente para bloquear el ataque y para mejorar nuestros sistemas de seguridad para prevenir que algo así no vuelva a suceder. También estamos trabajando con las redes de tarjetas de pago para que los bancos que emiten las tarjetas de pago estén informados y puedan iniciar un monitoreo elevado en las tarjetas afectadas. Le aseguramos que puede usar sus tarjetas de pago en los puntos de venta de comida y bebidas de Banner Health con confianza.

Para más información

Lamentamos profundamente cualquier contratiempo o preocupación que esto le puede causar. Si tiene alguna pregunta llame al 1-855-223-4412, de las 7 a.m. a las 7 p.m. hora del Pacífico, 7 días a la semana.

Atentamente,

Chuck Lehn
Executive Vice President
Banner Health

Kroll.

APROVECHE LOS SERVICIOS DE MONITOREO DE FRAUDE QUE LE OFRECE KROLL:*

Monitoreo de internet Web Watcher: Web Watcher monitorea los sitios de internet donde los criminales compran, venden e intercambian información personal. Se le notificará inmediatamente si descubren evidencia que su información personal está siendo negociada o vendida.

Consultas sobre fraude: Usted tiene acceso ilimitado a consultar con un investigador certificado de Kroll. El apoyo incluye enseñarle las formas más efectivas para proteger su identidad, explicarle sus derechos y protecciones bajo la ley, asistencia con alertas de fraude, e interpretar cómo se accede y se usa su información personal, incluido investigar actividades sospechosas que pueden estar relacionadas a un robo de identidad.

Restauración de fraude: Si usted se convierte en víctima de fraude, un investigador certificado experimentado trabajará en su nombre para resolver cualquier asunto relacionado. Usted tendrá acceso a un investigador dedicado a usted que entiende sus problemas y hará la mayoría del trabajo por usted. Su investigador puede investigar a fondo para descubrir todos los aspectos del fraude, y después trabajar para resolverlos.

Si usted decide no aprovechar este servicio de monitoreo de crédito sin cargo para usted, le recomendamos que permanezca vigilante a la posibilidad de fraude y robo de identidad, revise su estado de cuenta de su tarjeta de crédito, del banco y otros reportes de estados financieros para detectar cualquier actividad no autorizada. Puede obtener también una copia de su reporte de crédito, si costo para usted, directamente de cada una de las tres agencias nacionales de información de crédito. Para pedir su reporte de crédito, sin costo para usted, una vez cada 12 meses, por favor visite www.annualcreditreport.com o llame al número sin costo 1-877-322-8228. La información para contactar a las agencias nacionales de información de crédito es la siguiente:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 2002	PO Box 2000
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

Si usted cree que fue víctima de robo de identidad o tiene alguna razón para creer que su información personal ha sido usada de forma inapropiada, debe comunicarse inmediatamente con la Comisión Federal de Comercio (*the Federal Trade Commission*) o con la Oficina del Fiscal General de su estado. La información de la Comisión Federal de Comercio es la siguiente:

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

Puede obtener información en estos lugares sobre los pasos que una persona puede tomar para evitar el robo de identidad, así como información sobre alertas de fraude y bloqueos de seguridad. También debe contactar al departamento de policía local y hacer un reporte policiaco. Obtenga una copia del reporte policiaco en caso que sus acreedores le pidan una copia para corregir sus expedientes.

* El sitio de internet para activar la cuenta de Kroll es compatible únicamente con las versiones actuales, o una anterior, de los navegadores Internet Explorer, Chrome, Firefox y Safari.

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.

###

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

Banner Health®

<<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

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.

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.

Banner Health Identifies and Stops Payment Card Cyber Attack

August 3, 2016

California residents please click here [embed link]

Banner Health understands the importance of protecting the payment card information we handle at our food and beverage outlets. Regrettably, we are writing to inform our food and beverage outlet customers of a cyber attack involving that information.

What Happened

On July 7, 2016, we discovered that cyber attackers may have gained unauthorized access to computer systems that process payment card data at the food and beverage outlets at some of our Banner Health locations. 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 did not affect payment card payments used to pay for medical services.

What Information Was Involved

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 krollbreach.idmonitoringservice.com. Additionally, for at-risk transactions where a cardholder's name was affected, we are in the process of mailing letters to customers for whom we have a mailing address.

What You Can Do

We encourage you to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. You should also review the additional information on ways to protect yourself enclosed with this letter. Additionally, we have secured the services of Kroll to provide one year of Web Watcher services at no cost to affected customers. 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. Affected customers may visit krollbreach.idmonitoringservice.com to enroll and take advantage of the identity monitoring services.

What We Are Doing

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

For More Information

We deeply regret any inconvenience 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, Monday through Friday.

TAKE ADVANTAGE OF YOUR **FRAUD** MONITORING SERVICES **FROM KROLL:***

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.

Even if you choose not to take advantage of this free 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.

MORE INFORMATION ABOUT 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 105252, Atlanta, GA 30348, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-866-200-6020
TransUnion, PO Box 1000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

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. 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

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.

If you are a resident of Connecticut note that, pursuant to Connecticut law, you have the right to request a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any request you make for new loans, credit mortgages, employment, housing, or other services.

To place a freeze on your credit report, you must send a written request to each of the three major reporting agencies by certified mail or another secure method as authorized by a credit rating agency to the addresses below:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	Experian Security Freeze P.O.Box 9554 Allen, TX 75013	TransUnion Fraud Victim Assistance P.O.Box 6790 Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
- Social Security number
- Date of birth
- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years

- Proof of current address, such as a current utility bill or telephone bill
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

The credit reporting agencies have five (5) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within ten (10) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification, the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

If you are a resident of Maryland, you may contact the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

If you are a resident of Massachusetts, note that pursuant to Massachusetts law, you have the right to obtain a copy of any police report related to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

There are two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the toll-free numbers listed below:

Equifax	Experian	TransUnion
888-766-0008	888-397-3742	800-680-7289

Massachusetts law allows consumers to request a security freeze. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

The fee for placing a security freeze on a credit report is $5.00. If you are a victim of identity theft and submit a valid investigative report or complaint with a law enforcement agency, the fee will be waived. In all other instances, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. If you have not been a victim of identity theft, you will need to include payment to the credit reporting agency to place, lift, or remove a security freeze by check, money order, or credit card.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze PO Box 105788 Atlanta, GA 30374 www.equifax.com	Experian Security Freeze PO Box 9554 Allen, TX 75013 www.experian.com	TransUnion Fraud Victim Assistance Department PO Box 6790 Fullerton, CA 92834 www.transunion.com

In order to request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
- Proof of current address such as a current utility bill or telephone bill;
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
- If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days

after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

If you are a resident of North Carolina, you may contact the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, toll free at 1-877-566-7226 or 1-919-716-6400.

If you are a resident of Rhode Island, you may contact the Rhode Island Attorney General's office at:

Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400
http://www.riag.ri.gov/

You also have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies. Contact information for each of the three credit reporting agencies is as follows:

Equifax, PO Box 740256, Atlanta, GA 30374,www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com,1-888-397-3742
TransUnion, PO Box 6790, Fullerton, CA 92834,www.transunion.com, 1-800-680-7289

As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file. You may choose between two types of fraud alert. An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.ftc.gov/idtheft/.

You may also obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a security freeze on your credit report pursuant to Rhode Island law. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The fee for placing a security freeze on a credit report is $10.00. If you are a victim of identity theft and submit a valid investigative report or complaint with a law enforcement agency, or if you are sixty-five (65) years old or older, the fee will be waived. In all other instances, a credit reporting agency may charge you up to $10.00 each to place, temporarily lift, or permanently remove a security freeze. If you have not been a victim of identity theft, you will need to include payment to the credit reporting agency to place, lift, or remove a security freeze by check, money order, or credit card.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a unique personal identification number ("PIN") or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

(1) The unique personal identification number ("PIN") or password provided by the consumer reporting agency;
(2) Proper identification to verify your identity; and
(3) The period of time for which the report shall be available to users of the credit report.

The credit reporting agencies have five (5) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within ten (10) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities.

If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, a few days before actually applying for new credit.

If you are a resident of West Virginia, you also have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies. Contact information for each of the three credit reporting agencies is as follows:

Equifax, PO Box 740256, Atlanta, GA 30374,www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com,1-888-397-3742
TransUnion, PO Box 6790, Fullerton, CA 92834,www.transunion.com, 1-800-680-7289

As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file. You may choose between two types of fraud alert. An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.ftc.gov/idtheft/.

You may also obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a security freeze on your credit report pursuant to West Virginia law. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a unique personal identification number ("PIN") or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

(1) The unique personal identification number ("PIN") or password provided by the consumer reporting agency;
(2) Proper identification to verify your identity; and
(3) The period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request.

A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities.

If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, a few days before actually applying for new credit.