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

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

August 3, 2016

Re: NOTICE OF DATA BREACH

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

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

Ref: AVISO DE VIOLACIÓN DE DATOS

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 <<ClientDef1 (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

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.