<<VENDOR RETURN ADDRESS>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

16 de mayo de 2024

Ref.: Aviso de incidente de seguridad de datos

Estimado/a <<First Name>> <<Last Name>>:

Le escribimos para informarle acerca de un incidente de seguridad de datos que podría haber afectado a su información personal o su información de salud protegida. En Brockton Area Multi Services, Inc. ("BAMSI") estamos comprometidos a mantener la confianza de nuestros clientes y a demostrar nuestra responsabilidad con respecto a la privacidad y seguridad de toda la información en nuestro poder.Esta carta proporciona información sobre el incidente y los pasos que puede tomar para proteger su información.

Qué ocurrió: el 14 de abril de 2023, en BAMSI percibimos una actividad inusual en nuestra red. En respuesta a ello, inmediatamente comenzamos los esfuerzos de contención, mitigación y restauración para acabar con la actividad y proteger nuestra red, nuestros sistemas y nuestros datos. Además, contratamos a expertos en ciberseguridad independientes para llevar a cabo una investigación forense sobre el incidente y que nos ayudaran a determinar qué sucedió. Esta investigación forense determinó que probablemente se haya accedido a ciertos datos de BAMSI, o se hayan obtenido sin autorización, durante este incidente. Como resultado, iniciamos una revisión exhaustiva de los datos potencialmente afectados, y luego trabajamos diligentemente para validar los resultados y confirmar las direcciones de las personas potencialmente afectadas, en preparación para la notificación. Estos esfuerzos concluyeron el 29 de abril de 2024 e identificaron parte de su información dentro del conjunto de datos potencialmente afectados.

Qué información estuvo involucrada: la información potencialmente afectada incluyó su <<VARIABLE TEXT 2: Data Elements>>.

Qué estamos haciendo: tan pronto como descubrimos el incidente, tomamos las medidas descritas anteriormente. También implementamos medidas de seguridad adicionales para proteger nuestro entorno digital y minimizar la probabilidad de incidentes futuros.

Qué puede hacer: puede seguir las recomendaciones de la próxima página para ayudar a proteger su información. Asimismo debe revisar sus estados de cuenta y los formularios de explicación de beneficios e informar sobre cualquier error o actividad que no reconozca a su compañía de seguros.

Para obtener más información: si tiene alguna pregunta sobre esta carta, comuníquese con IDX, una compañía ZeroFox, al 1-888-807-8556, o visite https://response.idx.us/BAMSI para obtener ayuda. Los representantes de IDX están disponibles de 9:00 a. m. a 9:00 p. m., hora del este, de lunes a viernes.

Para BAMSI, su confianza en nosotros y en este asunto es algo muy importante. Le rogamos que acepte nuestras sinceras disculpas y sepa que lamentamos profundamente cualquier preocupación o inconveniente que esto pueda causarle.

Atentamente,

Peter Evers, Presidente y CEO
BAMSI
10 Christy's Drive,
Brockton, MA 02301

Medidas que puede tomar para proteger su información personal

Revisar los estados de cuenta y notificar a las autoridades sobre cualquier actividad sospechosa: como medida de precaución, le recomendamos que permanezca alerta y revise atentamente sus estados de cuenta e informes de crédito. Si detecta alguna actividad sospechosa en una cuenta, debe notificar de inmediato a la institución financiera o empresa donde tiene la cuenta. También debe informar de inmediato sobre cualquier actividad fraudulenta o cualquier sospecha de robo de identidad a las autoridades policiales correspondientes, al fiscal general de su estado o a la Comisión Federal de Comercio (Federal Trade Commission, FTC).

Copia del informe de crédito: puede obtener una copia gratuita de su informe de crédito de cada una de las tres principales agencias de informes de crédito una vez cada 12 meses visitando http://www.annualcreditreport.com/, llamando al número gratuito 1-877-322-8228 o completando un Formulario de solicitud de informe de crédito anual y enviándolo por correo a Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. También puede comunicarse con una de las tres agencias nacionales de informes crediticios:

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

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

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Alerta de fraude: es posible que quiera tener en cuenta incluir una alerta de fraude en su informe de crédito. Una alerta de fraude inicial es gratuita y permanecerá en su archivo de crédito durante al menos un año. La alerta informa a los acreedores de una posible actividad fraudulenta dentro de su informe y solicita que el acreedor se comunique con usted antes de abrir cualquier cuenta a su nombre. Para incluir una alerta de fraude en su informe crediticio, comuníquese con cualquiera de las tres agencias de informes crediticios identificadas anteriormente. Hay información adicional disponible en http://www.annualcreditreport.com.

Bloqueo de seguridad: tiene derecho a poner un bloqueo de seguridad en su archivo de crédito sin costo alguno. Esto evitará que se abra un nuevo crédito a su nombre sin el uso de un número de identificación personal (PIN) que se le proporcionará cuando solicite que se implemente el bloqueo. El bloqueo de seguridad está diseñado para evitar que los posibles acreedores accedan a su informe de crédito sin su consentimiento. Como resultado, el uso de un bloqueo de seguridad podría interferir con su capacidad de obtener crédito, o retrasarla. Es preciso poner un bloqueo de seguridad por separado en su archivo de crédito en cada una de las agencias de informes crediticios. Para poner un bloqueo de seguridad, es posible que se le solicite que proporcione a la agencia de informes crediticios información que lo identifique, incluyendo su nombre completo, su número de Seguro Social, su dirección actual y las anteriores, una copia de su tarjeta de identificación emitida por el gobierno y una factura de un servicio público, un estado de cuenta bancaria o un estado de cuenta del seguro reciente.

Recursos gratuitos adicionales: puede obtener información de las agencias de informes del consumidor, la FTC o del Fiscal General estatal que corresponda sobre alertas de fraude, bloqueos de seguridad y medidas que puede tomar para prevenir el robo de identidad. Puede denunciar un presunto robo de identidad ante la policía local, la FTC o el Fiscal General de su estado.

Comisión Federal de Comercio (Federal Trade Commission)
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, y
www.ftc.gov/idtheft
1-877-438-4338

Fiscal General de Maryland (Maryland Attorney General)
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

Fiscal General de Nueva York (New York Attorney General)
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

Fiscal General de Carolina del Norte (North Carolina Attorney General)
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Fiscal General de Rhode Island (Rhode Island Attorney General)
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Fiscal General de Washington D. C. (Washington D.C. Attorney General)
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

También tiene ciertos derechos en virtud de la Ley de Información Crediticia Justa (Fair Credit Reporting Act, FCRA): estos derechos incluyen saber qué hay en su archivo, disputar información incompleta o inexacta y hacer que las agencias de informes del consumidor corrijan o eliminen información inexacta, incompleta o no verificable, además de otros derechos. Para obtener más información sobre la FCRA y sus derechos en virtud de ella, visite https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.