



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

January 14, 2022

VIA ELECTRONIC SUBMISSION

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Re: Notice of Data Security Incident

To Whom It May Concern:

We represent The Brock Group (“Brock”), a company headquartered in Houston, Texas which provides industrial specialty services. This letter is being sent because Brock recently experienced a data security incident that may have impacted personal information belonging to Maryland residents. The potentially impacted information differed for each potentially impacted individual but may have included residents’ names as well as residents’ Social Security numbers, medical information, and username and password for non-financial electronic accounts.

On July 21, 2021, Brock learned of suspicious activity associated with certain Brock employee email accounts. Upon discovering this activity, Brock took immediate steps to secure the email accounts and commenced a preliminary investigation. In so doing, Brock engaged independent cybersecurity experts to determine what happened and whether Brock data was accessed or acquired without authorization. Through that investigation, Brock learned that certain employee email accounts had been accessed without authorization. Brock then engaged a vendor to review the contents of the relevant email accounts likely to contain sensitive data. As a result, on December 21, 2021, Brock learned that personal information belonging to Maryland residents may have been accessed or acquired without authorization.

Brock notified five (5) potentially impacted Maryland residents of this incident via the attached sample letter on January 14, 2022. In so doing, Brock offered notified individuals complimentary identity protection services through IDX, a data incident and recovery services expert. These services included credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

Please contact me should you have any questions.

January 14, 2022
Page 2

Very truly yours,

/s/ Alyssa R. Watzman

Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Sample Consumer Notification Letter



P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-365-2603
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [XXXXXXXXXX]

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

January 11, 2022

Re: Notice of Data <<Variable3>>

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a data security incident recently experienced by The Brock Group (“Brock”) which may have impacted your personal information. Brock takes the privacy and security of all information within its possession very seriously. This letter contains information about the incident and steps that can be taken to help safeguard your personal information.

What Happened: On July 21, 2021, Brock learned of suspicious activity associated with certain Brock employee email accounts. Upon discovering this activity, Brock took immediate steps to secure the email accounts and commenced a preliminary investigation. In so doing, Brock engaged independent cybersecurity experts to determine what happened and whether Brock data was accessed or acquired without authorization. Through that investigation, Brock learned that certain employee email accounts had been accessed without authorization. Brock then engaged a vendor to review the contents of the relevant email accounts likely to contain sensitive data. As a result, on December 21, 2021, Brock learned that one or more of the relevant email accounts contained some of your personal information.

Please note that Brock is not aware of the misuse of any information potentially affected in connection with this incident. Nevertheless, Brock is notifying potentially affected individuals out of an abundance of caution.

What Information Was Involved: The information potentially impacted in connection with this incident varied for each potentially impacted individual but may have included your name as well as your <<Variable4>>.

What We Are Doing: As soon as Brock learned of this incident, Brock promptly took the steps discussed above. In addition, Brock implemented additional security measures to further harden its email environment in an effort to prevent a similar event from occurring in the future. Further, out of an abundance of caution, Brock is offering you complimentary identity theft protection services through IDX, the data incident and recovery services expert. These services include <<12/24>> months of credit¹ and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you to resolve issues if your identity is compromised.

What You Can Do: Brock is not aware of any misuse of information potentially impacted in connection with this incident. However, as a precautionary measure, Brock recommends that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company that maintains your account. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.

¹ To receive credit monitoring services, you must be over the age of 18, 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.

In addition, Brock encourages you to contact IDX with any questions and to enroll in your complimentary identity protection services by calling 1-833-365-2603 or going to <https://app.idx.us/account-creation/protect> and using the enrollment code provided above. IDX representatives are available to assist you Monday through Friday from 8:00 AM – 8:00 PM Central Time. Please note the deadline to enroll is April 11, 2022. Brock also encourages you to review the resources provided on the following page for additional steps to protect your personal information.

For More Information: If you have questions or need assistance, please contact IDX at 1-833-365-2603, Monday through Friday from 8:00 AM – 8:00 PM Central Time.

The security of your information is a top priority for Brock, and Brock deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in dark ink, appearing to read 'Brian Narramore', with a stylized flourish extending to the right.

Brian Narramore, PHR, SHRM-CP
SVP, Global Human Resources
The Brock Group

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

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 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate,

incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-365-2603
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [XXXXXXXXXX]

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

El 11 de enero 2022

Re: Aviso de Datos <<Variable5>>

Estimado <<First Name>> <<Last Name>>:

Le escribimos para informarle acerca de un incidente de seguridad de datos que a ocurrido en The Brock Group, el cual puede ser que su informacion personal halla sido afectada. Brock toma su privacidad y seguridad de informacion muy en serio. Esta carta contiene informacion acerca de lo ocurrido y pasos de los cuales usted puede tomar para asegurar su informacion personal.

Que Ocurrió: El 21 de Julio 2021, Brock se enteró de la actividad sospechosa asociada con ciertas cuentas de correo electrónico de los empleados de Brock. Al descubrir esta actividad, Brock tomó medidas inmediatas para proteger las cuentas de correo electrónico y comenzó una investigación preliminar. Al hacerlo, Brock contrató a expertos independientes en ciberseguridad para determinar qué sucedió y si se accedió a los datos de Brock o se adquirieron sin autorización. A través de esa investigación, Brock se enteró de que se había accedido a determinadas cuentas de correo electrónico de los empleados sin autorización. Luego, Brock contrató a un proveedor para que revisara el contenido de las cuentas de correo electrónico relevantes que probablemente contengan datos confidenciales. Como resultado, el 21 de diciembre de 2021, Brock se enteró de que una o más de las cuentas de correo electrónico relevantes contenían parte de su información personal.

Tenga en cuenta que Brock no tiene conocimiento del uso indebido de cualquier información potencialmente afectada en relación con este incidente. Sin embargo, Brock está notificando a las personas potencialmente afectadas por precaución.

Qué tipo de información fue involucrada: La información impactada en conexión a este incidente varia para cada persona que pudo haber sido afectada, pero pudo haber incluido su nombre <<Variable6>>.

Que estamos haciendo: En cuanto Brock supo de lo ocurrido, Brock tomo las medidas de precaución que ya mencionamos anteriormente. Además, Brock implementó medidas de seguridad adicionales para fortalecer aún más su entorno de correo electrónico en un esfuerzo para evitar que ocurra un evento similar en el futuro. Además, por precaución, Brock le ofrece servicios complementarios de protección contra robo de identidad a través de IDX, el experto en servicios de recuperación e incidentes de datos. Estos servicios incluyen << 12/24 >> meses de crédito y monitoreo CyberScan, una póliza de reembolso de seguro de \$ 1,000,000 y servicios de recuperación de robo de identidad completamente administrados. Con esta protección, IDX lo ayudará a resolver problemas si su identidad se ve comprometida.

Que puede hacer: Brock no tiene conocimiento de ningún uso indebido de la información potencialmente afectada en relación con este incidente. Sin embargo, como medida de precaución, Brock recomienda que permanezca atento y revise 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 que mantiene su cuenta.

Además, debe informar de inmediato cualquier actividad fraudulenta o cualquier incidente sospechoso de robo de identidad a las autoridades policiales correspondientes.

Además, Brock aconseja a que se comunique con IDX si tiene alguna pregunta o para inscribirse en sus servicios de protección de identidad de cortesía llamando al 1-833-365-2603 o visitando <https://app.idx.us/account-creation/protect> y usando el código de inscripción proporcionado arriba. Representantes de IDX están disponibles para asistirlo de lunes a viernes de 8:00 AM – 8PM horario Central. Por favor tenga en cuenta que la fecha límite para inscribirse es el 11 de abril 2022. Brock también le recomienda a revisar los recursos proporcionados en la siguiente página para conocer los pasos adicionales para proteger su información personal.

Para más información: Si tiene alguna pregunta o necesita asistencia, por favor comuníquese con IDX al 1-833-365-2603, lunes a viernes de 8:00 AM – 8:00 PM horario central.

La seguridad de su información es una prioridad para Brock, y Brock lamenta profundamente cualquier preocupación o inconveniente que esto pueda causarle.

Sinceramente,

A handwritten signature in black ink, appearing to be 'Brian Narramore', with a stylized flourish extending to the right.

Brian Narramore, PHR, SHRM-CP
SVP, Global Human Resources
The Brock Group

Medidas que usted puede tomar para proteger su información

Revise sus estados de cuentas y notifique a autoridades policiacas de cualquier actividad sospechosa. Como medida preventiva es recomendable que revise sus estados de cuentas y reportes de crédito. Si nota cualquier actividad sospechosa en alguna cuenta, debe notificar a la institución financiera o compañía con la cual pertenece la cuenta. También debe reportar cualquier actividad sospechosa o si tiene dudas de que su identidad fue robada con autoridades policiacas, fiscal general del estado, y a la Comisión Federal de Comercio. (FTC).

Copia de Reporte de Crédito: Puede obtener una copia totalmente gratuita de su informe de crédito en cada una de las tres agencias principales de informes de crédito cada 12 meses visitando la página de internet <http://www.annualcreditreport.com/>, llamando al número gratuito 1-877-322-8228, o completando un formulario de solicitud de informe crédito anual y enviarlo a Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. Usted también puede contactar alguna de las siguientes agencias nacionales de informes de crédito:

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 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Alerta de Fraude: Debe considerar la posibilidad de incluir una alerta de fraude en su informe de crédito. Una alerta de fraude inicial es gratuita y permanecerá en su archivo de crédito por lo menos un año. La alerta informara a los acreedores de una posible actividad fraudulenta dentro de su informe y solicitara que el acreedor se comuniquen con usted antes de establecer cuentas a su nombre. Para colocar una alerta de fraude en su informe de crédito, comuníquese con cualquiera de las tres agencias de informes de crédito identificadas anteriormente. Puede encontrar más información en <http://www.annualcreditreport.com>.

Congelación de Seguridad: Usted tiene derecho a congelar su expediente crediticio por un año sin ningún costo. Esto evitara que se abra nuevo crédito a su nombre sin el uso de un numero de PIN que se le proporciona cuando inicia la congelación. Un congelamiento de seguridad está diseñado para evitar que los acreedores potenciales accedan a su informe crediticio sin su consentimiento. Como resultado, el uso de un congelamiento de seguridad puede interferir o retrasar su capacidad para obtener crédito. Debe colocar por separado un congelamiento de seguridad en su archive de crédito con cada agencia de informes crediticios. Para colocar un congelamiento de seguridad, es posible que se le solicite que proporcione a la agencia de informes del consumidor información que lo identifique, incluyendo su nombre complete, número de seguro social, fecha de nacimiento, dirección actual y anteriores, una copia de su tarjeta de identificación emitida por el estado, y una facture de servicios públicos, cuenta de bancos o comprobante de seguro.

Recursos gratuitos adicionales: Puede obtener información de las agencias de informes del consumidor, la FTC o del Fiscal general estatal sobre alertas de fraude, congelamientos de seguridad y pasos que puede tomar para prevenir el robo de identidad. Si sospecha de robo de identidad puede reportarlo a las autoridades, incluyendo a FTC o al Fiscal General de su estado.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

También tiene ciertos derechos en Fair Credit Reporting Act (FCRA): Estos derechos incluyen el saber que está incluido en su archivo; cuestionar cualquier información equivocada; hacer que las agencias de informes del consumidor corrijan o eliminen información inexacta, incompleta o no verificada; así como otros derechos. Para más información acerca de FCRA, y sus derechos por favor visite <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.