



Robert L. Slaughter III
633 West 5th Street, Suite 4000
Los Angeles, California 90071
Robert.Slaughter@lewisbrisbois.com
Direct: 213.680.5028

May 9, 2021

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey:

We represent San Diego Family Care ("SDFC"), a healthcare provider headquartered in San Diego, California. This letter is being sent on behalf of SDFC because personal information belonging to Maine residents may have been affected by a recent data security incident. This information may have included the Maine residents' names and Social Security numbers.

In December 2020, SDFC became aware that our information technology hosting provider, NetGain, experienced a data security incident that resulted in the encryption of certain data. The hosting provider took steps to secure and restore its systems and launched an investigation with the assistance of computer forensics experts. At that time, SDFC did not know what, if any, SDFC data may have been involved in the incident.

In late January 2021, SDFC received a follow up notification from its hosting provider advising that, based on its investigation into the incident, certain SDFC data may have been accessed or acquired by an unauthorized individual. SDFC obtained a copy of the impacted data and engaged an independent data review firm to conduct a thorough review to identify any individuals whose information may have been involved in the incident. That review concluded on April 12, 2021. Since that time, we have been working to identify up-to-date contact information needed to notify all individuals potentially affected by this incident. On April 30, 2021, SDFC identified six (6) Maine residents within the potentially affected population whose personal information was affected as a result of this incident.

SDFC issued notification letters to the potentially affected Maine residents via first-class U.S. mail on May 7, 2021. A sample copy of the notification letter is attached hereto.

Attorney General Aaron Frey
May 9, 2021
Page 2

SDFC is working with its hosting provider to ensure that appropriate remediation steps are taken to further secure the environment and reduce the likelihood of a similar incident occurring in the future. SDFC is also offering complimentary credit monitoring and identity theft protection services through IDX to all individuals whose Social Security numbers were potentially impacted by this incident, as an added layer of protection.

SDFC is committed to protecting the personal information in its possession. If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at (213) 680-5028 or via email at Robert.Slaughter@lewisbrisbois.com.

Very truly yours,

A handwritten signature in black ink, appearing to read "Robert L. Slaughter III". The signature is written in a cursive style with a horizontal line underneath the name.

Robert L. Slaughter III of
LEWIS BRISBOIS BISGAARD & SMITH LLP

RLS:ALW

Attachment: Consumer Notification Letter Template



SAN DIEGO FAMILY CARE
A California Non-Profit Corporation

C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
(833) 664-1997
Or Visit:
<https://response.idx.us/sdfcprotect>
Enrollment Code: <<XXXXXX>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

May 7, 2021

Subject: Notice of Data <<Variable 1>>

Dear <<FIRST NAME>> <<LAST NAME>>:

I am writing to inform you of a data security incident that may have affected your personal information. At San Diego Family Care (“SDFC”), we take the privacy and security of your personal information very seriously. We are contacting you to notify you that this incident occurred and inform you about steps you can take to ensure your information is protected, including enrolling in the complimentary identity protection services we are making available to you.

What Happened. In December 2020, SDFC became aware that our information technology hosting provider experienced a data security incident that resulted in the encryption of certain data. The hosting provider took steps to secure and restore its systems, and launched an investigation with the assistance of computer forensics experts. At that time, SDFC did not know what, if any, SDFC data may have been involved in the incident.

On January 20, 2021, we received a follow up notification from our hosting provider informing us that, based on its investigation into the incident, certain SDFC data may have been accessed or acquired by an unauthorized individual. We obtained a copy of the impacted data, and engaged experts to conduct a thorough review to identify individuals whose information may have been involved in the incident. That review concluded on April 12, 2021, and indicated that your information may have been involved.

Please note that this unauthorized access was limited to a system that stored information about insurance claims, and did not affect any other SDFC information systems, such as our electronic medical record system. We are not aware of the misuse of any personal information that may have been affected by this incident.

What Information Was Involved. The affected information may have included your <<Variable 2>>.

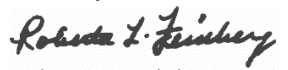
What Are We Doing. As soon as SDFC learned of the incident, we took the steps described above. We are also working with our hosting provider to ensure that appropriate remediation measures are taken to reduce the likelihood of a similar incident occurring in the future. In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. We recommend that you review the guidance included with this letter about how to protect your information. In addition, you can enroll in the free credit monitoring services that we are offering to you through IDX by calling (833) 664-1997 or going to <https://response.idx.us/sdfcprotect> and using the Enrollment Code provided above.

For More Information. If you have questions or need assistance, please contact (833) 664-1997, Monday through Friday, 6am – 6pm PT. Our representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your personal information.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,


Roberta L. Feinberg, M.S.
Chief Executive Officer
San Diego Family Care

<<Nombre>> <<Apellido>>
<<Dirección1>>
<<Dirección2>>
<<Ciudad>>, <<Estado>> <<Código postal>>

Para inscribirse, llame al:
(833) 664-1997
o visite:
<https://response.idx.us/sdfcprotect>
Código de inscripción: <<xxxxx>>

7 de mayo de 2021

Estimado/a <<Nombre>> <<Apellido>>:

Le escribo para informarle acerca de un incidente de seguridad de datos que puede haber afectado su información personal. En San Diego Family Care ("SDFC"), nos tomamos muy en serio la privacidad y seguridad de su información personal. Nos comunicamos con usted para informarle la existencia de este incidente y las medidas que puede tomar para asegurarse de que su información esté protegida, incluida la inscripción en los servicios complementarios de protección de identidad que ponemos a su disposición.

Qué ocurrió. En diciembre de 2020, SDFC tuvo conocimiento de que nuestro proveedor de hosting de tecnología de la información experimentó un incidente de seguridad de datos que dio como resultado el cifrado de cierta información. El proveedor de hosting tomó medidas para proteger y restaurar sus sistemas e inició una investigación con la ayuda de expertos en informática forense. En ese momento, SDFC no sabía qué datos de SDFC, en caso de que existiera alguno, podrían haber estado involucrados en el incidente.

El 20 de enero de 2021, recibimos una notificación de seguimiento de nuestro proveedor de hosting en la que nos informaban que, según la investigación del incidente, es posible que una persona no autorizada haya accedido o adquirido ciertos datos de SDFC. Obtuvimos una copia de los datos afectados y contratamos a expertos para realizar una revisión exhaustiva a fin de identificar a las personas cuya información puede haber estado involucrada en el incidente. Dicha revisión concluyó el 12 de abril de 2021 e indicó que su información puede haber estado involucrada.

Tenga en cuenta que este acceso no autorizado se limitó a un sistema que almacenaba información sobre reclamaciones de seguros y no afectó a ningún otro sistema de información de SDFC, como nuestro sistema de registro médico electrónico. No tenemos conocimiento del uso indebido de ninguna información personal que pueda haber sido afectada por este incidente.

Qué información estuvo involucrada. La información afectada incluye nombres de personas, números de seguro social, fechas de nacimiento, diagnósticos médicos o información sobre tratamientos, información del seguro médico o números de identificación de clientes. Sin embargo, no todos los elementos de los datos se vieron afectados para cada persona. Puede encontrar información adicional en la página 1 o al llamar al (833) 664-1997.

Medidas que tomamos. Tan pronto como SDFC tuvo conocimiento del incidente, tomamos las medidas descritas anteriormente. También estamos trabajando con nuestro proveedor de hosting para asegurarnos de que se tomen las medidas correctivas adecuadas para reducir la probabilidad de que ocurra un incidente similar en el futuro. Además, ofrecemos servicios de protección contra robo de identidad a través de IDX, el experto en servicios de violación y recuperación de datos. Los servicios de protección de identidad de IDX incluyen: 12 meses de supervisión de crédito y CyberScan, una política de reembolso de \$1,000,000 en concepto de seguro y servicios de recuperación de robo de identidad completamente administrados. Con esta protección, IDX lo ayudará a resolver problemas si su identidad está comprometida.

Qué puede hacer usted Le recomendamos que revise la orientación incluida con esta carta sobre cómo proteger su información. Además, para inscribirse en los servicios gratuitos de supervisión de crédito que le ofrecemos a través de IDX, puede llamar al (833) 664-1997 o visitar <https://response.idx.us/sdfcprotect> y usar el Código de inscripción proporcionado anteriormente.

Más información. Si tiene preguntas o necesita ayuda, comuníquese con el (833) 664-1997, de lunes a viernes, de 6 a. m. a 6 p. m., Hora del Pacífico. Nuestros representantes están plenamente informados sobre este incidente y pueden responder cualquier pregunta que pueda tener con respecto a la protección de su información personal.

Nos tomamos muy en serio su confianza y este asunto. Acepte nuestras más sinceras disculpas por cualquier preocupación o inconveniente que esto pueda ocasionarle.

Atentamente.



Roberta L. Feinberg, M.S.
Directora Ejecutiva

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 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 with which the account is maintained. You should also 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 (the "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 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 can also 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	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.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 90 days. 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. 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. There is no charge to place, lift or remove the security freeze. 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. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov or www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, Rhode Island, and the District of Columbia can obtain more information from their Attorneys General using the contact information below.

New York Attorney General Bureau of Internet and Technology Resources 28 Liberty Street New York, NY 10005 ifraud@ag.ny.gov 1-212-416-8433	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	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 riag.ri.gov 1-401-274-4400	District of Columbia Attorney General 400 6 th Street NW Washington, D.C., 20001 http://www.oag.dc.gov 202-727-3400
--	---	---	--	---

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. Contact information for the three national credit reporting agencies may be found above.

MEDIDAS QUE PUEDE TOMAR PARA PROTEGER AÚN MÁS SU INFORMACIÓN

Revise sus estados de cuenta y notifique actividades sospechosas a las autoridades policiales: Como medida de precaución, le recomendamos que se mantenga 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 empresa o institución financiera con la que se mantiene la cuenta. También debe informar de inmediato cualquier actividad fraudulenta o cualquier sospecha de robo de identidad a las autoridades policiales correspondientes, al Fiscal General de su estado y a la Comisión Federal de Comercio (la "FTC").

Copia del informe crediticio Para obtener una copia gratuita de su informe crediticio por parte de cada una de las tres principales agencias de informes de crédito una vez cada 12 meses, visite <http://www.annualcreditreport.com/>, llame a la línea gratuita 877-322-8228, o complete un Formulario de solicitud de informe crediticio anual y envíelo por correo al Servicio de solicitud de informe crediticio anual, P.O. Box 105281, Atlanta, GA 30348. También puede ponerse en contacto con una de las tres 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

Free Annual Report

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
www.annualcreditreport.com

Alerta de fraude: Es posible que considere colocar una alerta de fraude en su informe crediticio. Una alerta de fraude inicial es gratuita y permanecerá en su archivo de crédito durante al menos 90 días. La alerta informa a los acreedores posibles actividades fraudulentas dentro de su informe y solicita que el acreedor se comunique con usted antes de establecer cuentas a su nombre. Para colocar una alerta de fraude en su informe crediticio, comuníquese con cualquiera de las tres agencias de informes de crédito identificadas anteriormente. Puede encontrar información adicional en <http://www.annualcreditreport.com>.

Congelamiento de seguridad: Tiene derecho a aplicar un congelamiento de seguridad en su archivo de crédito. Esto evitará que se abra un crédito nuevo a su nombre sin el uso de un número PIN que se le emite cuando inicia el congelamiento. Un congelamiento de seguridad está diseñado para evitar que potenciales acreedores accedan a su informe crediticio sin su consentimiento. Como resultado, la utilización de un congelamiento de seguridad puede interferir con o demorar su capacidad para obtener crédito. Debe colocar un congelamiento de seguridad en su archivo de crédito por separado con cada agencia de informes de crédito. Colocar, levantar o quitar un congelamiento de seguridad no tienen ningún costo. Para colocar un congelamiento de seguridad, es posible que deba proporcionar a la agencia de informes del consumidor información que lo identifique, incluido su nombre completo, número de seguro social, fecha de nacimiento, direcciones actuales y anteriores, una copia de su tarjeta de identificación emitida por el estado y una factura de servicios públicos, un extracto bancario o un extracto de seguro recientes.

Recursos gratuitos adicionales: Puede obtener información de las agencias de informes del consumidor, la FTC o el Fiscal General de su respectivo estado sobre alertas de fraude, congelamientos de seguridad y medidas que puede tomar para prevenir el robo de identidad. Puede denunciar la sospecha de robo de identidad a las autoridades policiales locales, incluso a la FTC o al Fiscal General de su estado. La información de contacto de la FTC es: **Federal Trade Commission (Comisión Federal de Comercio)**, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov o www.ftc.gov/idtheft, 1-877-438-4338. Los residentes de Nueva York, Maryland, Carolina del Norte y Rhode Island pueden obtener más información de sus Fiscales Generales a través de la información de contacto a continuación.

New York Attorney General (Fiscal General de Nueva York) Bureau of Internet and Technology Resources 28 Liberty Street Nueva York, NY 10005 ifraud@ag.ny.gov 1-212-416-8433	Maryland Attorney General (Fiscal General de Maryland) 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General (Fiscal General de Carolina del Norte) 9001 Centro de servicio de correo Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General (Fiscal General de Rhode Island) 150 South Main Street Providence, RI, 02903 riag.ri.gov 1-401-274-4400	District of Columbia Attorney General (Fiscal General del Distrito de Columbia) 400 6 th Street NW Washington, D.C., 20001 http://www.oag.dc.gov 202-727-3400
---	--	---	---	---

También tiene otros derechos conforme a la Ley de Informe Imparcial de Crédito (FCRA, por sus siglas en inglés): Estos derechos incluyen el derecho a saber qué hay en su archivo; debatir información incompleta o inexacta; y solicitar a las agencias de informes del consumidor que corrijan o eliminen información inexacta, incompleta o no verificable. Para obtener más información sobre la FCRA, visite <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

Información personal de un menor: Puede solicitar que cada una de las tres agencias nacionales de informes de crédito realice una búsqueda manual del número de seguro social de un menor para determinar si existe un informe de crédito asociado. Es posible que se requieran copias de la información de identificación del menor y del padre/tutor, incluido el certificado de nacimiento o adopción, la tarjeta del Seguro Social y la tarjeta de identificación emitida por el gobierno. Si existe un informe de crédito, debe solicitar una copia del informe y comunicar de inmediato cualquier cuenta fraudulenta a la agencia de informes de crédito. También puede denunciar cualquier uso indebido de la información de un menor a la FTC en <https://www.identitytheft.gov/>. Para obtener más información sobre el robo de identidad infantil e instrucciones para solicitar una búsqueda manual de número de seguro social, visite el sitio web de la FTC: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. La información de contacto de las tres agencias nacionales de informes de crédito se puede encontrar más arriba.