LEWIS BRISBOIS BISGAARD & SMITH LLP

Maria Efaplomatidis
77 Water Street, Suite 2100
New York, NY 10005
Maria.Efaplomatidis@lewisbrisbois.com
Direct: 212.232.1366

May 24, 2022

VIA WEB PORTAL

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Notification of Data Security Incident

Dear Attorney General Frey:

Lewis Brisbois Bisgaard & Smith LLP represents Val Verde Regional Medical Center ("VVRMC"), a medical center located in Del Rio, Texas, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maine's data breach notification statute.

1. Nature of the Security Incident

On March 10, 2022, VVRMC experienced a data security incident that disrupted its network. VVRMC immediately initiated an investigation and retained third-party digital forensics experts to determine the source and scope of the incident as well as determine whether sensitive information may have been accessed or acquired in connection with the incident.

On March 24, 2022, the investigation determined that some personal information may have been impacted as a result of the incident. VVRMC then worked diligently to identify the individuals and up-to-date address information in order to provide notification of this incident. This process was completed on May 12, 2022.

2. Type of Information and Number of Maine Residents Involved

The incident involved personal information for approximately eighteen (18) Maine residents. The information involved may include name, Social Security number, date of birth, medical information, and health insurance information.

The affected individuals will receive a letter notifying them of the incident, offering complimentary identity monitoring services through Kroll, and providing additional steps they can take to protect their personal information. These services include credit monitoring, monitoring through Web Watcher, Public Persona, and Quick Cash Scan, a $1,000,000 identity fraud loss reimbursement policy, and access to fraud consultation services. The notification letters will be sent via U.S. First-Class Mail on May 24, 2022. A sample copy of the notification letter sent to the affected individuals is attached.

3. Measures Taken to Address the Incident

In response to the incident, VVRMC implemented additional measures to reduce the risk of a similar incident occurring in the future. VVRMC notified the FBI of this incident and will cooperate with any resulting investigation. Additionally, as discussed above, VVRMC is notifying the affected individuals and providing them with steps they can take to protect their personal information, including enrolling in complimentary identity monitoring services.

4. Contact Information

VVRMC is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at Maria.Efaplomatidis@lewisbrisbois.com.

Sincerely,

Maria Efaplomatidis of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Individual Notification Letter

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Header Vtext RE: Notice of…)>>

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

At Val Verde Regional Medical Center ("VVRMC"), we strive to deliver healthcare our community can trust, and we are committed to the security of all information within our possession. We are writing to inform you of a data security incident that may have involved some of your personal information. We would like to notify you of this incident, offer you complimentary identity monitoring services, and inform you about steps that can be taken to help safeguard your personal information. We acknowledge that this incident may cause you stress and we want to extend our sincere apologies.

What Happened. On March 10, 2022, VVRMC experienced a network disruption. We immediately initiated an investigation and secured our network. We also engaged third-party digital forensics experts to assist with the investigation and determine whether sensitive information may have been accessed or acquired during the incident. Through our investigation, we learned that certain files containing your personal information were accessed or acquired without authorization during the incident. We then took steps to identify up-to-date address information to notify you. While the extensive data identification and processing was lengthy and time-consuming, it was a necessary process that helped us thoroughly identify the impacted individuals as required by law. That process was completed on May 12, 2022.

What Information Was Involved. The information affected during the incident may have included your first name, last name, Social Security number, date of birth, medical information, health insurance information, and other information.

What Are We Doing. As soon as we discovered the incident, we took the steps described above. We also implemented enhanced security measures to help prevent a similar incident from occurring in the future. We also notified the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrators accountable. We are also offering you complimentary identity monitoring services for 12 months through Kroll, 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, Web Watcher, Public Persona, Quick Cash Scan, identity theft insurance reimbursement policy (see details below), Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

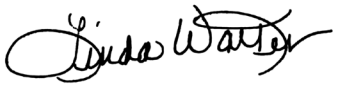
What You Can Do. Please follow the recommendations included with this letter to help protect your personal information. You can also activate the Kroll identity monitoring services being provided to you, at no cost, through Kroll.

Additional information describing the Kroll identity monitoring services, along with other recommendations to help protect your personal information, is included with this letter.

For More Information. Should you have any additional questions or concerns please contact us at: 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

With this letter, we hope that we have provided some reassurance that we will continue to focus on being the premier provider you deserve. Again, please accept our sincere apologies for any worry or inconvenience this incident might cause you.

Sincerely,



Linda Walker
Chief Executive Officer
Val Verde Regional Medical Center

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will 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 will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. 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.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
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.

Steps You Can Take to Help Protect Your Personal 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.

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Header Vtext RE: Notice of…)>>

Estimado(a) <<first_name>> <<last_name>>:

En Val Verde Regional Medical Center ("VVRMC"), nos esforzamos por brindar atención médica en la que nuestra comunidad pueda confiar, y estamos comprometidos con la seguridad de toda la información que tenemos en nuestro poder. Le escribimos para informar sobre un incidente de seguridad de datos que puede haber involucrado parte de su información personal. Esta carta es para para notificarle de este incidente, ofrecerle servicios complementarios de monitoreo de identidad e informarle sobre los pasos que se pueden tomar para ayudar a proteger su información personal. Reconocemos que este incidente puede causarle estrés y queremos extenderle nuestras más sinceras disculpas.

¿Qué sucedió? El 10 de marzo de 2022, VVRMC experimentó una interrupción de la red. Inmediatamente iniciamos una investigación y aseguramos nuestra red. También contratamos a expertos forenses digitales de terceros para ayudar con la investigación y determinar si se pudo haber accedido o adquirido información confidencial durante el incidente. A través de nuestra investigación, supimos que ciertos archivos que contenían su información personal fueron accedidos o adquiridos sin autorización durante el incidente. Luego tomamos medidas para identificar la información actualizada de la dirección para notificarle. Si bien la identificación y el procesamiento de datos extensos fueron prolongados y consumieron mucho tiempo, fue un proceso necesario que nos ayudó a identificar completamente a las personas afectadas según lo exige la ley. Ese proceso se completó el 12 de mayo de 2022.

¿Qué información estuvo involucrada? La información afectada durante el incidente puede haber incluido su nombre, apellido, número de Seguro Social, fecha de nacimiento, información médica, información del seguro médico y otra información.

¿Qué estamos haciendo? Tan pronto como descubrimos el incidente, tomamos los pasos mencionados anteriormente. Además, implementamos medidas de seguridad mejoradas para ayudar a evitar que ocurra un incidente similar en el futuro. También notificamos al Buró Federal de Investigaciones y brindaremos la cooperación que sea necesaria para responsabilizar a los perpetradores. Adicionalmente, le ofrecemos servicios de monitoreo de identidad gratuitos durante 12 meses a través de Kroll, un líder mundial en respuesta y mitigación de riesgos, y su equipo tiene una amplia experiencia en ayudar a las personas que han sufrido una exposición no intencional de datos confidenciales. Sus servicios de monitoreo de identidad incluyen Monitoreo de crédito, Observador Web, Persona pública, Escaneo rápido de efectivo, póliza de reembolso de seguro de robo de identidad (ver detalles a continuación), Consulta de fraude y Restauración de robo de identidad.

Visite **https://enroll.krollmonitoring.com** para activar y aprovechar los servicios de monitoreo de identidad.
Tiene hasta el <<b2b_text_5(ActivationDeadline)>> para activar los servicios de monitoreo de identidad.
Su número de membresía es: **<<Membership Number s_n>>**

Para obtener más información sobre Kroll y sus servicios de monitoreo de identidad, puede visitar info.krollmonitoring.com.

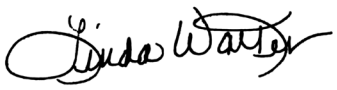
¿Qué puede hacer? Siga las recomendaciones incluidas en esta carta para ayudar a proteger su información personal. También puede activar los servicios de monitoreo de identidad de Kroll que se le brindan, sin costo alguno, a través de Kroll.

En esta carta se incluye información adicional que describe los servicios de monitoreo de identidad de Kroll, junto con otras recomendaciones para ayudar a proteger su información personal.

Para obtener más información. Si tiene alguna pregunta o inquietud adicional, comuníquese con nosotros al:1-???-???-????, de lunes a viernes de 8:00 a. m. a 5:30 p. m. Hora Central, excepto los principales días festivos de EE. UU.

Con esta carta, esperamos haberle brindado cierta seguridad de que continuaremos enfocándonos en ser el principal proveedor que usted se merece. Nuevamente, acepte nuestras más sinceras disculpas por cualquier preocupación o inconveniente que este incidente pueda causarle.

Atentamente,



Linda Walker
Chief Executive Officer
Val Verde Regional Medical Center

KROLL

APROVECHE LOS SERVICIOS DE MONITOREO DE IDENTIDAD

Se le ha brindado acceso a los siguientes servicios de Kroll:

Monitoreo de crédito de una oficina de crédito

Recibirá alertas cuando haya cambios en su información crediticia, por ejemplo, cuando se solicite una nueva línea de crédito a su nombre. Si no reconoce la actividad, tendrá la opción de llamar a un especialista en fraude de Kroll, que podrá ayudarlo a determinar si se trata de un indicador de robo de identidad.

Web Watcher

Web Watcher supervisa los sitios de Internet donde los delincuentes pueden comprar, vender e intercambiar información de identidad personal. Se generará una alerta si se encuentra evidencia de su información de identidad personal.

Public Persona

Public Persona monitorea y notifica cuando los nombres, alias y direcciones se asocian con su número de Seguro Social. Si se encuentra información, recibirá una alerta.

Quick Cash Scan

Quick Cash Scan monitorea las fuentes de préstamos a corto plazo y de anticipo de efectivo. Recibirá una alerta cuando se informe un préstamo y puede llamar a un especialista en fraudes de Kroll para obtener más información.

Reembolso de pérdida por fraude de identidad de $1 millón

Le reembolsa los gastos de bolsillo por un total de hasta $1 millón en costos y gastos legales cubiertos por cualquier evento de robo de identidad. Toda cobertura está sujeta a las condiciones y exclusiones de la póliza.

Asesoría sobre fraude

Tiene acceso ilimitado para realizar consultas con un especialista en fraude de Kroll. El asesoramiento incluye mostrarle las formas más efectivas de proteger su identidad, explicarle sus derechos y protecciones en virtud de la ley, ofrecer asistencia con las alertas de fraude e interpretar cómo se accede y utiliza la información personal, incluyendo la investigación de actividades sospechosas que podrían estar vinculadas con un incidente de robo de identidad.

Restauración por robo de identidad

Si resulta ser víctima de un robo de identidad, un investigador experto autorizado de Kroll trabajará en su representación para resolver cualquier problema relacionado. Tendrá acceso a un investigador especializado que entiende sus problemas y que puede realizar la mayor parte del trabajo por usted. El investigador podrá investigar a fondo para revelar todos los aspectos del robo de identidad y, luego, trabajar para resolverlo.

El sitio web de activación de Kroll solo es compatible con la versión actual o una versión anterior de Chrome, Firefox, Safari y Edge. Para recibir servicios de crédito, usted debe ser mayor de 18 años y tener un crédito en EE. UU., tener un número de seguro social a su nombre, así como un domicilio de residencia en EE. UU. asociado a su expediente de crédito.

Medidas que puede tomar para proteger su información personal

Revise los resúmenes de su cuenta y notifique a la policía sobre actividades sospechosas: como medida de precaución, le recomendamos que se mantenga alerta y revise de cerca sus estados de cuenta e informes crediticios. Si detecta alguna actividad sospechosa en una cuenta, debería notificar de inmediato a la institución financiera o empresa con la que mantiene la cuenta. También debería informar de inmediato 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 (FTC).

Copia del informe crediticio: puede obtener una copia gratuita de su informe crediticio de cada una de las tres principales agencias de informes crediticios 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 crediticio anual y enviándolo por correo postal a Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. También puede comunicarse con una de las siguientes 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 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Alerta de fraude: es posible que desee considerar la posibilidad de incluir una alerta de fraude en su informe crediticio. Una alerta de fraude inicial es gratuita y permanecerá en su archivo de crédito durante 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 establecer cuentas a su nombre. Para colocar una alerta de fraude en su informe crediticio, comuníquese con cualquiera de las tres agencias de informes crediticios identificadas anteriormente. Se encuentra disponible información adicional en http://www.annualcreditreport.com.

Bloqueo de seguridad: Tiene derecho a poner un congelamiento de seguridad en su archivo de crédito por hasta un año sin costo alguno. Esto evitará que se abra un nuevo crédito a su nombre sin el uso de un PIN que se emite para usted cuando inicia el bloqueo. El bloqueo de seguridad está diseñado para evitar que los posibles otorgantes de crédito accedan a su informe crediticio sin su consentimiento. Como resultado, el uso de un bloqueo de seguridad puede interferir o retrasar su capacidad para obtener crédito. Debe colocar por separado un bloqueo de seguridad en su archivo de crédito con cada agencia de informes crediticios. Para colocar un bloqueo de seguridad, es posible que se le solicite que proporcione 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 reciente de servicios públicos, estado de cuenta o extracto del seguro.

Recursos gratuitos adicionales: Puede obtener información de las agencias de informes del consumidor, la FTC o del Fiscal General de su estado respectivo sobre alertas de fraude, bloqueos de seguridad y pasos que puede tomar para prevenir el robo de identidad. Puede denunciar la sospecha de robo de identidad a la policía local, incluso a la FTC o al Fiscal General del estado.

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

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

Fiscal General de Nueva York
Oficina de Recursos de Internet y Tecnología
28 Liberty Street
New York, NY 10005
1-212-416-8433

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

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

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

También tiene ciertos derechos en virtud de la Ley de informes crediticios justos (FCRA): estos derechos incluyen saber qué hay en su archivo, disputar información incompleta o inexacta, y exigir que las agencias de informes del consumidor corrijan o eliminen información inexacta, incompleta o no verificable; así como otros derechos. Para obtener más información sobre la FCRA y sus derechos conforme a la FCRA, visite https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.