From: mail@msgbsvc.com on behalf of El Centro Regional Medical Center <noreply@ECRMC.org>
Sent: Tuesday, November 13, 2018 3:50 PM
To: DL-Data Breach Team
Subject: HTML Sample -- Notice of Data Breach

**** This is not a monitored inbox. Please do not reply. If you have any questions regarding this incident or if you desire further information or assistance, please do not hesitate to contact us toll-free at 888-891-0631, Monday through Friday, 6:00am to 6:00pm Pacific Time, except holidays. For international callers outside the United States, please call +1-503-597-7676 (some charges may apply).****

Dear [NAME]:

El Centro Regional Medical Center values the privacy and confidentiality of its employees and job applicants. Regretfully, we are writing to inform you about an incident that may have impacted some of your personal information. This notice explains what happened, what information was affected, what measures we have taken, and some steps you can take in response to the incident.

What Happened?

In late-August we were notified by Jobscience, a vendor we contract with to help us process job applications, that they experienced an intrusion into their systems and that information relating to ECRMC job applicants may have been impacted. Jobscience said they were continuing their investigation and would provide additional information. In early-October, Jobscience notified us that, based on their investigation, electronic information that job applicants had submitted when filling out online job applications and applying for positions at ECRMC, had been stolen from their server by an unknown third party. The theft occurred between May 8, 2018 and May 11, 2018. We then worked with Jobscience and an outside forensic vendor to determine what individuals were impacted.

What Information Was Involved?

Jobscience informed El Centro that the incident may have involved your name, address, phone number, username and password, and email information. The information **did not** include your Social Security number, health information, or financial information.

What Are We Doing?

Upon learning about the incident, we began working with Jobscience to determine which of our job applicants were impacted. We have confirmed that Jobscience has worked with the Federal Bureau of Investigation (FBI) and a service provider to investigate the incident. Jobscience has also made assurances that they have contained the incident, ended the third party's access to their system, and remediated the issues that led to the compromise. We understand from Jobscience that their investigation and notice to ECRMC was not delayed at the request of a law enforcement agency or as a result of a law enforcement investigation.

To date, we are not aware of any reports of identity fraud resulting from this incident and we do not have any evidence that suggests that your personal information has been misused. Nonetheless, out of an abundance

of caution wanted to take the proactive measure to notify you about the incident and provide you with information on how to safeguard against identity theft.

What You Can Do

We strongly recommend that you change your username and password for any accounts that use the same credentials that you may have used when applying for a job at ECRMC on the Jobscience platform. This will prevent the third party from accessing other accounts using the compromised credentials. There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). For information about these steps please see the following pages.

For More Information

ECRMC has setup a dedicated call center with bilingual agents to answer questions regarding this incident. If you have questions and reside in the U.S., please call 888-891-0631. If you reside outside of the U.S. please call 1-503-597-7676. The call center will be available Monday through Friday, 6:00 a.m. to 6:00 p.m. Pacific Time.

We understand and value the importance of our staff's and job applicants' privacy and confidentiality, and we deeply apologize for any inconvenience or concern that this incident might cause you.

Sincerely,

Dr. Adolphe Edward
Chief Executive Officer

Additional Steps You Can Take

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 may want to contact the three U.S. credit reporting agencies to report the incident and request a credit report:

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(866) 349-5191	(888) 397-3742	(888) 909-8872
www.equifax.com	www.experian.com	www.transunion.com

Credit Report: You can request a free credit report once a year at www.annualcreditreport.com, calling 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.

Fraud Alert: To protect yourself from possible identity theft you can place a fraud alert on your credit file. A credit alert informs creditors to follow certain procedures before establishing any accounts in your name. It may also delay your ability to obtain credit. You may place a fraud alert on your file by contacting the consumer reporting agencies listed above. To place an alert you may be asked to provide the consumer reporting agency with information that identifies you, including your Social Security number.

Security Freeze: In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. 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 apply for a new credit card, loan, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. There may be fees ranging from $5-$20 for placing, lifting, and/or removing a security freeze and you may be required to provide the consumer reporting agency with information that identifies you including your Social Security number. To put a security freeze on your credit file contact the consumer reporting agencies listed above.

If you suspect any identity theft has occurred, you may contact the Federal Trade Commission by calling (877) 438-4338 or online at www.ftc.gov. The FTC is located at 600 Pennsylvania Avenue, NW Washington, DC 20580. You can also contact local law enforcement or the attorney general in your state.

Maryland residents may wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.statemd.us, or calling 410-576-6491.

North Carolina residents may wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

Rhode Island resident may wish to review information provided by the Rhode Island Attorney General at http://www.riag.ri.gov, by calling 401-274-4400, or writing to 150 South Main Street, Providence, RI 02903.

Notificación sobre violación de datos

El Centro Regional Medical Center valora la privacidad y confidencialidad de sus empleados y candidatos a puestos de trabajo. Lamentablemente, le escribimos para informarle sobre un incidente que puede haber afectado parte de su información personal. Este aviso explica qué sucedió, qué información se vio afectada, qué medidas hemos tomado y algunos pasos que puede tomar en respuesta al incidente.

¿Qué ocurrió?

A finales de agosto, Jobscience, un proveedor que contratamos para ayudarnos a procesar las solicitudes de empleo, nos notificó que experimentaron una intromisión en sus sistemas y que la información relacionada con los candidatos a puestos de trabajo de ECRMC puede haber sido afectada. Jobscience afirmó que continuaría con su investigación y que proporcionaría información adicional. A principios de octubre, Jobscience nos notificó que, según su investigación, la información electrónica que los candidatos a puestos de trabajo enviaron al completar solicitudes de empleo en línea y solicitar puestos en ECRMC había sido robada de su servidor por un tercero desconocido. El robo ocurrió entre el 8 de mayo y el 11 de mayo de 2018. Luego trabajamos con Jobscience y un proveedor forense externo para determinar qué personas se vieron afectadas.

¿Qué información se vio involucrada?

Jobscience informó a El Centro que el incidente puede haber involucrado su nombre, dirección, número de teléfono, nombre de usuario y contraseña, e información de correo electrónico. La información **no** incluye su número del Seguro Social, información de salud o información financiera.

¿Qué estamos haciendo?

Al conocer el incidente, comenzamos a trabajar con Jobscience para determinar cuáles de nuestros candidatos a puestos de trabajo se vieron afectados. Hemos confirmado que Jobscience ha trabajado con la Oficina Federal de Investigaciones (FBI) y un proveedor de servicios para investigar el incidente. Jobscience también ha asegurado que contuvo el incidente, terminó con el acceso del tercero a su sistema y solucionó los problemas que llevaron a la violación. Sabemos por Jobscience que su investigación y notificación a ECRMC no se retrasó a solicitud de una agencia de cumplimiento de la ley o como resultado de una investigación de cumplimiento de la ley.

Hasta la fecha, no tenemos conocimiento de ninguna denuncia de fraude de identidad como resultado de este incidente y no tenemos evidencia que sugiera que su información personal ha sido mal utilizada. No obstante, para extremar las precauciones, quisimos tomar la medida proactiva de notificarle sobre el incidente y brindarle información sobre cómo protegerse contra el robo de identidad.

Qué puede hacer usted

Le recomendamos encarecidamente que cambie su nombre de usuario y contraseña para cualquier cuenta que use las mismas credenciales que pudo haber utilizado al solicitar un trabajo en ECRMC a través de la plataforma Jobscience. Esto evitará que el tercero acceda a otras cuentas utilizando las credenciales comprometidas. También puede considerar otras acciones para disminuir la posibilidad de robo de identidad o fraude en su(s) cuenta(s). Para obtener información sobre estos pasos, consulte las siguientes páginas.

Para obtener más información

ECRMC ha instalado un centro de llamadas dedicado con agentes bilingües para responder preguntas relacionadas con este incidente. Si tiene preguntas y reside en los EE. UU., llame al 888-891-0631. Si reside fuera de los EE. UU., llame al 1-503-597-7676. El centro de llamadas estará disponible de lunes a viernes, de 6:00 a. m. a 6:00 p. m., hora del Pacífico.

Comprendemos y valoramos la importancia de la privacidad y confidencialidad de nuestros empleados y candidatos a puestos de trabajo, y nos disculpamos profundamente por cualquier inconveniente o preocupación que este incidente pueda causarle.

Atentamente.

Dr. Adolphe Edward
Director Ejecutivo

Medidas adicionales que puede tomar

Como medida de precaución, le recomendamos que permanezca atento y revise detenidamente sus estados de cuenta e informes crediticios. Si detecta cualquier actividad sospechosa en una cuenta, debe notificar de inmediato a la institución financiera o empresa con la que mantiene la cuenta.

Es posible que desee comunicarse con las tres agencias de informes crediticios de EE. UU. para informar el incidente y solicitar un informe de crédito:

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(866) 349-5191	(888) 397-3742	(888) 909-8872
www.equifax.com	www.experian.com	www.transunion.com

Informe crediticio: Puede solicitar un informe crediticio gratuito una vez al año en www.annualcreditreport.com, llamando al 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.

Alerta de fraude: Para protegerse contra un posible robo de identidad, puede poner un alerta de fraude en su expediente de crédito. Un alerta de crédito le informa a las entidades crediticias que deben seguir ciertos procedimientos antes de abrir cuentas a su nombre. También puede retrasar su capacidad para obtener crédito. Puede poner un alerta de fraude en su expediente comunicándose con las agencias de informes del consumidor mencionadas anteriormente. Para poner un alerta, se le puede solicitar que proporcione a la agencia de informes del consumidor información que lo identifique, incluido su número del Seguro Social.

Bloqueo de seguridad: En algunos estados de los EE. UU., tiene derecho a poner un bloqueo de seguridad en su archivo de crédito. Un bloqueo de seguridad (también conocido como congelación de crédito) dificulta que alguien abra una cuenta nueva a su nombre. Un bloqueo de seguridad está diseñado para evitar que posibles entidades crediticias accedan a su informe crediticio sin su consentimiento. Como resultado, usar un bloqueo de seguridad puede interferir o retrasar su capacidad de solicitar una nueva tarjeta de crédito, préstamo, teléfono inalámbrico o cualquier servicio que requiera una verificación de crédito. Debe poner un bloqueo de seguridad en su expediente de crédito con cada agencia de informes crediticios por separado. Puede haber tarifas que oscilan entre $5 y $20 por poner, levantar y/o eliminar un bloqueo de seguridad y es posible que deba proporcionar a la agencia de informes del consumidor información que lo identifique, incluido su número del Seguro Social. Para poner un bloqueo de seguridad en su expediente de crédito, comuníquese con las agencias de informes del consumidor enumeradas anteriormente.

Si sospecha que ha ocurrido un robo de identidad, puede comunicarse con la Comisión Federal de Comercio llamando al (877) 438-4338, o en línea en www.ftc.gov. La FTC está ubicada en 600 Pennsylvania Avenue, NW Washington, DC 20580. También puede comunicarse con la policía local o con el fiscal general de su estado.

Los residentes de Maryland pueden querer revisar la información proporcionada por el Procurador General de Maryland sobre cómo evitar el robo de identidad en http://www.oag.state.md.us/idtheft, o enviando un correo electrónico a idtheft@oag.statemd.us, o llamando al 410-576-6491.

Los residentes de Carolina del Norte pueden querer revisar la información proporcionada por el Procurador General de Carolina del Norte en http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, llamando al 877-566-7226, o escribiendo al 9001 Mail Service Center, Raleigh, NC 27699.

Los residentes de Rhode Island pueden querer revisar la información proporcionada por el Fiscal General de Rhode Island en http://www.riag.ri.gov, llamando al 401-274-4400, o escribiendo a 150 South Main Street, Providence, RI 02903.