Leon Medical Centers, LLC Provee Notificación Acerca De Incidente De Seguridad de Data

El 8 de enero del 2021, Leon Medical Centers, LLC ("Leon Medical") anunció un evento reciente que puede haber impactado la información personal de ciertas personas. Aunque al día de hoy continúa el proceso de identificar a aquellas personas que hayan sido impactadas y de notificarles por escrito lo antes posible, le estamos proveyendo información aquí en nuestra página de internet acerca del incidente y medidas que personas afectadas pueden tomar para protegerse mejor contra el robo de identidad y fraude en caso de que lo estimen necesario.

¿Qué Sucedió? El 8 de noviembre del 2020, Leon Medical se enteró de que fue blanco de un ataque por cibercriminales y que algunos sistemas habían quedado infectados por programas informáticos maliciosos. LEON MEDICAL inmediatamente desconectó de internet los sistemas y emprendió una investigación sobre el tipo y alcance del incidente con la ayuda de especialistas forenses externos en materia de informática. El 9 de noviembre del 2020, recibimos confirmación que algunos de nuestros archivos electrónicos conteniendo información personal habían sido extraídos por los ciberciminales.

¿Qué Información Estuvo Envuelta? Leon Medical ha podido determinar que el tipo de información impactada varia grandemente de una persona a otra y que las siguientes categorías de información pueden haber sido impactadas: nombre, información de contacto, número de seguro social, información financiera, fecha de nacimiento, información familiar, número de archivo médico, datos sobre prescripciones, información médica y/o clínica, incluyendo historial diagnóstico y de tratamiento, e información de seguro de salud.

¿Qué está Haciendo Leon Medical en Respuesta a este Incidente? La privacidad y seguridad de la información confidencial en sus sistemas es una de las más altas prioridades para Leon Medical. Al enterarse del incidente, Leon Medical tomó pasos inmediatos para identificar y corregir aquellas vulnerabilidades que permitieron el acceso indebido a nuestras bases de datos. Leon Medical continúa llevando una investigación profunda para identificar a aquellas personas cuya información puede haber quedad afectada por el incidente. Leon Medical continúa también proveyendo notificación por escrito a todas aquellas personas que Leon Medical determine hayan sido impactadas.

Al día de hoy, Leon Medical ya ha notificado al Departamento de Salud y Servicios Humanos (HHS), a la a oficina del Fiscal General (*Attorney General*) de Florida, al FBI y a medios de comunicación prominentes en el estado de Florida. Leon Medical puede que notifique a otras autoridades adecuadas a medida que reciba información adicional.

Qué pueden hacer las personas afectadas. Personas que estimen que hayan podido ser afectadas por este incidente pueden llamar a nuestra línea exclusiva de ayuda proveída a continuación y también pueden referirse a la información que aparece a continuación bajo el título "*Medidas que puede tomar para proteger su información contra el robo y/o fraude*."

Si desea más información. Si usted entiende que ha sido impactado por este incidente y tiene preguntas, por favor llame a nuestra línea exclusiva de ayuda al 855-914-4725 entre las horas de 9am – 9pm ET.

MEDIDAS QUE PUEDE TOMAR PARA PROTEGER SU INFORMACIÓN CONTRA EL ROBO Y/O FRAUDE.

Leon Medical recomienda que se mantenga alerta y siga monitoreando sus cuentas buscando actividades poco comunes o cargos que usted no hizo. Si nota algo sospechoso y sospecha que hay actividades fraudulentas, debe llamar inmediatamente a la institución financiera que emitió la tarjeta de crédito o débito. La ley de Estados Unidos le da a usted el derecho a un informe gratuito sobre su crédito anualmente procedente de cada una de las tres agencias principales de información crediticia. Pida el informe gratuito sobre su crédito al visitar por internet la dirección www.annualcreditreport.com o llame gratis al 1-877-322-8228. También puede comunicarse directamente con las tres agencias principales de información crediticia para pedir un ejemplar gratis del informe sobre su crédito.

Tiene el derecho de pedir que se ponga la paralización por seguridad (*security freeze*) del informe sobre su crédito, por lo que se prohibiría que las agencias de información al consumidor divulguen información en el informe sobre su crédito sin que usted las autorice expresamente. El objetivo de la paralización por seguridad o *security freeze* es el de evitar que se aprueben en nombre suyo, sin su consentimiento, créditos, préstamos y servicios. Sin embargo, debe saber que emplear la paralización por seguridad o *security freeze* para tomar el control de quienes obtienen acceso a la información personal y financiera del informe sobre su crédito puede retrasar la aprobación oportuna de toda solicitud o petición que usted haga en relación con un préstamo, crédito o hipoteca nuevos o cualquier otra cuenta que tenga que ver con el otorgamiento de crédito y también puede interferir en lo anterior o prohibirlo.

Según las leyes federales, a usted no se le puede cobrar por pedir que se ponga o se quite la paralización por seguridad o *security freeze* en el informe sobre su crédito. Si quiere poner la paralización por seguridad o *security freeze*, favor de comunicarse con las agencias principales de información al consumidor que aparecen a continuación:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	**www.transunion.com/credit-freeze**	www.equifax.com/personal/credit-report-services

Tiene que suministrar la información señalada seguidamente para pedir la paralización por seguridad o *security freeze*:

1. Su nombre completo (inclusive la letra inicial de su segundo nombre de pila y también el sufijo Jr., Sr., II, III, etc.);
2. El número del Seguro Social;
3. La fecha de nacimiento;
4. Si se ha mudado en los últimos cinco (5) años, indique las direcciones en que ha vivido en los últimos cinco años;
5. Prueba de su dirección actual, como la última cuenta de la electricidad, agua o teléfono;
6. Una fotocopia que se pueda leer de un documento de identidad expedido por el gobierno (la licencia de conducción o documento de identidad del estado, el documento de identidad de las fuerzas armadas, etc.);
7. Si es víctima de robo de identidad, incluya la copia del informa a la policía, el informe sobre la investigación o denuncia relacionada con el robo de identidad ante la autoridad policíaca.

Como alternativa a la paralización por seguridad o *security freeze*, tiene el derecho de pedir que se ponga en su expediente la alerta inicial por fraude o la alerta por fraude prolongada (*fraud alert)* sin que le cueste nada. La alerta inicial por fraude es la alerta que dura un año que se pone en el expediente de crédito del consumidor. Cuando una empresa ve que se muestra la alerta por fraude en el expediente de crédito del consumidor, la empresa tiene que tomar las medidas correspondientes para verificar la identidad del consumidor antes de volver a darle crédito. Si es víctima de robo de identidad, tiene el derecho a la alerta por fraude prolongada, que es la alerta por fraude que dura siete años. Si quiere poner la alerta por fraude, se ruega que se comunique con cualquiera de las agencias que aparecen a continuación:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Pueden informarse más acerca del robo de identidad, alertas por fraude, paralizaciones por seguridad y las medidas que se pueden tomar para protegerse comunicándose con las agencias de información al consumidor, la Comisión Federal de Comercio (Federal Trade Commission) o el Fiscal General (Attorney General). He aquí la información para comunicarse con la Comisión Federal de Comercio: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); y TTY: 1-866-653-4261. La Comisión Federal de Comercio también aconseja a aquéllos que descubren que se ha hecho uso inadecuado de su información que presenten la denuncia correspondiente ante dicha entidad. Pueden obtener más datos sobre cómo presentar dicha denuncia por medio de la información de contacto que aparece más abajo. Tienen el derecho de presentar el informe a la policía si llegan a ser víctima de robo de identidad o fraude. Se ruega que noten que para presentar la denuncia por robo de identidad ante las autoridades policíacas es posible que tengan que aportar alguna prueba de que han sido víctima. Los casos en que se conoce o se sospeche que ha habido robo de identidad también deben denunciarse ante las autoridades policíacas y el Fiscal General (Attorney General) estatal. Esta notificación do ha sido demorada por las autoridades policiacas.