

Leon Medical Centers, LLC Provee Notificación Actualizada Acercas Del Incidente De Seguridad de Data del 2020

Doral, Florida, 12 de mayo del 2021 – El 8 de enero del 2021, Leon Medical Centers, LLC (“Leon Medical”) anunció un incidente de seguridad relacionado con la información personal de algunos de nuestros pacientes y empleados. Al enterarse del incidente, Leon Medical llevó a cabo una investigación comprensiva y meticulosa sobre la información que potencialmente fue impactada con la meta de identificar aquellas personas que fueron afectadas o que pudiesen ser habido afectadas. Habiendo concluido este proceso, Leon Medical les provee ahora la actualización que aparece a continuación. Leon Medical toma muy en serio la confidencialidad, privacidad y seguridad de la información en su cuidado. Hasta el día de hoy, Leon Medical no ha recibido ningún reporte de que haya habido algún uso o intento de hacer uso impropio de dicha información.

¿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 cibercriminales.

Aproximadamente en el 23 de diciembre del 2020, Leon Medical se entero de que los cibercriminales habían extraído información de los sistemas de Leon Medical y que habían empezado a publicar la información robada en el Internet. Desde el 23 de diciembre del 2020, Leon Medical ha ido llevando una investigación sobre el contenido de los archivos que fueron publicados ilegalmente por los cibercriminales con la meta de identificar a aquellos individuos que hayan sido o que pueden haber sido afectados, tanto como los tipos de información envueltos. Este proceso fue concluido recientemente.

¿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, dirección, fecha de nacimiento, número de Seguro Social, nombre del proveedor, número de historia clínica, información de tratamiento y diagnóstico y /o información de seguro médico, incluyendo el número de Medicare, el número de la póliza y el número de ID de miembro.

¿Qué está Haciendo Leon Medical en Respuesta a este Incidente? Leon Medical se toma muy en serio la privacidad y la seguridad de la información confidencial a su cuidado. En respuesta al incidente, Leon Medical tomó pasos inmediatos para identificar y corregir aquellos problemas 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 quedado afectada por el incidente. Leon Medical continúa también proveyendo notificación por escrito a todas aquellas personas que Leon Medical determine hayan sido impactadas.

En este momento, Leon Medical ya ha notificado al Departamento de Salud y Servicios Humanos (HHS), a las autoridades reguladoras estatales, la Oficina Federal de Investigaciones (FBI) y a medios de comunicación destacados en todo el estado de Florida.

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. Por favor, visite nuestro sitio web en <http://www.leonmedicalcenters.com>, donde hemos publicado información relevante y actualizaciones sobre esta situación desde enero de 2021.

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

La ley de Estados Unidos le da al consumidor el derecho a un informe gratuito sobre su crédito anualmente procedente de cada una de las tres agencias principales de información crediticia, Equifax, Experian y TransUnion. 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.

Consumidores tienen el derecho de pedir que se ponga sin consto una alerta de fraude (*fraud alert*), inicial o prolongada, sobre el archivo de su crédito. 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 desea poner la alerta por fraude, se ruega que se comunique con cualquiera de las tres agencias que aparecen abajo.

Como alternativa a la alerta de fraude, los consumidores tienen el derecho de obtener una paralización de crédito o *credit freeze*, por lo que se prohibiría que las agencias de crédito divulguen información contenida en el informe de crédito sin la autorización expresa del consumidor. El objetivo de la paralización de crédito o *credit 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 de crédito o *credit 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 de crédito o *credit freeze* en el informe sobre su crédito. Si quiere poner la paralización de crédito o *credit freeze*, tendrá que suministrar la información señalada a continuación:

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. Las direcciones en que ha vivido en los últimos dos a 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.); y
7. Si es víctima de robo de identidad, incluya la copia del informe a la policía, el informe sobre la investigación o denuncia relacionada con el robo de identidad ante la autoridad policíaca.

Si quiere poner la paralización de crédito (*credit freeze*) o una alerta de fraude (*fraud alert*), favor de comunicarse directamente con una de las tres agencias principales de información de crédito que aparecen a continuación:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Más información

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 adviertan 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 sospecha que ha habido robo de identidad también deben denunciarse ante las autoridades policíacas y el Fiscal General (*Attorney General*). Esta notificación no ha sido demorada por las autoridades policíacas.