



November 8, 2023

Anjali C. Das
312.821.6164 (Direct)
anjali.das@wilsonelser.com

Via E-Mail: Idtheft@oaq.state.md.us

Attorney General Anthony Brown
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Cybersecurity Incident

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Riverdale Mental Health d/b/a Mosaic Mental Health (“MOSAIC”), a mental healthcare provider based in the Bronx, New York, with respect to a cybersecurity incident that was discovered by MOSAIC on July 27, 2023 (hereinafter, the “Incident”). Please note MOSAIC takes the security and privacy of the information within its control seriously, and has taken steps to prevent a similar incident from occurring in the future. This letter will serve as a notice of the Incident and to inform you of the steps MOSAIC has taken in response to the Incident.

1. Nature of the Incident

On July 27, 2023, MOSAIC was made aware that its computer systems had been impacted by a ransomware incident resulting in the encryption of its computer systems (the “Incident”). Immediately upon discovery of the Incident, MOSAIC engaged a specialized incident response vendor to conduct a forensic investigation to determine the extent and root cause of the incident. The forensic investigation concluded on September 20, 2023, which confirmed unauthorized access to MOSAIC’s computer systems. The investigation further determined the time period of unauthorized activity within MOSAIC’s network was limited only to July 27, 2023.

Upon confirming unauthorized access to its systems, MOSAIC conducted a review of the compromised servers to determine whether personally identifiable information was maintained within the impacted computer servers for purposes of notifying those individuals whose sensitive personal information may have been impacted by the Incident. Based on its review of the data maintained within the compromised computer systems, MOSAIC determined that the following elements of personal information may have been accessed and/or acquired by an unauthorized individual: names, addresses, dates of birth, and Social Security numbers.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky
Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Missouri • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix
San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

To mitigate the incident, MOSAIC mailed notification letters to the potentially affected individuals along with an offer for complimentary credit monitoring services and further instructions on how to protect their personal information. As of this writing, MOSAIC has not received any reports of related identity theft, since the date of the Incident to the present.

2. Number of Maryland residents affected.

MOSAIC discovered that the Incident may have resulted in unauthorized exposure of information pertaining to seven (7) Maryland residents. Notification letters to these individuals were mailed on October 25, 2023, by First Class Mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

MOSAIC is committed to ensuring the security and privacy of all personal information within its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, MOSAIC moved quickly to investigate and respond to the Incident. Specifically, MOSAIC engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, MOSAIC has taken steps to strengthen its security posture to prevent a similar event from occurring again in the future.

MOSAIC is also offering twelve (12) months of complimentary credit monitoring and identity theft restoration services through TransUnion to potentially affected individuals residing in Maryland to help protect their identity. Additionally, MOSAIC provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact Information

MOSAIC remains dedicated to protecting the sensitive information within its control. Should you have any questions or need additional information, please do not hesitate to contact me at anjali.das@wilsonelser.com or 312.821.6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



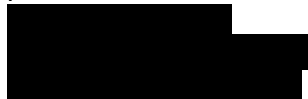
Anjali C. Das

EXHIBIT A

Mosaic Mental Health
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



P



October 24, 2023

VIA FIRST-CLASS MAIL

Notice of Data Security Incident

Dear [REDACTED],

Riverdale Mental Health d/b/a Mosaic Mental Health ("MOSAIC") is writing to inform you of a recent cybersecurity incident that may have involved your protected health information ("PHI"). MOSAIC takes the privacy of client information very seriously and sincerely apologizes for any inconvenience this Incident may cause. This letter contains details about the Incident, steps we have taken in response to mitigate any risk, and services we are making available to protect your information.

What Happened?

On July 27, 2023, MOSAIC discovered that its computer systems had been impacted by a ransomware incident resulting in the encryption of its computer systems (the "Incident"). Immediately upon discovery of the Incident, MOSAIC engaged a specialized incident response vendor to conduct a forensic investigation to determine the extent and root cause of the incident. The forensic investigation confirmed unauthorized access to MOSAIC's computer systems first occurring on July 27, 2023. On August 24, 2023, MOSAIC completed its review of the compromised servers and identified those individuals whose information may have been impacted as a result of the Incident. Based upon the results of its review, MOSAIC is notifying all those clients whose information may have been accessed by an unauthorized user.

What Information Was Involved?

The investigation confirmed that client information maintained within the compromised computer systems may have been subject to unauthorized access. The data contained in this system may include protected health information such as your: name, address, date of birth, and Social Security number.

While MOSAIC has no reason to believe that any client's information has been misused, we are nonetheless notifying our clients out of an abundance of caution.

What We Are Doing

MOSAIC takes the privacy and security of our personal information very seriously, and has taken steps to prevent a similar event from occurring in the future.

In order to address any individual concerns and mitigate any exposure or risk of harm following this Incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit

Score/Cyber Monitoring services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/mosaic> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED].

In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under eighteen (18) years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do

Although MOSAIC is not aware of any instances of misuse of any client information, we recommend that our clients take advantage of the complimentary services that are being offered. Instructions on how to enroll in these services are included in the materials enclosed with this letter. You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. The FTC also provides information on-line at www.ftc.gov/idtheft.

We encourage you to remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following page, which contains important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. MOSAIC recognizes that you may have questions not addressed in this letter. If you have additional questions, please call 1-833-441-0319 (toll free) during the hours of 8:00 am and 8:00 pm Eastern Time, Monday through Friday (excluding U.S. national holidays).

MOSAIC sincerely regrets any inconvenience or concern that this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Mosaic Mental Health

Additional Important Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-alerts

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Identity Protection PIN: You can get a six-digit Identity Protection PIN to prevent someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. An IP PIN is used by the IRS to verify your identity when filing your electronic or paper tax return. To receive an IP Pin, you must register to validate your identity at IRS.gov. Use the Get an IP PIN tool available between mid-January through mid-November to receive your IP PIN.

<https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>



00001020580000

P

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov



00001030500000

P

P



24 de octubre de 2023

POR SERVICIO POSTAL URGENTE

Aviso de incidente de seguridad de datos

Estimado/a :

Riverdale Mental Health, que opera comercialmente como Mosaic Mental Health (“MOSAIC”), le escribe para informarle sobre un incidente reciente de ciberseguridad que pudo incluir su información protegida de salud (protected health information, PHI). MOSAIC se toma muy en serio la privacidad de la información de los clientes y le pide sinceras disculpas por cualquier inconveniente que este Incidente pueda causar. Esta carta contiene detalles sobre el Incidente, las medidas que tomamos para mitigar cualquier riesgo y los servicios que pusimos a disposición para proteger su información.

¿Qué sucedió?

El 27 de julio de 2023, MOSAIC descubrió que sus sistemas informáticos se vieron afectados por un incidente de ransomware que dio lugar al cifrado de sus sistemas informáticos (el “Incidente”). Inmediatamente después de descubrir el incidente, MOSAIC contrató a un proveedor especializado en respuesta ante incidentes para que llevara a cabo una investigación forense a fin de determinar el alcance y la causa del incidente. La investigación forense confirmó el acceso no autorizado a los sistemas informáticos de MOSAIC que se produjo por primera vez el 27 de julio de 2023. El 24 de agosto de 2023, MOSAIC completó su revisión de los servidores comprometidos e identificó a aquellas personas cuya información podría haberse visto afectada como resultado del Incidente. En función de los resultados de su revisión, MOSAIC notifica a todos los clientes a cuya información es posible que haya accedido un usuario no autorizado.

¿De qué información se trató?

La investigación confirmó que la información de los clientes mantenida dentro de los sistemas informáticos comprometidos puede haber estado sujeta a acceso no autorizado. Los datos contenidos en este sistema pueden incluir información de protegida de salud, como su nombre, dirección, fecha de nacimiento y número de Seguro Social.

Si bien MOSAIC no tiene motivos para creer que se haya utilizado indebidamente cualquier información de los clientes, de igual forma notificamos a las personas por precaución.

¿Que estamos haciendo?

MOSAIC se toma muy en serio la privacidad y seguridad de nuestra información personal y ya tomó medidas para evitar que ocurra un evento similar en el futuro.

A fin de abordar cualquier inquietud individual y mitigar cualquier exposición o riesgo de daño después de este Incidente, le proporcionamos acceso a los servicios de una agencia de monitoreo de crédito, una agencia de informe de crédito, una agencia de puntaje de crédito o monitoreo cibernético sin cargo. Estos servicios le proporcionan alertas, durante doce (12) meses a partir de la fecha de inscripción, cuando se producen cambios en su archivo de crédito. Esta notificación se le envía el mismo día en que se realiza el cambio o la actualización con la agencia. Mediante la vigilancia cibernética, se buscarán sus datos personales en la dark web (web oscura) y se le alertará si detectamos en línea su información de identificación personal. Por último, le proporcionamos asistencia proactiva para casos de fraude para ayudarlo con cualquier pregunta que tenga o en caso de ser víctima de fraude. Cyberscout brindará estos servicios a través de Identity Force, una compañía de TransUnion especializada en asistencia para casos de fraude y servicios de reparación.

Para inscribirse sin cargo en los servicios de monitoreo de crédito, inicie sesión en <https://secure.identityforce.com/benefit/mosaic> y siga las instrucciones proporcionadas. Cuando se lo soliciten, proporcione el siguiente código para recibir los servicios: [REDACTED].

Para que usted pueda recibir los servicios de vigilancia que se describen anteriormente, deberá inscribirse en un plazo de noventa (90) días a partir de la fecha de esta carta. La inscripción requiere conexión a internet y una cuenta de correo electrónico y es posible que no esté disponible para menores de dieciocho (18) años. Tenga en cuenta que, al inscribirse en los servicios de vigilancia, es posible que se le pida que verifique la información personal para su propia protección a fin de confirmar su identidad.

¿Qué puede hacer usted?

Aunque MOSAIC no tiene conocimiento de ningún caso de uso indebido de cualquier información de clientes, recomendamos que nuestros clientes aprovechen los servicios gratuitos que se ofrecen. Las instrucciones sobre cómo inscribirse en estos servicios se incluyen en los materiales adjuntos a esta carta. También puede obtener más información de la Comisión Federal de Comercio (Federal Trade Commission, FTC) sobre el robo de identidad y las formas de protegerse. La FTC tiene una línea directa de robo de identidad: 877-438-4338; TTY: 1-866-653-4261. La FTC también proporciona información en línea en www.ftc.gov/idtheft.

Le recomendamos que permanezca atento, monitoree sus cuentas e informe de inmediato cualquier actividad sospechosa o sospecha de uso indebido de su información personal. Además, le recomendamos que revise la siguiente página, la cual contiene información adicional importante sobre las medidas que puede tomar para proteger su información personal, como la implementación de alertas de fraude y congelamientos de seguridad.

Para más información

Tenga en cuenta que la protección de su información personal es una prioridad principal y le pedimos sinceras disculpas por cualquier inquietud o inconveniente que este asunto pueda causarle. MOSAIC reconoce que es posible que tenga preguntas que no se abordan en esta carta. Si tiene preguntas adicionales, llame al 1-833-441-0319 (número gratuito) de lunes a viernes de 8:00 a. m. a 8:00 p. m., hora del este (excepto los feriados nacionales de EE. UU.).

MOSAIC lamenta sinceramente cualquier inconveniente o inquietud que este asunto pueda causar y sigue dedicado a garantizar la privacidad y seguridad de toda la información bajo nuestro control.

Atentamente,

Mosaic Mental Health



00001040540000

P

Información adicional importante

Informes de crédito: puede obtener una copia de su informe de crédito sin cargo independientemente de si sospecha o no de que hubo actividad no autorizada en su cuenta. Puede obtener una copia gratuita de su informe de crédito de cada una de las tres agencias nacionales de informes de crédito. Para solicitar su informe de crédito gratuito, visite www.annualcreditreport.com o llame sin cargo al 1-877-322-8228. También puede solicitar su informe de crédito anual gratuito, para lo cual deberá completar y enviar por correo un formulario de solicitud de informe de crédito anual (disponible en <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) a: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Alertas de fraude: puede activar alertas de fraude con las tres agencias de informes de crédito por teléfono o en línea. Una alerta de fraude les indica a los acreedores que sigan ciertos procedimientos, incluido comunicarse con usted, antes de abrir cuentas nuevas o cambiar sus cuentas existentes. Por ese motivo, implementar una alerta de fraude puede protegerlo, pero también puede retrasarlo cuando busque obtener crédito. Desde el 21 de septiembre de 2018, las alertas iniciales de fraude duran un año. Las víctimas de robo de identidad también pueden extender la alerta de fraude a siete años.

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-alerts

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Monitoreo: siempre debe estar atento a incidentes de fraude y robo de identidad al revisar los estados de cuenta de la tarjeta de crédito y monitorear su informe de crédito para detectar actividades sospechosas o inusuales.

PIN de protección de identidad: puede obtener un PIN de protección de identidad de seis dígitos para evitar que otra persona presente una declaración de impuestos utilizando su número de Seguro Social o su número de identificación de contribuyente individual. El IRS utiliza un PIN de protección de identidad para verificar su identidad al presentar su declaración de impuestos electrónica o impresa. Para recibir un PIN de protección de identidad, debe registrarse para validar su identidad en IRS.gov. Utilice la herramienta Obtener un PIN de protección de identidad disponible entre mediados de enero y mediados de noviembre para recibir su PIN de protección de identidad.

<https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>

Congelamiento de seguridad: tiene derecho a aplicar un congelamiento de seguridad a su informe de crédito. Un congelamiento de seguridad tiene como objetivo evitar que se aprueben créditos, préstamos y servicios a su nombre sin su consentimiento. Para aplicar un congelamiento de seguridad a su informe de crédito, debe hacer una solicitud a cada agencia de informes del consumidor. Puede realizar esa solicitud por correo certificado, correo con entrega al día siguiente, correo postal con sello postal regular o al seguir las instrucciones que encuentran en los sitios web detallados más adelante. Se debe incluir la información siguiente al solicitar un congelamiento de seguridad (tenga en cuenta que si solicita un informe de crédito para su cónyuge o un menor de 16 años, también debe proporcionar esta información respecto a dicha persona): (1) nombre completo, con la inicial del segundo nombre y cualquier sufijo; (2) número de Seguro Social; (3) fecha de nacimiento; (4) dirección actual y cualquier dirección anterior de los últimos cinco años y (5) cualquier informe de incidente o queja aplicable ante una agencia de aplicación de la ley o el Registro de Vehículos Motorizados. La solicitud también debe incluir una copia de una tarjeta de identificación emitida por el gobierno y una copia de una factura de servicios públicos o estado de cuenta bancario o de seguro recientes. Es esencial que cada copia sea legible y muestre su nombre y dirección postal actual y la fecha de emisión. Desde el 21 de septiembre de 2018, es gratuito aplicar, levantar o eliminar un congelamiento de seguridad. También puede aplicar un congelamiento de seguridad a menores de 16 años. Puede obtener un congelamiento de seguridad gratuito al comunicarse con una o más de las siguientes agencias nacionales de informes del consumidor:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

Hacer una denuncia policial: tiene derecho a realizar u obtener una denuncia policial si experimenta fraude de identidad. Tenga en cuenta que, para realizar una denuncia penal o informar un incidente por robo de identidad ante un organismo de aplicación de la ley, es probable que deba proporcionar pruebas de que fue víctima. A menudo, se requiere una denuncia policial para disputar artículos que han sido objeto de fraude. Por lo general, puede denunciar presuntos incidentes de robo de identidad a las autoridades locales o al fiscal general.

FTC y fiscal general: puede informarse aún más sobre robo de identidad, alertas de fraude, congelamientos de seguridad y las medidas que puede tomar para protegerse al comunicarse con las agencias de informes del consumidor, la Comisión Federal de Comercio (Federal Trade Commission, FTC) o el fiscal general de su estado. Puede comunicarse con la Comisión Federal de Comercio en la siguiente dirección: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. La Comisión Federal de Comercio también alienta a quienes descubran que su información se utilizó de manera indebida a que presenten una queja ante la FTC. Puede obtener más información sobre cómo presentar dicha queja a través de la información de contacto indicada con anterioridad. Los casos de robo de identidad conocidos o presuntos también deben denunciarse ante los organismos de aplicación de las leyes.

Para residentes de Iowa: la ley estatal le aconseja que informe cualquier sospecha de robo de identidad a las autoridades policiales o al fiscal general.

Para residentes de Massachusetts: la ley estatal exige que se le informe sobre su derecho a presentar una denuncia policial con respecto a este incidente. Si es víctima de robo de identidad, también tiene derecho a presentar una denuncia policial y obtener una copia de ella.

Para residentes de Nuevo México: la ley estatal le aconseja que revise los estados de cuenta personales y los informes de crédito, según corresponda, para detectar errores resultantes de la violación de seguridad. Tiene derechos de conformidad con la Ley de Informe Justo de Crédito (Fair Credit Reporting Act), como, por ejemplo, el derecho a que se le comunique si la información de su archivo de crédito se utilizó en su contra, el derecho a saber qué hay en su archivo de crédito, el derecho a solicitar su puntaje de crédito y el derecho a disputar información incompleta o inexacta. Además, de conformidad con la Ley de Informe Justo de Crédito, las agencias de informes de crédito del consumidor deben corregir o eliminar información inexacta, incompleta o no verificable; las agencias de informes de crédito del consumidor no pueden proporcionar información negativa desactualizada; el acceso a su archivo es limitado; usted debe dar su consentimiento para que los informes de crédito se proporcionen a los empleadores; puede limitar las ofertas de crédito y seguro “preseleccionadas” que reciba en función de la información de su informe de crédito y puede reclamar daños y perjuicios a los infractores. En virtud de la Ley de Informe Justo de Crédito, es posible que tenga derechos adicionales que no están aquí resumidos. Las víctimas de robo de identidad y el personal militar en servicio activo tienen derechos adicionales específicos de conformidad con la Ley de Informe Justo de Crédito. Le recomendamos que revise sus derechos de conformidad con la Ley de Informe Justo de Crédito en www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf o Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

Para residentes de Oregón: la ley estatal le aconseja que informe cualquier sospecha de robo de identidad a las autoridades policiales, al fiscal general y la Comisión Federal de Comercio.

Para residentes de Rhode Island: la ley estatal exige que se le informe sobre su derecho a presentar u obtener un informe policial con respecto a este incidente.

Para residentes de Arizona, Colorado, Distrito de Columbia, Illinois, Maryland, Nueva York, Carolina del Norte y Rhode Island: puede obtener información de las oficinas del fiscal general y de la Comisión Federal de Comercio sobre alertas de fraude, congelamientos de seguridad y medidas que puede tomar para prevenir el robo de identidad.



000010505K0000

P.

Comisión Federal de Comercio: Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Oficina del fiscal general de Arizona: Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Oficina del fiscal general de Colorado: Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

Oficina del fiscal general del Distrito de Columbia: Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Oficina del fiscal general de Illinois: 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Oficina del fiscal general de Maryland: Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

Oficina del fiscal general de Nueva York: Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

Oficina del fiscal general de Carolina del Norte: Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Oficina del fiscal general de Rhode Island: Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov