

Harbor Regional Center
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024



Via First-Class Mail

3 1 480 *****SNGLP



July 13, 2026

Notice of Data Breach

Dear [REDACTED]:

Harbor Developmental Disabilities Foundation, DBA Harbor Regional Center (“Harbor”) writes to inform you of a recent event that may impact some of your personal information. We take the privacy and security of all information very seriously, and while we are not aware of any actual or attempted misuse of your information to perpetrate fraud, we are providing you with an overview of the event, our response, and resources to help further protect your information.

What Happened?

On or about March 7, 2026, we became aware of unusual activity in our network environment. Upon becoming aware, we promptly began an investigation into the scope and nature of the suspicious activity and retained legal counsel and third-party forensic specialists to investigate the unusual activity. That investigation revealed that certain information may have been accessed by an unauthorized individual as part of the event. This activity occurred on March 6 and 7, 2026. We then began a comprehensive review of the data set to determine what sensitive and/or personal information was impacted and to whom it related. On July 7, 2026, we finished our review of the impacted information.

At this time, there is no indication that any information has been misused. However, we are providing this notification to you out of an abundance of caution so that you may take steps to safeguard your information.

What Information Was Involved?

The potentially impacted information varied by individual. Based on our investigation, the following information relating to you may have been viewed or copied without authorization: [REDACTED]

What We Are Doing.

The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon detecting this data event, we moved promptly to investigate and respond to the event and notify potentially impacted individuals. As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this event, and we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 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. 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, a TransUnion company specializing in fraud assistance and remediation services. While we are covering the cost of these services, you will need to complete the activation process yourself.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Personal Information*, to learn more about how to protect against potential information misuse.

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. Please note that the code is case-sensitive and will need to be entered as it appears.

In order for you to receive the monitoring services described above, you must enroll within 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 the age of 18 years of age. Once enrolled you will have 12 months of monitoring services. At the end of 12 months, the services will be deactivated. 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.

For More Information

We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the assistance line at 1-800-405-6108, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding major U.S. holidays. Please have this letter ready if you call.

Sincerely,

Harbor Developmental Disabilities Foundation DBA
Harbor Regional Center

Steps You Can Take to Help Protect Personal 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.

Security Freeze: You also 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; (5) proof of current address (such as a copy of a government-issued identification card, a recent utility bill, or bank or insurance statement); and (6) other personal information as required by the applicable credit reporting agency. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

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. Instances of known or suspected identity theft should also be reported to law enforcement or to the Attorney General's office in your home jurisdiction. This notice has not been delayed by law enforcement.

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.

Harbor Regional Center
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024



A través de correo prioritario

3 1 457 *****SNGLP



July 13, 2026

Aviso de Violación de Datos

Estimado(a) [REDACTED]:

Harbor Developmental Disabilities Foundation, que opera bajo el nombre de DBA Harbor Regional Center ("Harbor"), escribe para informarle de un evento reciente que puede afectar parte de su información personal. Tomamos muy en serio la privacidad y la seguridad de toda la información, y si bien no tenemos conocimiento de ningún uso indebido real o intento de uso indebido de su información para cometer fraude, le proporcionamos una descripción general del evento, nuestra reacción y recursos para ayudar a proteger aún más su información.

¿Qué sucedió?

Alrededor del 7 de marzo de 2026 tomamos conocimiento de una actividad inusual en nuestro entorno de red. Al darnos por enterados, comenzamos inmediatamente una investigación sobre el alcance y la naturaleza de la actividad sospechosa y contratamos a un asesor legal y a especialistas forenses externos para investigar la actividad inusual. Esa investigación reveló que una persona no autorizada podría haber accedido a cierta información como parte del evento. Esta actividad tuvo lugar el 6 y 7 de marzo de 2026. Luego comenzamos una revisión integral del conjunto de datos para determinar qué información confidencial y/o personal se vio afectada y a quién se relacionaba. El 7 de julio 2026, terminamos nuestra revisión de la información afectada.

En este momento, no hay indicios de que se haya utilizado indebidamente ninguna información. Sin embargo, le proporcionamos esta notificación por precaución para que pueda tomar medidas para resguardar su información.

¿Qué información se vio involucrada?

La información potencialmente afectada varió según la persona. Según nuestra investigación, la siguiente información relacionada con usted podría haberse visto y copiado sin autorización: [REDACTED]

Lo que estamos haciendo

La confidencialidad, privacidad y seguridad de la información bajo nuestro cuidado se encuentran entre nuestras más altas prioridades. Al detectar este evento de datos, actuamos rápidamente para investigar y responder al evento y notificar a las personas potencialmente afectadas. Como parte de nuestro compromiso continuo con la privacidad de la información y la seguridad de la información, le notificamos

este evento y le proporcionamos acceso a los servicios de **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** sin cargo. Estos servicios le proporcionarán alertas durante 12 meses a partir de la fecha de inscripción cuando se produzcan cambios en su archivo de crédito. Esta notificación se le enviará el mismo día en que se realice el cambio o la actualización con la oficina. Por último, le proporcionaremos asistencia proactiva contra el fraude para ayudarle con cualquier pregunta que pueda tener o en caso de que sea víctima de fraude. Estos servicios se ofrecerán a través de Cyberscout, una empresa de TransUnion que se especializa en servicios de asistencia y remediación de fraudes. Si bien cubrimos el costo de estos servicios, usted tendrá que completar el proceso de activación.

Qué puede hacer

Le recomendamos que esté atento a los incidentes de robo de identidad y fraude revisando sus estados de cuenta y vigilando sus informes de crédito para detectar actividades sospechosas o no autorizadas. Además, los expertos en seguridad sugieren que se comunique con su institución financiera y con todas las principales agencias de informes de crédito para informarles de dicha filtración y luego tome las medidas recomendadas para proteger sus intereses, incluida la posible implementación de una alerta de fraude en su expediente de crédito. Revise la información adjunta *Medidas que puede tomar para proteger la información personal*, para obtener más información sobre cómo protegerse contra el uso indebido de su información.

Para inscribirse en los servicios de Monitoreo de crédito sin cargo, inicie sesión en <https://bfs.cyberscout.com/activate> y siga las instrucciones que se indican. Cuando se le solicite, proporcione el siguiente código único para recibir servicios: [REDACTED]. Tenga en cuenta que el código distingue entre mayúsculas y minúsculas, y deberá ingresarse tal como aparece.

Para que pueda recibir los servicios de monitoreo descritos anteriormente, debe inscribirse dentro de los 90 días a partir de la fecha de esta carta. La inscripción requiere una conexión a Internet y una cuenta de correo electrónico, y es posible que no esté disponible para menores de 18 años. Una vez inscrito, obtendrá 12 meses de servicios de monitoreo. Al finalizar el período de 12 meses, los servicios se desactivarán. Tenga en cuenta que, al inscribirse en los servicios de monitoreo, es posible que se le pida que verifique su información personal para su propia protección a fin de confirmar su identidad.

Para obtener más información

Entendemos que podría tener preguntas sobre este incidente que no se abordan en esta carta. Si tiene preguntas adicionales, llame a la línea de asistencia al 1-800-405-6108, de lunes a viernes, de 8:00 a.m. a 8:00 p.m., hora del este, excepto los principales días feriados de EE. UU. Tenga a mano esta carta si llama.

Atentamente,

Harbor Developmental Disabilities Foundation DBA
Harbor Regional Center

Medidas que puede tomar para proteger la información personal

Informes de crédito: puede obtener una copia de su informe de crédito, sin cargo, independientemente de si sospecha o no de alguna 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 al número gratuito 1-877-322-8228. También puede solicitar su informe de crédito anual gratuito enviando por correo un Formulario de solicitud de informe de crédito anual completo (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.

Congelamiento de seguridad: también tiene derecho a aplicar un congelamiento de seguridad en su informe de crédito. Un congelamiento de crédito pretende evitar que el crédito, los préstamos y los servicios se aprueben en su nombre sin su consentimiento. Para implementar un congelamiento de seguridad en 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 con sello postal regular o siguiendo las instrucciones que se encuentran en los sitios web que se enumeran a continuación. Se debe incluir la siguiente información al solicitar un congelamiento de seguridad: (tome en cuenta que, si solicita un informe de crédito para su cónyuge o un menor de 16 años, también debe proporcionar esta información para él/ella) 1) nombre completo, con la inicial del segundo nombre y cualquier sufijo; 2) número de Seguridad Social; 3) fecha de nacimiento; 4) dirección actual y cualquier dirección anterior de los últimos cinco años; 5) comprobante de domicilio actual (como una copia de una tarjeta de identificación emitida por el gobierno, un recibo reciente de servicios públicos, o un estado de cuenta bancario o del seguro), y 6) otra información personal según lo requiera la agencia de informes de crédito correspondiente. Es esencial que cada copia sea legible, muestre su nombre y dirección postal actual, y la fecha de emisión. De conformidad con la ley federal, no se puede cobrar a los consumidores por colocar o levantar un congelamiento de crédito en su informe de crédito. Puede obtener un congelamiento de seguridad gratuito comunicándose con una o más de las siguientes agencias nacionales de informes del consumidor:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze
---	---	--

Alertas de fraude: Puede colocar alertas de fraude con las tres agencias de crédito por teléfono y en línea con:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); o
- Experian (<https://www.experian.com/fraud/center.html>).

Una alerta de fraude indica a los acreedores que deben seguir ciertos procedimientos, entre ellos, comunicarse con usted, antes de abrir nuevas cuentas o cambiar sus cuentas existentes. Por ese motivo, colocar una alerta de fraude puede protegerlo, pero también puede retrasarlo cuando busca obtener crédito. Las alertas de fraude iniciales duran un año. Las víctimas de robo de identidad también pueden obtener una alerta de fraude extendida por siete años. Los números de teléfono de las tres agencias de crédito se encuentran en la parte inferior de esta página.

Monitoreo: siempre debe permanecer alerta y monitorear sus cuentas para detectar actividad sospechosa o inusual.

Presentar informe policial: usted tiene derecho a presentar u obtener una denuncia policial si alguna vez sufre de fraude de identidad. Tenga en cuenta que, para presentar una denuncia policial o de incidente ante las autoridades por robo de identidad, es probable que tenga que proporcionar alguna prueba de que ha sido víctima. A menudo se requiere un informe policial para disputar artículos fraudulentos. Los casos de robo de identidad conocido o presunto también deben denunciarse ante las autoridades policiales o ante el fiscal general en la jurisdicción de donde usted reside. Este aviso no ha sido demorado por las fuerzas del orden público.

FTC y fiscales generales: usted puede informarse aún más sobre el robo de identidad, las alertas de fraude, los congelamientos de seguridad y los pasos que debe tomar para protegerse contactando a las agencias de informes del consumidor, la Comisión Federal de Comercio o con el fiscal general de su estado. Puede comunicarse con la Comisión Federal de Comercio en: 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 los que descubran que su información se ha utilizado indebidamente a presentar una queja ante ellos. Usted puede obtener más información de cómo presentar dicha queja a través de la información de contacto mencionada anteriormente.