<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <NameSuffix>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Re: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to inform you of a recent event that may affect the security of your personal information. While we are unaware of any actual or attempted misuse of your personal information, out of an abundance of caution, we are providing you with information about the incident, steps we are taking in response, and steps you can take to protect against fraud should you feel it is appropriate.

What Happened? On October 27, 2017, SAY San Diego was notified by the County of San Diego Health & Human Services Agency ("HHSA") that a citizen had returned some paper files to their office that were found in a filing cabinet purchased from a salvage store. The files were reviewed and assessed by our team on October 30, 2017 at which time we confirmed the documents in the files related to participants in SAY San Diego's Dual Diagnosis youth program from January through June 2013. However, the files from March and April of 2013 were not returned, and have not been recovered to date. Upon learning this information, we launched an investigation to determine how the files were found in a filing cabinet at a salvage store. We determined that the files were inadvertently left in a filing cabinet by a SAY San Diego employee when SAY San Diego moved to a different office building.

What Information Was Involved? While we currently have no evidence that the information was subject to misuse, we have confirmed that the files contained the name, case number, dates and length of service, location of service, and provider name. The files did not contain any Social Security numbers, dates of birth, or Driver's License numbers or financial account information.

What We Are Doing. We take the security of client information and privacy very seriously. While we have no evidence information was misused in any way, we want to ensure people that their information remains protected. To help prevent something like this from happening in the future, we have reviewed our current safeguards and procedures and have also established stricter procedures for the handling and inventorying of paper records.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Web Watcher, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **March 26, 2018** to activate your identity monitoring services.*

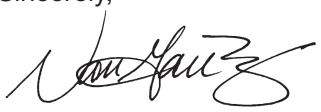
Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

What You Can Do. We encourage you to enroll and receive the Web Watcher services we are offering with Kroll. We also encourage you to take the steps described in the enclosed "Privacy Safeguards" to better protect yourself against the possibility of identity theft and fraud.

For More Information. We are very sorry for any inconvenience or concern this incident causes you. The security of your information is a priority to us. Should you have any questions about the content of this letter or ways you can better protect yourself from the possibility of identity theft, please call 1-833-214-8738 between 9:00 am and 6:00 pm PT, Monday through Friday, excluding major holidays.

Sincerely,



Nancy Gannon Hornberger
President & CEO
SAY San Diego

PRIVACY SAFEGUARDS

We encourage everyone to remain vigilant against incidents of identity theft and financial loss by:

Reviewing account statements, medical bills, and health insurance statements regularly for suspicious activity, to ensure that no one has submitted fraudulent medical claims using your name and address. Report all suspicious or fraudulent charges to your account and insurance providers. If you do not receive regular Explanation of Benefits statements, you can contact your health plan and request them to send such statements following the provision of services.

Ordering and monitoring your credit reports for suspicious activity. Under U.S. law, everyone is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit http://www.annualcreditreport.com/or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
800-680-7289
www.transunion.com

Placing a "fraud alert" on your credit file. A "fraud alert" will tell creditors to take additional steps to verify your identity prior to granting credit in your name; however, because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the credit bureaus verify your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your files. You may use the contact information listed above to contact the major credit bureaus and place a "fraud alert" on your credit report.

Placing a "security freeze" on your credit file, that prohibits a credit reporting agency from releasing any information from your credit report without your written authorization but may delay, interfere with, or prevent the timely approval of any requests for new credit. If you have been a victim of identity theft, and provide the credit reporting agency with a valid police report, the credit reporting agency cannot charge to place, lift or remove a security freeze. In all other cases, a credit agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You must contact each of the credit reporting agencies separately to place a security freeze on your credit file:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
(NY residents please call
1-800-349-9960)
https://www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/
freeze/center.html

TransUnion Fraud Victim Assistance
P.O. Box 2000
Chester, PA 19022
Fraud Division
888-909-8872
http://www.transunion.com/
credit-freeze/place-credit-freeze

Educating yourself further on identity theft, fraud alerts, and the steps one can take to protect against identity theft and fraud by contacting 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.ftc.gov/idtheft/; 1-877-ID-THEFT (1-877-438-4338); and 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. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 3 Rhode Island residents may be impacted by this incident. Instances of known or suspected identity theft should also be reported to law enforcement.

Reporting suspicious activity or incidents of identity theft and fraud to local law enforcement.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.

<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <NameSuffix>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Asunto: Aviso de Violación de Datos

Estimado <<MemberFirstName>> <<MemberLastName>>,

Nos dirigimos a usted para informarle acerca de un evento reciente que pudiese afectar la seguridad de su información personal. Aunque no sabemos si su información personal ha sido usada indebidamente o si existe la intención de hacerlo, deseamos ser suficientemente precavidos e informarle sobre el incidente, así como sobre las medidas que estamos tomando en respuesta al mismo y las medidas que usted pudiese tomar para protegerse contra el fraude, si lo considera conveniente.

¿Qué sucedió? El 27 de octubre de 2017, la Agencia de Salud y Servicios Humanos del Condado de San Diego (San Diego County's Health & Human Services Agency, HHSA) notificó a SAY San Diego que un ciudadano había devuelto algunos archivos en papel a su oficina, los cuales había encontrado dentro de un archivador adquirido en un almacén de artículos de recuperación. El 30 de octubre de 2017, nuestro equipo revisó y evaluó tales archivos y confirmó que los mismos estaban relacionados con los participantes del programa juvenil Dual Diagnosis de SAY San Diego, entre enero y junio de 2013. Sin embargo, los archivos de marzo y abril de 2013 no fueron devueltos y hasta la fecha no han sido recuperados. Una vez conocida esta información, iniciamos una investigación para determinar por qué esos archivos fueron encontrados en un archivador que se vendía en un almacén de artículos de recuperación. Se determinó que los archivos fueron dejados involuntariamente dentro de un archivador por un empleado de SAY San Diego, cuando nos mudamos a otro edificio.

¿De qué información se trataba? Aunque actualmente no tenemos evidencia de que dicha información haya sido usada indebidamente, hemos confirmado que dichos archivos contenían el nombre, el número de caso, las fechas y la duración del servicio, el lugar del servicio y el nombre del proveedor. Los archivos no contenían los números del seguro social, las fechas de nacimiento, los números de las licencias de conducir ni tampoco información financiera de la cuenta.

Lo que estamos haciendo. Nosotros nos tomamos muy seriamente la seguridad de la información y la privacidad del cliente. Aunque no tenemos evidencia de que la información haya sido usada indebidamente de alguna manera, queremos asegurarles a las personas que su información se mantiene protegida. Para ayudar a prevenir que esta situación se repita en el futuro, hemos revisado nuestras protecciones y procedimientos actuales y hemos establecido procedimientos más estrictos para el manejo e inventario de los archivos en papel.

Visite **my.idmonitoringservice.com** para activar y tomar ventaja de su servicio de monitoreo de su identidad.

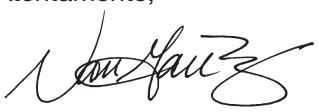
*Usted tiene hasta **March 26, 2018** para activar su servicio de monitoreo de identidad.*

Numero de membresia: **<<Member ID>>**

Lo que usted puede hacer. Le recomendamos que se inscriba y reciba los servicios de Web Watcher que estamos ofreciendo a través de Kroll. Asimismo, recomendamos que siga los pasos descritos en el anexo **"Protecciones de la Privacidad"** para que se proteja mejor contra la posibilidad de un robo de identidad y fraude.

Para obtener más información. Lamentamos cualquier inconveniente o preocupación que este incidente le cause. La seguridad de su información es una prioridad para nosotros. Si tiene alguna pregunta acerca del contenido de esta carta o cómo puede protegerse mejor de la posibilidad de un robo de identidad, llame al 1-833-214-8738 entre 9:00 AM y 6:00 PM, hora del Pacífico, de lunes a viernes, excepto los días feriados.

Atentamente,



Nancy Gannon Hornberger
Presidente y CEO
SAY San Diego

PROTECCIONES DE PRIVACIDAD

Les recomendamos a todas las personas mantenerse alertas contra incidentes de robo de identidad y pérdidas financieras, al realizar lo siguiente:

Revisar regularmente los estados de cuenta, facturas médicas e informes del seguro de salud para detectar cualquier actividad sospechosa, asegurarse de que nadie haya presentado reclamos médicos fraudulentos, usando su nombre y su dirección. Informe cualquier cargo sospechoso o fraudulento a su proveedor de seguros y a su corredor. Si no recibe regularmente un estado de cuenta con la Explicación de sus Beneficios, contacte a su plan de salud y solicite que envíen los estados de cuenta tras la prestación de servicios.

Solicitar y controlar sus informes crediticios para detectar cualquier actividad sospechosa. De acuerdo con la ley en los EE.UU., todos tenemos derecho de recibir un informe crediticio anual y gratuito de cada una de las tres grandes oficinas de crédito. Para solicitar dicho informe crediticio, visite http://www.annualcreditreport.com/o llame sin costo al 1-877-322-8228. También puede contactar directamente a las tres grandes oficinas de crédito para solicitar una copia gratuita de su informe crediticio:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
800-680-7289
www.transunion.com

Colocar un "alerta de fraude" en su expediente de crédito. Un "alerta de fraude" avisará a sus acreedores que tomen medidas adicionales para verificar su identidad antes de otorgar un crédito a su nombre. Sin embargo, dado que el acreedor debe seguir determinados procedimientos para protegerlo, esto puede retrasar su capacidad para obtener un crédito mientras la oficina de crédito verifica su identidad. Tan pronto como una de las oficinas de crédito confirme la alerta de fraude, las otras serán notificadas de colocar la misma alerta en su expediente. Usted también puede usar la información de contacto indicada arriba para solicitar que las grandes oficinas de crédito coloquen el "alerta de fraude" en su informe crediticio.

Colocar un "congelamiento de seguridad" en su expediente crediticio, que prohíba que una agencia de información crediticia divulgue su información sin una autorización escrita. Esto puede demorar, interferir o prevenir la aprobación oportuna de cualquier solicitud de un nuevo crédito. Si usted ha sido víctima de robo de identidad y le provee a la agencia de información crediticia un informe policial válido, la agencia no podrá hacer cobros por colocar, levantar o retirar un congelamiento de seguridad. En todos los otros casos, una agencia de crédito puede hacer cobros por colocar, levantar temporalmente o retirar permanentemente un congelamiento de seguridad. Usted debe contactar separadamente a cada agencia de información crediticia para colocar un congelamiento de seguridad en su expediente de crédito:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
(NY residents please call
1-800-349-9960)
https://www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/
freeze/center.html

TransUnion Fraud Victim Assistance
P.O. Box 2000
Chester, PA 19022
Fraud Division
888-909-8872
http://www.transunion.com/
credit-freeze/place-credit-freeze

Ampliar su conocimiento acerca del robo de identidad, alertas de fraude y las medidas que uno debe tomar para protegerse contra tales delitos, a través de la Comisión Federal de Comercio o el Fiscal General de su estado. La Comisión Federal de Comercio puede contactarse en: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.ftc.gov/idtheft/; 1-877-ID-THEFT (1-877-438-4338); y TTY: 1-866-653-4261. La Comisión Federal de Comercio también exhorta a quienes descubren que su información ha sido usada indebidamente que presenten un reclamo ante ella. **Los residentes de Maryland**, pueden contactar al Fiscal General en: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; y a través de www.oag.state.md.us. **Los residentes de North Carolina**, pueden contactar al Fiscal General por correo en: 9001 Mail Service Center, Raleigh, NC 27699-9001; llamada sin costo al 1-877-566-7226; vía telefónica por el 1-919-716-6400; o a través de www.ncdoj.gov. **Los residentes de Rhode Island**, pueden contactar al Fiscal General por correo en: 150 South Main Street, Providence, RI 02903; por el teléfono (401) 274-4400; o a través de www.riag.ri.gov. Un total de 3 residentes de Rhode Island pudieran ser afectados por este incidente. Las instancias conocidas o sospechosas de robo de identidad también deben reportarse a la policía.

Denunciar cualquier actividad sospechosa o incidentes de robo de identidad y fraude a la policía local.

APROVECHE LOS SERVICIOS DE MONITOREO DE IDENTIDAD

Ahora tiene acceso a los siguientes servicios[1] prestados por la empresa Kroll:

Web Watcher

Web Watcher monitorea sitios de internet donde criminales podrían comprar, vender e intercambiar información de identidad personal. Se emitirá una alerta si se encuentra evidencia de su información de identidad personal.

Consulta de Fraude

Usted contará con acceso ilimitado a asesoramiento con un especialista en fraude de Kroll. Este servicio incluye—indicarle las maneras más eficaces para proteger su identidad; explicarle sus derechos y garantías previstos por la Ley; brindar asistencia con los alertas de fraude; e interpretar la manera de acceder y utilizar los datos personales, incluso la investigación de actividades sospechosas que podrían atribuirse a un evento de robo de identidad.

Recuperación de Robo de Identidad

Si usted es víctima de robo de identidad, un investigador certificado y experimentado de Kroll trabajará por usted para solucionar los problemas relacionados. Será asistido por un investigador especialista que entiende sus problemas y va a hacer la mayor parte del trabajo por usted. El investigador puede ahondar en el caso para descubrir todos los aspectos del robo de identidad y, luego, buscar la forma de resolverlo.

[1] El sitio web de activación de Kroll solo es compatible con la versión actual o una versión anterior de Internet Explorer, Chrome, Firefox y Safari.