LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

February 15, 2019

VIA ELECTRONIC SUBMISSION

Attorney General Xavier Becerra
Office of the Attorney General
California Department of Justice
Attn: Public Inquiry Unit
P.O. Box 944255
Sacramento, CA 94244-2550

Re: Notification of Data Breach

Dear Attorney General Becerra:

We represent AltaMed Health Services Corporation ("AltaMed") in connection with a recent data security incident experienced by Sharecare Health Data Services ("SHDS"), an AltaMed business associate, which is described in greater detail below.

1. Nature of the security incident.

On December 31, 2018, SHDS informed AltaMed that it had experienced a data security incident involving the SHDS network which affected information belonging to certain AltaMed patients. In doing so, SHDS stated that it first detected abnormal activity within the SHDS network on June 22, 2018 and that it ultimately determined that an unauthorized third-party gained access to the SHDS network as early as May 21, 2018. According to SHDS, its investigation relating to this incident revealed that the unauthorized third-party accessed and/or acquired SHDS files containing AltaMed patient information. This information may have included patient names, addresses, dates of birth, and unique identification numbers as well as names and addresses of facilities that provided health services and, in some instances, medical record numbers, and/or internal SHDS processing notes.

2. Number of California residents affected.

AltaMed notified 5,767 California residents regarding this data security incident. Notification letters were mailed via first class U.S. mail on February 15, 2019. A sample copy of the notification letter is included with this letter.

3. Steps taken relating to the incident.

Since receiving notice from SHDS about this incident, AltaMed has worked diligently to learn as much as possible about it and to identify those AltaMed patients whose information may have been

affected for purposes of notification. According to SHDS, SHDS has also taken affirmative steps to respond to this incident and to help prevent similar incidents from occurring in the future.

4. Contact information.

AltaMed is dedicated to protecting the sensitive information that is in its control. If you have any questions or need additional information, please do not hesitate to contact me at (720) 202-2052, or by e-mail at Alyssa.Watzman@lewisbrisbois.com.

Sincerely,

/s/ Alyssa R. Watzman

Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure

AltaMed

QUALITY CARE WITHOUT EXCEPTION™

Processing Center ● P.O. BOX 141578 ● Austin, TX 78714

00001
R904301

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

February 15, 2019

Subject: Notice of Data Breach

Dear John Sample,

At AltaMed Health Services Corporation ("AltaMed"), we take the privacy and security of your personal information very seriously. Therefore, we are writing you to notify you of a recent data security incident experienced by Sharecare Health Data Services ("SHDS"), an AltaMed business associate, which may have involved some of your personal information. This letter serves to inform you of steps you can take to help protect your information and services available to assist you.

What Happened? On December 31, 2018, SHDS informed AltaMed that it had experienced a data security incident involving SHDS's network which, according to SHDS, affected information belonging to certain AltaMed patients. In its letter to AltaMed, SHDS stated that it first detected abnormal activity within its network on June 22, 2018. Upon detecting this activity, SHDS launched an investigation and engaged a forensics firm to support its inquiry. SHDS ultimately determined that an unauthorized third-party gained access to SHDS's network as early as May 21, 2018 and acquired files containing patient information. SHDS also notified the Federal Bureau of Investigation ("FBI") about this incident and will cooperate fully with the FBI's investigation.

This incident was not the result of any action by AltaMed and did not affect the integrity or security of AltaMed's systems. Neither SHDS nor AltaMed are aware of any misuse of information belonging to AltaMed patients that may have been involved in this incident.

Since receiving notice from SHDS, AltaMed has worked diligently to learn as much as possible from SHDS about this incident and to identify those AltaMed patients whose information may have been affected for purposes of notification. According to SHDS, it has also taken measures to respond and to help prevent similar incidents from occurring in the future.

What Information Was Involved? The following information may have been affected: names, addresses, dates of birth, unique customer identification numbers, names and addresses of facilities that provided health services and, in some instances, medical record numbers, and internal SHDS processing notes. There is no evidence that detailed clinical information was impacted in any way.

What Are We Doing? Upon being notified of this incident by SHDS, we took the steps referenced above. We are reporting the incident to the appropriate authorities and are providing you with information about how to protect your personal information.

Additionally, SHDS has arranged to have AllClear ID provide you with twelve (12) months of credit monitoring and identity theft protection services at no cost to you. AllClear ID's services include:

- AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call **1-855-904-5738**, and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

- AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 1-year fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at **enroll.allclearid.com** or by phone by calling **1-855-904-5738** using the following redemption code: **Redemption Code**.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

What You Can Do: We encourage you to enroll and receive the free credit monitoring and identity restoration services SHDS is offering through AllClear ID. Please also review the recommendations for protecting your personal information provided on the following page.

For More Information: If you have any further questions about the incident of the services being offered, please call 1-855-904-5738, Monday through Saturday, 8:00 a.m. – 8:00 p.m. Central Time.

Please accept our sincere apologies for any worry or inconvenience this may cause you.

Sincerely,

Kimberly E. Silverio, CHPC
Office of Compliance and Risk Management, Privacy Officer

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1-855-434-8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 816 Congress Avenue Suite 1800 Austin, Texas 78701	1-855-434-8077

AltaMed

QUALITY CARE WITHOUT EXCEPTION™

Processing Center ● P.O. BOX 141578 ● Austin, TX 78714

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

15 de febrero de 2019

Asunto: Aviso de violación de datos

Estimado/a John Sample,

En AltaMed Health Services Corporation (en adelante, "AltaMed"), tomamos muy en serio la privacidad y seguridad de tu información personal. Por lo tanto, en esta oportunidad, nos comunicamos para informarte que, recientemente, en Sharecare Health Data Services (en adelante, "SHDS"), uno de los socios comerciales de AltaMed, se produjo un incidente relacionado con la seguridad de datos, que podría haber incluido parte de tu información personal. A través de esta carta, queremos informarte acerca de los pasos que puedes tomar para proteger tu información, así como de los servicios que se encuentran disponibles para ayudarte.

¿Qué sucedió? El 31 de diciembre de 2018, SHDS informó a AltaMed acerca de un incidente relacionado con la seguridad de datos que ocurrió en la red de la empresa, el cual, de acuerdo con la misma empresa, involucró información perteneciente a algunos pacientes de AltaMed. En su correspondencia dirigida a AltaMed, SHDS indicó que detectó por primera vez una actividad anormal en su red el 22 de junio de 2018. Tras detectarla, comenzó una investigación y contrató a una empresa forense para que la ayudara en el proceso. Finalmente, SHDS determinó que, desde el 21 de mayo de 2018, un tercero sin autorización tuvo acceso a su red y obtuvo archivos que contenían información de los pacientes. Además, SHDS informó sobre este incidente a la Oficina Federal de Investigaciones de los Estados Unidos (en adelante, "FBI") y cooperará plenamente con la investigación que esta lleve a cabo.

Este incidente no fue provocado por ninguna acción por parte de AltaMed, ni tampoco afectó la integridad ni la seguridad de los sistemas de AltaMed. No se ha puesto al conocimiento de SHDS ni de AltaMed ningún uso indebido de la información de los pacientes de AltaMed que pudieron haber sido víctimas de este incidente.

Desde el momento en que se recibió el aviso por parte de SHDS, en AltaMed se ha trabajado con diligencia para conocer todos los detalles posibles acerca del incidente e identificar a los pacientes de AltaMed que pudieron haber sido afectados con el fin de notificarlos. Según SHDS, también tomaron las medidas correspondientes para responder frente a esta situación y evitar que ocurra un incidente similar en el futuro.

¿Qué tipo de información se vio afectada? Probablemente, la siguiente información haya sido afectada: nombres, domicilios, fechas de nacimiento, números de identificación única de los clientes, nombres y domicilios de los centros que proporcionaron atención médica y, en algunos casos, números del historial médico y notas de procesos internos de SHDS. No hay pruebas que indiquen que se haya vulnerado de ninguna forma información clínica detallada.

¿Qué medidas tomamos? Luego de que SHDS nos informara acerca del incidente, tomamos las medidas que mencionamos anteriormente. Además, estamos informando a las autoridades correspondientes acerca del incidente y estamos brindándote información sobre cómo proteger tu información personal.

Por su parte, SHDS coordinó con AllClear ID para que te proporcionen doce (12) meses de servicios de supervisión de créditos y protección contra el robo de identidad en forma totalmente gratuita. Entre los servicios de AllClear ID, se incluyen los siguientes:

- AllClear Identity Repair: Este servicio está disponible para usted automáticamente y no requiere ningún tipo de inscripción. Si surge un problema, simplemente llame al **1-855-904-5738** y un investigador dedicado le ayudará a recuperar las pérdidas financieras, restaurar su crédito y asegurarse de que su identidad vuelve a su condición apropiada.

- AllClear Fraud Alerts with Credit Monitoring: Este servicio ofrece la posibilidad de definir, renovar y remover alertas de fraude por un año en su archivo crediticio para ayudarlo a protegerse contra el fraude en el crédito. Además, brinda servicios de monitorización del crédito, un puntaje crediticio anual e informe crediticio por año y una póliza de seguro del robo de identidad de $1 millón. Para inscribirse en este servicio, necesitará proveer su información personal a AllClear ID. Puede inscribirse en línea en **enroll.allclearid.com** o por teléfono llamando al **1-855-904-5738** usando el siguiente código de rescate: **Redemption Code**.

Por favor, tome nota: Luego de la inscripción, se requieren pasos adicionales suyos para activar sus alertas telefónicas y alertas de fraude, y obtener su puntaje crediticio y archivo crediticio. Pasos adicionales también podrían requerirse para poder activar sus opciones de monitorización.

Para recibir los servicios de supervisión de créditos, debes tener más de 18 años y contar con un crédito establecido en los Estados Unidos, además, debes tener un número de Seguro Social a tu nombre y un domicilio residencial en los Estados Unidos que esté vinculado a tu historial crediticio.

¿Qué puedes hacer tú? Te recomendamos que te inscribas para recibir en forma gratuita los servicios de AllClearID de supervisión de créditos y recuperación de identidad que te ofrece SHDS. También es importante que revises las recomendaciones con respecto a cómo proteger tu información personal que se detallan en la página siguiente.

¿Dónde puedes obtener más información? Si tienes preguntas sobre el incidente o los servicios ofrecidos o si necesitas ayuda para inscribirte, comunícate con AllClear ID al teléfono 1-855-904-5738 de lunas a sábado entre 8:00 a.m. – 8:00 p.m. tiempo central.

Te pedimos que aceptes nuestras más sinceras disculpas por cualquier tipo de preocupación o inconveniente que haya podido causarte esta situación.

Atentamente,

Kimberly E. Silverio, CHPC
Oficina de Gestión de Riesgos y Cumplimiento Normativo, Responsable de privacidad

MEDIDAS QUE PUEDES TOMAR PARA PROTEGER AÚN MÁS TU INFORMACIÓN

Revisa los estados de tus cuentas bancarias y notifica a las autoridades policiales si adviertes alguna actividad sospechosa: Como medida de precaución, te recomendamos que siempre estés atento y revises en detalle los informes crediticios y estados de tus cuentas bancarias. Si detectas alguna actividad sospechosa en alguna de tus cuentas, informa de inmediato a la empresa o entidad financiera que aloja tu cuenta. También debes informar de inmediato cualquier actividad fraudulenta o presunto robo de identidad a las autoridades policiales correspondientes, al fiscal general del estado o a la Comisión Federal de Comercio (FTC, Federal Trade Commission).

Copia del informe crediticio: Una vez por año, puedes obtener en forma gratuita una copia de tu informe crediticio por parte de cualquiera de las tres principales agencias de informes crediticios; visita http://www.annualcreditreport.com/, llama a través de la línea telefónica gratuita 877-322-8228 o rellena un formulario de solicitud del informe crediticio anual y envíalo por correo a: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. Puedes obtener este formulario ingresando a https://www.annualcreditreport.com/cra/requestformfinal.pdf. También puedes ponerte en contacto con cualquiera de las siguientes tres agencias nacionales de informes crediticios:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Alerta de fraude: Asimismo, puedes colocar una alerta de fraude en tu informe crediticio. La primera alerta de fraude se coloca en forma gratuita y se conserva en tu historial crediticio durante, al menos, 90 días. A través de esta alerta, si se advierte una posible actividad fraudulenta en tu informe, se envía un aviso a los acreedores y se les solicita que te contacten antes de generar cuentas a tu nombre. Si deseas colocar una alerta de fraude para tu informe crediticio, puedes contactar a cualquiera de las tres agencias de informes crediticios que se mencionaron anteriormente. Para obtener más información, visita http://www.annualcreditreport.com.

Congelamiento de crédito: De conformidad con las leyes de los Estados Unidos, tienes derecho a congelar tu historial crediticio hasta un año en forma gratuita. De esta forma, no podrán abrirse cuentas a tu nombre a menos que se utilice el número de PIN que recibes cuando activas el congelamiento. El congelamiento de crédito está diseñado para evitar que los potenciales acreedores accedan a tu historial crediticio sin tu consentimiento. Como consecuencia, es posible que este congelamiento modifique o retrase tu capacidad de obtención de crédito. Para colocar un congelamiento de crédito en tu historial crediticio, debes hacerlo con cada una de las tres agencias de informe crediticio por separado. Es posible que tengas que brindar a las agencias de informes del cliente algún tipo de información que te identifique, incluidos: nombre completo, número de Seguro Social, fecha de nacimiento, domicilio actual y domicilios previos, copia de tu tarjeta de identificación emitida por el estado y una declaración bancaria o del seguro.

Recursos gratuitos adicionales: Para obtener más recomendaciones sobre cómo prevenir el robo de identidad, puedes comunicarte con las agencias de informes del cliente, la FTC o el fiscal general del estado correspondiente. Puedes denunciar un presunto robo de identidad ante los organismos policiales locales, incluidos la FTC o el fiscal general de tu estado. Los habitantes de Maryland, Carolina del Norte y Rhode Island pueden recurrir a sus fiscales generales para obtener más información utilizando los siguientes datos:

Comisión Federal de Comercio	**Fiscal general de Maryland**	**Fiscal general de Carolina del Norte**	**Fiscal general de Rhode Island**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov y	oag.state.md.us	ncdoj.gov	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

Además, gozas de determinados derechos en virtud de la Ley de Informe Imparcial de Crédito (FCRA, Fair Credit Reporting Act), entre los que se incluyen el derecho a conocer todo lo que se encuentra en tu historial, el derecho a disputar cualquier información imprecisa o incompleta y el derecho a que las agencias de informes del cliente corrijan o eliminen todo tipo de información imprecisa, incompleta o incomprobable. Si deseas obtener más información acerca de la FCRA y de los derechos que se estipulan en esta ley, visita http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Términos de uso de reparación de la identidad AllClear

Si usted es víctima del fraude debido al uso de su información personal sin autorización, AllClear ID ayudará a recuperar sus pérdidas financieras y restaurar su identidad. Los beneficios incluyen:

- 12 meses de cobertura sin requisito de inscripción.
- Sin costo alguno para usted, nunca. La compañía participante paga por reparación de la identidad AllClear.

Servicios provistos
Si usted sospecha el robo de su identidad, simplemente llame a AllClear ID para presentar una reclamación. AllClear ID proveerá los servicios necesarios y apropiados de resolución ("Servicios") para ayudar a restaurar sus cuentas comprometidas y su identidad según el estado previo al incidente de fraude. Los servicios son determinados a entera discreción de AllClear ID y están sujetos a los términos y condiciones que se indican en el sitio Web de AllClear ID. Reparación de la identidad AllClear no es una póliza de seguros y AllClear ID no realizará pagos ni reembolsos por pérdidas financieras, obligaciones o gastos que usted incurra.

Período de cobertura
El servicio está automáticamente disponible para usted sin requisito de inscripción durante 12 meses desde la fecha de la notificación del incidente que recibió de la Compañía (el "Período de cobertura"). Los eventos de fraude que ocurrieron antes de su Período de cobertura no están cubiertos por los servicios de reparación de la identidad AllClear.

Requisitos de participación
Para cumplir los requisitos de los Servicios bajo la cobertura de reparación de la identidad AllClear, debe cumplir totalmente, sin limitaciones, con sus obligaciones según los términos de la presente, debe ser un ciudadano o residente legal, tener (18) años de edad o más y tener un número válido del Seguro Social de EE.UU. Las personas menores de dieciocho (18) años podrían cumplir los requisitos pero deben ser patrocinados por un padre o tutor. Los Servicios solamente lo cubren a usted y a sus cuentas personales médicas y financieras que estén directamente asociadas con su número válido del Seguro Social, incluyendo pero sin limitación a cuentas de tarjetas de crédito, bancarias u otras cuentas financieras y/o cuentas médicas.

Cómo presentar una reclamación
Si usted es víctima de un fraude cubierto por los servicios de reparación de la identidad AllClear (un "Evento"), debe:

- notificar a AllClear ID llamando al 1-855-434-8077 para reportar el fraude antes del vencimiento de su Período de cobertura;
- presentar una prueba de elegibilidad de reparación de la identidad AllClear al proveer el código de rescate de la carta de notificación que recibió de la Compañía patrocinadora;
- cooperar total y verazmente con AllClear ID sobre el Evento y aceptar presentar cualquier documento que AllClear ID pudiera razonablemente requerir; y
- cooperar totalmente con AllClear ID en cualquier proceso de resolución, que incluye pero no se limita a, presentar a AllClear ID copias de todos los informes o archivos de la investigación disponible de cualquier institución, que incluye pero no se limita a, instituciones crediticias o departamentos de policía, relacionados con el supuesto robo.

La cobertura bajo reparación de la identidad AllClear no se aplica a lo siguiente:
Cualquier gasto, daño o pérdida:

- debido a
  - cualquier transacción en sus cuentas financieras hechas por usuarios autorizados, incluso si actúan sin su conocimiento, o
  - cualquier acto de robo, engaño, confabulación, deshonestidad o criminal suyo o de cualquier persona que actúa junto con usted o por cualquiera de sus representantes autorizados, actúen por cuenta propia o conjuntamente con usted u otros (conjuntamente, su "Falsificación");
- incurrido por usted de un Evento que no ocurrió durante el período de cobertura; o
- relacionado con un Evento que usted no reporta a AllClear ID antes del vencimiento del período de cobertura de reparación de la identidad AllClear.

Otras exclusiones:

- AllClear ID no pagará ni tendrá ninguna obligación ante ninguno de los costos o gastos excepto los que se describen en la presente, incluyendo pero sin limitación, honorarios de proveedores de servicios no contratados por AllClear ID; AllClear ID se reserva el derecho a investigar cualquier reclamación presentada para determinar su validez.
- AllClear ID no es una compañía de seguros y reparación de la identidad AllClear no es una póliza de seguro; AllClear ID no realizará pagos ni reembolsos a usted por cualquier pérdida u obligación que pudiera incurrir.
- AllClear ID no es una organización de reparación del crédito, no es un servicio de asesoramiento crediticio y no promete ayudarle a mejorar su historia crediticia o calificación por encima de la resolución de incidentes de fraude.
- AllClear ID se reserva el derecho a investigar razonablemente cualquier demanda presentada para determinar su validez. Se espera que todos los beneficiarios de la cobertura de reparación de la identidad AllClear protejan su información personal de manera razonable en todo momento. Por lo tanto, los beneficiarios no divulgarán ni publicarán deliberadamente o de manera inapropiada su número del Seguro Social o cualquier otra información personal a quienes se pudiera esperar que usen de manera inadecuada o divulguen dicha Información personal.

Política de rechazo
Si por cualquier razón usted desea que su información sea eliminada de la base de datos de elegibilidad de reparación de la identidad AllClear, por favor, comuníquese con AllClear ID:

Correo electrónico	Correo	Teléfono
support@allclearid.com	AllClear ID, Inc. 816 Congress Avenue Suite 1800 Austin, Texas 78701	1-855-434-8077