Helping Our Neighbors Manage Hardship, Make Connections & Move Forward.

EMERGENCY ASSISTANCE • LANGUAGE ACCESS • LATINO SERVICES • COMMUNITY EDUCATION

Recientemente una computadora fue robada de nuestras oficinas. Esta computadora puede haber tenido cierta información personal almacenada. No sabemos por qué se produjo el robo de la computadora y no tenemos razones para creer que la computadora haya sido robada con el objetivo de tener acceso a información personal. El documento adjunto le ayudará a entender mejor lo que pasó y cómo protegerse de cualquier daño que resulte del robo de la computadora. Si su información de tarjeta de crédito u otra relacionada con la cuenta bancaria se perdieran, podría ser necesario compartir esta información con su banco o institución financiera para que así le puedan ayudar a determinar la mejor forma de protegerse de cualquier fraude financiero.

Si después de que leer el documento adjunto tiene dudas o requiere información adicional, por favor, comuníquese con nosotros a este número telefónico de forma gratuita: 866-426-7163.

Atentamente,

Sharel Love
Director ejecutivo
One22

Documento adjunto: Información adicional sobre robo de computadora desde One22

Información adicional sobre robo de computadora desde One22

¿Qué pasó y qué estamos haciendo al respecto?
El 13 de agosto 2017, una computadora fue robada desde las oficinas de One22 en Jackson, Wyoming. Informamos inmediatamente el robo a la policía local y contratamos a expertos en tecnología para determinar qué información personal, si existiere, se almacenó en la computadora robada. One22 no tiene razones para creer que la computadora haya sido robada para obtener información personal, y es posible que el ladrón no haya obtenido su información personal de la computadora robada. Sin embargo, no podemos excluir la posibilidad que su información se haya visto afectada. Aunque la investigación se encuentra en curso, quisimos comunicarnos con usted para entregarle esta información y para así poder tomar las medidas necesarias para protegerse de ahora en adelante.

¿Qué información pudiera haberse visto potencialmente afectada?
Según nuestra información, es posible que la computadora robada contenía algunas o todas de la siguiente información: nombres, números de la tarjeta de crédito, números de seguro social, números de teléfono, fechas de nacimiento, números de Medicaid, y números de cuenta bancaria. Enviamos cartas con detalles a las personas afectadas para quienes teníamos una dirección postal. Por favor, contáctanos para saber si fuiste afectado y qué información se vio comprometida.

Le recomendamos estar atento, examinando sus estados de cuenta y sus informes de crédito, especialmente si su número de seguro social se puede haber puesto en peligro en el robo. Si su número de cuenta bancaria o número de la tarjeta de crédito se vieron afectados, por favor considere informar esta filtración de datos a su banco para que se tomen las medidas necesarias para proteger sus cuentas del acceso no autorizado. Si descubre alguna actividad sospechosa o extraña en sus cuentas, asegúrese de informar inmediatamente a sus instituciones financieras, ya que las principales compañías de tarjetas de crédito tienen normas que las limitan al exigirle que pague gastos fraudulentos informados inmediatamente.

Para aprender más sobre cómo protegerse contra el robo de identidad, por favor, visite los sitios web de protección de robo de identidad de la Comisión Federal de Comercio (FTC) en https://www.robodeidentidad.gov/(español) o https://www.identitytheft.gov/(inglés) o comuníquese con la FTC por teléfono al (877) 438-4338.

Si descubre que su información se ha empleado indebidamente, la FTC le recomienda presentar una queja ante la FTC y tomar estas medidas adicionales: (1) cerrar cualquier cuenta que crea se manipuló o se abrió fraudulentamente; y (2) presente y guarde una copia de un informe de la policía local como prueba.

Obtenga su informe de crédito
También debería considerar la revisión de sus informes de crédito. Puede obtener periódicamente informes de crédito de cada oficina de información de crédito a nivel nacional. Si descubre información inexacta o una cuenta fraudulenta en su informe de crédito, tiene derecho a solicitar que la oficina de información de crédito elimine esa información de su archivo de informe de crédito.

Además, según la ley federal, tiene derecho a una copia gratuita de su informe de crédito cada 12 meses de cada una de las tres oficinas de información del crédito de escala nacional. Puede obtener una copia gratuita de su informe de crédito en www.AnnualCreditReport.com o llamando al (877) 322-8228. También puede completar el Formulario de solicitud de Informe de crédito Anual disponible de la FTC en https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf y enviarlo al Servicio de Solicitud del Informe de Crédito Anual, Apartado Postal 105281, Atlanta, Georgia 30348-5281. También se puede comunicar con cualquiera de las tres oficinas principales de información de crédito para solicitar una copia de su informe.

Envíe una alarma de fraude o congelamiento de seguridad en su archivo de informe de crédito
También puede considerar ponerse en contacto con las oficinas de información de crédito sobre alarmas de fraude y congelamientos de seguridad. Una alarma de fraude puede dificultar aún más que una persona obtenga crédito a su nombre, ya que le indica a los acreedores seguir ciertos procedimientos para protegerle, aunque también puede retrasar su capacidad de obtener crédito. Si sospecha que puede ser víctima de robo de identidad, puede enviar una alarma de fraude en su archivo llamando sólo a una de las tres oficinas de información de crédito de escala nacional que se detallan a continuación. Tan pronto como esa agencia procesa su alarma de fraude, notificará a las otras dos agencias, que entonces también deben colocar alarmas de fraude en su archivo. Una alarma de fraude inicial durará 90 días. Una alarma ampliada permanece en su archivo durante siete años. Para enviar cualquiera de estas alarmas, la oficina de información del consumidor requerirá que entregue prueba adecuada de identidad, que puede incluir su número

de seguro social. Si solicita una alarma ampliada, tendrá que proporcionar un informe de robo de identidad.

Además, se puede comunicar con las oficinas de información de crédito a nivel nacional en cuanto a si y cómo puede colocar un congelamiento de seguridad en su informe de crédito. Un congelamiento de seguridad le prohíbe a una oficina de información de crédito entregar la información de su informe de crédito sin su autorización previa por escrito, lo que hace más difícil para partes no autorizadas abrir nuevas cuentas a su nombre. Sin embargo, por favor tenga en cuenta que el establecer un congelamiento en su informe de crédito puede retrasar, interferir con o prevenir la aprobación oportuna de cualquier solicitud que haga para nuevos préstamos, créditos hipotecarios, empleo, alojamiento u otros servicios. Las oficinas de información de crédito tienen tres días hábiles después de recibir una solicitud congelamiento de seguridad en el informe de crédito de un consumidor. Se le puede cobrar por colocar o levantar un congelamiento de seguridad. A diferencia de una alarma de fraude, debe enviar por separada la solicitud de congelamiento de crédito en su archivo de crédito a cada compañía de informe de crédito.

Se puede comunicar con las oficinas de información de crédito a nivel nacional en:

Equifax
Apartado postal 105788
Atlanta, Georgia 30348
(800) 525-6285
www.equifax.com

Experian
Apartado postal 9554
Allen, Texas 75013
(888) 397-3742
www.experian.com

TransUnion
Apartado postal 2000
Chester, Pensilvania 19016
(800) 680-7289

www.transunion.com

Si tiene dudas o necesita la información adicional para comunicarse con las tres oficinas de información de crédito a nivel nacional, por favor póngase en contacto con nosotros a este número telefónico de forma gratuita: 866-426-7163.

Helping Our Neighbors Manage Hardship, Make Connections & Move Forward.

EMERGENCY ASSISTANCE • LANGUAGE ACCESS • LATINO SERVICES • COMMUNITY EDUCATION

A computer was recently stolen from our offices. This computer may have had certain personal information stored on it. We do not know why the computer was stolen and we have no reason to believe that the computer was stolen for purpose of accessing personal information. The attachment to this notification will help you better understand what happened and how you may wish to protect yourself from any harm resulting from the theft of the computer. If your credit card information or other bank account information was lost, you may wish to share this information with your bank or financial institution so they can help you determine the best way to protect you from any financial fraud.

If, after you read the attachment to this notification, you have questions or need additional information, please contact us at this toll-free number: 866-426-7163.

Sincerely yours,

Sharel Love
Executive Director
One22
Attachment: Additional Information About Computer Theft from One22

Additional Information About Computer Theft from One22

What happened and what we are doing about it?
On August 13, 2017, a computer was stolen from One22's offices in Jackson, WY. We promptly reported the theft to local law enforcement and hired technology experts to determine what personal information, if any, was stored on the stolen computer. One22 has no reason to believe that the computer was stolen to obtain personal information, and it is possible that the thief has not retrieved your personal information from the stolen computer. However, we cannot rule out the possibility that your information was compromised. Although the local law enforcement investigation is ongoing, we wanted to contact you to provide this information to allow you to take steps to protect yourself now.

What information was potentially compromised?
According to our information, the stolen computer may have contained some or all of following information: names, dates of birth, social security numbers, telephone numbers, credit card numbers, bank account numbers, and Medicaid numbers. We sent letters with specifics to affected persons for whom we had a mailing address. Please feel free to contact us to learn if you were affected and what information was compromised.

We encourage you to remain vigilant by reviewing your account statements and monitoring your credit reports, particularly if your social security number may have been compromised in the theft. If your bank account number or credit card number was compromised, please consider reporting this data breach to your bank to allow them to take steps to protect your accounts from unauthorized access. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are promptly reported.
To learn more about how to protect yourself against identity theft, please visit the Federal Trade Commission (FTC) identity theft protection websites at https://www.robodeidentidad.gov/ (Español) or https://www.identitytheft.gov/ (English) or contact the FTC by telephone at (877) 438-4338.

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close any accounts that you believe were tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence.

Obtain Your Credit Report

You should also consider monitoring your credit reports. You may periodically obtain credit reports from each nationwide credit reporting agency. If you discover inaccurate information or a fraudulent account on your credit report, you have the right to request that the credit reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major credit reporting agencies to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit Report File

You may also wish to consider contacting the credit reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. The credit reporting agencies have three business days after receiving a request to place a security freeze on a consumer's credit report.

You may be charged to place or lift a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide credit reporting agencies at:

Equifax
P.O. Box 105788
Atlanta, GA 30348
(800) 525-6285
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(800) 680-7289
www.transunion.com

If you have any further questions or need additional information to contact the three nationwide credit reporting agencies, please contact us at this toll-free number: 866-426-7163.