harder + co | community research
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-608-2377
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [XXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

January 12, 2022

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We are writing to notify you of a recent data security incident experienced at our firm, Harder+Company Community Research, and which may have affected your personal information. Please read this letter carefully.

Who We Are

Harder+Company Community Research is a California-based research, evaluation, and planning firm that works within the social sector. We work with nonprofit, philanthropic, and government clients—providing them with the information and tools they need to do their work effectively. We conduct program and organizational evaluations and studies across many areas including health, education, and community services.

What Happened

We recently learned that an unauthorized user gained access to some of our firm's business email accounts that contained messages with some of our clients' information. We worked diligently with a specialized computer forensics firm to investigate the matter and determined that this unauthorized access occurred between April 17, 2021 and August 12, 2021, without our knowledge. While we cannot confirm with certainty all information that was accessed by the unauthorized user during that time, we conducted a detailed review of all messages in the affected email accounts to identify information that may have been affected. That review process required a lot of time and effort, but we wanted to be thorough and make sure we did it right. We completed our review on December 3, 2021, and then promptly began notifying all potentially affected individuals that we identified through our process.

What Information Was Involved

You are receiving this message because our investigation and review process found that your personal information was contained in one or more emails in the accounts that were affected by this incident. We want to emphasize that, at this time, we have no evidence that your information has been misused in any way. However, we are providing you with this notice out of an abundance of caution. In that regard, we believe there may have been unauthorized access to emails in the affected accounts that contained your personal information. Information that may have been accessed could include any combination of the following: your full name, address, date of birth, Social Security Number, driver's license number, health insurance information, and/or medical treatment information.

What We Are Doing

Please know that we take the protection of our clients' personal information seriously and we are taking steps to continue investigating this incident, help mitigate the potential for harm, and prevent future incidents from happening. At this time,

we have not found the person behind the unauthorized access or determined his or her motives, but we have notified law enforcement and will continue cooperating with their investigations. Out of an abundance of caution, we also have changed all passwords used to access our email system and computer network. We also are reviewing our policies and procedures to identify any additional ways to further strengthen the confidentiality and security of our clients' information.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: [12 months/24 months] of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

In light of this incident, we recommend that you remain vigilant by reviewing and monitoring your account statements and credit reports. If you find any errors or unauthorized activity, you should contact your financial institution or call the number on the back of your payment card. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. In addition, please refer to the enclosed documentation which contains additional steps you may take to protect your information from misuse, including some information that may be specific to your state of residence.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-608-2377 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is April 12, 2022.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

We very sorry for any concern or inconvenience this incident has caused or may cause you. You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-608-2377 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Harder+Company Community Research

(Enclosure)

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-608-2377 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: 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 a violator. 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

harder + co | community research
P.O. Box 1907
Suwanee, GA 30024

Para inscribirse, llame al:
1-833-608-2377
O visite:
https://app.idx.us/account-creation/protect
Código de inscripción:
[XXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

1/12/2022

Aviso de violación de datos

Estimado/a <<Nombre>> <<Apellido>>:

Le escribimos para notificarle sobre un incidente reciente de seguridad de datos experimentado en nuestra firma, Harder + Company Community Research, y que puede haber afectado su información personal. Lea esta carta atentamente.

Quiénes somos

Harder+Company Community Research es una empresa de investigación, evaluación y planificación con sede en California que trabaja dentro del sector social. Trabajamos con clientes gubernamentales, filantrópicos y sin fines de lucro, y les proporcionamos la información y las herramientas que necesitan para hacer su trabajo de manera eficaz. Realizamos evaluaciones y estudios de programas y organizaciones en muchas áreas, que incluyen la salud, la educación y los servicios comunitarios.

¿Qué ocurrió?

Recientemente nos enteramos de que un usuario no autorizado obtuvo acceso a algunas de las cuentas de correo electrónico comerciales de nuestra empresa que contenían mensajes con parte de la información de nuestros clientes. Trabajamos diligentemente con una firma especializada en informática forense para investigar el asunto, y determinamos que este acceso no autorizado ocurrió entre el 17 de abril de 2021 y el 12 de agosto de 2021, sin nuestro conocimiento. Si bien no podemos confirmar con certeza toda la información a la que accedió el usuario no autorizado durante ese tiempo, realizamos una revisión detallada de todos los mensajes en las cuentas de correo electrónico afectadas para identificar la información que puede haber sido afectada. Ese proceso de revisión requirió mucho tiempo y esfuerzo, pero queríamos ser minuciosos y asegurarnos de hacerlo bien. Completamos nuestra revisión el 3 de diciembre de 2021 y, luego, comenzamos a notificar de inmediato a todas las personas potencialmente afectadas que identificamos a través de nuestro proceso.

¿Qué información se vio involucrada?

Usted recibió este mensaje porque nuestro proceso de investigación y revisión determinó que su información personal estaba incluida en uno o más correos electrónicos en las cuentas que se vieron afectadas por este incidente. Queremos enfatizar que, en este momento, no tenemos evidencia de que su información haya sido utilizada incorrectamente de alguna manera. Sin embargo, le proporcionamos este aviso por precaución. En ese sentido, creemos que puede haber habido acceso no autorizado a correos electrónicos en las cuentas afectadas que contenían su información personal. La información a la que se pudo haber accedido podría incluir cualquier combinación de lo siguiente: su nombre completo, dirección, fecha de nacimiento, número de seguro social, número de licencia de conducir, información de seguro médico o información de tratamiento médico.

¿Qué medidas estamos tomando?

Tenga en cuenta que nos tomamos muy en serio la protección de la información personal de nuestros clientes, y estamos tomando medidas para continuar investigando este incidente, para ayudar a mitigar posibles daños y para evitar que ocurran

incidentes futuros. En este momento, no hemos encontrado a la persona detrás del acceso no autorizado ni hemos determinado sus motivos, pero hemos notificado a la policía y continuaremos cooperando con sus investigaciones. Por precaución, también hemos cambiado todas las contraseñas utilizadas para acceder a nuestro sistema de correo electrónico y a la red informática. También estamos revisando nuestras políticas y procedimientos para identificar formas adicionales de fortalecer aún más la confidencialidad y seguridad de la información de nuestros clientes.

Además, ofrecemos servicios de protección contra robo de identidad a través de IDX, el experto en servicios de violación y recuperación de datos. Los servicios de protección de identidad de IDX incluyen: [12 meses/24 meses] de supervisión de crédito y CyberScan, una política de reembolso de $1 000 000 en concepto de seguro y servicios de recuperación de robo de identidad completamente administrados. Con esta protección, IDX lo ayudará a resolver problemas si su identidad está comprometida.

¿Qué puede hacer usted?

A la luz de este incidente, le recomendamos que permanezca alerta, y que revise y supervise sus estados de cuenta e informes de crédito. Si encuentra algún error o actividad no autorizada, debe comunicarse con su institución financiera o llamar al número que figura en el reverso de su tarjeta de pago. También puede presentar un informe ante la policía, el fiscal general de su estado o la Comisión Federal de Comercio. Además, consulte la documentación adjunta que contiene pasos adicionales que usted puede tomar para proteger su información del uso indebido, lo que incluye algún tipo de información que puede ser específica de su estado de residencia.

Le recomendamos que se ponga en contacto con IDX ante cualquier duda y que se inscriba en los servicios gratuitos de protección de identidad llamando al 1-833-608-2377 o visitando el sitio web https://app.idx.us/account-creation/protect y utilizando el Código de inscripción proporcionado anteriormente. Los representantes de IDX están disponibles de lunes a viernes, de 6 a. m. a 6 p. m., Hora del Pacífico. Tenga en cuenta que la fecha límite para inscribirse es el 4/12/2022.

Le reiteramos que, en este momento, no hay evidencia de que su información haya sido utilizada indebidamente. Sin embargo, lo alentamos a aprovechar al máximo esta oferta de servicios. Los representantes de IDX han sido plenamente informados sobre el incidente, y pueden responder preguntas o inquietudes que usted pueda tener con respecto a la protección de su información personal.

Más información

Lamentamos mucho cualquier inquietud o inconveniente que este incidente pudo haberle causado. Encontrará instrucciones detalladas para la inscripción en el documento adjunto Recommended Steps (Pasos recomendados). Además, deberá hacer referencia al código de inscripción en la parte superior de esta carta cuando llame o se inscriba en línea, por lo que no debe tirar esta carta.

Llame al 1-833-608-2377 o visite https://app.idx.us/account-creation/protect para obtener asistencia o para hacer cualquier otra pregunta que pueda tener.

Atentamente.

Harder+Company Community Research

(Adjunto)

Pasos recomendados para ayudar a proteger su información

1. **Sitio web e inscripción.** Ingrese en https://app.idx.us/account-creation/protect y siga las instrucciones para inscribirse con el código de inscripción proporcionado en la parte superior de esta carta.

2. Active el servicio de supervisión de crédito proporcionado como parte de su membresía de protección de identidad IDX. El servicio de supervisión incluido en la membresía debe activarse para que entre en vigencia. Nota: Para usar este servicio, deberá tener crédito establecido y acceso a una computadora con Internet. Si necesita ayuda, IDX podrá brindarle asistencia.

3. Teléfono. Comuníquese con IDX al 1-833-608-2377 para obtener información adicional sobre este evento y para hablar con representantes informados sobre las medidas apropiadas a seguir para proteger su identidad crediticia.

4. Supervise sus informes de crédito. Le recomendamos que se mantenga alerta revisando los estados de cuenta y supervisando los informes de crédito. Conforme a la ley federal, usted también tiene derecho a obtener una copia gratuita de su informe crediticio en forma anual de cada una de las tres principales agencias de informes de crédito. Para obtener un informe crediticio anual gratuito, visite el sitio web www.annualcreditreport.com o llame al 1-877-322-8228. Es posible que desee hacer solicitudes en forma escalonada, a fin recibir un informe gratuito por parte de una de las tres agencias de crédito cada cuatro meses.

Si descubre algún elemento sospechoso y se ha inscrito en el servicio de protección de identidad IDX, notifíquelo de inmediato llamando o iniciando sesión en el sitio web de MyIDCare y presentando una solicitud de ayuda.

Si presenta una solicitud de ayuda o informa actividades sospechosas, un miembro de nuestro equipo de ID Care lo contactará y lo ayudará a determinar la causa de los elementos sospechosos. En el caso improbable de que sea víctima de un robo de identidad como consecuencia de este incidente, se le asignará un Especialista de ID Care que trabajará en su nombre para identificar, detener y revertir el daño rápidamente.

También debe saber que usted tiene derecho a presentar un informe policial si alguna vez experimenta un robo de identidad o fraude. Tenga en cuenta que, para presentar un informe de delito o incidente ante las autoridades policiales por robo de identidad, es probable que deba proporcionar algún tipo de prueba de que ha sido víctima de dicho evento. A menudo se requiere un informe policial para disputar elementos fraudulentos. Puede informar cualquier presunto incidente de robo de identidad a la policía local o al Fiscal General.

5. Coloque alertas de fraude en las tres agencias de crédito. Si elige colocar una alerta de fraude, le recomendamos que haga esto luego de activar su servicio de supervisión de crédito. Puede enviar una alerta de fraude a una de las tres agencias principales de crédito por teléfono y también a través del sitio web de Experian o Equifax. Una alerta de fraude les informa a los acreedores que sigan ciertos procedimientos, incluido el contacto con usted, antes de abrir cuentas nuevas o cambiar sus cuentas existentes. Por ese motivo, colocar una alerta de fraude puede protegerlo, pero también puede causar demoras cuando desee obtener crédito. La información de contacto de las tres agencias es la siguiente:

Agencias de crédito

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

Es necesario contactar solo a UNA de estas agencias y usar solo UNO de estos métodos. Tan pronto como una de las tres agencias confirma su alerta de fraude, se notifica al resto de las agencias para que estas coloquen alertas de fraude en su

archivo. Recibirá cartas de confirmación por correo y, luego, podrá solicitar los tres informes de crédito sin cargo para su revisión. Una alerta de fraude inicial durará un año.

Tenga en cuenta lo siguiente: Nadie puede colocar una alerta de fraude en su informe de crédito, excepto usted.

6. Congelamiento de seguridad. Al aplicar un congelamiento de seguridad, cualquier persona que adquiera de manera fraudulenta su información de identificación personal no podrá usar dicha información para abrir nuevas cuentas ni para pedir dinero prestado a su nombre. Deberá ponerse en contacto con las tres agencias nacionales de informes de crédito mencionadas más arriba para aplicar el congelamiento. Tenga en cuenta que, cuando aplique el congelamiento, no podrá pedir dinero prestado, obtener crédito instantáneo ni obtener una nueva tarjeta de crédito hasta que levante temporalmente o elimine en forma permanente el congelamiento. Puede congelar o descongelar sus archivos de crédito sin costo alguno.

7. Usted puede obtener información adicional sobre los pasos que puede seguir para evitar el robo de identidad de las siguientes agencias. La Comisión Federal de Comercio también anima a que aquellos que descubren que su información ha sido utilizada indebidamente presenten una queja ante dicha institución.

Residentes de California: Visite la Oficina de Protección de la Privacidad de California (www.oag.ca.gov/privacy) para obtener información adicional sobre la protección contra el robo de identidad.

Residentes de Kentucky: Oficina del Fiscal General de Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Teléfono: 1-502-696-5300.

Residentes de Maryland: Oficina del Fiscal General de Maryland**,** División de Protección al Consumidor 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Teléfono: 1-888-743-0023.

Residentes de Nuevo México: Conforme a la Ley de Informe Imparcial de Crédito (*Fair Credit Reporting Act*), usted tiene ciertos derechos, tales como el derecho a que se le notifique si la información en su archivo de crédito ha sido utilizada en su contra, el derecho a saber qué hay en dicho archivo, el derecho a solicitar su puntaje de crédito, y el derecho a disputar información incompleta o inexacta. Además, conforme a la Ley de Informe Imparcial de Crédito: las agencias de informes de crédito deben corregir o eliminar la información inexacta, incompleta o no verificable; dichas agencias no pueden reportar información negativa desactualizada; el acceso a su archivo es limitado; usted debe dar su consentimiento para que se proporcionen informes de crédito a los empleadores; usted puede limitar las ofertas de crédito y seguro "preseleccionadas" que recibe según la información de su informe crediticio; y puede reclamar daños y perjuicios de un infractor. También podría tener otros derechos conforme a la Ley de Informe Imparcial de Crédito que no están resumidos en este documento. Las víctimas de robo de identidad y el personal militar en servicio activo tienen derechos adicionales específicos de conformidad con la ley mencionada anteriormente. Puede revisar sus derechos de conformidad con la Ley de Informe Imparcial de Crédito, visitando www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, o bien; escribiendo un correo a Centro de Respuesta al Consumidor, Sala 130-A, Comisión Federal de Comercio, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Residentes de Nueva York: puede comunicarse con el Fiscal General en: Oficina del Fiscal General, El Capitolio, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

Residentes de Carolina del Norte: Oficina del Fiscal General de Carolina del Norte**,** 9001 Centro de servicio de correo Raleigh, NC 27699-9001, www.ncdoj.gov, Teléfono: 1-919-716-6400.

Residentes de Oregón: Departamento de Justicia de Oregón, 1162 Court Street NE, Salem, O 97301-4096, www.doj.state.or.us/, Teléfono: 877-877-9392

Residentes de Rhode Island: Oficina del Fiscal General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Teléfono: 401-274-4400

Todos los residentes de los Estados Unidos: Centro de Información de Robo de Identidad, Comisión Federal de Comercio, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.