24520

ONE COMMUNITY HEALTH

CARING FOR ALL, CARING WITH HEART

[redacted]

[redacted]

[redacted]

Dear [redacted]:

We are writing to inform you of a ransomware cyber-attack that happened between April 19 and April 20, 2021, and the results of our investigation.

On April 20, 2021, our information systems partner found abnormal activity in our network. As part of our investigation, we worked very closely with cybersecurity professionals to quickly isolate the affected systems and identify the nature of the attack. Based on our comprehensive investigation and document review, which concluded on October 6, 2021, we discovered that your Social Security number and one or more of the following resided on our network during this incident: full name, date of birth, address and other demographic information, insurance information, diagnosis information, and/or treatment information. **We do not at this time have any evidence that your information was accessed or taken from our network.**

We have no reports of identity fraud arising out of this incident. Nevertheless, out of an abundance of caution, we are offering a free, two-year membership to Experian IdentityWorks℠ Credit 3B. This is an identity theft program that helps find and fix any potential misuse of your personal information or identity theft. IdentityWorks Credit 3B is completely free to you and using this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, instructions on how to start a free two-year membership, and other useful tips, please see the additional information provided in this letter.

Please accept our apologies that this attack happened. As a result of this attack, we have partnered with cybersecurity experts to significantly increase our cybersecurity defenses to better protect our patients, our staff, and the services we provide our community. This includes: improved endpoint detection, 24x7 managed detection and response, and email and attachment security enhancements, in addition to other cybersecurity improvements.

If you have any further questions regarding the cyber-attack, please call us at [redacted].

Sincerely,

One Community Health

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary 24-Month Credit Monitoring.**

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the Experian IdentityWorks website to enroll: [redacted]
3. PROVIDE the Activation Code: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted]. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and TransUnion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at [redacted]
or call [redacted] to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [redacted].

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 24-month credit monitoring services, we recommend that you place an initial one (1) year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion LLC
P.O. Box 6790
Fullerton, PA 92834-6790
https://www.transunion.com/fraud-alerts
(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(800) 349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

6. Protecting Your Medical Information.

The following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with the insurance company or the care provider for any items you do not recognize.

ONE COMMUNITY HEALTH

CARING FOR ALL, CARING WITH HEART

[redacted]

[redacted]

[redacted]

Estimado [redacted]:

Le escribimos para informarle sobre un ataque cibernético de ransomware que ocurrió entre el 19 y el 20 de abril de 2021, y los resultados de nuestra investigación.

El 20 de abril de 2021, nuestro socio de sistemas de información encontró actividad anormal en nuestra red. Como parte de nuestra investigación, trabajamos en estrecha colaboración con profesionales de ciberseguridad para aislar rápidamente los sistemas afectados e identificar la naturaleza del ataque. En función de nuestra investigación integral y revisión de documentos, que concluyó el 6 de octubre de 2021, descubrimos que su número de Seguro Social y uno o varios de los siguientes datos residían en nuestra red durante este incidente: nombre completo, fecha de nacimiento, dirección y otra información demográfica, información del seguro, información de diagnóstico y/o información del tratamiento. **En este momento, no tenemos ninguna evidencia de que se haya accedido a su información o que esta haya sido obtenida de nuestra red.**

No tenemos informes de fraude de identidad que surjan de este incidente. Sin embargo, como medida de precaución, ofrecemos una membresía gratuita por dos años a Experian IdentityWorks℠ Credit 3B. Este es un programa contra el robo de identidad que ayuda a encontrar y solucionar cualquier posible uso indebido de su información personal o robo de identidad. IdentityWorks Credit 3B es completamente gratuito para usted y el uso de este programa no dañará su calificación crediticia. Para obtener más información sobre cómo prevenir el robo de identidad y sobre IdentityWorks Credit 3B, y para obtener instrucciones sobre cómo iniciar una membresía de dos años de cortesía, consulte la información adicional proporcionada en esta carta.

Acepte nuestras disculpas por este ataque. Como resultado de este ataque, nos hemos asociado con expertos en seguridad cibernética para aumentar significativamente nuestras defensas de seguridad cibernética para proteger mejor a nuestros pacientes, a nuestro personal y a los servicios que brindamos a nuestra comunidad. Esto incluye: detección mejorada de terminales, detección y respuesta gestionadas las 24 horas del día, los 7 días de la semana, y mejoras de seguridad de correo electrónico y archivos adjuntos, además de otras mejoras de ciberseguridad.

Si tiene más preguntas sobre el ataque cibernético, llámenos al [redacted].

Atentamente,

One Community Health

– OTRA INFORMACIÓN IMPORTANTE –

1. **Inscripción en una supervisión de crédito de cortesía de 24 meses.**

Active ahora IdentityWorks Credit 3B en tres pasos sencillos

1. INSCRÍBASE antes del: [redacted] (Su código no será válido después de esta fecha.)
2. VISITE el **sitio web de Experian IdentityWorks** para inscribirse: [redacted]
3. PROPORCIONE el **código de activación**: [redacted]

Si tiene preguntas sobre el producto, necesita asistencia con la restauración de identidad o le gustaría conocer una alternativa a la inscripción en Experian IdentityWorks en línea, comuníquese con el equipo de atención al cliente de Experian llamando al [redacted]. Esté preparado para brindar el número [redacted] como prueba de elegibilidad para recibir los servicios de restauración de identidad proporcionados por Experian.

DETALLES ADICIONALES RELACIONADOS CON SU MEMBRESÍA DE 24 MESES DE EXPERIAN IDENTITYWORKS CREDIT 3B:

No se requiere una tarjeta de crédito para inscribirse en Experian IdentityWorks Credit 3B.

Puede comunicarse con Experian **de manera inmediata sin tener que inscribirse para obtener el producto** con respecto a cualquier asunto de fraude. Los especialistas en restauración de identidad se encuentran disponibles para ayudarlo(a) a abordar el fraude relacionado con asuntos de créditos y otros asuntos.

Una vez que se inscriba en Experian IdentityWorks, tendrá acceso a las siguientes funciones adicionales:

- **Informe crediticio de Experian al momento de la inscripción:** Consulte la información asociada con su expediente de crédito. Los informes crediticios diarios se encuentran disponibles solo para los miembros en línea.*
- **Supervisión de crédito:** Controla activamente los archivos de Experian, Equifax y TransUnion para determinar indicadores de fraude.
- **Experian IdentityWorks ExtendCARE™:** Usted recibe el mismo nivel superior de apoyo de restauración de identidad incluso después de que su membresía de IdentityWorks haya vencido.
- **Seguro contra robo de identidad de $1 millón**:** Ofrece cobertura para determinados costos y transferencias electrónicas de fondos no autorizadas.

Active su membresía hoy en [redacted]
o llame al [redacted] para registrarse con el código de activación mencionado anteriormente.

Qué puede hacer para proteger su información: También puede considerar otras acciones para disminuir las posibilidades de robo de identidad o fraude en sus cuentas. Visite www.ExperianIDWorks.com/restoration para obtener esta información. Si tiene preguntas sobre IdentityWorks, necesita ayuda para comprender algo en su informe crediticio o sospecha que un elemento en su informe crediticio puede ser fraudulento, comuníquese con el equipo de atención al cliente de Experian al [redacted].

* Los miembros que no estén en línea podrán llamar para obtener informes adicionales trimestralmente luego de registrarse.

** El seguro contra robo de identidad es suscrito por las empresas de seguro afiliadas o las subsidiarias de American International Group, Inc. (AIG). La descripción en este documento es un resumen, se creó únicamente para fines informativos, y no incluye todos los términos, las condiciones y las exclusiones de las políticas descritas. Consulte las políticas reales para conocer los términos, las condiciones y las exclusiones de la cobertura. Es posible que la cobertura no esté disponible en todas las jurisdicciones.

2. Implementación de una alerta de fraude en su expediente de crédito.

Independientemente de si elige, o no, usar los servicios de monitoreo crediticio de cortesía por 24 meses, le recomendamos que implemente una "Alerta de fraude" de un (1) año en sus expedientes de crédito, sin ningún cargo. Una alerta de fraude le informa a los acreedores que se comuniquen con usted personalmente antes de abrir una cuenta nueva. Para implementar una alerta de fraude, llame a cualquiera de las tres agencias de crédito principales a los números que figuran a continuación. En cuanto una agencia de crédito confirma su alerta de fraude, esta le notificará a las otras agencias.

Equifax	*Experian*	*TransUnion LLC*
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, PA 92834-6790
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/	https://www.experian.com/fraud/center.html	https://www.transunion.com/fraud-alerts
(800) 525-6285	(888) 397-3742	(800) 680-7289

3. Implementación de un congelamiento de seguridad en su expediente de crédito.

Si está muy preocupado(a) por convertirse en una víctima de fraude o robo de identidad, puede solicitar que se coloque un "congelamiento de seguridad" en su expediente de crédito, sin costo. Con determinadas excepciones específicas, un congelamiento de seguridad prohíbe que las agencias de informes del consumidor publiquen su informe crediticio o cualquier información obtenida de ese documento sin su autorización explícita. Puede realizar un congelamiento de seguridad en su informe crediticio comunicándose con las tres empresas nacionales de informes crediticios a los números que se indican a continuación y siguiendo las instrucciones establecidas o enviando una solicitud por escrito, por correo postal, a las tres empresas de informes crediticios:

Equifax Security Freeze	*Experian Security Freeze*	*TransUnion Security Freeze*
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.equifax.com/personal/credit-report-services/credit-freeze/	http://experian.com/freeze	http://www.transunion.com/securityfreeze
(800) 349-9960	(888) 397-3742	(888) 909-8872

Para implementar el congelamiento de seguridad, deberá proporcionar su nombre, dirección, fecha de nacimiento, número del Seguro Social y otra información personal. Después de recibir su solicitud de congelamiento, cada compañía de informes crediticios le enviará una carta de confirmación con un PIN (número de identificación personal) o una contraseña únicos. Mantenga el PIN o la contraseña en un lugar seguro. Lo necesitará si decide levantar el congelamiento.

Si su información personal se ha utilizado para presentar una declaración de impuestos falsa, para abrir una cuenta o para intentar abrir una cuenta a su nombre o para cometer fraude u otros delitos contra usted, puede presentar una denuncia policial en la ciudad en la que reside actualmente.

Si realiza un congelamiento de seguridad *antes* de inscribirse en el servicio de supervisión de crédito como se describió anteriormente, deberá eliminar el congelamiento para inscribirse en el servicio de supervisión de crédito. Después de inscribirse en el servicio de supervisión de crédito, puede volver a congelar su expediente de crédito.

4. Obtención de un informe crediticio sin cargo.

Según la ley federal, usted tiene derecho a que cada una de las tres empresas nacionales principales de informes crediticios antes mencionadas le proporcionen un informe crediticio sin cargo cada 12 meses. Llame al **1-877-322-8228** o solicite sus informes crediticios sin cargo en línea en **www.annualcreditreport.com**. Cuando reciba sus informes crediticios, revíselos para confirmar que no haya discrepancias. Identifique las cuentas que no abrió o las consultas de acreedores que no autorizó. Verifique que toda la información sea correcta. Si tiene preguntas u observa información incorrecta, comuníquese con la empresa de informes crediticios.

5. Recursos útiles adicionales.

Aunque no encuentre ninguna actividad sospechosa en sus informes crediticios iniciales, la Comisión Federal de Comercio (Federal Trade Commission, FTC) le recomienda que verifique sus informes crediticios de forma periódica. Si controla su informe crediticio de forma periódica, podrá detectar problemas y abordarlos rápidamente.

Si encuentra actividad sospechosa en sus informes crediticios o tiene algún motivo para creer que su información ha sido usada de forma indebida, llame a su agencia de cumplimiento de la ley local y presente una denuncia ante la policía. Asegúrese de obtener una copia de la denuncia ante la policía, ya que muchos acreedores desearán recibir la información allí contenida para absolverlo(a) de las deudas fraudulentas. También puede presentar una queja ante la FTC; para ello, comuníquese con este organismo en la Web en www.ftc.gov/idtheft, por teléfono al 1-877-IDTHEFT (1-877-438-4338) o por correo postal a Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Su queja se agregará al Centro de información de robo de identidad de la FTC, donde estará disponible para los encargados del cumplimiento de la ley que lleven a cabo investigaciones. Además, puede obtener información de la FTC acerca de alertas de fraude y congelamientos de seguridad.

6. Protección de su información médica.

Las siguientes prácticas pueden proporcionar medidas de seguridad adicionales para protegerse contra el robo de identidad médica.

- Solo comparta sus tarjetas de seguro médico con sus proveedores de atención médica y otros miembros de su familia que tengan cobertura en su plan de seguro o que le ayuden con su atención médica.
- Revise su "declaración de explicación de beneficios", la cual recibe a través de su compañía de seguro médico. Realice un seguimiento con su compañía de seguro o el proveedor de atención si existe algún elemento que no reconoce. Si fuera necesario, comuníquese con el proveedor de atención médica sobre la declaración de explicación de beneficios y solicite copias de los registros médicos desde la fecha del potencial acceso (observado más arriba) hasta la fecha actual.
- Solicítele a su compañía de seguros un informe actual del año hasta la fecha de todos los servicios pagados por usted como beneficiario. Realice un seguimiento con la compañía de seguro o el proveedor de atención si existe algún elemento que no reconoce.