LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH
hope. recovery. wellbeing.

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to provide you with information about a cybersecurity incident we experienced. This notice explains what happened, what information of yours may have been affected, what measures we are taking, and steps you can take in response. While we are not aware of any actual or attempted misuse of your information, we are providing you with an overview of the incident, our ongoing response, and resources available to you right now to help protect your information, should you feel it is appropriate to do so.

What Happened

On May 28, 2024, several employees received a phishing email originating from a trusted business partner. Users interacted with the phishing email, allowing the malicious actor or actors to obtain the log-in credentials for the Microsoft Office 365 user accounts, compromising the accounts of three employees. We believe the cyber-attack provided the attacker access to certain personal information, as described below. Though we have no evidence that any personal information has been misused, out of an abundance of caution, we are notifying you now of this cyber-attack and providing you information you can use to proactively take steps to protect yourself and your information.

What Information Was Involved

The personal information that may have been obtained includes your name, date of birth, social security number, address, telephone number, medical record number, health insurance information, diagnosis, and treatment information.

What We Are Doing

Data privacy and security are among our highest priorities, and we have extensive measures in place to protect information entrusted to us. Upon discovering the incident, we acted swiftly to disable the impacted accounts and reset the Microsoft Office 365 and multi-factor authentication credentials. We also notified law enforcement and cooperated with law enforcement's investigation. Once our investigation determined which accounts had been compromised, we initiated a comprehensive review, with the assistance of industry leading forensic specialists, to identify any personally identifying information or personal health information in the impacted accounts. On July 15, 2024, we completed our investigation and determined that certain elements of your personal information may have been impacted by this event.

We are also reviewing and updating our security policies, procedures, and controls. We have also notified Microsoft of the vulnerability in the Microsoft Office 365 multi-factor authentication that was exploited by the malicious actor or actors. We have since implemented new security controls to address this specific attack.

What You Can Do

Although we have no evidence that any of your personal information has been misused, we encourage you to remain vigilant for any suspicious activity on any of your accounts. We also encourage you to review your financial and account statements and immediately report all suspicious activity to the institution that issued the record. Enclosed with this letter are some steps you can take to protect your information.

For More Information

We sincerely regret any inconvenience or concern this incident has caused. We understand that you may have questions about this incident that are not addressed in this letter. We have established a dedicated call center available toll free in the U.S. at (866) 997-5807, from 6:00 a.m. to 5:00 p.m. Pacific Time (Excluding major U.S. holidays).

Sincerely,

Maurnie V. Thomas

Maurnie V. Thomas – Privacy Officer
Los Angeles County Department of Mental Health

Steps You Can Take to Protect Your Information

Monitor Your Accounts.

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Security Freeze.

You can place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-836-6351
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information.

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General.

The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.identitytheft.gov ; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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

LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH
hope. recovery. wellbeing.

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Aviso de violación de datos

Estimado <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Le escribo para proporcionarle información sobre un incidente de ciberseguridad que experimentamos. Este aviso explica lo que sucedió, qué información suya puede haberse visto afectada, qué medidas estamos tomando y los pasos que puede tomar en respuesta. Si bien no tenemos conocimiento de ningún uso indebido real o intento de uso indebido de su información, le proporcionamos una descripción general del incidente, nuestra respuesta continua y los recursos disponibles para usted en este momento para ayudar a proteger su información, en caso de que considere apropiado hacerlo.

¿Qué pasó

El 28 de mayo de 2024, varios empleados recibieron un correo electrónico de phishing procedente de un socio comercial de confianza. Los usuarios interactuaron con el correo electrónico de phishing, lo que permitió que el actor o actores malintencionados obtuvieran las credenciales de inicio de sesión de las cuentas de usuario de Microsoft Office 365, comprometiendo las cuentas de tres empleados. Creemos que el ciberataque proporcionó al atacante acceso a cierta información personal, como se describe a continuación. Aunque no tenemos pruebas de que se haya hecho un uso indebido de la información personal, por precaución, le notificamos ahora de este ciberataque y le proporcionamos información que puede utilizar para tomar medidas proactivas para protegerse a sí mismo y a su información.

¿Qué información estaba involucrada?

La información personal que se puede haber obtenido incluye su nombre, fecha de nacimiento, número de seguro social, dirección, número de teléfono, número de registro médico, información de seguro médico, diagnóstico e información de tratamiento.

Lo que estamos haciendo

La privacidad y la seguridad de los datos se encuentran entre nuestras principales prioridades, y contamos con amplias medidas para proteger la información que se nos confía. Al descubrir el incidente, actuamos rápidamente para deshabilitar las cuentas afectadas y restablecer las credenciales de autenticación multifactor y de Microsoft Office 365. También notificamos a las fuerzas del orden y cooperamos con la investigación de las fuerzas del orden. Una vez que nuestra investigación determinó qué cuentas se habían visto comprometidas, iniciamos una revisión exhaustiva, con la ayuda de especialistas forenses líderes en la industria, para identificar cualquier información de identificación personal o información de salud personal en las cuentas afectadas. El 15 de julio de 2024, completamos nuestra investigación y determinamos que ciertos elementos de su información personal pueden haberse visto afectados por este evento.

También estamos revisando y actualizando nuestras políticas, procedimientos y controles de seguridad. También hemos notificado a Microsoft de la vulnerabilidad en la autenticación multifactor de Microsoft Office 365 que fue explotada por el actor o actores malintencionados. Desde entonces, hemos implementado nuevos controles de seguridad para hacer frente a este ataque específico.

Lo que puedes hacer

Aunque no tenemos pruebas de que se haya hecho un uso indebido de su información personal, le recomendamos que permanezca atento a cualquier actividad sospechosa en cualquiera de sus cuentas. También le recomendamos que revise sus estados financieros y de cuenta y que informe inmediatamente toda actividad sospechosa a la institución que emitió el registro. Adjunto a esta carta se encuentran algunos pasos que puede seguir para proteger su información.

Para más información

Lamentamos sinceramente cualquier inconveniente o preocupación que este incidente haya causado. Entendemos que puede tener preguntas sobre este incidente que no se abordan en esta carta. Hemos establecido un centro de llamadas dedicado disponible de forma gratuita en los EE. UU. al (866) 997-5807, de 6:00 a. m. a 5:00 p. m., hora del Pacífico (excepto los principales días festivos de EE. UU.).

Sinceramente

Maurnie V. Thomas

Maurnie V. Thomas – Oficial
de Privacidad Departamento de Salud Mental del Condado de Los Ángeles

Medidas que puede seguir para proteger su información

Monitorea tus cuentas.

Para protegerse contra la posibilidad de robo de identidad u otras pérdidas financieras, le recomendamos que permanezca alerta, revise sus estados de cuenta y controle sus informes crediticios para detectar actividades sospechosas. Según la ley de los EE. UU., usted tiene derecho a un informe de crédito gratuito al año de cada una de las tres principales agencias de informes de crédito. Para solicitar su informe de crédito gratuito, visite www.annualcreditreport.com o llame al número gratuito 1-877-322-8228. También puede comunicarse directamente con las tres principales agencias de crédito para solicitar una copia gratuita de su informe de crédito.

Congelación de seguridad.

Puede colocar un "congelamiento de seguridad" en su informe de crédito, lo que prohibirá que una agencia de informes del consumidor divulgue información en su informe de crédito sin su autorización expresa. El congelamiento de seguridad está diseñado para evitar que se aprueben créditos, préstamos y servicios a su nombre sin su consentimiento. Sin embargo, debe tener en cuenta que el uso de un congelamiento de seguridad para tomar el control sobre quién tiene acceso a la información personal y financiera en su informe de crédito puede retrasar, interferir o prohibir la aprobación oportuna de cualquier solicitud o solicitud posterior que realice con respecto a un nuevo préstamo, crédito, hipoteca o cualquier otra cuenta que implique la extensión de crédito. De acuerdo con la ley federal, no se le puede cobrar por colocar o levantar un congelamiento de seguridad en su informe de crédito. Si desea realizar un congelamiento de seguridad, comuníquese con las principales agencias de informes del consumidor que se enumeran a continuación:

Experian	**TransUnion**	**Equifax**
PO Box 9554 Allen, TX 75013	P.O. Box 160 Woodlyn, PA 19016	PO Box 105788 Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

Para solicitar un congelamiento de seguridad, deberá proporcionar la siguiente información:

1. Su nombre completo (incluyendo la inicial del segundo nombre, así como Jr., Sr., II, III, etc.);
2. Número de Seguro Social;
3. Fecha de nacimiento;
4. Si se ha mudado en los últimos cinco (5) años, proporcione las direcciones donde ha vivido durante los cinco años anteriores;
5. Comprobante de domicilio actual, como una factura actual de servicios públicos o una factura de teléfono;
6. Una fotocopia legible de una tarjeta de identificación emitida por el gobierno (licencia de conducir o tarjeta de identificación estatal, identificación militar, etc.);
7. Si es víctima de robo de identidad, incluya una copia del informe policial, el informe de investigación o la queja ante una agencia de aplicación de la ley sobre el robo de identidad.

Para eliminar el congelamiento de seguridad, debe enviar una solicitud por escrito a cada una de las tres agencias de crédito por correo e incluir la identificación adecuada (nombre, dirección y número de seguro social) y el número PIN o contraseña que se le proporcionó cuando realizó el congelamiento de seguridad. Las agencias de crédito tienen tres (3) días hábiles después de recibir su solicitud para eliminar el congelamiento de seguridad.

Como alternativa a un congelamiento de seguridad, tiene derecho a colocar una "alerta de fraude" inicial o extendida en su archivo sin costo alguno. Una alerta de fraude inicial es una alerta de 1 año que se coloca en el archivo de crédito de un consumidor. Al ver una alerta de fraude en el archivo de crédito de un consumidor, una empresa debe tomar medidas para verificar la identidad del consumidor antes de otorgar un nuevo crédito. Si usted es víctima de robo de identidad, tiene derecho a una alerta de fraude extendida, que es una alerta de fraude que dura siete años. Si desea colocar una alerta de fraude, comuníquese con cualquiera de las agencias que se enumeran a continuación:

Experian	**TransUnion**	**Equifax**
Apartado Postal 2002	Apartado Postal 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-836-6351
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Información adicional.

Puede informarse más sobre el robo de identidad y los pasos que puede tomar para protegerse, comunicándose con el Fiscal General de su estado o con la Comisión Federal de Comercio. También puedes informarte más sobre cómo colocar una alerta de fraude o un congelamiento de seguridad en tu expediente de crédito comunicándote con la FTC o con el Fiscal General de tu estado.

La Comisión Federal de Comercio (FTC, por sus siglas en inglés) también alienta a aquellos que descubran que su información ha sido utilizada indebidamente a presentar una queja ante ellos. Puede comunicarse con la Comisión Federal de Comercio en: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.identitytheft.gov ; 1-877-ID-THEFT (1-877-438-4338); y TTY: 1-866-653-4261.

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