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

<<DATE>>

<<first name>> <<last name>> <<suffix>>,
<<address_1>>
<<address_2>>
<<city>>, <<state>> <<postal code>>

Re: Notice of Data Breach

Dear <<first 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 March 20, 2024, an external entity's compromised email account sent a phishing email to a DMH employee. The phishing email included an attached document with a QR code. The employee followed the instructions included in the document and scanned the QR code, sending the email to a malicious website, allowing the threat actor the ability to get access to the employee's Microsoft Office 365 account. We believe the cyber-attack gave the perpetrator access to specific personal information, as detailed below. It is important to note, there is no evidence that any personal information was exploited. Out of an abundance of caution, we are informing you of this cyber-attack information that can be used 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, and treatment information.

What We Are Doing

Data privacy and security are among our top objectives, and we have extensive safeguards in place to protect the information entrusted to us. When we discovered the issue, we proceeded quickly to disable the affected accounts and reset the Microsoft Office 365 and multi-factor authentication credentials. We also informed law enforcement and helped with their inquiry. After determining which accounts had been compromised, we conducted a thorough assessment with the assistance of industry leading forensic specialists to identify any personally identifiable information or personal health information

in the affected accounts.

We have also notified Microsoft of the vulnerability in Microsoft Office 365 multi-factor authentication, which was exploited by the malicious actor or actors. We have since introduced new security procedures to address this specific issue.

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.

Sincerely,

Maurnie V. Thomas
Maurnie V. Thomas – MA, MPA
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 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19016 1-888-909-8872 www.transunion.com/credit-freeze	PO Box 105788 Atlanta, GA 30348 1-888-298-0045 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 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-836-6351 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