Notice of Breach / Cybersecurity Incident

Network180 – the Kent County Community Mental Health Authority ("Network180"), is posting this Notice to inform you about an incident that involved unauthorized access to personal information of its clients and employees maintained by Network180. Network180 takes its patients' and employees' privacy seriously, and it is important to us that you and the community that we serve are made fully aware of this recent security incident.

WHAT HAPPENED?

On October 18, 2023, a Network180 user noticed unusual activity on their email account and immediately notified our IT department of the situation. Our IT team was immediately deployed to address and contain the situation. Containment was completed on October 18, 2023 and Network180 IT engaged outside third-party forensic and cybersecurity experts to assist in the investigation and remediation of the incident. The third-party experts worked with Network180 IT personnel to assess the scope of the incident and recommend additional security measures. On October 25, 2023, the forensic experts determined that Network180 was the victim of a phishing attack by unknown threat actors, whereby the individual unknowingly clicked on a link in a malicious email which affected the user's Network180 secure email account. Clicking this link enabled the threat actors to access the user's email account and credentials, bypassing various security protections in effect, including multi-factor authentication. Our investigation revealed that the unauthorized threat actors had access to the affected email account between September 28, 2023 – October 18, 2023 and were able to access and export certain data contained on the user's e-mail account, the full extent of which was not known until early December 2023. In addition, law enforcement, including the FBI, was notified of the incident.

What Information Was Involved?

The third-party experts worked around the clock with Network180 IT personnel to implement containment and security measures. Based upon the forensic team's investigation and analysis of the data impacted, we discovered that the personal information of Network180's current and former employees and current and former clients serviced by Network180 was involved, which may have included full names and one or more of the following: address, date of birth, driver's license number (for a small number of individuals), full or partial Social Security Number, health insurance policy information (including Subscriber Number and designated insurer), medical information, other demographic information (i.e., race or gender), and in a limited number of cases, financial account of payment card numbers. As a result, your personal information may have been potentially exposed to others. Please be assured that we have taken every step necessary to address the incident.

What did Network180 do?

As noted above, after suspicious activity was detected on the Network180 user's email account, Network180 took quick and decisive action to contain the incident. Network180 has also taken additional steps to strengthen the security of the IT environment and to ensure that future incidents are

unsuccessful, including hiring cybersecurity staff to proactively monitor Network180's systems and implement the recommendations of the forensics experts.

What should you do?

Network180 will be notifying all affected individuals for whom we have an address and whose sensitive personal information was involved in the incident. Out of an abundance of caution, we are offering individuals whose sensitive information may have been involved in this incident complimentary credit monitoring services for 12 months at no charge. Letters were mailed beginning on December 22, 2023. Please allow at least 5 business days for these letters to arrive. If you believe you are affected by this incident and did not receive a notification letter by March 21, 2024, please call Experian at 1-833-713-9013, Monday through Friday 9 a.m. – 11 p.m. EST, Saturday and Sunday 10:00 a.m. – 7:00 p.m. CST (excluding major holidays). Please provide this engagement number to the Experian operator: B112415 (adults) or B112416 (minors).

We also recommend that you regularly review statements from your accounts (*i.e.*, account statements and Explanations of Benefits ("EOB")) and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase additional copies of your credit report by contacting one or more of the three nationwide consumer reporting agencies listed below.

Equifax:	P.O. Box 740241, Atlanta, GA 30374, 1-800-685-1111, www.equifax.com
Experian:	P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion:	P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, account statements and EOBs, review them carefully. Look for accounts or creditor inquiries, transactions, or services that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report, the company issuing the account statement, your provider rendering services, or the insurance company issuing your EOB. Additional information regarding Identity Theft Protection is available here: https://www.network180.org/document/information-about-identity-theft. We have also posted a list of Frequently Asked Questions, which is available here: https:// www.network180.org/document/network180-security-faqs.

Individuals may also contact the Federal Trade Commission (FTC) or law enforcement to report incidents of identity theft or to learn about steps to protect themselves from identity theft. To learn more, individuals can go to the FTC's website at www. ftc.gov/idtheft, call the FTC at (877) IDTHEFT (438-4338), or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580.

In addition, individuals may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. Individuals can add a fraud alert to their credit report file to help protect their credit information. A fraud alert can make it more difficult for someone to get credit in an individual's name because it tells creditors to follow certain procedures to verify that individual's identity. Individuals may place a fraud alert in their file by calling any of the nationwide credit reporting agencies listed above. As soon as that

agency processes a fraud alert, it will notify the other two agencies, which then must also place fraud alerts in an individual's file.

Individuals also can contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze to restrict access to their credit report. Individuals will need to provide the credit reporting agency with certain information, such as their name, address, date of birth, and Social Security number. After receiving their request, the credit reporting agency will send the individual a confirmation letter containing a unique PIN or password that they will need in order to lift or remove the security freeze in the future. This PIN or password should be kept in a safe place.

We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. We have changed the affected user's credential and added protections to our O365 accounts to limit access to Network180's IT environment and are training our workforce in safeguards and detecting malicious phishing attempts.

We sincerely apologize to you and all of our employees and healthcare clients for concern caused by this incident.

Sincerely,

Network180

William J. Ward
Executive Director