MORRISON FOERSTER

2100 L STREET, NW
SUITE 900
WASHINGTON
DC 20037

TELEPHONE: 202.887.1500
FACSIMILE: 202.887.0763

WWW.MOFO.COM

AUSTIN, BEIJING, BERLIN, BOSTON,
BRUSSELS, DENVER, HONG KONG,
LONDON, LOS ANGELES, MIAMI,
NEW YORK, PALO ALTO, SAN DIEGO,
SAN FRANCISCO, SHANGHAI, SINGAPORE,
TOKYO, WASHINGTON, D.C.

April 15, 2025

The Honorable Mike Hilgers
Office of the Nebraska Attorney General
Consumer Affairs Response Team
2115 State Capitol
Lincoln, NE 68509

Via Online Form

Re: Notice Pursuant to Neb. Rev. Stat. §§ 87-801–87-808

Dear Attorney General Hilgers,

Pursuant to Nebraska Revised Statute Sections 87-801 to 87-808, we write on behalf of Unanet, Inc. ("Unanet" or Company") to notify you of a data security matter, which we believe affected approximately three Nebraska residents. Unanet is a provider of enterprise resource planning and customer relationship management solutions located in Dulles, Virginia.

Unanet was the victim of a cybersecurity incident in which an unauthorized third party gained access to a limited portion of its internal network. On March 13, 2025, Unanet identified anomalous activity in one of its standard third-party support tools. Unanet quickly launched an investigation with the help of leading cybersecurity experts and took steps to secure its network. As part of the investigation, Unanet identified that a file containing personal information of Unanet employees was obtained by the unauthorized party on or around March 14, 2025. The investigation confirmed that neither customer information, customer environments, nor Unanet's production environment were impacted. On or around March 24, 2025, Unanet determined that personal information from Nebraska residents was contained in the affected file.

Based on Unanet's investigation, the impacted file included personal information of approximately three Nebraska residents. The types of personal information included in the file will depend on the information the individual provided to Unanet but may include: first and last name; address; Social Security number; email address; phone number; date of birth; and other employment-related information.

Notification of this matter will be mailed to the Nebraska residents on or around April 16, 2025. A copy of this notification is attached as **Exhibit A**.

We currently have no evidence of misuse of any personal information as a result of this incident.

MORRISON FOERSTER

2100 L STREET, NW
SUITE 900
WASHINGTON
DC 20037

TELEPHONE: 202.887.1500
FACSIMILE: 202.887.0763

WWW.MOFO.COM

AUSTIN, BEIJING, BERLIN, BOSTON, BRUSSELS, DENVER, HONG KONG, LONDON, LOS ANGELES, MIAMI, NEW YORK, PALO ALTO, SAN DIEGO, SAN FRANCISCO, SHANGHAI, SINGAPORE, TOKYO, WASHINGTON, D.C.

Unanet takes the protection of employee information seriously. Unanet is offering two years of identity protection services, at no cost, to potentially affected individuals through Kroll. In addition, in response to this matter, Unanet implemented measures to contain and remediate the incident and has taken steps to further enhance the security of its network. In addition, Unanet notified federal law enforcement in the course its investigation. Finally, Unanet has taken steps to further enhance its security controls, including updates to processes and procedures, in an effort to prevent a similar occurrence from happening again.

Should you have any questions about this matter, please do not hesitate to contact me directly. Thank you for your attention to this matter.

Sincerely,

Kaylee Cox Bankston

Kaylee Cox Bankston

Exhibit A

Unanet

<<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>> <<last_name>>,

On behalf of Unanet, Inc., I am writing to inform you about an incident at Unanet that involved your personal information. We are providing you with information about the incident and steps you may take to help protect your information. We regret that this incident occurred and take the security of your information seriously.

WHAT HAPPENED

Unanet was the victim of a cybersecurity incident in which an unauthorized third party gained access to a limited portion of our internal network. On March 13, 2025, Unanet identified anomalous activity in one of its standard third-party support tools. We quickly launched an investigation with the help of leading cybersecurity experts and took steps to secure our internal network. As part of the investigation, we identified that a file containing personal information was obtained by the unauthorized party on or around March 14, 2025. Our investigation confirmed that neither customer information, customer environments, nor Unanet's production environment were impacted by this incident.

While we currently have no evidence of identity theft, fraud, or other misuse of your information as a result of this incident, we are notifying you to provide you with information and steps you can take to help protect your information.

WHAT INFORMATION WAS INVOLVED

The information involved included personal information that you provided to Unanet or that was otherwise collected or generated in the course of your <<b2b_text_1 (employment status)>> with Unanet, including: <<b2b_text_2 (data elements)>>. At this time, we have no evidence of misuse of your personal information as a result of this incident, but we encourage you to activate the free identity monitoring services offered in this letter.

WHAT WE ARE DOING

We take the protection of your personal information very seriously, and we began investigating the incident as soon as we learned of it. To help protect your information, we are providing you with **free identity monitoring services for 24 months through Kroll**, as described in detail in this letter. After becoming aware of the incident, we promptly initiated a comprehensive investigation to determine what occurred and retained third-party experts to assist with our investigation. We also implemented measures to contain and remediate the incident and to further secure the environment. We have also notified federal law enforcement. In addition, we have taken steps, and are in the process of taking additional measures, to further enhance our security controls, including updates to processes and procedures, in an effort to prevent a similar occurrence from happening again.

WHAT YOU CAN DO

Consistent with certain laws, we are providing you with the following information about steps that you can take to protect against potential misuse of personal information. There are steps you can take to protect yourself in this situation, including activating the identity monitoring service we are offering to you for free. Details regarding the service and how to activate are provided below. As a best practice, we encourage you to remain vigilant for suspicious activity and to regularly review your financial statements and credit reports. We have also enclosed an attachment with additional information and resources where you can obtain additional information about identity theft and ways to protect yourself.

As a precaution, we have arranged for you, at your option, to activate a complimentary **two-year** identity monitoring service. We have engaged **Kroll** to provide you with its **Identity Monitoring** services, which include Credit Monitoring, Web Watcher, Fraud Consultation, and Identity Theft Restoration. You have **until <<b2b_text_6 (activation deadline)>>** to activate the free identity monitoring service by using the Membership Number below. This Membership Number is unique for your use and should not be shared. To activate, **go to https://enroll.krollmonitoring.com**.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

We encourage you to take full advantage of this service offering. Kroll representatives can answer questions or concerns you may have regarding these services.

FOR MORE INFORMATION

You will find additional information about steps to protect yourself as well as detailed instructions for activating the identity monitoring services in the enclosed Additional Resources document. You will need to reference the Membership Number in this letter when calling or activating online, so please do not discard this letter.

Please call (866) 408-2237, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays, for assistance or for any additional questions you many have.

Sincerely,

John W. McMonagle III

John W. McMonagle III
CFO

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL RESOURCES

The following provides additional information and actions you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

Federal Trade Commission		
Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft		
Credit Reporting Agencies		
Equifax P.O. Box 740241 Atlanta, GA 30374 1-800-525-6285 www.equifax.com	Experian P.O. Box 4500 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com

You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditreport.com, by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any 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 agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them.

For District of Columbia Residents. You may obtain information about avoiding identity theft from the District of Columbia Attorney General's Office. These offices can be reached at:

Office of the Attorney General
400 6th Street, NW
Washington, DC 20001
(202) 727-3400
oag.dc.gov

For Maryland Residents. You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023
www.marylandattorneygeneral.gov

For Massachusetts Residents: You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub or statement) in order to implement your request for a security freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

For New York Residents. You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

New York Attorney General
The Capitol
Albany, NY 12224
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, New York 12231
(800) 697-1220
www.dos.ny.gov

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov

For Rhode Island Residents: You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
1-401-274-4400
www.riag.ri.gov