Our ref 1325219

Kennedys

22 Vanderbilt Ave.
Suite 2400
New York, NY 10017

t +1 267.479.6700
f +1 215.665.8475

kennedyslaw.com

t +1 646 625 4030

Daniel.Marvin@kennedyslaw.com

May 13, 2026

Via Email

Attorney General Nick Brown
Office of the Attorney General for Washington State
1125 Washington St SE
P.O. Box 40100
Olympia, WA 98504
SecurityBreach@atg.wa.gov

Re: **Nursa – Notice of Security Breach**

Dear Attorney General Brown:

We represent Nursa, a healthcare staffing platform, headquartered in Murray, Utah. We write in accordance with WA ST § 19.255.010, to report a data event resulting in the unauthorized acquisition of personal information concerning thirteen thousand one hundred and sixty-eight (13,168) residents of Washington. This notice shall not be construed as an admission of jurisdiction or liability, nor does Nursa waive its rights or defenses regarding the applicability of Washington law or personal jurisdiction.

On February 27, 2026, and March 18, 2026, an unauthorized party accessed and exported a limited number of user profiles from Nursa's web application. On March 20, 2026, Nursa became aware of the unauthorized activity and took immediate steps to resecure its platform, which involved retaining our firm. We engaged a forensics firm to assist with the investigation and remediation efforts, and for the provision of rendering legal advice.

Individuals will be notified via First Class U.S. mail on May 13, 2026. A sample copy of the notification letter is attached as Exhibit A. The information included the individuals' name and date of birth. Nursa confirmed the types of personal information subject to unauthorized access and enclosed contact information to the major consumer reporting bureaus, state-specific regulators, and a number for a professional call center for obtaining resources to protect against fraud or misuse, should the individual find it appropriate to do so.

Kennedys is a trading name of Kennedys CMK LLP, a limited liability partnership, in New Jersey, United States (with registered number 0450171416)

Kennedys Law LLP, a UK Limited Liability Partnership, is a partner of Kennedys CMK LLP

Kennedys offices, associations and cooperations: Argentina, Australia, Belgium, Bermuda, Bolivia, Brazil, Canada, Chile, China, Colombia, Denmark, Dominican Republic, Ecuador, England and Wales, France, Guatemala, Hong Kong, India, Ireland, Israel, Italy, Mexico, New Zealand, Northern Ireland, Norway, Oman, Pakistan, Panama, Peru, Poland, Puerto Rico, Scotland, Singapore, Spain, Sweden, Turkey, United Arab Emirates, United States of America.

Attorney General Nick Brown
Office of Attorney General for Washington State
Nursa

Kennedys

Nursa is reviewing its existing security policies and protections already in place on its network for additional ways to safeguard against evolving threats. This notice provides your Office with all information necessary to comply with Washington law. Please do not hesitate to contact me directly if you have additional questions.

Respectfully,

Daniel Marvin
Partner
for Kennedys

Exhibit A

Kennedys is a trading name of Kennedys CMK LLP, a limited liability partnership, in New Jersey, United States (with registered number 0450171416)

Kennedys Law LLP, a UK Limited Liability Partnership, is a partner of Kennedys CMK LLP

Kennedys offices, associations and cooperations: Argentina, Australia, Belgium, Bermuda, Bolivia, Brazil, Canada, Chile, China, Colombia, Denmark, Dominican Republic, Ecuador, England and Wales, France, Guatemala, Hong Kong, India, Ireland, Israel, Italy, Mexico, New Zealand, Northern Ireland, Norway, Oman, Pakistan, Panama, Peru, Poland, Puerto Rico, Scotland, Singapore, Spain, Sweden, Turkey, United Arab Emirates, United States of America.

Nursa
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

13764 [redacted]

May 13, 2026

NOTICE OF DATA BREACH

Dear [redacted]:

We recently experienced a security incident that involved your personal information. This notice is intended to provide you with details about the incident, our response, and additional steps you may consider to protect your information.

What Happened? On February 27, 2026, and March 18, 2026, an unauthorized party accessed and exported a limited number of user profiles from our web application. On March 20, 2026, we became aware of the unauthorized activity and took immediate steps to resecure our platform, which involved retaining cybersecurity specialists to investigate the incident. We are notifying you because your profile was among those acquired.

What Information Was Involved? The information includes your first and last name, in combination with the following data element(s): [redacted]

What We Are Doing. Upon discovery, we took immediate steps to review our security posture. We are providing you with proactive fraud assistance to help with any questions that you might have. The professional call center may be reached at 1-833-380-7404 (toll free), Monday through Friday 8:00 a.m. - 8:00 p.m., Eastern time, excluding major U.S. holidays.

What You Can Do. To date, we are not aware of any reports of identity fraud or fraudulent activity involving your information because of this incident. Generally speaking, however, it is best practice to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. You may also refer to the enclosed "*Steps You Can Take to Help Protect Your Information*" for additional resources you may take advantage of to protect your information.

For More Information. Should you have any questions or concerns, please contact our assistance line at 1-833-380-7404 (toll free), Monday through Friday, 8:00 a.m. - 8:00 p.m., Eastern time, excluding major U.S. holidays. We regret any concern this event has caused or may cause you.

Sincerely,

Nursa
Enclosure: *Steps You Can Take to Help Protect Your Information*

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts and Credit Reports: Generally speaking, it is good practice to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors.

You May Obtain a Free Credit Report: Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit https://annualcreditreport.com, call toll-free at 1-877-322-8228, complete the Annual Credit Report Request Form on the Federal Trade Commission's (FTC) website at https://ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact one of the credit reporting bureaus.

Fraud Alert Services: You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified below.

Credit Freeze Instructions: As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit 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 credit freeze 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 credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address information from the prior two to five years;
5. Proof of current address, such as current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, you may contact a major credit reporting bureau listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

This notice has not been delayed by law enforcement. If you experience identity theft or fraud, you have the right to file a police report with your local law enforcement agency. When filing a report, you may be required to provide documentation showing that you have been a victim, and you are entitled to obtain a copy of the report for your records. If you discover suspicious activity on your credit reports or otherwise believe your information is being misused, you should promptly contact local law enforcement to file a report.

Instances of known or suspected identity theft should also be reported to your state Attorney General and the FTC. A complaint may be filed with the FTC online at https://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. Complaints submitted to the FTC are added to its Identity Theft Data Clearinghouse and made available to law enforcement for investigative purposes. The FTC also provides information about fraud alerts and security freezes.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or https://oag.dc.gov/consumer-protection.

For Oregon residents, the Oregon Attorney General may be contacted at Justice Building, 1162 Court St. NE, Salem, OR 97301; 1-877-877-9392; or https://doj.state.or.us.

You also have rights under the federal Fair Credit Reporting Act (FCRA) and Identity Security Act, which governs the collection and use of information pertaining to you by consumer reporting agencies. These rights include the right to access the information in your file, dispute incomplete or inaccurate information, and request correction or deletion of inaccurate, incomplete, or unverifiable information. For more information about the FCRA and your rights, you may visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf. or https://ftc.gov.

You may contact Nursa via mail at 5295 Commerce Dr #600, Murray, UT 84107.