EXHIBIT 1

By providing this notice, Forward, The National Databank for Rheumatic Diseases ("Forward") located at 727 N Waco Avenue Suite 200, Wichita, Kansas 67203, does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

In March 2025, Forward became aware of suspicious activity affecting certain systems within its network. Forward promptly initiated an investigation into the nature and scope of the event with the assistance of third-party cybersecurity and digital forensics specialists. The investigation determined there was unauthorized access to Forward's network between March 17, 2025, and March 22, 2025. In response, Forward conducted a comprehensive internal review of the systems impacted to identify the type of information stored therein and to whom that information related. This review was recently completed.

The information that could have been subject to unauthorized access for Maine residents includes: name, address, and Social Security number. While Forward is unaware of any identity theft or fraud related to this event, Forward is notifying individuals out of an abundance of caution.

Notice to Maine Residents

On July 22, 2025, Forward provided written notice of this incident to thirty-eight (38) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of this incident, Forward moved quickly to investigate and respond, assess the security of Forward systems, and identify potentially affected individuals. Forward is also working to implement additional safeguards and cybersecurity training to its employees. Forward is providing access to credit monitoring services for twenty-four (24 months), through CyberScout, a TransUnion company, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Forward is providing potentially affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud. Forward is also providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state attorney general, and law enforcement to report attempted or actual identity theft and fraud.

Forward is providing written notice of this event to appropriate state regulators, and to the three major consumer reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

Forward, The National Databank for Rheumatic Diseases
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P
[redacted]

July 22, 2025

P 0000101102G0500

Dear [redacted]:

Forward, The National Databank for Rheumatic Diseases ("Forward") writes to inform you of a recent data security event that may involve certain information related to you. We are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you determine it appropriate to do so.

What Happened? In March 2025, Forward became aware of suspicious activity affecting certain systems within its network. We immediately took steps to secure our environment and launched a comprehensive investigation with the assistance of third-party cybersecurity specialists to determine the full nature and scope of the event. The investigation determined there was unauthorized access to Forward's network between March 17, 2025, and March 22, 2025, and that certain files and folders within the network were potentially viewed and/or taken without authorization during that time. In response, we conducted a thorough review of the files to determine whether any sensitive information could be affected and to whom it relates. We recently completed our internal review.

What Information Was Involved? The investigation determined that your name and [redacted] may have been present in the affected systems and accessible during this event. Although there is no indication of identity theft or fraud resulting from this event, we are providing this notice out of an abundance of caution.

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities. Upon becoming aware of this event, we immediately took steps to secure our environment and conducted a comprehensive investigation to confirm the nature and scope of the activity and determine who may be affected. We implemented additional cybersecurity measures and reviewed existing security policies to further protect against similar events moving forward.

As an added precaution, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. These services will be provided to you at no cost by CyberScout, a TransUnion company specializing in fraud assistance and remediation services. Enrollment instructions are enclosed within this letter. Please note the deadline is October 21, 2025 and we are unable to enroll in these services for you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Help Protect Your Personal Information* for useful information on what you can do to better protect against possible misuse of your information. You may also enroll in the free credit monitoring services we have provided for you.

For More Information. If you have additional questions, you may contact our call center at 1-833-380-7005 (toll free), Monday through Friday, 8:00 AM - 8:00 PM Eastern Time, excluding U.S. holidays. You may also write to Forward at 727 Waco Avenue Suite 200, Wichita, Kansas 67203.

Sincerely,

Forward, The National Databank for Rheumatic Diseases

Steps You Can Take to Help Protect Your Personal Information.

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 15 Rhode Island residents that may be impacted by this event.