

EXHIBIT 1

Please note, Kettering Health is providing this notice on behalf of KH Credit Union (“KHCU”), as they are the entity that owns the data which was potentially subject to unauthorized access and/or acquisition, as outlined below. By providing this notice, Kettering Health does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about May 20, 2025, Kettering Health became aware of suspicious activity affecting certain systems within its network. Kettering Health promptly took steps to secure their 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 Kettering Health’s environment between April 9, 2025, and May 20, 2025, and that certain files and folders within the network were potentially viewed and/or acquired without authorization during that time, which related to KHCU. Thereafter, Kettering Health conducted a time intensive and comprehensive third-party review of the data potentially impacted to determine the contents of the impacted data and to whom it relates. On January 14, 2026, this review was completed. KHCU was notified shortly thereafter as a potential owner of data determined to be impacted as a result of this matter. KHCU then worked with Kettering Health to evaluate the data and corresponding notification obligations. Kettering Health provided written notice of this incident to individuals, and to your office, on behalf of KHCU on June 16, 2026.

The information that could have been subject to unauthorized access includes name, bank and/or financial account number.

Notice to Nebraska Resident

On January 30, 2026, Kettering Health began providing written notice of this incident to Nebraska residents. Kettering Health is now providing written notice to the remaining population related to KHCU, which was completed on June 16, 2026. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Kettering Health previously provided notice via a website posting and notice to Ohio media in the areas from which Kettering Health draws its patient population on July 21, 2025. Kettering will maintain its website posting for ninety-days subsequent to this final wave of notice.

Other Steps Taken and To Be Taken

Upon discovering the event, Kettering Health moved quickly to investigate and respond, assess the security of Kettering Health systems, and identify potentially affected individuals. Further, Kettering Health notified its primary federal regulator, the U.S. Department of Health and Human Services on July 21, 2025. Kettering Health is also working to implement additional safeguards and training to its employees. Kettering Health is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Kettering Health is providing impacted 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. Kettering Health is 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.

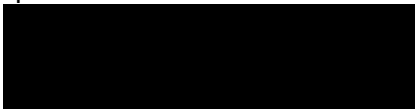
Kettering Health is providing written notice of this event to appropriate state regulators, and to the three major consumer reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

Kettering Adventist Credit Union
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



P



June 16, 2026

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [REDACTED]:

Kettering Health ("Kettering") is writing to notify you on behalf of KH Credit Union ("KHCU") of a recent data security event involving certain information related to you. KHCU is a financial institution providing services to employees, contractors, volunteers, affiliates and their families, within the Kettering healthcare system. Kettering is providing you with information about the event, its 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? On or about May 20, 2025, Kettering became aware of suspicious activity affecting certain systems within its network. We promptly 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 Kettering's environment between April 9, 2025, and May 20, 2025, and that certain files and folders within the network were potentially viewed and/or acquired without authorization during that time. We recently completed a time-intensive and comprehensive review of the files to determine whether any sensitive information could be involved and to whom it relates. That review identified a limited amount of data related to KHCU members, which resided on Kettering's network. It is important to note that this incident did not involve KHCU's network and was limited solely to Kettering.

What Information Was Affected? The potentially impacted information includes your full name and the following: bank and/or financial account number, medical billing and/or claims information, patient account number, Social Security number, and driver's license and/or state identification number.

What We Are Doing. 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 what information may be involved. We built upon existing cybersecurity practices and reviewed existing security policies to further protect against similar events moving forward. Kettering has also actively been working with federal law enforcement agencies throughout the incident. As part of our ongoing commitment to the privacy of information in our care, Kettering is reviewing policies, procedures and processes to reduce the likelihood of a similar future event.

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 twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

000010102G0500

P

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. Please note the enrollment deadline is September 12, 2026 and we are unable to enroll in these services for you, if you decide you would like these services.

For More Information. If you have additional questions, you may contact our toll-free dedicated assistance line at 1-844-784-5351, Monday through Friday, 8:00 AM - 8:00 PM Eastern Time, excluding U.S. holidays. You may also write to Kettering at 1 Prestige Place, Suite 580, Miamisburg, OH 45342.

Sincerely,

Joseph L. Feller
Chief Legal Officer
www.ketteringhealth.org

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:

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-resources/what-to-do-after-a-data-breach
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



00001020280000

P

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 Massachusetts residents, under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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 Oregon residents, you may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392.