WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

February 18, 2026

Jennifer S. Stegmaier
312.821.6167
jennifer.stegmaier@wilsonelser.com

Via Online Portal

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

Re: Notice of Cybersecurity Incident Involving represents ICM Properties, Inc.

Dear Attorney General Hilgers:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents ICM Properties, Inc. ("ICM Properties"), located at 3080 N. Lincoln Ave., Chicago, IL, 60657, with respect to a recent data security incident that may have resulted in unauthorized access to some individuals' personal information ("Incident"). ICM Properties take the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Nebraska residents being notified, and the steps that ICM Properties has taken in response to the Incident. We have also enclosed hereto a sample of the notification letter that to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On December 10, 2025, ICM became aware of suspicious activity within its network environment. Upon discovery of the incident, ICM promptly shut down our servers and workstations, contacted their IT vendor, and engaged a specialized cybersecurity firm to assist with securing their environment and to conduct a forensic investigation to determine the nature and scope of the incident. The forensic investigation concluded on or about January 5, 2026, and determined that unauthorized access to the ICM network occurred during a limited time window between December 9, 2025, and December 10, 2025.

Based on these findings, ICM conducted a comprehensive review of the affected files to identify the individuals potentially impacted by this incident and the types of information that may have been compromised. ICM completed its review and prepared the list of individuals to notify on February 2, 2026.

2. Number of State residents affected.

ICM Properties identified two (2) residents of Nebraska potentially affected by this Incident. Notification letters were mailed to these individuals on February 18, 2026, by United States Postal Service first-class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

Data privacy and security are among ICM Property's highest priorities, and it is committed to doing everything it can to protect the personal information in its care. Upon discovery of the Incident, ICM moved quickly and diligently to investigate, respond, and assess the security of its systems with the assistance of outside experts.

ICM has also taken additional steps to further enhance the security of our systems and data to reduce the risk of this type of incident from occurring in the future. Specifically, ICM has engaged external cybersecurity experts to further assess and strengthen its systems, enhance monitoring and access controls, and implement additional safeguards to protect personal information.

In addition, ICM Properties offered 12 months of complimentary credit monitoring and identity theft restoration services through Kroll to all affected individuals to help protect their identity. ICM Properties also provided guidance on how to better protect against identity theft and fraud, including providing 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 the contact details for the Federal Trade Commission.

4. Contact information

ICM Properties remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 312.821.6167 or jennifer.stegmaier@wilsonelser.com.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Jennifer S. Stegmaier

EXHIBIT A

Sample Individual Notice Letter

ICM PROPERTIES
Proudly Managing Apartments Since 1966

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

KROLL

SCAN TO ENROLL

<<Date>> (Format: Month Day, Year)

<<b2b_text_1 (Variable Header: Re: Notice of [Data Security Incident/Data Breach])>>

Dear <<First_name>> <<Last_name>>,

ICM Properties, Inc. ("ICM"), located at 3080 N. Lincoln Ave., Chicago, Illinois 60657, is writing to inform you of a recent data security incident that may have resulted in unauthorized access to some individuals' personal information ("Incident"). Below you will find information about what happened, the steps we are taking in response to the Incident, and additional resources and guidance to help you protect against the potential misuse of your information, if you feel it is appropriate.

What Happened?

On December 10, 2025, ICM became aware of suspicious activity within its network environment. Upon discovery of the incident, we promptly shut down our servers and workstations, contacted our IT vendor, and engaged a specialized cybersecurity firm to assist with securing our environment and to conduct a forensic investigation to determine the nature and scope of the incident. The forensic investigation concluded on or about January 5, 2026, and determined that unauthorized access to the ICM network occurred during a limited time window between December 9, 2025, and December 10, 2025.

Based on these findings, ICM conducted a comprehensive review of the affected files to identify the individuals potentially impacted by this incident and the types of information that may have been compromised. We completed our review and prepared the list of individuals to notify on February 2, 2026. We determined that some of your personal information may have been affected by this incident.

What Information Was Involved?

The personal information that may have been subject to unauthorized access includes: <<b2b_text_2 (Exposed Data Elements)>>.

What We Are Doing.

Data privacy and security are among our highest priorities, and we are committed to doing everything we can to protect the personal information in our care. Upon discovery of the Incident, ICM moved quickly and diligently to investigate, respond, and assess the security of its systems with the assistance of outside experts.

ICM has also taken additional steps to further enhance the security of our systems and data to reduce the risk of this type of incident from occurring in the future. Specifically, ICM has engaged external cybersecurity experts to further assess and strengthen our systems, enhance monitoring and access controls, and implement additional safeguards to protect personal information. We also notified the appropriate regulatory and law enforcement authorities, as applicable, and will cooperate fully with any related inquiries.

In addition, we are also 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 <<ServiceTermInMonths>> 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 event that you become a victim of fraud. These services will be provided through Kroll.

What You Can Do.

We encourage you to take advantage of the complimentary credit monitoring and identity theft protection we are making available to you. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

How do I enroll for the free services?

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<ServiceTerminMonths>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

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>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additionally, we encourage you to remain vigilant against incidents of identity theft and fraud, review your account statements, and monitor your credit reports for suspicious or unauthorized activity. Security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach, and then take recommended steps to protect your interests, including the possible placement of a free fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information* to learn more about how to protect against the possibility of information misuse.

For More Information.

If you have any questions or concerns not addressed in this notice, you may contact us by calling (844) 443-1425 (toll free) Monday through Friday, during the hours of 9:00 a.m. and 6:30 p.m. Eastern Standard Time (excluding U.S. national holidays). This resource will be available to you for 90 days after the date of this letter.

ICM sincerely regrets that this incident occurred and any inconvenience that it may cause and remains dedicated to ensuring the privacy and security of all information within our control.

Sincerely,

ICM Properties, Inc.

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed 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 a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. You can obtain further information on how to file such a complaint by way of the contact information listed above.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit-report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.