27777 Franklin Road, Suite 2500
Southfield, MI 48034-8214
Tel: 248.351.3000 | Fax: 248.351.3082
taftlaw.com

Jon Sriro
313.800.6502
jsriro@taftlaw.com

February 6, 2026

VIA E-MAIL AND U.S. MAIL

New Hampshire Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
DOJ-CPB@DOJ.NH.GOV

Re: Notice of Security Incident – Sun Communities, Inc.

To Whom It May Concern:

Pursuant to Section 359-C:20 of the New Hampshire Revised Statutes, I am providing notice of a security incident on behalf of our client, Sun Communities, Inc. ("Sun") located in Southfield, Michigan. An electronic copy of notice to affected New Hampshire residents is enclosed. As noted below, Sun is providing written notice to affected individuals via mail starting Friday, February 6, 2026.

Name and Contact Information of Person Reporting the Incident.

Jon Sriro, Esq., CIPP/US
Outside Counsel for Sun
Taft Stettinius & Hollister LLP
27777 Franklin Rd, Suite 2500
Southfield, MI 48034
(313) 800-6502
jsriro@taftlaw.com

A Description of the Incident.

On January 6, 2026, Sun first identified suspicious activity involving two user accounts of Sun personnel, which occurred on December 25, 2025, and January 5, 2026. The activity was traced to a social engineering scheme in which an unknown third party, posing as IT support, convinced two Sun users to complete a fraudulent multi-factor authentication

("MFA") setup, which enabled unauthorized access aligned with those users' existing system permissions. As part of this activity, the unauthorized party accessed certain Sun systems and exfiltrated data consistent with the limited access rights of those two user accounts (collectively the "Incident").

Upon learning of the Incident, Sun immediately activated its incident response procedures, shut down certain systems, restricted the compromised users' access, and worked with third-party forensics specialists to secure all systems and remediate further risks. Sun concluded its investigation on January 26, 2026. In addition to confirming the interference and disruption of some Sun information systems, Sun's investigation revealed the Incident resulted in the unauthorized access, viewing or removal of certain personal information and company data on some Sun file systems linked to the two compromised user accounts. Since that confirmation, Sun has analyzed impacted files to understand what personal information may be at risk and provide notice to individuals and authorities, as applicable.

The Number of New Hampshire Residents Affected by the Incident.

Sun's investigation identified three (3) individuals with a New Hampshire address that may have been impacted. In the event that Sun determines any additional New Hampshire residents are impacted, Sun shall update this notice accordingly.

The Steps Taken to Remedy the Incident**.**

Upon learning of the Incident, Sun followed its incident response procedures and engaged third-party forensic specialists to identify the scope of the Incident and to assist with securing its systems and data. Sun has taken steps to secure the affected accounts, prevent reuse of the compromised credentials, and enhance monitoring for similar activity. Sun has also reinforced security awareness with its personnel regarding social engineering and MFA-related requests through several communication channels. Sun continues to actively monitor its network and information systems for any unusual activity.

Additionally, Sun is taking all appropriate steps to protect personal information and is implementing its third-party forensics specialists' recommendations to strengthen Sun's administrative, technical, and physical safeguards to mitigate a recurrence of this type of incident in the future.

Sun is also providing complimentary credit monitoring and identity theft prevention services through Cyberscout, a TransUnion company.

Sample of the Notice Letter to Affected Parties.

A sample of the notice letter to be sent to the affected parties, including New Hampshire residents, and enrollment instructions for Cyberscout's credit monitoring, identity theft protection, and identity theft insurance is enclosed in this letter. These notice letters will be sent to individuals via U.S. mail beginning Friday, February 6, 2026.

Sincerely,

Taft Stettinius & Hollister LLP

Jon Sriro

Jon Sriro

JS
Attachment/Enclosure

Sun Communities, Inc.
c/o Cyberscout
<Return Address>
<City>, <State> <Zip>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<PostalCode+4>>

February 9, 2026

RE: NOTICE OF <<Custom Field 1>>

Dear <<FirstName>> <<LastName>>,

Sun Communities, Inc. ("Sun", "company," "we" or "our") takes the security and protection of your personal information seriously. This letter is in regard to an incident that Sun experienced involving the security of your personal information on our systems. Through the investigation of the security incident, unauthorized access or viewing of your personal information stored by the company may have occurred. Once aware of the incident, Sun quickly took steps to eliminate the threat of further unauthorized access, safeguarded the information in its possession, and conducted a forensics investigation to determine the scope of the incident. Sun is providing this letter to you out of an abundance of caution and to provide you information about the incident, our response to it and what you can do to remain vigilant and protect your personal information.

While we have no evidence that any of your personal information was compromised or misused in any manner, we are taking appropriate precautionary measures to ensure your financial security and help alleviate concerns you may have.

What is Sun doing to address this situation?

Sun has made immediate enhancements to our systems, security and practices.

In response to the incident, 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 <<service length>> 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. We are also 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 and a **$1 million identity theft insurance policy**. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free 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: **<UNIQUE CODE>** 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.

What Information Was Involved. At this time, we cannot definitively state whether your particular personal information was impacted due to the Incident or to what extent. We can only confirm that access, viewing and removal of certain personal information occurred, which may include, among other personal information, some or all the following:

First and last name	Address	Date of birth
Driver's license/Passport number/National ID	Financial account information (e.g., bank account numbers, routing numbers)	Social Security number

What You Can Do. While we have received no reports or indications of such activity at this time, the risks related to the unauthorized use of a Social Security number and other personal information may include identity theft, financial fraud, and tax fraud. Please be vigilant about monitoring your personally identifiable information, particularly your credit report information and financial accounts, to protect against fraudulent activity. Please also pay attention when submitting tax returns to protect against possible fraudulent submissions made on your behalf.

If you are concerned about identity theft, you may also contact local law enforcement and file a police report. You can contact your state's Attorney General, as well as the Federal Trade Commission or one of the credit bureaus listed below for more information about how to protect your identity.

For More Information. You can place an identity theft/fraud alert, get credit freeze information for your state, or order a free credit report by calling any of the following credit reporting agencies at one of the phone numbers listed below or visiting their respective websites. In some cases, fees may apply.

Equifax - 1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374
https://www.equifax.com/personal/credit-report-services/

Experian - 1-888-397-3742
P.O. Box 4500
Allen, TX 75013
https://www.experian.com/help/

TransUnion - 1-877-322-8228
P.O. Box 2000
Chester, PA 19016
https://www.transunion.com/credit-help

Credit Reports. You can request credit reports from all three credit bureaus be sent to you free of charge. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Periodically checking your credit reports can help you spot problems and address them quickly.

Fraud Alerts. You can place a fraud alert with the credit bureaus free of charge. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus to place an alert. As soon as one credit bureau confirms your fraud alert, the

others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Security Freeze. Under state law, a security freeze (or a credit freeze) prohibits a credit bureau from releasing any information from a consumer's credit report without written authorization. There is no fee associated with freezing or thawing your credit. The process of freezing your credit takes only a few minutes. You must contact each credit bureau individually to freeze your credit with each bureau. To place a security freeze, you may need to provide the following information:

1. Your full name;
2. Social Security number;
3. Date of birth;
4. Mobile number;
5. Current postal address;
6. Email address; and
7. Any other information that the Credit Bureau may require.

The credit bureaus have one (1) business day after your request to place a security freeze if made by telephone or secure electronic means. If the request is made by mail, the credit bureaus have three (3) business days. The credit bureaus must also send written confirmation to you within five (5) business days.

To lift the security freeze, in order to allow a specific entity or individual access to your credit report, you must apply online, call, or send a written request to the credit bureaus by mail. When you contact a credit bureau to lift the security freeze, you will need to include proper identification (name, address, and Social Security number) and the PIN number or password that was provided to you (if provided) when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. If you request a credit thaw online or by phone, the credit bureaus are required by law to complete the request within one (1) hour. If you request the thaw by regular mail, the credit bureaus have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

The Federal Trade Commission (FTC) provides more information about how to protect your identity at either https://www.ftc.gov/ or https://www.identitytheft.gov/. You may also find additional information on any applicable rights under the Fair Credit Reporting Act. You can also contact the FTC by using the information below.

Federal Trade Commission - 1-877-438-4338
Bureau of Consumer Protection
600 Pennsylvania Avenue, NW
Washington, DC 20580

For District of Columbia Residents:	For Maryland Residents:
You may also contact the Attorney General for the District of Columbia for more information about how to protect your identity by using the information below: Attorney General's Office 400 6th Street, NW Washington, DC 20001 Phone: (202) 727-3400 Website: https://oag.dc.gov/	You may also contact the Maryland Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office 200 St. Paul Place Baltimore, MD 21202 Phone: 410-528-8662 Website: https://www.marylandattorneygeneral.gov/

For New York Residents: You may also contact the New York Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office Toll Free Phone Number: (800) 771-7755 Website: https://ag.ny.gov/	For North Carolina Residents: You may also contact the North Carolina Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001 Toll Free in NC: 1-877-566-7226 Outside NC: 919-716-6000 Website: https://ncdoj.gov/
For Oregon Residents: You can contact the Oregon Attorney General at: Oregon Department of Justice 1162 Court Street NE Salem, OR 97301-4096 Toll Free Phone Number: (877) 877- 9392 Website: www.doj.state.or.us.	For Rhode Island Residents: You may also contact the Rhode Island Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office Phone Number: (401) 274-4400 Website: http://www.riag.ri.gov/

What if I want to speak with OUR COMPANY regarding this incident?

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at **1-800-405-6108** and supply the fraud specialist with your unique code listed above.

We sincerely apologize for any inconvenience that has been caused by this Incident. If you have any questions, please contact us at:

Address: Sun Communities, Inc.
27777 Franklin Road
Suite 300
Southfield, MI 48034

Sincerely,

Sun Communities, Inc.