



Atlanta, GA  
Charleston, SC  
Charlotte, NC  
Columbia, SC  
Greenville, SC  
Raleigh, NC  
Spartanburg, SC  
Washington, DC

March 5, 2024

**Via E-mail (DOJ-CPB@doj.nh.gov)**

Attorney General John Formella  
Office of the Attorney General  
Consumer Protection Bureau  
33 Capitol Street  
Concord, NH 03301

**Re: NALS Apartment Homes LLC - Notice of Data Event**

To Whom It May Concern:

We represent NALS Apartment Homes LLC ("NALS"), located at 920 Garden Street, Santa Barbara, California 93101, and are writing to notify you of an event that may affect the security of certain personal information relating to approximately 2 New Hampshire residents. By providing this notice, NALS does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On December 2, 2023, NALS became aware of suspicious activity within its server environment. Upon becoming aware of the incident, NALS immediately shut down access to its systems in order to secure its environment. NALS commenced an investigation with the assistance of third-party professionals and notified law enforcement in an effort to determine the nature and scope of the event. Through the investigation, it was determined that there was unauthorized access to the NALS network on or before December 2, 2023. The investigation determined that the unauthorized actor acquired certain files and folders within NALS' system during that period of access. NALS undertook a review of the information contained on its systems to determine the type of information contained within its files and to whom the information related. On February 16, 2024, NALS completed the review and identified contact information to notify potentially impacted individuals about the event.

The information that could have been subject to unauthorized access includes

### **Notice to New Hampshire Residents**

On or about March 5, 2024, NALS provided written notice of this event to approximately 2 New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached as ***Exhibit A***.

### **Other Steps Taken and to Be Taken**

NALS has forced all users to change their passwords, has implemented multi-factor authentication, has replaced every potentially compromised endpoint machine on its system, has revised some of its policies, is upgrading its firewall, and is working to implement additional safeguards and training for its employees. NALS is currently rolling out KnowBe4 security training for employees. NALS also plans to remove unnecessary sensitive personal information from its system.

Furthermore, NALS is providing access to \_\_\_\_\_ of credit monitoring services through Kroll at no cost to individuals whose personal information was potentially affected by this event. The identity monitoring services include Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. NALS is also establishing a call center to address questions regarding the event.

Additionally, NALS is providing impacted individuals with guidance on how to better protect against identity theft and fraud. NALS is providing potentially affected 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 and law enforcement to report attempted or actual identity theft and fraud.

NALS is also providing written notice of this event to relevant government agencies, as necessary, and to the three major credit reporting agencies: Equifax, Experian, and TransUnion.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please do not hesitate to contact me.

Sincerely,

Sarah Fulton Hutchins

SFH:ark  
Enclosure

# EXHIBIT A

NALS Apartment Homes, LLC.

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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

Re: NOTICE OF DATA BREACH

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>:

We are writing to notify you of a recent event that may have impacted your personal information. We are providing you with further information about the event, our response to it, and resources available to help protect your information, should you feel it appropriate to do so.

**What Happened?**

On December 2, 2023, NALS Apartment Homes became aware of suspicious activity within our server environment. Upon becoming aware of the incident, we immediately shut down access to our systems in order to secure our environment. We commenced an investigation with the assistance of third-party professionals and notified law enforcement in an effort to determine the nature and scope of the event. Through the investigation, it was determined that there was unauthorized access to the NALS network on or before December 2, 2023. The investigation determined that the unauthorized actor acquired certain files and folders within our system during that period of access. We undertook a review of the information contained on our systems to determine the type of information contained within our files and to whom the information related. On February 16, 2024, we completed the review and identified contact information to notify potentially impacted individuals about the event.

**What Information Was Involved?**

Based on our investigation, we understand that your \_\_\_\_\_ may have been accessed and/or acquired by the unauthorized third party.

**What We Are Doing**

We at NALS take this event and the security of your information seriously. Upon learning of the incident, we moved quickly to investigate and respond to the event, assess the security of our systems, restore functionality to our environment, and notify potentially affected individuals. As a part of our ongoing, commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional administrative and technical safeguards to further secure the information on our systems.

As an added precaution, we have secured the services of Kroll to provide identity monitoring at no cost to you for \_\_\_\_\_. Your identity monitoring services include Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. Additional information describing these services is included in this letter below. To activate these services, please take the following steps:

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>>

**What You Can Do**

It is always advisable to review and monitor your account(s) for suspicious activity. If you discover any suspicious or unusual activity on any of your accounts, we recommend that you promptly change your password and take any additional steps to protect your account. We also recommend that you notify your financial institution or other third-party company if applicable.

**For More Information**

We understand the concern and inconvenience this situation may cause; if you have questions, please feel free to call (866) 495-2646, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time (excluding major bank holidays). You can also write to NALS at [care@nals.com](mailto:care@nals.com) or to 920 Garden Street, Santa Barbara, California 93101 for additional assistance.

Sincerely,

NALS Apartment Homes, LLC.

## **Description of Monitoring Services**

**You have been provided with access to the following services from Kroll:**

### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

### **Web Watcher**

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

### **\$1 Million Identity Fraud Loss Reimbursement**

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

### **Additional Ways to Protect Your Identity:**

You may wish to take additional steps to protect your identity. Here are some you may consider:

### **Reviewing Your Accounts and Credit Reports**

Regulators recommend that you be especially vigilant for the next 12 to 24 months and that you promptly report incidents of suspected identity theft to your financial institution. As part of staying vigilant, you should regularly review your account statements, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

<b>Equifax</b> 1-800-525-6285 Equifax.com Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	<b>Experian</b> 1-888-397-3742 Experian.com Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	<b>TransUnion</b> 1-800-680-7289 Transunion.com TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094
---	---	--

You can obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at [www.annualcreditreport.com](http://www.annualcreditreport.com). You may also obtain a free report by calling toll free 1-877-322- 8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

### **Placing a Fraud Alert**

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

## **Requesting a Security Freeze on Your Credit Report**

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze, and should be careful to record it somewhere secure.

## **Suggestions if You Are a Victim of Identity Theft**

If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

**File a Police Report.** Get a copy of the report to submit to your creditors and others that may require proof of a crime.

**Contact the U.S. Federal Trade Commission (FTC).** The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at [www.IdentityTheft.gov](http://www.IdentityTheft.gov). You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of *Identity Theft: A Recovery Plan*, a guide from the FTC to help you guard against and deal with identity theft. It is available online at [https://www.bulkorder.ftc.gov/system/files/publications/501a\\_idt\\_a\\_recovery\\_plan\\_508.pdf](https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf).

**Exercise Your Rights Under the Fair Credit Reporting Act (FCRA).** You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

**Keep a record of your contacts.** Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

## **Special Information for Residents of the District of Columbia, Iowa, Maryland, Massachusetts, New Mexico, New York, North Carolina, Oregon, Rhode Island, and Vermont.-**

District of Columbia residents can learn more about preventing identity theft from the District of Columbia Office of the Attorney General, by visiting their website at <https://oag.dc.gov>, calling 1.202.727.3400, or requesting more information via email [oag@dc.gov](mailto:oag@dc.gov) or mail 400 6th Street NW, Washington DC 20001.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov), calling 1.515.281.5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <http://www.marylandattorneygeneral.gov>, calling the Identity Theft Unit at 1.410.576.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 25<sup>th</sup> Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to its honoring your request.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

New York residents may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 1.800.771.7755.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at <https://ncdoj.gov/protecting-consumers/protecting-your-identity>; calling 1.919.716.6400, 1.877.566.7226, or 1.919.716.6000; or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at [www.doj.state.or.us](http://www.doj.state.or.us), calling 1.503.378.4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by visiting the website at <https://riag.ri.gov>, by phone at 1.401.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at <https://ago.vermont.gov/cap/scam-prevention-through-awareness-and-education/identity-theft>.