



MULLEN  
COUGHLIN<sup>LLC</sup>  
ATTORNEYS AT LAW

RECEIVED

AUG 13 2021

CONSUMER PROTECTION  
1127 High Ridge Road, #301  
Stamford, CT 06905

Gregory J. Bautista  
Office: (267) 930-1509  
Fax: (267) 930-4771  
Email: [gbautista@mullen.law](mailto:gbautista@mullen.law)

August 4, 2021

**VIA U.S. MAIL**

Consumer Protection Bureau  
Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Beacon Communities, LLC (“Beacon”) located at Two Center Plaza Suite 700, Boston, MA 02108, and are writing to notify your office of an incident that may affect the security of some personal information relating to twenty (20) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Beacon 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 7, 2020, Beacon became aware of unusual activity in employee e-mail accounts. In response, Beacon took steps to secure the mailboxes, and began working with a third-party forensic specialist firm to investigate the nature and scope of the incident. The investigation determined that there was unauthorized access by an unknown individual to some employee e-mail accounts between September 28, 2020 and December 23, 2020. The investigation, however, was not able to identify access to any particular email or attachment. Following this determination, Beacon undertook an in-depth, lengthy, and labor-intensive process to identify whether sensitive information may have been contained within the e-mail accounts at issue, identify the individuals whose information may have been impacted, and review internal Beacon records to identify address information for impacted individuals. This review completed on June 30, 2021. The information that could have been subject to unauthorized access includes name, address, Social Security number, Driver's License or State Issued ID Number, and Financial Account Information.

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

On or about August 4, 2021, Beacon provided written notice of this incident to all affected individuals, which includes twenty (20) New Hampshire 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**

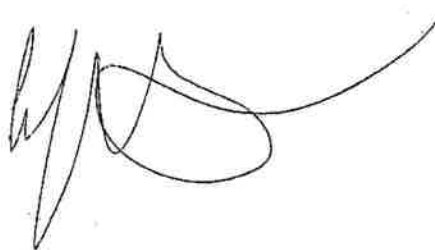
Upon discovering the event, Beacon moved quickly to investigate and respond to the incident, assess the security of Beacon systems, and notify potentially affected individuals. Beacon is also working to implement additional safeguards and training to its employees. Beacon is providing access to credit monitoring services for twelve (12) months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Beacon 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 to their credit card company and/or bank. Beacon is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

A handwritten signature in black ink, appearing to read 'GJB', with a long, sweeping horizontal line extending to the right.

Gregory J. Bautista of  
MULLEN COUGHLIN LLC

# EXHIBIT A



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

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

<<b2b\_text\_2(Variable Text)>>

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

Beacon Communities LLC (“Beacon”) is writing to inform you, out of an abundance of caution, of a recent incident that may have involved some of your personal information. We want to provide you with an overview of the incident, our response thus far, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it necessary. While we do not currently have any reason to believe that any identity theft has occurred, we nonetheless want to keep you informed.

**What Happened?** On December 7, 2020, Beacon became aware of unusual activity in employee e-mail accounts. In response, Beacon took steps to secure the mailboxes, and began working with a third-party forensic specialist firm to investigate the nature and scope of the incident. The investigation determined that there was unauthorized access by an unknown individual to some employee e-mail accounts between September 28, 2020 and December 23, 2020. The investigation, however, was not able to identify access to any particular email or attachment.

Following this determination, we undertook an in-depth, lengthy, and labor-intensive process to identify whether sensitive information may have been contained within the e-mail accounts at issue, identify the individuals whose information may have been impacted, and review internal Beacon records to identify address information for impacted individuals. This review completed on June 30, 2021. Beacon is notifying you out of an abundance of caution because the investigation determined that certain information relating to you may have been in the email accounts.

**What Information Was Involved?** The following information about you was present within the employees’ email accounts: <<b2b\_text\_1(Impacted Data)>>. There is no indication that your information was subject to actual or attempted misuse.

**What We Are Doing.** We take this incident and the security of information within our care very seriously. In addition to the steps described above, as part of our ongoing commitment to the privacy of personal information in our care, we are undertaking a review of our existing policies, procedures, and training programs and we implemented additional safeguards to further secure the information in our systems.

As an added precaution, we are also offering twelve (12) months of complimentary access to identity monitoring services. Individuals who wish to receive these services must activate by following the attached activation instructions.

**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. You can find out more about how to help protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Help Protect Your Personal Information*. There you will also find more information on the identity monitoring services we are offering and how to activate.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 1-855-545-2014 8:00 a.m. to 5:30 p.m. Monday through Friday excluding major U.S. holidays.

Sincerely,

A handwritten signature in black ink, appearing to read 'Samuel Ross', with a stylized flourish at the end.

Samuel Ross  
Chief Operating Officer  
Beacon Communities LLC

## STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

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 one year. 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, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

*You have until **October 24, 2021** to activate your identity monitoring services.*

Membership Number: <<Membership Number s\_n>>



### TAKE ADVANTAGE OF YOUR IDENTITY 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.

#### **Public Persona**

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

#### **Quick Cash Scan**

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

#### **\$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.

## **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 your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

## **Additional Information**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your 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 6<sup>th</sup> Street, NW, Washington, D.C. 20001; 202-727-3400; and [oag@dc.gov](mailto:oag@dc.gov).

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and [www.oag.state.md.us](http://www.oag.state.md.us).

*For New Mexico residents*, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You 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 you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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](http://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](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 16 Rhode Island residents impacted by this incident.

2021 MAR 15 PM 1:58  
STATE OF RHODE ISLAND  
DIVISION OF