MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

August 9, 2019

VIA U.S. MAIL

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

Re: Notice of Data Incident

Dear Attorney General MacDonald:

We represent Brixmor Property Group ("Brixmor"), 450 Lexington Avenue, Floor 13, New York, NY 10017 and are writing to notify your office of an incident that may affect the security of personal information relating to a New Hampshire resident. The investigation into this matter is ongoing, and this notice may be supplemented if new significant facts are learned subsequent to its submission. By providing this notice, Brixmor 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.

Background

Brixmor recently learned of an unauthorized login by a third party to a limited number of Brixmor employee email accounts. Brixmor immediately changed the employees' credentials and launched an internal investigation to determine the full nature and scope of this incident. A forensic investigation firm was retained to assist with Brixmor's investigation. On June 14, 2019, the investigation confirmed that an unauthorized actor logged in to the impacted accounts one time on May 26, 2019 for a very limited period of time.

The emails and attachments contained within the impacted email accounts were programmatically and manually reviewed as the investigation was unable to determine which emails or attachments, if any were accessed or viewed. On July 9, 2019 Brixmor determined what information was

accessible within the accounts and to whom that information related. Over the following weeks, Brixmor obtained contact information for all impacted individuals.

Notice to New Hampshire Resident

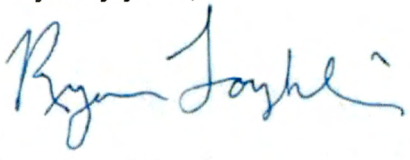
On September 9, 2019, Brixmor began mailing written notice of this incident to the individuals whose information was accessible within the email accounts, which includes approximately one (1) New Hampshire resident. Notice was mailed in substantially the same form as the letter attached hereto as ***Exhibit A***.

Brixmor is providing those individuals whose information was accessible within the email accounts access to one year of credit monitoring through TransUnion. Additionally, Brixmor is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including 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. Brixmor is also providing written notice of this incident to other state regulators as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4786.

Very truly yours,



Ryan Loughlin of
MULLEN COUGHLIN LLC

RCL/vfr
Enclosures

EXHIBIT A

BRIXMOR
Property Group

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

Brixmor Property Group ("Brixmor") is writing to inform you of a recent event that may impact the privacy of some of your personal information. We wanted to provide you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it necessary to do so.

We recently learned of an unauthorized login by a third party to a limited number of Brixmor employee email accounts. We immediately changed the login credentials of all impacted employees and launched an internal investigation to determine the full nature and scope of the incident. Shortly thereafter, a third-party forensic investigation firm was retained to assist with Brixmor's investigation. On June 14, 2019, the investigation confirmed that an unauthorized actor logged in to the impacted accounts one time on May 26, 2019.

On July 9, 2019, we confirmed that information relating to you was included in the impacted email accounts. The investigation confirmed that the specific account that contained information relating to you was accessed on only one date for a very limited period of time. The investigation is not able to determine if the information related to you was accessed or viewed. However, we are notifying you of this event out of an abundance of caution.

The following information may have been accessible within the impacted employees' email accounts: your name and <<Data Elements1>>. To date, the investigation has found no evidence that any of this information has been subject to actual or attempted misuse.

We take this incident and the security of personal information on our computer systems very seriously. Upon discovery of this incident, we immediately took steps to secure the email accounts impacted and we launched an in-depth investigation with the assistance of a third-party forensic investigation firm to determine the nature and scope of this incident. We have also notified regulatory authorities, as required by law.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<Data Elements2>> months provided by TransUnion Interactive. To enroll in this service, go to the *my*TrueIdentity website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<Engagement Number>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain <<Data Elements2>> months of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can learn more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud.*

We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 855-964-0523, Monday through Friday from 9:00 am to 9:00 pm ET. You may also write to Brixmor at: 450 Lexington Avenue, Floor 13, New York, NY 10017.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

Kristina Angus
VP, Risk Management & Counsel
Brixmor Property Group

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus, listed below, directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security freeze to control 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

If you identify any fraudulent or suspicious charges on your credit or debit card, you should immediately contact the issuing bank or financial institution. It is also good practice to remain vigilant of unsolicited communications seeking your credit card or other financial information. Incidents of identity theft should also be reported to your local law enforcement.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the aforementioned consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached 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 have

the right to file a police report if you experience or suspect identity theft or fraud. Please note that 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 your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, 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 agencies 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 violators. 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, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.
For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-274-4400. There is one (1) Rhode Island resident affected by this event. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident.