GOODWIN | PROCTER

April 1, 2015

VIA CERTIFIED MAIL

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Sir or Madam:

We write on behalf of Essex Property Trust, Inc. ("Essex") regarding Essex's recent report that certain of its computer networks containing personal information had been compromised by a cyber-intrusion. Essex took immediate steps to contain the intrusion and secure its systems. As a result of the incident, and as a precautionary measure during the pendency of the investigation, in October 2014 Essex provided notice and credit-monitoring services to its current residents and employees. At the time that notice was provided, Essex had no evidence that any individual's personal information had been accessed or acquired by an unauthorized person.

Since this initial notice was sent, Essex has continued to investigate the incident and determined that one (1) New Hampshire resident's personal information was stored on the affected systems. While Essex still has no evidence that the New Hampshire resident's personal information was accessed or acquired by an unauthorized person, Essex is notifying and providing credit-monitoring services to all persons whose Social Security or driver's license numbers were stored on affected Essex systems. Essex plans to mail all of its notices over the five business day period from March 19 to March 26.

I am enclosing a sample copy of the notice sent to the New Hampshire resident. By providing this notice, Essex does not waive any rights or defenses regarding the applicability of

GOODWIN | PROCTER

[redacted]

[redacted]

New Hampshire law, personal jurisdiction, or the applicability of the New Hampshire data incident notification statute. Please contact me if you have any questions.

Sincerely,

Gerard M. Stegmaier

ESSEX
PROPERTY TRUST, INC.
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

00001
ACD1234
00-ACIDLT1E-3

April 2, 2015

Re: **IMPORTANT NOTICE ABOUT ESSEX DATA INCIDENT**

Dear John Sample,

We are writing to you regarding the cyber attack that affected some of Essex's computer networks. As we shared in our September 29, 2014 public announcement, after detecting unusual activity on the Essex systems, we launched an immediate investigation and took steps to assess and contain the network intrusion and secure our systems. We retained independent forensic computer experts to analyze the impacted data systems and consulted with law enforcement. While we have confirmed that evidence exists of exfiltration of data on company systems, the precise nature of the data has not been identified. Based on our investigation, we believe that certain systems were affected as early as August 13, 2013, and until Essex secured its systems on September 25, 2014.

We understand that security and privacy of personal information is important. At this time we have no evidence that any personal information has been misused. However, we have determined that some of your information was hosted on our affected systems, including your: **First and last name and Social Security number.**

Although we have no evidence that any personal information has been misused, as a precaution, we are informing you of this incident to help safeguard you from potential misuse of your personal information and to recommend ways for you to protect yourself. **Essex is also offering complimentary identity theft protection services from AllClear ID for 12 months, at no charge to you, starting from the date of this letter. More details about these services are enclosed with this letter.**

As always, we recommend that you remain vigilant for incidents of fraud and identity theft, including by regularly viewing your account activity and monitoring your credit reports. While we do not expect any additional information to be uncovered, we will update you if information relevant to you is discovered. For more information on how you can help protect yourself, please review the enclosed *Steps You Can Take to Protect Yourself From Identity Theft.*

01-03-1-00

Thank you for working with us to protect your personal information. If you have any questions or concerns, please call 1-855-398-6434.

Sincerely,

Michael J. Schall
President and CEO
Essex Property Trust, Inc.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. This protection is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-398-6434 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear ID maintains an A+ rating at the Better Business Bureau.

AllClear PRO: This service offers additional layers of protection including credit monitoring. For a child under 18 years old, AllClear ID ChildScan identifies fraud by searching various databases for evidence of misuse of the child's information. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-398-6434 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts.

Key features of the AllClear SECURE with PRO Plan are:

- **Identity Repair:** AllClear ID investigators will work to resolve any harm that comes to affected individuals in resolving financial identity theft cases.
- **Identity Theft Monitoring:** Alerts consumers when stolen identity information is detected and reported to AllClear ID. This service is in partnership with the National Cyber-Forensics & Training Alliance (NCFTA) and IFA.
- **Lost Wallet Protection:** Licensed fraud investigators expedite cancelling and replacing credit and debit cards if a customer's wallet is lost or stolen.
- **$1M Identity Theft Insurance:** Zero deductible policy provides reimbursement of certain fees, lost wages, and fraud losses related to recovering an identity.
- **Credit Monitoring:** Alerts consumers of important changes to their credit file.
- **Child Identity Protection:** Scans databases to find out if thieves are using a child's Social Security number and repairs the child's identity if any issues are discovered.

Steps You Can Take to Protect Yourself From Identity Theft

1. Review your account statements and credit reports and notify law enforcement and Essex of suspicious activity.

Even if you do not feel the need to register for a credit monitoring service, as a precautionary measure, we recommend that you regularly review statements from your bank, credit card, and other accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1.877.322.8228, or by mailing an 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 by contacting one or more of the three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 9532	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com
1.888.766.0008	1.888.397.3742	1.800.680.7289

When you receive your credit reports, look them over carefully. Look for accounts that you did not open and/or inquiries from creditors that you did not initiate. Also check to see if your personal information on the credit report is accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend that you remain vigilant in your review of your account activities and credit reports. You should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement and/or the Federal Trade Commission. A copy of a police report may be required by creditors to clear up your records.

2. Consider placing a fraud alert or a credit freeze on your credit files.

If you suspect that you may be a victim of identity theft, consider placing a fraud alert or a security freeze (also called a credit freeze) on your credit file. Security freeze laws vary from state to state. For more information about fraud alerts and security freezes, please see the Federal Trade Commission's guidance at http://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes.

3. Protect your passwords.

You can minimize the threat of identity theft by improving your password practices. Use different passwords for all your accounts. Make those passwords strong with at least eight characters, including a mix of letters, numbers, and symbols ($%#!*@). Change your passwords from time to time. For additional guidance on passwords and securing your accounts, see http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/passwords-and-securing-your-accounts.

4. Fight "phishing" — don't take the bait.

Scam artists "phish" for victims by pretending to be banks, stores, government agencies, or other trusted sources. They do this over the phone, by email, and by postal mail. Do not respond to any request to verify your account number or password. Legitimate companies do not request this kind of information in this way. If an email looks suspicious, don't click on any links in that email.

5. Learn more about how to protect yourself from identity theft.

You may wish to review the Federal Trade Commission's guidance on how consumers can protect themselves against identity theft. For more information contact the **Federal Trade Commission** at:

600 Pennsylvania Avenue NW
Washington, DC 20580
www.ftc.gov/idtheft
1.877.ID.THEFT (1.877.438.4338)