



PUBLIC STORAGE, INC.

701 Western Avenue
Glendale, CA 91201-2349
Tel (818) 244-8080

January 29, 2007

New York State Consumer Protection Board
5 Empire State Plaza, Suite 2101
Albany, New York 12223

Dear Sir/Madam:

Public Storage has reason to believe that someone recently gained unauthorized access to certain electronic company personnel files located at the corporate headquarters for Public Storage in Glendale, California. These personnel files include substantially all active employees, and include data such as Social Security numbers, dates of birth, home addresses, and other information as summarized in the attached notices. One Hundred, Eighty-Eight of these employees are residents of New York.

Public Storage has no evidence at this time that any personal information has been misused. Public Storage has already contacted local law enforcement officials and the three principal reporting bureaus.

Public Storage discovered the breach on or about December 11, 2006 and provided the enclosed letter by email to all affected employees on or about December 22, 2006. Public Storage followed up with the addendum notice, also enclosed, which provides more information and offers credit monitoring to affected employees on or about January 24, 2007.

Should you have any questions about this incident, please contact Ammar Kharouf at (818) 244-8080 ext. 1450.

Sincerely,

Ammar Kharouf
Vice President and Litigation Counsel

Enclosure



701 Western Ave., Glendale, CA 91201
818.244.8080 ■ www.publicstorage.com

January 24, 2007

Update to Important Notice Regarding Your Personal Information

Dear Fellow Public Storage Employee:

Attached is a copy of a letter regarding a possible incident of unauthorized access to company electronic personnel files that was sent to active employees by email on December 22, 2006. You should read this letter carefully if you have not already done so. We continue to monitor the situation and still have no evidence that any information has been misused.

As stated in the attached letter, the electronic files of substantially all active employees are potentially affected. In addition to the information specifically mentioned in the attached letter, these files may include dependent names and social security numbers, for whom we do not have contact information. We recommend that employees with such dependent information in their personnel files take the same steps to protect that information as recommended in the attached letter for employee information.

Personnel files generally contain pre-employment information (which may include applications, credit reports, offer letter information, employee numbers, employee relations information, performance evaluation information, payroll information (such as W-4 forms and direct deposit forms) and benefits information (such as health enrollment forms, company group insurance information, leave of absence forms, disability documentation, and beneficiary designation forms). In addition, the personnel file of any given employee may contain information unique to that employee that is not listed above or in the attached letter. If you have any questions, please call the hotline we have established at **1 (877) 682-6937** so that we may address them.

We regret this unfortunate situation. To help you through this process, we would like to offer a free credit monitoring service for up to one year, if you choose to access it. Please contact us at the toll-free number above if you would like enrollment information.

Enclosure



PUBLIC STORAGE, INC.

701 Western Avenue
Glendale, CA 91201-2349

Tel: (818) 244-8080

December 22, 2006

Important Notice Regarding Your Personal Information

Dear Fellow Public Storage Employees:

Public Storage has reason to believe that someone recently gained unauthorized access to certain electronic company personnel files. These personnel files include substantially all active employees, with data such as Social Security numbers, dates of birth, home addresses, and other contact information. The information also contains bank information for employees who have direct deposit accounts.

We have no evidence at this time that any employee's personal information has been misused. Nevertheless, the security of your private information is very important to us and because it is possible that your confidential information may have been unlawfully accessed, we are writing so that you may take steps to protect yourself from fraud and identity theft.

As a precaution, we recommend that you place a fraud alert on your consumer credit file. By doing so, you let potential creditors know to look for unusual or suspicious activity. We also recommend that you monitor credit card and bank card statements and bank account information for unusual or suspicious activity, especially for those employees whose pay is directly deposited to their bank accounts.

Specific information about how to take the above steps and protect your credit lines and financial information is enclosed with this letter. ***Please review it closely.*** Because of the increasing number of incidents of identity theft in the United States, the Federal Trade Commission (the "FTC") has made available excellent advice on how you can protect yourself against such frauds. We recommend that you review the identity theft materials posted for consumers on the FTC's Web site, www.consumer.gov/idtheft/ and particularly, the posted copy of the FTC's booklet, *"Take Charge: Fighting Back Against Identity Theft."*

Law enforcement officials have been contacted and we will continue to investigate and closely monitor the situation. We have also contacted the three principal credit reporting bureaus, Equifax, Experian and TransUnion, to advise them of the situation.

Public Storage takes data security very seriously and endeavors to provide employees with the highest levels of protection. To this end, we are reaching out right away to

Steps to take to protect your credit and identity

Should you ever believe your identity has been stolen or that you are at risk of having your identity stolen, you can follow the Federal Trade Commission's ("FTC's") guidelines on protecting yourself against identity theft. The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them.

You may wish to consider placing a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing credit accounts. Because creditors seek additional verification from you when a fraud alert is in place on your credit file, one effect of the fraud alert is that it slows the processing time for opening new accounts and making changes on your existing accounts.

To place a fraud alert on your credit file, call any one of the three major credit bureaus. As soon as one credit bureau processes your fraud alert, it will notify the other credit bureaus on your behalf to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax
1 (800) 525-6285

Experian
1 (888) 397-3742

TransUnionCorp
1 (800) 680-7289

Moreover, you should review credit, bank card, and bank account information as soon as possible to review your accounts for unauthorized charges or transactions. If there are unauthorized charges or if you otherwise believe that your information is being used by an unauthorized person, you should immediately inform your card issuer and/or bank on the phone and in writing. You should also request that your current account be closed and a new account opened in your name.

Even if you do not initially find any suspicious activity on your card accounts, credit reports and/or bank statements, the FTC recommends that you check your credit reports, card charges and financial statements regularly. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports, card charges and financial statements periodically can help you spot problems and address them quickly. Once a year you can obtain a free credit report by calling **1 (877) 322-8228** or going online to www.annualcreditreport.com.

If you find suspicious activity on your accounts or have reason to believe that your personal information is being misused, please contact us at **1 (877) 682-6937** because it may be necessary for you to file a police report and obtain a copy of that police report. Many creditors require the information the police report contains to absolve you of the fraudulent debts.

You may also want to file a complaint with the FTC, which will be logged into its database of identity theft cases used by law enforcement agencies for investigations. To get free information or file a complaint with the FTC, you may call the FTC at **1 (877) 382-4357**, or use the complaint form at <http://www.consumer.gov/idtheft/>.