



Dear Sir or Madam:

Sony Pictures Entertainment (“SPE”) is writing to provide you with information about a significant system disruption SPE experienced on Monday, November 24, 2014.

SPE has determined that the cause of the disruption was a brazen cyber attack. After identifying the disruption, SPE took prompt action to contain the cyber attack, engaged recognized security consultants and contacted law enforcement.

SPE learned on December 1, 2014, that the security of personally identifiable information that SPE received about you and/or your dependents during the course of your current or prior employment with SPE potentially may have been compromised as a result of such brazen cyber attack. Although SPE is in the process of investigating the scope of the cyber attack, SPE believes that the following types of personally identifiable information that you provided to SPE may have been obtained by unauthorized individuals: (i) name, (ii) address, (iii) social security number, driver’s license number, passport number, and/or other government identifier, (iv) bank account information, (v) credit card information for corporate travel and expense, (vi) username and passwords, (vii) compensation and (viii) other employment related information. In addition, unauthorized individuals may have obtained (ix) HIPAA protected health information, such as name, social security number, claims appeals information you submitted to SPE (including diagnosis), date of birth, home address, and member ID number to the extent that you and/or your dependents participated in SPE health plans, and (x) health/medical information that you provided to SPE outside of SPE health plans.

SPE has made arrangements with a third-party service provider, AllClear ID, to offer potentially impacted current and former employees and dependents twelve (12) months of identity protection services at no charge. If you believe you are eligible for these services and have not yet received your enrollment information, please contact us at the number below. UPDATE: As of January 15, 2015, you may also enroll by visiting <https://spe.allclearid.com>.

For your security SPE encourages you to be especially aware of email, telephone and postal mail scams that ask for personal or sensitive information. Neither SPE nor anyone acting on its behalf will contact you in any way, including by email, asking for your credit card number, social security number or other personally identifiable information. If you are asked for this information, you can be confident SPE is not the entity asking. To protect against possible identity theft or other financial loss, SPE encourages you to remain vigilant, review your account statements, monitor your credit reports and change your passwords. SPE is providing the following information for those who wish to consider it:

- You may wish to visit the web site of the U.S. Federal Trade Commission at <http://www.consumer.ftc.gov/features/feature-0014-identity-theft> or reach the FTC at 1-877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC. You can reach the Maryland Attorney General at (888) 743-0023 (toll free in Maryland) or Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202.
- U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free (877) 322-8228.
- You can request information regarding "fraud alerts" and "security freezes" from the three major U.S. credit bureaus are listed below. At no charge, if you are a U.S. resident, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. A "security freeze" generally prohibits the credit reporting agency from releasing your credit report or any information from it without your written authorization. You should be aware that placing a security freeze on your credit account may delay or interfere with the timely approval of any requests that you make for new loans, credit mortgages, or other services. Unlike fraud alerts, to obtain a security freeze you must send a written request to each of the three major reporting agencies. Should you wish to place a fraud alert or a security freeze, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.
  - Experian: (888) 397-3742; [www.experian.com](http://www.experian.com); P.O. Box 9532, Allen, TX 75013
  - Equifax: (800) 525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241
  - TransUnion: (800) 680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Please contact us at (855) 731-6013 should you have any additional questions.