

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

AMERICAN FEDERATION OF)
GOVERNMENT EMPLOYEES)
80 F Street, N.W.)
Washington, D.C. 20001, and)

AMERICAN FEDERATION OF)
GOVERNMENT EMPLOYEES LOCAL 1)
80 F Street, N.W.)
Washington, D.C. 20001, and)

AMERICAN FEDERATION OF)
GOVERNMENT EMPLOYEES LOCAL 1234)
P.O. Box 34688)
San Diego, CA 92163, and)

AMERICAN FEDERATION OF)
GOVERNMENT EMPLOYEES LOCAL 777)
6435 South Stewart #2B)
Chicago, IL 60621, and)

JOSEPH JONES)
307 Todd Place NW)
Washington, DC 20002, and)

JANETTE NAGEL)
2174 Rosemont)
Berkley, MI 48072, and)

CRIS SOULIA)
4046 Mississippi Street, Apt. 1)
San Diego, CA 92104, and)

DON THOMAS)
1437 Amaryllis Circle)
Orlando, FL 32825,)

Plaintiffs,)

v.)

KIP HAWLEY, in his official capacity as)
Administrator,)

CIVIL ACTION NO.

Transportation Security Administration)
 U.S. Department of Homeland Security)
 601 South 12th St.)
 Arlington, VA 22202-4220, and)
)
 TRANSPORTATION SECURITY)
 ADMINISTRATION)
 U.S. Department of Homeland Security)
 601 South 12th St.)
 Arlington, VA 22202-4220, and)
)
 MICHAEL CHERTOFF, in his official capacity)
 as Secretary,)
 U.S. DEPARTMENT OF HOMELAND)
 SECURITY)
 Washington, D.C. 20528 and)
)
 U.S. DEPARTMENT OF HOMELAND)
 SECURITY)
 Washington, D.C. 20528)
)
)
 Defendants.)
 _____)

CLASS ACTION COMPLAINT

Plaintiffs bring this action to challenge the failure by Defendants Kip Hawley, in his official capacity as Administrator, the Transportation Security Administration (TSA), Michael Chertoff, in his official capacity as Secretary, and the U.S. Department of Homeland Security (DHS), to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of personnel records as evidenced by the disclosure of private, personnel information of approximately 100,000 former and current employees to include their names, social security numbers, bank account numbers, and birthdates, in violation of the Aviation and Transportation Security Act (ATSA) and the Privacy Act of 1974.

Plaintiffs request this Court to declare the Defendants in violation of the ATSA and in violation of the Privacy Act. Plaintiffs further seek from this Court an order to require the Defendants to create a security procedure with lawfully required safeguards to properly protect personnel data.

JURISDICTION

1. Jurisdiction over this action is conferred upon the United States District Court by 28 U.S.C. §1331. Jurisdiction is also invoked pursuant to 5 U.S.C. §552a(g)(1)(D).

VENUE

2. Venue is properly laid before this Court in accordance with 28 U.S.C. §1391(e).

PARTIES

3. Plaintiff American Federation of Government Employees (AFGE) represents approximately 600,000 federal government employees throughout numerous federal government departments and agencies. Its headquarters is located at 80 F Street, N.W., Washington, D.C. 20001. AFGE represents the interests of employees within its bargaining units by, among other things, negotiating collective bargaining agreements, arbitrating grievances, filing unfair labor practices, lobbying, and litigating employees' collective and individual rights in the federal courts.
4. AFGE Local 1, AFL-CIO, is a labor organization chartered by the AFGE to represent the interests of TSA security screeners. Thirteen TSA security screeners from various U.S. airports were the founding members of AFGE TSA Local 1. AFGE Local 1 represents the interests of TSA security screeners by, among other things, acting as personal representatives in the filing of

grievances, discrimination complaints, and administrative appeals; lobbying; and litigating employees' collective and individual rights in the federal courts.

5. AFGE Local 1234, AFL-CIO is a labor organization chartered by the AFGE to represent the interests of TSA security screeners who work in California, Arizona, Hawaii, and Nevada. AFGE Local 1234 represents the interests of TSA security screeners by, among other things, acting as personal representatives in the filing of grievances, discrimination complaints, and administrative appeals; lobbying; and litigating employees' collective and individual rights in the federal courts.
6. AFGE Local 777, AFL-CIO is a labor organization chartered by the AFGE to represent the interests of TSA security screeners who work in Illinois, Michigan, and Wisconsin. AFGE Local 777 represents the interests of TSA security screeners by, among other things, acting as personal representatives in the filing of grievances, discrimination complaints, and administrative appeals; lobbying; and litigating employees' collective and individual rights in the federal courts.
7. Plaintiff Joseph Jones is a member of AFGE and AFGE Local 1. He is currently, and has continuously been, employed as a transportation security officer with the TSA at the Ronald Reagan Washington National Airport since September 2002. On or about May 4, 2007, he received a broadcast email from the TSA stating that

an external hard drive containing personnel data (including name, social security number, date of birth, payroll information, financial allotments, and bank account and routing information) was discovered missing from a controlled area at the Headquarters Office of Human Capital..... We are notifying you of this incident because you may be one of the employees whose information was contained on the device. TSA has no evidence that an unauthorized individual is using your personal information, but we bring this incident to your attention so that you can be alert to signs of any possible misuse of your identity. We are notifying you out of an abundance of caution at this early stage of the investigation given the significance of the information contained on the device. We apologize that your information may be subject to unauthorized access, and I deeply regret this incident.

8. Plaintiff Janette Nagel is a member of AFGE and AFGE Local 777. She is currently, and has continuously been, employed as a transportation security officer with the TSA at the Detroit Metropolitan Wayne County Airport since in 2003. On or about May 4, 2007, she received a broadcast email from the TSA stating that

an external hard drive containing personnel data (including name, social security number, date of birth, payroll information, financial allotments, and bank account and routing information) was discovered missing from a controlled area at the Headquarters Office of Human Capital..... We are notifying you of this incident because you may be one of the employees whose information was contained on the device. TSA has no evidence that an unauthorized individual is using your personal information, but we bring this incident to your attention so that you can be alert to signs of any possible misuse of your identity. We are notifying you out of an abundance of caution at this early stage of the investigation given the significance of the information contained on the device. We apologize that your information may be subject to unauthorized access, and I deeply regret this incident.

9. Plaintiff Cris Soulia is a member of AFGE and AFGE Local 1234. He is currently, and has continuously been, employed as a transportation security officer with the TSA at the San Diego International Airport since 2002. On or about May 4, 2007, he received a broadcast email from the TSA stating that

an external hard drive containing personnel data (including name, social security number, date of birth, payroll information, financial allotments, and bank account and routing information) was discovered missing from a controlled area at the Headquarters Office of Human Capital..... We are notifying you of this incident because you may be one of the employees whose information was contained on the device. TSA has no evidence that an unauthorized individual is using your personal information, but we bring this incident to your attention so that you can be alert to signs of any possible misuse of your identity. We are notifying you out of an abundance of caution at this early stage of the investigation given the significance of the information contained on the device. We apologize that your information may be subject to unauthorized access, and I deeply regret this incident.

10. Plaintiff Don Thomas is a member of AFGE and AFGE Local 1. He is currently, and has continuously been, employed as a transportation security officer with the TSA at the Orlando International Airport since December 2002. On or about May 4, 2007, he received a broadcast

email from the TSA stating that

an external hard drive containing personnel data (including name, social security number, date of birth, payroll information, financial allotments, and bank account and routing information) was discovered missing from a controlled area at the Headquarters Office of Human Capital..... We are notifying you of this incident because you may be one of the employees whose information was contained on the device. TSA has no evidence that an unauthorized individual is using your personal information, but we bring this incident to your attention so that you can be alert to signs of any possible misuse of your identity. We are notifying you out of an abundance of caution at this early stage of the investigation given the significance of the information contained on the device. We apologize that your information may be subject to unauthorized access, and I deeply regret this incident.

11. Defendant Kip Hawley is the Administrator of the TSA and the official responsible for the proper execution and administration of all laws by the TSA. He is being sued in his official capacity.
12. Defendant Michael Chertoff is the Secretary of the DHS and the official responsible for the proper execution and administration of all laws by the DHS. He is being sued in his official capacity.
13. The TSA is a component of the DHS and is an executive department of the federal government. Therefore, it is an “agency” for the purposes of the Privacy Act of 1974.
14. The DHS is an executive department of the federal government and is, therefore, an “agency” for the purposes of the Privacy Act of 1974.

CLASS ALLEGATIONS

15. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23 and Local Rule 23.1. Plaintiffs seek certification of the following class: all current and former TSA Security Screener Officers, specifically security screener officers, lead security

screeners officers, and supervisory security screener officers, whose private information including but not limited to name, social security number, date of birth, payroll information, financial allotments, and bank account and routing information, was disclosed when the TSA lost control of an external hard drive containing said information.

16. Upon information and belief, the class size is approximately 100,000, which is the number of individuals whose information Defendants admits was collected and maintained in the missing system of records.

17. The class consists of all persons who have been adversely affected by Defendants' Privacy Act violations.

18. The class is so numerous that joinder of all members would be impracticable due to the geographical diversity of class members and the limited ability of individual class members to institute separate suits.

19. The same facts, circumstances, and merits of the case apply equally to all class members.

Common questions of law include:

- a. Whether Defendants violated ATSA when it failed to maintain proper security procedures to protect personnel information; and
- b. Whether Defendants violated the Privacy Act by failing to properly maintain proper security procedures to protect personnel information.

20. The claims of the individually named Plaintiffs are typical of the claims of the Plaintiff class members. Plaintiffs and all members of the Plaintiff Class have been similarly affected by the Defendants' common course of conduct. The claims of all class members depend on a showing of Defendants' common failure to implement a security regime that properly protects against disclosure of private information.

21. There is no conflict as between Plaintiffs and the other members of the class with respect to this action or the claims for relief. Plaintiffs know and understand their asserted rights and their roles as class representatives.
22. Plaintiffs and their attorneys are able to and will fairly, and adequately, protect the interest of the class. Attorney Mark D. Roth and Charles A. Hobbie are experienced litigators and will be able to supervise other experienced staff in conducting the proposed litigation. Plaintiffs' attorneys can vigorously prosecute the rights of the proposed class members.
23. Separate actions by individual Plaintiffs will create the risk of inconsistent and varying results that may establish incompatible standards.

STATEMENT OF FACTS

24. In 2001, Congress enacted the Aviation and Transportation Security Act (ATSA), Pub. L. 107-71, in part, in order to federalize security screening operations for passenger air transportation and intrastate air transportation under 49 U.S.C. §§44901 and 44935. The ATSA created the TSA and as such, defines that agency's duties and authorities.
25. The ATSA explicitly mandates the Administrator to "enforce security-related regulations and requirements," as well as "oversee the implementation, and ensure the adequacy, of security measures at airports."
26. Similarly, the Privacy Act requires agencies that maintain a system of records to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness

to any individual on whom information is maintained.” 5 U.S.C. §552a(e)(10).

27. The TSA maintains a system of personnel records that includes by name the social security number, date of birth, payroll information, bank account and routing information for its current and former screening personnel.
28. On Thursday, May 3, 2007, the TSA became aware of a data security incident involving approximately 100,000 archived employment records of individuals employed by the agency from January 2002 until August 2005.
29. Specifically, an external hard drive containing personnel data, including but not limited to name, social security number, date of birth, payroll information, bank account and routing information [hereinafter “Personnel Data”], was discovered missing from a controlled area at the TSA Headquarters Office of Human Capital.
30. Defendants cannot account for the present location of the external hard drive, or for the present location of the Personnel Data contained therein.
31. On or about May 4, 2007, the TSA issued a broadcast e-mail to its employees stating that:

an external hard drive containing personnel data (including name, social security number, date of birth, payroll information, financial allotments, and bank account and routing information) was discovered missing from a controlled area at the Headquarters Office of Human Capital.....We are notifying you of this incident because you may be one of the employees whose information was contained on the device. TSA has no evidence that an unauthorized individual is using your personal information, but we bring this incident to your attention so that you can be alert to signs of any possible misuse of your identity. We are notifying you out of an abundance of caution at this early stage of the investigation given the significance of the information contained on the device. We apologize that your information may be subject to unauthorized access, and I deeply regret this incident.
32. The maintenance and safeguarding of Personnel Data is vital to the protection of security at the airports.
33. The maintenance, safeguarding, and non-disclosure of Personnel Data by Defendants is a

security-related regulation.

34. Terrorists and terrorist groups with access to the names, social security numbers, birthdates, and banking information of transportation security screeners can disrupt proper and vital airport screening by creating false identity badges to gain access to secure areas; steal the identity of transportation security screeners thereby gaining access to secure areas or TSA network systems; and disrupt the financial lives of transportation security screeners thus causing them to miss work to correct the problem or be distracted at work.
35. Defendants have been repeatedly informed of recurring, systemic, and fundamental deficiencies in its information security. *See* Office of Inspector General (OIG), Department of Homeland Security (DHS) report “Improved Security Required for Transportation Security Administration Networks, OIG-05-31 (August 2005).
36. Defendants demonstrated reckless disregard for privacy rights when it failed to effectively secure the external hard drive that maintained the personal information of its personnel workforce.
37. Upon information and belief, Defendants disclosed private information when the external hard drive including the Personnel Data of transportation security screeners was lost from a secure area of the Defendants’ headquarters office.
38. The privacy rights of the individually named Plaintiffs and the privacy rights of the members of the union Plaintiffs privacy rights were invaded when the external hard drive including the Personnel Data of transportation security screeners was lost from a secure area of the Defendants’ headquarters office.
39. Defendants did not have Plaintiffs’ consent, either express or implied, to disclose their Personnel Data.
40. Defendants require transportation security screeners to be suitable for employment. In

determining suitability, Defendants requires its employees to have financial suitability, specifically, less than \$5,000.00 of overdue debt. Defendants have terminated employees for lack of financial suitability.

41. The individually named Plaintiffs and the membership of the union Plaintiffs experienced adverse effects due to Defendants' failure to safeguard the Personnel Data and/or disclosure, including but not limited to, embarrassment, inconvenience, mental distress, concern for identity theft, concern for damage to credit report, concern for damage to financial suitability requirements in employment, and future substantial financial harm.
42. The individually named Plaintiffs and the membership of the union Plaintiffs who are members of the traveling public experienced adverse effects due to Defendants' disclosure, including but not limited to, mental distress due to the possibility of security breach at airports.
43. The individually named Plaintiffs and the membership of the union Plaintiffs must take affirmative steps to recover peace of mind, emotional stability, and personal security, including but not limited to, frequently obtaining and reviewing credit reports, bank statements, and other similar information. As a result, the individually named Plaintiffs and the membership of the union Plaintiffs have and will continue to suffer tangible and intangible damages for the foreseeable future.

COUNT I

44. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 39 above.
45. The Defendants violated the ATSA when he failed to maintain personnel data from loss consistent with security-related regulations.

46. The Defendants violated the ATSA when he failed to ensure the adequacy of security measures at airports resulting in the loss of personnel data.

COUNT II

47. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 39 above.

48. The Defendants violated the Privacy Act of 1974 when it failed to “establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.”

49. The Defendants further violated the Privacy Act of 1974 when on or about May 3, 2007, there was an unauthorized disclosure of private, personnel data.

50. The Defendants’ violation was intentional or willful.

51. The TSA has no administrative appeal process by which to correct the Defendants’ failure to conform to the Privacy Act’s safeguard requirements and the unauthorized disclosure at issue herein.

52. Defendants’ violation of the Privacy Act caused Plaintiffs’ adverse effects, including but not limited to actual damages.

53. Defendants’ violation of the Privacy Act has placed each Plaintiff in legitimate fear of identity theft, corruption of their credit files, plundering of bank accounts, and instability of employment due to Defendants’ financial suitability requirements.

WHEREFORE, Plaintiffs pray that this Honorable Court enter an Order:

- (1) Requiring *in camera* review of Defendants' security procedures taken to comply with the Privacy Act;
- (2) Declaring that Defendants violated ATSA when it failed to properly maintain from disclosure private information of transportation security screeners;
- (3) Declaring that the Defendants violated the Privacy Act when it failed to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.
- (4) Declaring that Defendants violated the Privacy Act when it disclosed private information of transportation security screeners;
- (5) Ordering the Defendants to grant administrative leave to transportation security screeners requesting leave in order to protect against or correct identity theft or financial disruption caused by this data security incident;
- (6) Ordering the Defendants to provide credit monitoring to current and former employees who were employed from January 2002 to August 2005, free of charge, for five years;
- (7) Ordering the Defendants to provide identity theft protection to current and former employees who were employed from January 2002 to August 2005 screeners, free of charge, for five years;
- (8) Enjoining the Defendants from charging any transportation security screeners absent without leave or placing any transportation security screeners on leave restriction when the leave taken is to correct financial disruption caused by the unauthorized disclosure of

private information;

- (9) Enjoining the Defendants from disciplining, including but not limited to termination, any transportation security screeners on the basis when the underlying reason is a result of identity theft or the financial disruption caused by the unauthorized disclosure of private information;
- (10) Granting to Plaintiffs judgment against Defendants for all actual damages incurred as a result of the Defendants' Privacy Act violations;
- (11) Granting to Plaintiffs judgment against Defendants in an amount of at-least \$1,000.00 for each individual who was adversely affected by Defendants' Privacy Act violations;
- (12) Ordering the Defendants to create a security procedure that is consistent with ATSA and the Privacy Act; specifically:
 - (a) Ordering the Defendants to tag and electronically monitor the location of all of Defendants' external hard drives, laptops or any other mobile equipment which stores personnel data;
 - (b) Encrypt all personnel data;
 - (c) Destroy all former employee's bank account and routing information after six months and within one year of the effective date of resignation or termination;
- (13) Ordering Defendants to pay Plaintiffs' attorney fees and costs; and

(14) Granting such other relief as this Court finds necessary and proper.

Respectfully submitted,

Mark D. Roth (D.C. Bar #235473)
General Counsel

Charles A. Hobbie
Deputy General Counsel

Gony Frieder (D.C. Bar #457706)
Assistant General Counsel

Hampton H. Stennis (DC Bar #500815)
Staff Counsel
American Federation of Government Employees,
AFL-CIO
80 F Street, NW
Washington, D.C. 20001
(202) 639-6434

Attorneys for Plaintiffs