Rosemary M. Rivas (State Bar No. 209147)
rrivas@finkelsteinthompson.com
Mark Punzalan (State Bar No. 247599)
mpunzalan@finkelsteinthompson.com
Daniel T. LeBel (State Bar No. 246169)
dlebel@finkelsteinthompson.com
FINKELSTEIN THOMPSON LLP
100 Bush Street, Suite 1450
San Francisco, CA 94104
Telephone: (415) 398-8700
Facsimile: (415) 398-8704

[Additional Counsel Listed on Signature Page]

Counsel for Individual and Representative Plaintiff Joel Ruiz

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JOEL RUIZ, On Behalf of Himself and All Others Similarly Situated,

Plaintiff,

vs.

GAP, INC. and VANGENT, INC.,

Defendants.

Case No. CV07-05739-SC

FIRST AMENDED COMPLAINT

CLASS ACTION

DEMAND FOR JURY TRIAL

Plaintiff Joel Ruiz ("Plaintiff"), on behalf of himself and all others similarly situated, alleges the following against the above-captioned Defendants, based upon personal knowledge, where applicable, and on information and belief and the investigation and research of counsel:

PARTIES

1. Plaintiff Joel Ruiz ("Plaintiff") is a citizen of the State of Texas. Plaintiff has been injured as a result of Defendants' unlawful conduct herein by spending time and money to prevent the fraudulent use of his personal information.

2. Defendant Gap Inc. ("Gap" or the "Company") is a clothing and accessories retailer based in San Francisco, California. Gap operates stores under its various brands, including Old Navy, Banana Republic, and Gap outlet stores. Gap is headquartered at Two Folsom Street, San Francisco, California 94105.

3. Defendant Vangent Inc. (hereinafter, "Vangent" or "vendor") is a provider of information management and business process outsourcing services based in Arlington, Virginia. Vangent managed the process for telephone and job applications to several Gap brand stores. Vangent is headquartered at 4250 North Fairfax Drive, Suite 1200, Arlington, Virginia 22203.

NATURE OF ACTION

4. Gap is a clothing and accessories dealer with more than 154,000 employees and 3,100 stores worldwide. Thousands of people apply for positions in Gap brand stores each year.

5. Vangent managed online and telephone applications for jobs with Gap brand stores. Vangent processes approximately 75,000 online applications per month for Gap.

6. On September 17, 2007, a thief gained entry to Vangent's facility in Chicago, Illinois and stole two laptop computers. One of the laptops contained the personally identifying information ("PII") of approximately 750,000 people who applied for retail jobs with Gap brand stores ("job applicants").

7. Encrypting data is a standard business practice employed to protect sensitive business information from unauthorized access. The PII on the laptop stolen from Vangent's Chicago

office, however, was not encrypted, allowing anyone with the computer to easily and readily view Plaintiff and job applicants' sensitive information.

8. Plaintiff applied for a position online with Old Navy, one of Gap's brand stores, through the online application process managed by Vangent. As part of the application, Plaintiff was required to provide PII, including his SSN. Plaintiff entrusted his SSN and other PII to Gap and Vangent, but his PII was compromised in the laptop theft.

9. The data on the laptop computers included the names, SSNs, addresses, and other PII of people from the United States, Puerto Rico, and Canada who applied online or by phone for store positions with Gap, Old Navy, Banana Republic, and Gap Outlet stores, between July 2006 and June 2007.

10. Defendants' failure to maintain reasonable and adequate security procedures to protect against the theft of the job applicants' PII has put Plaintiff and other Class members at an increased risk of becoming victims of identity theft crimes. In addition, Plaintiff and the Class have spent (or will need to spend) considerable time and/or money to protect themselves as a result of Defendants' conduct.

11. Plaintiff and the Class have not only had sensitive identifying information disclosed, but, most critical of all, their SSNs are now out in the open. Plaintiff and the Class will have to consistently monitor their credit card accounts, credit reports and other financial information due to the nature of the stolen information.

12. As a result, Plaintiff and the Class seek damages, restitution, declaratory relief, injunctive relief, and any other such relief as the Court may award.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because Plaintiff is of diverse citizenship from Defendants; there are more than 100 Class members nationwide; and the aggregate amount in controversy exceeds $5,000,000, excluding interest and costs. This Court has personal jurisdiction over the parties because Defendants conduct substantial business in this state, have

systematic and continuous contacts with this state, and have agents and representatives that can be found in this state.

14. Venue is appropriate under the authority of 28 U.S.C. § 1391(b) because one of the Defendants resides in this District and a substantial part of the challenged actions took place and/or emanated from this District.

FACTUAL ALLEGATIONS

Background of Gap

15. Gap operates approximately 3,131 retail and outlet stores throughout the United States and overseas under several different brands: Gap, Old Navy, Banana Republic, and Piperlime.

16. As of February 3, 2007, Gap had a work force of approximately 154,000 employees, which includes a combination of part-time and full-time employees.

Standard Business Practices for Ensuring Information Safety

17. Federal and state legislatures have passed a number of laws in recent years to ensure companies protect the security of sensitive PII in the company's files. These laws include requirements for the handling of PII by financial institutions[1] and also impose proactive obligations on companies to maintain reasonable security measures to protect the PII of individuals.[2] Specifically, the California legislature has passed a law aimed at protecting the proliferation of the SSNs of individuals.[3]

---

[1] The Gramm-Leach-Bliley Act, enacted on November 12, 1999, requires the FTC and other government agencies that regulate financial institutions to implement regulations to carry out the Act's financial privacy provisions. The regulations required all covered businesses to comply with the Act by July 1, 2001.

[2] Cal Civ. Code § 17980.80 *et seq.* obligates companies that possess personal information to take all reasonable steps to destroy the personal information no longer needed by the business, notify residents whose unencrypted information has been acquired in an unauthorized manner, and to implement reasonable security measures.

[3] Cal. Civ Code. § 1798.85(3) prohibits any company from requiring a person to transmit his or her Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted.

18. The Federal Trade Commission ("FTC") has issued a publication entitled "Protecting Personal Information: A Guide for Business" ("FTC Report"), attached hereto as Exhibit A. In this publication, the FTC provides guidelines for businesses on how to develop a "sound data security plan" to protect against crimes of identity theft. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow the following guidelines:

a. Keep inventory of all computers and laptops where the company stores sensitive data;

b. Do not collect PII if there is no legitimate business need. If there is a legitimate business need, only keep the information as long as necessary;

c. Use SSNs only for required and lawful purposes and do not store these numbers unnecessarily, such as for an employee or customer identification number;

d. Encrypt the PII particularly if the sensitive information is shipped to outside carriers or contractors. In addition, the business should keep an inventory of all the information it ships;

e. Do not store sensitive computer data on any computer with an Internet connection unless it is essential for conducting the business;

f. Control access to sensitive information by requiring that employees use "strong" passwords; tech security experts believe the longer the password, the better; and

g. Implement information disposal practices reasonable and appropriate to prevent an unauthorized access to personally identifying information.

19. In addition, the FTC Report states a number of guidelines concerning the use of laptops in storing PII. As the FTC Report states:

a. Restrict the use of laptops to employees who need them to perform their jobs;

b. Assess whether sensitive PII needs to be stored on a laptop, and if not, delete the information with a "wiping" program overwriting the data on the laptop;

c. Consider allowing laptop users only to access sensitive information but not to store the information on their laptops;

d. Require employees to store laptops in a secure place; and

e. Encrypt any sensitive data contained on a laptop and configure the data so users cannot download any software or change security settings without approval from Information Technology specialists.

20. The FTC Report also instructs companies that outsource any business functions to proactively investigate the data security practices of the outsourced company and examine their standards.

21. Gap was well aware of the FTC Report and other data security publications before the September 17, 2007 data breach.

22. The California Department of Consumer Affairs' Office of Privacy Protection published a similar set of guidelines in February 2007 report entitled "Recommendation Practices of Notice of Security Breach Involving Personal Information" ("California privacy report"), attached hereto as Exhibit B. The California Privacy report states guidelines similar to those found in the FTC Report, including one for businesses to encrypt higher-risk PII when they are contained in portable computers and devices.

23. Thefts of portable devices containing PII have frequently occurred in recent years. Various members of the news media have questioned the safety precautions used by companies to protect such PII. As the San Francisco Chronicle reported on September 29, 2007:

> The increasing frequency of these thefts has raised questions about why companies and government agencies keep sensitive personal information on laptops and other portable devices. Many security experts say that such information should be stored only on secure centralized servers.

24. A September 28, 2007 article from CNNMoney.com quotes David Perry, a data security expert with a computer software company, Trend Micro. In the article, Perry specifically questioned Gap's failure to protect the PII of its job applicants. As Perry stated:

> [W]hy is this kind of data on a laptop? And if it was on a laptop, it should certainly have been encrypted… This is just one of the many number of incidents where the value of the stolen property is no longer the computer itself but the information that's on it… Even though Gap says it believes that the data wasn't the target of the theft, whoever has the laptop now knows what's on it… That's a big concern to those job applicants and to Gap if that information is misused.

25. As the United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report"), more than 570 breaches involving theft of personal identifiers such as SSNs were reported by the news media from January 2005 through January 2006. As the GAO Report states, these data breaches involve the "unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers." A number of these breaches have occurred at retailers.

26. In September 2008, The President's Identity Theft Task Force Report noted that "[p]ublic concerns about the security of personal information and identity theft remain at high levels, with potentially serious consequences for the function of our economy." http://www.ftc.gov/os/2008/10/081021taskforcereport.pdf, at viii (last visited January 14, 2009).

The Use of PII In Identity Theft

27. Data breaches can lead to identity theft. As the GAO Report has stated, "identity theft" is a broad term encompassing various types of criminal activities. Generally, identity theft occurs when a person's identifying information is used to commit fraud or other crimes. These crimes include credit card fraud, phone or utilities fraud, bank fraud, and government fraud. The FTC has stated that identity theft has been a serious problem in recent years, with approximately 9 million Americans as the victims of identity theft each year.

28. The GAO Report stated that identity thieves can use identifying data such as SSNs to open financial accounts and incur charges and credit in a person's name. As the GAO has stated, this type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft and can cause significant harm to the victim's credit rating.

29. Identity thieves use SSNs to commit other sorts of fraud as well, such as obtaining false identification cards, obtaining government benefits in the victim's name, committing crimes, or filing fraudulent tax returns on the victim's behalf. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

30. The release of SSNs are particularly damaging because identity thieves are able to not only fraudulently open credit card accounts and to obtain loans, but to fraudulently access consumers' existing accounts. SSNs, however, cannot be easily changed like a credit card account number. If an individual's SSN has been compromised, it is much more difficult to protect against identity theft than it would be if credit card information were stolen. Even if an individual overcomes the barriers to changing the SSN, the defensive measure is still not a guarantee of protection against identity theft.

31. Identity theft crimes often encompass more than just immediate financial loss. Identity thieves often hold onto stolen personal and financial information for several years before using and/or selling the information to other identity thieves. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

Gap and Vangent's Job Application Process

32. To apply for an in-store position with any of the different Gap brand stores, job applicants may fill out an in-person application, apply over the telephone, or apply online.

33. Gap employs Vangent to manage its job application process for in-store positions. Vangent had full access to all of the PII provided by job applicants through the job application process. In fact, the PII collected through the job application process was stored in Vangent's database.

34. During Gap's online application process, Gap and Vangent inform the applicant of the following "Privacy Statement":

> Vangent has adopted the following Privacy Policy. We provide and support Gap Inc.'s recruitment system that you are accessing. We use reasonable precautions to protect your personal information from unauthorized use, access, disclosure, alteration or destruction. We do not release any of your information with any party other than Gap Inc., unless directed by Gap Inc. or legally mandated to do so. Gap Inc. may require that your application information be given to a third party provider for the purposes of performing background checks and/or pursuing Work Opportunity Tax Credits.

https://gapinc.reidsystems.com/US/start.htm?lang=01&ctry=US (last accessed on November 5, 2007).

35. Throughout the online application, Gap requires the job applicant to provide a large amount of PII, including the applicant's SSN, birthdate, address, and phone number.

36. Job applicants cannot complete the online job application process unless they provide their SSN. In fact, it is the very first request made of an applicant. Gap and the vendor's online Web site does not offer the option to use a password, personal identification number, or authentication device other than the applicant's SSN, to access the online job application.

37. Job applicants are also required to consent to a background check as part of the application. Gap states in its online application that a SSN is required to enter the online application process but that it is solely used for the purpose of obtaining the applicant's credit report. If the job applicant does not enter his/her SSN, the application instructs the applicant that, "If you do not agree, please exit the system now by pressing QUIT."

38. Plaintiff applied for a position with Old Navy through Gap's online application website in late 2006. As part of the application process, Plaintiff was required to provide all of the aforementioned PII to complete the application process. Among the information provided, Plaintiff provided his SSN, email, home address, and telephone number, as well as responses to other personal questions on the website.

The Data Breach

39. On September 17, 2007, a thief stole two laptop computers from Vangent's high-security office in Chicago, Illinois ("the data breach"). One of the laptops contained the PII of approximately 750,000 persons (including Plaintiff) that had applied to Old Navy, Gap, Banana Republic, or Gap outlet stores by telephone or the Internet from July 2006 to June 2007 ("job applicants"). The thief appears to have targeted the vendor's office, bypassed a myriad of unsecured laptops, computers, and other electronic hardware or items of value and stole these two specific laptops – one of which was downloading job applicant PII.

40. Earlier in the day of the data breach, a staff psychologist employed by Vangent placed the laptop on a desk to download information about job applicants from the vendor's

database to his laptop hard drive. Gap had directed the psychologist to download data for a report on geographic hiring trends. Although the job applicants' SSNs and other PII were not required for this report, the psychologist downloaded the PII to his laptop hard drive from the main server. The downloaded PII, however, was not encrypted on the laptop.

41. The psychologist left the laptop unattended after working hours while the laptop downloaded the PII from the main server. Despite the sensitive nature of the PII, the psychologist (or any other employees of the vendor) did not lock the laptop with cables, failed to place the laptop in a non-visible, secure location, and neglected to encrypt the PII.

42. After working hours, and while the laptop was downloading the unencrypted PII, the thief entered the building of Vangent's facility. Dressed in business attire and carrying a laptop bag, the thief checked in with ground-level building security and signed in with an illegible signature.

43. Vangent only occupies the 16th floor of the building and shares the floor with only one other company. The thief made no attempt to enter any offices other than the Vangent's.

44. A surveillance video of the data breach shows that the thief made numerous attempts to enter the Vangent facility. Although the doors to the Vangent's facility were protected by key-card access, the thief was able to enter through one of the doors.

45. The thief stole two laptops - one of which was powered up, connected to the Vangent's main server, and in the process of downloading PII.

46. The laptop that was connected to the server at the time of the theft contained, among other things, the names, SSNs, and addresses of job applicants from the United States and Puerto Rico. For applicants that provided the information, the laptop also contained job applicants' race and sex. The job applicants' PII contained on the stolen laptop was not encrypted. Thus, any person in possession of one of the stolen computers could readily view the sensitive information.

47. The laptop also included the PII of job applicants from Canada, but not the Social Insurance numbers of Canadian applicants. Gap did not notify or send letters to Canadian job

applicants whose information was compromised, however, because Gap believed that this group is "not at a higher risk for identity theft."

Gap and Vangent Failed to Protect Plaintiff and Class Members' PII

48. Gap and Vangent failed to exercise reasonable practices in protecting the job applicants' PII. At the time of the data breach in September 2007, data breaches were not a new phenomenon, and Gap was well aware of these incidents and the importance of protecting PII. In addition, Gap had also lost or misplaced 70 laptop computers since 2005 and was clearly aware that laptops could be stolen or misplaced. Gap nevertheless allowed Vangent to store the sensitive PII on portable laptop computers and, furthermore, failed to ensure that the PII was encrypted.

49. Gap and Vangent signed an Employment Screening Services Agreement ("Agreement") (effective on July 14, 2005), which described Vangent's responsibilities in the telephone and online recruitment application process, including technical requirements in handling the PII.

50. The Agreement described the steps of the online and telephone application process. To enter the application Web site, Plaintiff and the Class were required to enter their SSNs without having to enter some other unique password or authentication code, which violated Cal. Civ. Code §1798.85.

51. The Agreement set forth several encryption requirements, namely, that: (a) connections between job applicants' computers and Vangent's servers would be encrypted; (b) connections between Gap and Vangent's servers would be encrypted; and (c) encryption keys for Gap databases would be protected against disclosure and misuse and restricted to the fewest number of custodians necessary.

52. The Agreement, however, had no specific policy requiring the encryption of job applicant PII while it was being stored or downloaded. Moreover, despite Gap's knowledge of data breaches and knowledge of Gap laptops being lost or misplaced, the Agreement did not

contain encryption requirements for storing or downloading PII onto laptop or portable computers.

53. The Agreement, in particular, did not prohibit storing or downloading job applicant PII onto laptop computers or that such laptops were required to have some encryption software. Gap was well aware of the importance of encryption, especially since it mandated encryption software for any computers storing PII in Gap offices.

54. The Agreement also had no requirement that laptop computers downloading or storing PII be locked down by cables (or other secure devices). This despite the fact that Gap itself required in its own offices that laptops be cable-locked or locked inside a desk.

55. Despite touting itself as specializing in "industry-leading human capital management and business process outsourcing services," Vangent also failed to use reasonable practices to protect the PII. Although Gap's Agreement with Vangent stated that encryption private keys would be restricted to the fewest number of custodians necessary, the vendor allowed a number of people to have access to the PII who did not need the PII to perform their jobs. For instance, although Gap and Vangent stated they collected SSNs to - among other things, do background checks on potential applicants - psychologists, information technology ("IT") employees, and store managers had no need for the job applicants' SSNs to perform their duties.

56. Gap also failed to audit Vangent's practices for protecting the job applicants' PII. As part of the services Agreement, Gap personnel could perform an audit of the vendor. Not once, however, did Gap audit Vangent about the handling of PII before the data breach.

57. Moreover, Gap maintained the PII of its job applicants for over a year, well beyond its usefulness. This is in spite of Gap and Vangent's representation during the job application process that it would only consider the application for 90 days:

> This application will only be considered for 90 days. If you have not been hired within 90 days of completing the application and you wish to continue to be considered for employment, you must complete another application. It's only necessary to complete this application once every 90 days.

https://gapinc.reidsystems.com/US/start.htm?lang=01&ctry= (as accessed on November 5, 2007).

58. Instead of disposing of the PII beyond the 90 days as promised, Gap, in fact, instructed Vangent to maintain and not destroy the job applicants' PII, despite the fact that Gap was no longer considering the applications.

The Inadequate Remedy

59. Plaintiff received a letter dated September 28, 2007, from Gap signed by Gap Chairman and CEO Glenn Murphy (the "notice letter"). The notice letter stated that Plaintiff's PII was among those compromised in the theft of the laptop.

60. The notice letter stated that Gap did not believe Plaintiff's PII was the target of the theft. For reasons not disclosed, the letter also indicated that Gap did not believe PII had been "accessed or used improperly." However, Gap provided no basis for this conclusion.

61. Now that Gap and Vangent have compromised the Class' PII, Plaintiff and the Class have spent and will continue to spend considerable time and/or money to try to prevent, and monitor for, fraudulent activity.

62. The notice letter provided a limited remedy to Plaintiff and the Class. Gap offered Plaintiff twelve months of credit monitoring and fraud assistance without charge. Gap offered the Experian "Triple Advantage Credit Monitoring Plan" to most of the affected job applicants. Plaintiff and the Class had until January 31, 2008 to sign up for one of this coverage. For job applicants under 18 years old, Gap offered Experian's "Family Secure" plan.

63. Plaintiff and the Class have faced a number of problems (which increased their time commitment to the process) in signing up for the Triple Advantage plan, including among other things:

a. Incorrect access codes were provided in the notice letter:

b. The Experian website where putative Class members were directed to sign up for the credit monitoring program malfunctioned;

c. A short time period for Class members to sign up for Triple Advantage offer;

d. Conflicting representations by Gap and Experian about a deadline extension to sign up for the remedy;

e. The inability to sign up for credit monitoring because of a limited credit history; and;

f. Receiving notice letters that appeared fraudulent because they were not printed on Gap letterhead, leading some job applicants to believe the letter was a hoax.

64. Signing up for the Family Secure plan was also difficult for minors. In order to sign up for Family Secure, the minor's parent was required to pay $250 up front. The minor's parent would then have to contact Gap and get reimbursed for the $250 cost. Gap, however, did not provide reimbursement for the time value of money. Regardless, many parents could not afford the outlay of the $250 in the first place and were left without a remedy for their child. Additionally, Defendants did not reimburse Plaintiff and the Class for the time spent in attempting to receive credit monitoring or the time spent in resolving problems signing up for the credit monitoring plans.

65. Gap received a large number of calls from angry customers who were not able to sign up for the program for the aforementioned reasons. As a result of these hurdles, as of September 18, 2008, only 6% of the 750,000 affected job applicants were able to sign up for the Triple Advantage or Family Secure plans.

66. The year of credit monitoring and fraud assistance offered by Gap inadequately protects Plaintiff and the putative class from identity theft. One year is not nearly long enough to protect Plaintiff and the putative class from the effects of the security breach which has caused their PII to fall into the hands of criminals.

67. The credit monitoring and fraud assistance is further weakened by forcing Plaintiff and the putative class to waive fundamental rights. Buried in the "Terms and Conditions" of the credit monitoring plan is a requirement that Plaintiff, and the putative class, must waive their Constitutional rights to a jury trial should the credit monitoring service fail in its essential function. In short, the credit monitoring could fail, and Gap's potential and current employees

could be victims of data theft, and there would effectively be no recourse against Experian. Pre-dispute binding mandatory arbitration has been the center of much controversy for its bias against consumers resulting in a recent report by Public Citizen titled "The Arbitration Trap" (found at http://www.citizen.org/documents/Final_wcover.pdf), as well as Congressional scrutiny in the presently pending Arbitration Fairness Act of 2007.

CLASS ACTION ALLEGATIONS

68. Plaintiff brings this suit as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of himself and all other similarly situated persons as members of a Class initially defined as follows:

> All persons that applied for an in-store position with a Gap brand store, through Gap and Vangent, Inc.'s ("Vangent") application process from July 1, 2006 to July 31, 2007, and whose personal information was stored in the laptop stolen on September 17, 2007 from Vangent's Chicago, Illinois facility.

69. Numerosity. The proposed class is sufficiently numerous, as more than 750,000 job applicants have had their PII compromised. Class members are so numerous and dispersed throughout the United States that joinder of all members is impracticable. Class members, can be identified by records maintained by Defendants.

70. Common Questions of Fact and Law. Common questions of fact and law exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class, pursuant to Rule 23(b)(3). Among the questions of fact and law that that predominate over any individual issues are:

a. Whether Defendants owed a legal duty to Plaintiff and Class members to exercise due care in collecting, safeguarding and storing their PII;

b. Whether Defendants failed to exercise due care, and thus, were negligent;

c. Whether Plaintiff and Class members are third party beneficiaries under Defendants' Employee Services Screening Agreement;

d. Whether Vangent breached the Employee Services Screening Agreement;

e. Whether Defendants violated Cal. Civ. Code § 1798.85; and

f. Whether the time and/or money Plaintiff and the Class spent, and will continue to spend in the future to protect themselves from identity theft, is compensable.

71. Typicality. Plaintiff's claims are typical of the claims of members of the Class because Plaintiff and the Class sustained damages arising out of Defendants' wrongful conduct as detailed herein. Specifically, Plaintiff's and Class members' claims arise from Defendants' failure to install and maintain reasonable security measures to protect the Plaintiff and the Class' PII.

72. Adequacy. Plaintiff will fairly and adequately protect the interests of Class members and has retained counsel competent and experienced in class action lawsuits. Plaintiff has no interests antagonistic to or in conflict with those of Class members and therefore is an adequate representatives for Class members.

73. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because the joinder of all Class members is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of an inconsistent and potentially conflicting adjudication of the claims asserted herein. There will be no difficulty in the management of this action as a class action.

74. Notice. Plaintiff will provide the individual notice and/or notice by publication to the Class to the extent required by the Federal Rules of Civil Procedure, due process considerations, and as approved by the Court.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

75. Plaintiff repeats and realleges the allegations contained in each of the paragraphs of this complaint as if fully set forth herein.

76. Defendants owed Plaintiff and the Class a duty to protect their private PII.

77. Defendants were aware of a standard or "best practice" in the industry when it came to protecting the private information of employees and applicants. Given the considerable news

coverage of similar data breaches in recent years, Gap was clearly aware of the need to protect the PII of its job applicants.

78. Defendants breached this duty by failing to take adequate measures to safeguard this information and and failed to maintain reasonable security procedures and practices appropriate to protect the PII of Plaintiff and the Class.

79. Defendants failed to adhere to a number of reasonable and appropriate business practices regarding the PII of Plaintiff and the Class, including:

a. Failing to keep an adequate inventory of all laptops on which PII is stored;

b. Requiring Plaintiff and the Class to use their SSNs to access the website;

c. Failing to comply with Cal. Civ. Code § 1798.85;

d. Storing the PII of Plaintiff and the Class beyond the time necessary to process their job applications;

e. Failing to properly ensure that all PII was encrypted; and

f. Allowing the PII to be stored on portable laptop computers.

80. Defendants failed to exercise due care. As a direct and proximate result of Defendants' breach of their duties, Plaintiff and the Class have been injured and harmed since Defendants' compromising of their PII has placed them at an increased risk of identity theft. Plaintiff and the Class have suffered damages; they have spent and will continue to spend time and/or money in the future to protect themselves as a result of Defendants' conduct.

COUNT II
Violation of Cal. Civ. Code § 1798.85

81. Plaintiff repeats and realleges the allegations contained in each of the paragraphs of this complaint as if fully set forth herein.

82. By requiring Plaintiff and Class members to use SSNs to enter the application Web site without also requiring a unique personal identification number or other authentication device, Defendants have violated Cal. Civ. Code § 1798.85.

83. As a direct and proximate result of Defendants' violation of Cal. Civ. Code § 1798.85, Plaintiff and the Class have been injured and harmed since Defendants' compromising

of their PII has placed them at an increased risk of identity theft. Plaintiff and the Class have suffered damages; they have spent and will continue to spend time and/or money in the future to protect themselves as a result of Defendants' conduct. Plaintiff and Class members are thus entitled to damages as a result of the violation of Cal Civ. Code § 1798.85.

COUNT III

Breach of Contract (Against Vangent only)

84. Plaintiff repeats and realleges the allegations contained in each of the paragraphs of this complaint as if fully set forth herein.

85. Gap and Vangent signed an Employment Screening Services Agreement ("Agreement") (effective on July 14, 2005), which contained express provisions obligating Vangent to protect the personal data of job applicants and the vendor's obligation to comply with all Legal Requirements with respect to access to, disclosure of, and processing of Personal Data. The Agreement provides that Vangent has the right to use personal data solely to the extent necessary to provide services to Gap in accordance with the terms of the Agreement and the Legal Requirements[4] and for no other purpose.

86. The Agreement specifically required, in addition to the other requirements of the Agreement, that Vangent employ commercially reasonable efforts to preserve the security and confidentiality of Personal Data under its control and to prevent the unauthorized or unlawful access to Personal Data. This establishes Gap and Vangent's intent to expressly benefit Plaintiff and the Class, and, thus, Plaintiff and other members of the Class are third-party beneficiaries of the Agreement.

87. The Agreement provides that it shall be construed and enforced in accordance with the laws of the State of California.

[4] "Legal Requirements" is defined in the Agreement as "all statutes, ordinances, orders, rules, regulations, and judgments or requirements of public authorities with jurisdiction, to the extent applicable to specified roles and activities of the parties or as specified in Section 9." Section 9 concerns insurance.

88. California law provides for the enforcement of contracts by third-party beneficiaries. Cal. Civ. Code §1559.

89. Vangent breached the Agreement by not employing commercially reasonable efforts to preserve the security and confidentiality of Personal Data under its control and to prevent the unauthorized or unlawful access to Personal Data. For example, Vangent allowed people who did not need the PII to perform their jobs to have access to the PII.[5] Further, the job applicant PII was not encrypted on the laptop. Also, the laptop was not cable-locked or locked inside a desk and, instead, was left unattended after working hours while the PII was being downloaded from the main server.

90. Additionally, Vangent breached the Agreement because, among other things, it did not comply with all Legal Requirements by requiring Plaintiff and Class members to use SSNs to enter the application process without also requiring a unique personal identification number or other authentication device, in violation of Cal. Civ. Code § 1798.85.

91. Plaintiff and the Class have been injured and harmed by Vangent's failure to comply with the terms of the Agreement. As a direct and proximate result of Vangent's breach, Plaintiff and the Class have suffered damages; they have spent time and/or money, and will continue to spend time and/or money in the future to protect themselves from harm. Plaintiff and the Class are entitled to compensation for those reasonable efforts to protect their interests, as well as for all detriment proximately caused by Vangent's breach, or in the alternative, for nominal damages and/or restitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment on behalf of himself and those similarly situated as follows:

A. For an order certifying the proposed Class herein under Federal Rule of Civil Procedure 23(a) and (b)(3) and appointing Plaintiff and Plaintiff's counsel of record to represent said Class;

---

[5] This also violates Section 1.D.2. of the Agreement because SSN's were not necessary for the psychologist to perform his work.

B. Awarding Plaintiff and Class members compensatory damages or, in the alternative, nominal damages and/or restitution against Defendants in an amount to be determined at trial, together with prejudgment interest at the maximum rate allowable by law;

C. Grant all appropriate relief under Cal. Civ. Code § 1798.85;

D. Grant all appropriate relief under Cal. Civ. Code §1559;

E. Awarding Plaintiff and Class members the reasonable costs and expenses of suit, including attorneys' fees, filing fees; and

F. Grant additional legal or equitable relief as this Court may find just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury.

Dated: February 9, 2009

Respectfully submitted,

FINKELSTEIN THOMPSON LLP

/s/ Mark Punzalan
Mark Punzalan

Rosemary M. Rivas
Daniel T. LeBel
100 Bush Street, Suite 1450
San Francisco, CA 94104
Telephone: (415) 398-8700
Facsimile: (415) 398-8704

-and-

Tracy Rezvani (Pro hac vice)
Karen J. Marcus (Pro hac vice)
1050 30th Street, NW
Washington, D.C. 20007
Telephone: (202).337-8000
Facsimile: (202)337-8090

Ben Barnow (Pro hac vice)
Sharon Harris (Pro hac vice)
Barnow and Associates, P.C.
One N. LaSalle Street
Suite 4600
Chicago, IL 60602