SEAN P. REIS (SBN 184044)
(sreis@edelson.com)
EDELSON MCGUIRE LLP
30021 Tomas Street, Suite 300
Rancho Santa Margarita, California 92688
Telephone: (949) 459-2124

JAY EDELSON*
(jedelson@edelson.com)
RAFEY S. BALABANIAN*
(rbalabanian@edelson.com)
ARI J. SCHARG*
(ascharg@edelson.com)
CHRISTOPHER L. DORE*
(cdore@edelson.com)
EDELSON MCGUIRE LLC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Telephone: (312) 589-6370

*Motion for admission pro hac vice to be filed

ATTORNEYS FOR PLAINTIFF AND THE PUTATIVE CLASS

E-filing

HRL

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

KATIE SZPYRKA, individually and on behalf of all others similarly situated,

Plaintiff,

v.

LINKEDIN CORPORATION, a Delaware corporation,

Defendant.

CV 12 3088

Case No.

CLASS ACTION COMPLAINT FOR:

(1) Violations of Cal. Bus. & Prof. Code § 17200;
(2) Violations of Cal. Civ. Code § 1750;
(3) Breach of Contract;
(4) Breach of the Implied Covenant of Good Faith and Fair Dealing;
(5) Breach of Implied Contracts;
(6) Negligence;
(7) Negligence Per Se;

DEMAND FOR JURY TRIAL

Plaintiff Katie Szpyrka, by and through her attorneys, upon personal knowledge as to herself and her own acts, and upon information and belief as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Plaintiff Katie Szpyrka brings this class action complaint against LinkedIn Corporation ("LinkedIn") for failing to properly safeguard its users' digitally stored personally identifiable information ("PII"), including e-mail addresses, passwords, and login credentials. LinkedIn violated its own User Agreement and Privacy Policy by failing to utilize long-standing industry standard protocols and technology to protect Plaintiff and the Class members' PII.

2. LinkedIn is an Internet company that owns and operates the website www.LinkedIn.com — a social networking website with over 120 million registered users worldwide.

3. Through its Privacy Policy, LinkedIn promises its users that "[a]ll information that [they] provide [to LinkedIn] will be protected with industry standards protocols and technology,"[1] In direct contradiction to this promise, LinkedIn failed to comply with basic industry standards by maintaining millions of users' PII in its servers' databases in a weak encryption format, and without implementing other crucial security measures.

4. Sometime this year, hackers infiltrated LinkedIn's servers and accessed database(s) containing its users' PII. After retrieving this data, the hackers publicly posted over 6 million LinkedIn users' passwords online. Because LinkedIn used insufficient encryption methods to secure the user data, hackers were able to easily decipher a large number of the passwords.

5. While some security threats are unavoidable in a rapidly developing

[1] LinkedIn "Privacy Policy," http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv (last visited June 12, 2012).

technological environment, LinkedIn's failure to comply with long standing industry standard encryption protocols jeopardized its users' PII, and diminished the value of the services provided by Defendant — as guaranteed by its own contractual terms.

PARTIES

6. Plaintiff Katie Szpyrka is a natural person and resident of the State of Illinois. Plaintiff is a registered user of LinkedIn's services.

7. Defendant LinkedIn Corporation is a corporation incorporated and existing under the laws of the State of Delaware, with its principal place of business at 2029 Stierlin Court, Mountain View, California 94043. LinkedIn does business throughout the State of California and the United States.

JURISDICTION AND VENUE

8. This Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1331. The Court also has subject matter jurisdiction pursuant to § 1332(d), because (a) at least one member of the putative class is a citizen of a state different from Defendant, (b) the amount in controversy exceeds $5,000,000.00, exclusive of interest and costs, and (c) none of the exceptions under the subsection apply to this action.

9. Venue is proper in this District under 28 U.S.C. § 1391(a) because Defendant maintains its headquarters and principal place of business in this District and a substantial part of the events giving rise to Plaintiff's Complaint occurred in this District.

FACTUAL BACKGROUND

10. LinkedIn's website states that it "operates the world's largest professional network on the Internet with more than 120 million members in over 200 countries and territories [and] represents a valuable demographic for marketers with an affluent & influential membership."[2]

11. A customer may sign up for a membership at www.LinkedIn.com by

[2] LinkedIn "About Us," http://press.linkedin.com/about (last visited June 12, 2012).

providing a valid e-mail address and a registration password. LinkedIn then stores these credentials in databases located on its servers. Once registered, users build personal "profiles" by providing LinkedIn with various types of demographic, occupational, and cultural information, including employment and educational history.

12. Defendant also offers users the ability to upgrade to a paid "premium" account, with prices ranging from $19.95 to $99.95 per month.

13. Regardless of whether a user signs up for a free or premium account, LinkedIn asserts through its Privacy Policy that it will safeguard its users' sensitive PII, specifically that: "All information that you provide will be protected with industry standard protocols and technology." Plaintiff and the Class agreed to LinkedIn's User Agreement and Privacy Policy in order to register and use LinkedIn's services.

14. Importantly, Plaintiff and the Class members relied on LinkedIn's representation that it uses "industry standard protocols and technology" to preserve the integrity and security of their personal information in agreeing to create an account and provide their PII to the company, and when deciding to purchase "premium" accounts.

LinkedIn Fails to Properly Encrypt its Users' PII

15. As introduced above, LinkedIn digitally stores millions of users' PII in a large-scale commercial database on its servers, and promises through its Privacy Policy that it uses "industry standard protocols and technology" to protect such PII.

16. However, and despite its contractual obligation to use best practices in storing user data, LinkedIn failed to utilize basic industry standard encryption methods. In particular, LinkedIn failed to adequately protect user data because it stored passwords in unsalted SHA1 hashed[3] format. The problem with this practice is two-fold. First, SHA-1 is an outdated hashing function, first published by the National Security Agency in 1995. Secondly, storing

---

[3] In simplest terms for purposes of this Complaint, "hashing" refers to the process by which a password is inputted into a cryptographic hash function and converted into an unreadable, encrypted format.

users' passwords in hashed format without first "salting" the password runs afoul of conventional data protection methods, and poses significant risks to the integrity users' sensitive data.

17. Industry standards require at least the additional process of adding "salt" to a password before running it through a hashing function — a process whereby random values are combined with a password before the text is input into a hashing function. This procedure drastically increases the difficulty of deciphering the resulting encrypted password.

18. More common standard practice is to salt passwords before inputting them into a hash function, to then salt the resulting hash value, and again run the hash value through a hashing function. Finally, that fully encrypted password is stored on a separate and secure server apart from all other user information. Defendant's data protection procedures fall well short of this level of security.

19. LinkedIn failed to use a modern hashing and salting function, and therefore drastically exacerbated the consequences of a hacker bypassing its outer layer of security. In so doing, Defendant violated its Privacy Policy's promise to comply with industry standard protocols and technology for data security.

The Attack on LinkedIn's Database

20. Preliminary reports indicate that LinkedIn's servers were breached through a common hacking method known as an "SQL injection" attack. This hacking technique involves exploiting weaknesses existing in a company's website to penetrate deeper into back-end servers that contain databases of sensitive user information.

21. If true, LinkedIn's failure to adequately protect its website against SQL injection attacks — in conjunction with improperly securing its users' PII — would demonstrate that the company employed a troubling lack of security measures.

22. In fact, the Federal Trade Commission ("FTC") has filed complaints against corporations claiming to secure customer data while remaining vulnerable to SQL injection

attacks.[4] In the referenced case, the FTC filed a complaint in 2003 against the "Guess?" clothing company. The complaint alleges that despite a posted policy ensuring reasonable Internet security measures, "Guess?" stored customers' PII in an unencrypted database concomitantly with poor website security. The FTC argued that these practices constituted unfair or deceptive practices affecting commerce in violation of federal law.

23. Moreover, the National Institute of Standards and Technology ("NIST") provides basic network security checklists that enumerate steps to avoid SQL injection vulnerabilities.[5] The failure of a large company tasked with protecting millions of users' PII, such as LinkedIn, to act pursuant to these basic security checklists would further belie its assertion that it employed industry standard protocols and technology to secure its customers' PII.

24. Had LinkedIn used proper encryption methods, and a hacker were able to penetrate LinkedIn's network, he would be limited in his ability to inflict harm. For example, a hacker still might be able cause temporary internal havoc in the operation of the website, or "vandalize" the appearance of pages by altering its code, he would not be able to access user databases. Moreover, if LinkedIn used appropriate encryption methods — yet failed to secure its database — the stolen PII would be useless, as it would be indecipherable.

25. On June 6, 2012, a list of approximately 6.5 million hashed passwords retrieved from LinkedIn's database was publicly posted online by hackers. Because the passwords were only hashed with a weak hashing function (and not salted), individuals were able to quickly decipher a large contingency of the posted passwords in a matter of hours. It quickly became apparent that the passwords belonged to LinkedIn users.

26. Only after third party observers publicly announced the origin of the password

---

[4] *In the Matter of Guess?, Inc. and Guess.com Inc.*, (Case No. C-4091) (FTC, July 30, 2003) (available at http://www.ftc.gov/os/2003/08/guesscomp.pdf).

[5] National Checklist Program Repository, http://checklists.nist.gov (last visited June 14, 2012).

list did LinkedIn become aware that its security had been breached and that confidential information had been removed. Initially, LinkedIn publicly responded by stating, "Our security team continues to investigate this morning's reports of stolen passwords. At this time, we're still unable to confirm that any security breach has occurred."[6]

27. However, on June 9, 2012, LinkedIn admitted that it was not handling user data in accordance with best practices. LinkedIn stated that "one of our major initiatives was the transition from a password database system that hashed passwords, i.e. provided one layer of encoding, to a system that both hashed and salted the passwords, i.e. provided an extra layer of protection that is a widely recognized best practice within the industry. That transition was completed prior to news of the password theft breaking on Wednesday. We continue to execute on our security roadmap, and we'll be releasing additional enhancements to better protect our members."[7] But these actions were too little too late — LinkedIn's transition to more stringent data protection practices clearly occurred *after* its servers were breached, as the passwords publicly posted were, by its own admission, only hashed.

28. That LinkedIn did not recognize its databases had been compromised until it was informed through public channels provides further evidence that the company didn't adhere to industry standards. Specifically, LinkedIn did not implement, or it poorly implemented, an intrusion detection system to properly identify and quickly respond to attacks on its servers.

LinkedIn's Business Model

29. LinkedIn offers products and services in the form of online applications to be used in conjunction with online social networks.

---

[6] Updating Your Password on LinkedIn and Other Account Security Best Practices, http://blog.linkedin.com/2012/06/06/updating-your-password-on-linkedin-and-other-account-security-best-practices/ (last visited June 12, 2012).

[7] An Update On Taking Steps To Protect Our Members, http://blog.linkedin.com/2012/06/09/an-update-on-taking-steps-to-protect-our-members/ (last visited June 12, 2012).

30. LinkedIn's consumers pay for LinkedIn's products and services both with actual dollars and with their PII. Put another way, in addition to a more conventional subscription fee, "free" account users buy products and services by paying LinkedIn in the form of contact information (first name, last name, and an email address). Put yet another way, LinkedIn users provide something valuable — access to their personal information — in exchange for LinkedIn's products and services, which include LinkedIn's promise to employ industry standard protocols and technology to safeguard their PII.

31. Even for customers that it does not directly charge using traditional legal tender, LinkedIn is able to generate earnings from users through the receipt of their personal information. LinkedIn describes itself as a "unique social application-based advertising network." In other words, LinkedIn makes money by selling targeted advertising space, similar to a newspaper or television program.

32. But unlike traditional newspaper or television marketing, LinkedIn is a particularly attractive advertising platform because it possesses detailed demographic information that may be used to direct highly targeted ads to its customers.

33. If not for the inherent and quantifiable value of access to its users' personal data, LinkedIn could not sustain financial viability, as a considerable portion of its user base are not "premium" members, and thus do not pay monthly fees. Thus, the promises contained in its Privacy Policy concerning the safeguarding of consumer data that LinkedIn receives in exchange for its products and services are vital to its business and to its consumers.

FACTS RELATING TO PLAINTIFF

34. During the relevant time period, Plaintiff Katie Szpyrka was a registered account holder with LinkedIn. She registered with LinkedIn in or around late 2010.

35. Beyond simply being a registered user of LinkedIn, Plaintiff additionally paid a monthly fee to use LinkedIn's upgraded services. From approximately late 2010 to November 2011 she paid $24.95 per month, and from December 2011 to the present she has

paid $26.95 per month.

36. In signing up to utilize LinkedIn, Plaintiff submitted her first name, last name, email address and a unique password to LinkedIn.

37. In creating an account with Defendant, Plaintiff agreed to LinkedIn's User Agreement and Privacy Policy, including the material term that "Personal information you provide will be secured in accordance with industry standards protocols and technology."

CLASS ALLEGATIONS

38. Plaintiff Katie Szpyrka brings this action pursuant to Fed. R. Civ. P. 23(b)(2) and (3) on behalf of herself and a Class and SubClass of similarly situated individuals, defined as

> **LinkedIn User Class:** All individuals and entities in the United States who had a LinkedIn account on or before June 6, 2012.
>
> **Upgraded LinkedIn User SubClass:** All LinkedIn User Class Members who paid a monthly fee to LinkedIn for an upgraded account.

Excluded from the Class and SubClass are: 1) any Judge or Magistrate presiding over this action and members of their families; 2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current or former employees, officers and directors; 3) counsel for Plaintiff and Defendant; 4) persons who properly execute and file a timely request for exclusion from the class; 5) the legal representatives, successors or assigns of any such excluded persons; and 6) all persons who have previously had claims similar to those alleged herein finally adjudicated or who have released their claims against Defendant; 7) as well as any individual who contributed to the unauthorized access of LinkedIn's database.

39. The exact number of Class and SubClass members is unknown to Plaintiff at this time, but on information and belief, there are hundreds of thousands of persons in the Class and SubClass, making joinder of each individual member impracticable. Ultimately,

Class and SubClass members will be easily identified through Defendant's records.

40. Plaintiff's claims are typical of the claims of all of the other members of the Class and SubClass.

41. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class and SubClass. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and SubClass, and have the financial resources to do so. Neither Plaintiff nor her counsel have any interest adverse to those of the other members of the Class and SubClass.

42. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitive and will have no effective remedy. The class treatment of common questions of law and fact is also superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants, and promotes consistency and efficiency of adjudication.

43. LinkedIn has acted and failed to act on grounds generally applicable to Plaintiff and the other members of the Class and SubClass, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and SubClass.

44. The factual and legal bases of LinkedIn's liability to Plaintiff and to the other members of the Class and SubClass are the same and resulted in injury to Plaintiff and all of the other members of the Class. Plaintiff and the other members of the Class and SubClass have all suffered harm as a result of LinkedIn's wrongful conduct.

45. There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class and SubClass, and those questions predominate over any questions that may affect individual members of the Class and SubClass. Common questions for the Class and SubClass include but are not limited to the following:

(a) whether LinkedIn failed to protect users' PII with industry standard protocols and technology;

(b) whether storing user e-mails and passwords in a partially unencrypted format complied with industry standard protocols and technology;

(c) whether LinkedIn's conduct described herein violated the Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200, *et seq.*);

(d) whether LinkedIn's conduct describe herein violated the California Legal Remedies Act (Cal. Civ. Code §§ 1750, *et seq.*);

(e) whether LinkedIn's conduct described herein constitutes a breach of contract;

(f) whether LinkedIn's conduct described herein constitutes breach of the implied covenants of good faith and fair dealing;

(g) whether LinkedIn's conduct described herein constitutes breach of implied contracts;

(h) whether LinkedIn's conduct described herein was negligent and/or grossly negligent; and,

(i) whether LinkedIn's conduct described herein constitutes negligence *per se*.

46. Plaintiff reserves the right to revise the definitions of the Class and SubClass based on further investigation, including facts learned in discovery.

FIRST CAUSE OF ACTION
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On Behalf of Plaintiff and the Class and SubClass)

47. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

48. California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq.*, protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

49. The UCL prohibits any unlawful, unfair or fraudulent business act or practice. A business practice need only meet one of the three criteria to be considered unfair competition. An unlawful business practice is anything that can properly be called a business practice and that at the same time is forbidden by law.

50. As described herein, Defendant's knowing and willful failure to safeguard and secure its users' sensitive PII violates the UCL.

51. Commonly accepted and widely practiced industry standards provide that sensitive PII stored in a commercial database should be not be accessible to extraction and simple decryption, and commercially reasonable methods to prevent such access are widely known throughout the security industry.

52. LinkedIn willfully and knowingly failed to expend the resources necessary to protect the sensitive data entrusted to it by Plaintiff and the Class in clear contradiction of accepted industry standards for database security and its own agreements. In creating the perception that it followed industry standard protocols for database protection, and explicitly stating as much, LinkedIn gained an unfair advantage over its competitors.

53. Additionally, LinkedIn deceived consumers by providing in its Privacy Policy that its users' PII would be "protected with industry standard protocols and technology."

54. By failing to maintain its consumers' personal data in a properly encrypted database, LinkedIn failed to use commercially reasonable safeguards to protect its consumers' personal data. Storing sensitive PII in simple hashed values is not commercially reasonable and does not comport with industry standard protocols and technology, as promised.

55. Plaintiff and the Class members relied on LinkedIn's misrepresentations that it would employ industry standard protocols and technology to safeguard their personal data.

56. By failing to employ industry standard protocols and technology to safeguard its users' personal data, LinkedIn violated its own written policy and acted deceptively.

57. Defendant has violated the "unlawful" prong of the UCL because its conduct as alleged herein violated the Consumer Legal Remedies Act, Cal. Civ. Code §§ 1750 *et seq.*

58. Defendant has violated the fraudulent prong of the UCL by misrepresenting to its users that it would employ industry standard protocols and technology to safeguard and secure their PII in order to induce reliance on its statements for commercial gain.

59. LinkedIn's misrepresentations regarding its security procedures were likely to deceive the public because they were authoritative descriptions made in the contracts between LinkedIn and its users. Because PII privacy and security is likely to, and does, affect consumers' willingness to use and pay for a service, LinkedIn's misrepresentations were material.

60. Defendant has violated the unfair prong of the UCL because it operated a business that induced consumers to submit PII with the written assurance that the data would be protected through industry standard protocols and technology. However, Defendant knowingly failed to employ industry standard protocols and technology for data protection, causing the widespread exposure of its users' PII. Thus, Defendant's failure to implement industry-standard security practices caused harm to consumers that substantially outweigh any benefit LinkedIn received from its practices.

61. Defendant's unfair or deceptive practices occurred primarily and substantially in California. Decisions concerning the retention and safeguarding of user information were made in California, LinkedIn maintains all or a substantial part of its computer systems containing user information in California, and the security breach of its computer systems took place primarily and substantially in California.

62. As a result of LinkedIn's conduct as alleged herein, Plaintiff and the Class members have lost money and/or property. All Class members have lost money in the form of the value of their personal data. They have lost property in the form of their breached personal data, which is of great value to LinkedIn, LinkedIn's advertisers, and malicious

actors. Additionally, SubClass members have lost money in the form of monthly membership fees paid partially in exchange for LinkedIn promising to use industry standard protocols and technology to protect their personal data. Because LinkedIn failed to deliver on its bargained-and paid-for promise, SubClass members have suffered economic damage.

63. Pursuant to Cal. Bus. & Prof. Code §§ 17203 and/or 17204, Plaintiff seeks an order permanently enjoining Defendant from continuing to engage in the unfair and unlawful conduct described herein. Plaintiff seeks an order requiring Defendant to (1) immediately stop the unlawful practices stated in this Complaint; (2) ensure that LinkedIn user data does not appear in Internet search engines; (3) ensure that LinkedIn employs commercially reasonable methods to safeguard its user data; and, (4) pay attorney's fees, and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

SECOND CAUSE OF ACTION
Violation of the Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.*
(On Behalf of Plaintiff and the Class and SubClass)

64. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

65. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") prohibits the act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, concealment, suppression or omission of any material fact with intent that others rely upon such act in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.

66. As described within, Defendant has engaged in deceptive practices, unlawful methods of competition, and/or unfair acts as defined by the CLRA, to the detriment of Plaintiff and the Class.

67. Defendant, acting with knowledge, intentionally and unlawfully brought harm upon Plaintiff and the Class by deceptively inducing Plaintiff and the Class to register with LinkedIn based upon deceptive and misleading representations that it would take

commercially reasonable steps to safeguard its users' sensitive PII in line with industry standards and technology. Specifically, Defendant violated the CLRA by violating § 1770(a)(5) by representing that goods or services have characteristics and benefits, which they do not have. Specifically, LinkedIn represented that it used industry standard protocols and technology to protect its consumers' data, which it did not actually do.

68. Plaintiff and the Class members purchased LinkedIn's products and services by paying LinkedIn with valuable personal information, thereby making them consumers under the CLRA. Likewise, Plaintiff and SubClass members paid money to Defendant in the form of monthly subscription fees for Defendant's services.

69. Plaintiff and the Class members relied on LinkedIn's promise to use industry standard protocols and technology to safeguard their personal data in registering a LinkedIn account. Because LinkedIn intended Plaintiff and the Class to rely as such, LinkedIn's misstatements occurred as part of a transaction intended to result in a sale or lease of goods to consumers.

70. Plaintiff and the Class have suffered harm as a direct and proximate result of the Defendant's violations of law and wrongful conduct.

71. Under Cal. Civ. Code §§ 1780(a) and (b), Plaintiff and the Class seek injunctive relief requiring Defendant to cease and desist the illegal conduct described herein, and any other appropriate remedy for violations of the CLRA. For the sake of clarity, Plaintiff explicitly disclaims any claim for damages under the CLRA at this time.

THIRD CAUSE OF ACTION
Breach of Contract
(On Behalf of Plaintiff and the Class)

72. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

73. In order to use its social-networking applications, Defendant required that Plaintiff and the other Class members affirmatively assent to its User Agreement and Privacy Policy (the "Agreement"). Plaintiff and the other Class members assented to the Agreement

by registering for and using LinkedIn's service.

74. The Agreement's provisions constitute a valid and enforceable contract between Plaintiff and Class members on the one hand, and Defendant on the other.

75. Under the terms of the Agreement, Plaintiff and the other Class members agreed to pay LinkedIn in the form of their valuable personal data in exchange for LinkedIn's products and services and LinkedIn's promise to use industry standard protocols and technology to protect Class members' data.

76. Under the Agreement, in order to use Defendant's social networking applications, Plaintiff and the other Class members transmitted several pieces of sensitive PII to Defendant, including but not limited to their e-mail addresses and corresponding passwords. In turn, under the Agreement, Defendant promised that LinkedIn would protect its users' PII with "industry standard protocols and technology."

77. Defendant materially breached the terms of the Agreement by its wrongful conduct alleged herein, including failing to properly secure its databases, thereby allowing Plaintiff's and the Class's sensitive PII to be compromised, exposing Plaintiff and the other Class members to a heightened risk of identity theft, causing Plaintiff and the other Class members distress related to their unsecured personal data, as well as distress related to the security of their other personal accounts being exposed and accessed without authorization.

78. As a result of Defendant's misconduct and breach of the Agreement described herein, Plaintiff and Class members suffered injury. Plaintiff and the other Class members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their personal information, which has ascertainable value to be proven at trial.

FOURTH CAUSE OF ACTION
Breach of Contract
(On Behalf of Plaintiff and the SubClass)

79. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

80. In order to use its social-networking applications, Defendant required that Plaintiff and the other SubClass members affirmatively assent to its User Agreement and Privacy Policy (the "Agreement"). Plaintiff and the SubClass members assented to the Agreement by registering for and using LinkedIn's service.

81. The Agreement's provisions constitute a valid and enforceable contract between Plaintiff and SubClass members on the one hand, and Defendant on the other.

82. Under the terms of the Agreement, Plaintiff and the other SubClass members agreed to pay LinkedIn a monthly fee in exchange for upgraded versions of LinkedIn's products and services, and LinkedIn's promise to use industry standard protocols and technology to protect SubClass members' data.

83. As described herein, Defendant materially breached the terms of the Agreement by failing to use industry standard protocols and technology to protect Plaintiff's and the other SubClass members' data as promised.

84. As a result of Defendant's misconduct and breach of the Agreement described herein, Plaintiff and the other SubClass members suffered injury in the form of monies paid to Defendant. Plaintiff and SubClass members did not receive the benefit of the bargain for which they contracted, and for which they paid monthly fees.

FIFTH CAUSE OF ACTION
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff and the Class and SubClass)

85. Plaintiff incorporates the foregoing allegations as if fully set forth herein, excluding paragraphs 71–84).

86. Plaintiff hereby pleads in the alternative to the Third and Fourth Causes of Action.

87. In order to use Defendant's social-networking site, Plaintiff and the other Class and SubClass members affirmatively assented to Defendant's User Agreement and Privacy Policy.

88. The Agreement's provisions constitute a valid and enforceable contract between Plaintiff and Class and SubClass members on the one hand, and Defendant on the other.

89. Implicit in the Agreement were contract provisions that prevented Defendant from engaging in conduct that frustrated or injured Plaintiff and the other Class and SubClass members' rights to receive the benefits of the Agreement.

90. Defendant's obligation to use industry standard protocols and technology to safeguard and secure Plaintiff and the other Class and SubClass members' sensitive PII was a material term of the Agreement.

91. Furthermore, implicit in the terms of the Agreement was Defendant's obligation to comply with Cal. Bus. & Prof. Code §§ 17200, *et seq.* and Cal. Civ. Code §§ 1750, *et seq.*

92. Defendant breached the implied covenant of good faith and fair dealing by failing to safeguard and secure sensitive PII from unauthorized access and theft and further by failing to fully comply with the proscriptions of applicable statutory law. In so doing, LinkedIn acted consciously and deliberately.

93. Defendant's misconduct and breach of the implied covenant of good faith and fair dealing as described herein resulted in injury to Plaintiff and the other Class and SubClass members. Plaintiff and the other Class members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their personal information that has ascertainable value to be proven at trial, and in the case of SubClass members, in the form of monthly fees paid to Defendant.

SIXTH CAUSE OF ACTION
Breach of Implied Contracts
(On Behalf of Plaintiff and the Class and SubClass)

94. Plaintiff incorporates the foregoing allegations as if fully set forth herein, paragraphs 71–84.

95. Plaintiff hereby pleads in the alternative to her Third and Fourth Causes of Action.

96. In order to use Defendant's social-networking site, Plaintiff and the other Class and SubClass members transmitted several pieces of sensitive PII to Defendant, including their e-mail addresses and corresponding passwords. Additionally, Plaintiff and the other SubClass members paid monthly fees in order to use Defendant's upgraded services.

97. By providing that sensitive PII, and upon Defendant's acceptance of such information and monthly fees, Plaintiff and the other Class and SubClass members, on the one hand, and Defendant, on the other hand, entered into implied contracts whereby Defendant was obligated to take commercially reasonable steps to secure and safeguard Plaintiff's and the other Class and SubClass members' information.

98. Without such implied contracts, Plaintiff and the other Class and SubClass members would not have provided their personal information to Defendant, or in the case SubClass members, would not have paid monthly fees to LinkedIn.

99. By failing to properly secure Plaintiff and the other Class and SubClass members' sensitive PII, Defendant breached its implied contracts with Plaintiff and the other Class and SubClass members.

100. Defendant's breaches and other misconduct described herein resulted in injury to Plaintiff and the other Class and SubClass members. Plaintiff and the other Class and SubClass members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their personal information that has ascertainable value to be proven at trial, and in the case of SubClass members, in the form of monthly fees paid to Defendant.

SEVENTH CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class and SubClass)

101. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

102. In order to use Defendant's social-networking site, Plaintiff and the other Class and SubClass members transmitted sensitive PII to Defendant, including their e-mail addresses and corresponding passwords. Additionally, SubClass members paid monthly fees in order to use Defendant's upgraded services.

103. By agreeing to accept Plaintiff and the other Class and SubClass members' sensitive PII, Defendant assumed a duty, which required it to exercise reasonable care to secure and safeguard that information and to utilize industry standard protocols and technology to do so.

104. Defendant failed to properly encrypt Plaintiff's and the other Class and SubClass members' passwords in line with industry standards and best practices, thereby breaching its duties to Plaintiff and the other Class and SubClass members.

105. By failing to take proper security measures to protect Plaintiff's and the other Class and SubClass members' sensitive PII as described herein, Defendant acted with gross negligence and departed from all reasonable standards of care.

106. As a direct and proximate result of Defendant's failure to exercise reasonable care and use commercially reasonable security measures, its databases were accessed (*i.e.*, "hacked") without authorization and Plaintiff's and the other Class and SubClass members' sensitive PII was compromised and their information was exposed to unauthorized access.

107. A security breach and unauthorized access was reasonably foreseeable by Defendant, particularly in light of the fact that protections necessary to secure and safeguard databases were well-known within the industry and had been successfully used to protect sensitive PII for years prior to this breach.

108. Neither Plaintiff nor the other members of the Class and SubClass contributed to the security breach or insufficient security described herein.

109. As a direct and proximate result of Defendant's misconduct described herein, Plaintiff and the other Class and SubClass members were injured because their personal

information was not properly secured and was thus subject to public disclosure without consent, and because they were deprived the benefit of the services for which they bargained and for, for which they paid valuable consideration in the form of their personal information, which has ascertainable value to be proven at trial. Additionally, SubClass members lost money in the form of monthly fees paid in order to use Defendant's upgraded services.

EIGHTH CAUSE OF ACTION
Negligence *Per Se*
(On behalf of Plaintiff and the Class and SubClass)

110. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

111. Defendant's violations of Cal. Bus. & Prof. Code §§ 17200, *et seq.* and Cal. Civ. Code §§ 1750, *et seq.*, resulted in injury to Plaintiff and the other Class and SubClass members.

112. The harm Defendant caused to Plaintiff and the other Class and SubClass members are injuries that result from the type of occurrences those statutes were designed to prevent.

113. Plaintiff and the other Class and SubClass members are the type of persons for whose protection those statutes were adopted.

114. The harm caused to Plaintiff and the other Class and SubClass members was reasonably foreseeable as a result of LinkedIn's breach of its statutory duties, as the consequences of insufficient information security practices are particularly well known within the social networking and data management industry.

115. Defendant's violations of the foregoing statutes as described herein resulted in injury to Plaintiff and the other Class and SubClass members. Plaintiff and the other Class and SubClass members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their personal information, which has ascertainable value to be proven at trial. Additionally, SubClass members lost money in the form of monthly fees paid in order to use Defendant's upgraded services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class and SubClass, prays for the following relief:

A. Certify this case as a class action on behalf of the Class and SubClass defined above, appoint Katie Szpyrka as Class and SubClass representative, and appoint her counsel as Class and SubClass counsel;

B. Declare that LinkedIn's actions, as described herein, violate the California Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200, *et seq.*) and the Consumer Legal Remedies Act (Cal. Bus. & Prof. Code §§ 1750), and constitute breach of contract, or in the alternative, breach of the implied covenant of good faith and fair dealing, or in the alternative, breach of implied contract, as well as negligence and negligence *per se*.

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff the other Class and SubClass members, including, *inter alia*: (i) an order prohibiting LinkedIn from engaging in the wrongful and unlawful acts described herein; (ii) ensuring that LinkedIn user data does not appear in Internet search engines; and (iii) requiring LinkedIn to protect all data collected through the course of its business in accordance with industry standards;

D. Award damages to Plaintiff and the other Class and SubClass members in an amount to be determined at trial;

E. Award Plaintiff and the other Class and SubClass members their reasonable litigation expenses and attorneys' fees;

F. Award Plaintiff and the other Class and SubClass members pre- and post-judgment interest, to the extent allowable; and

G. Award such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Respectfully submitted,

Dated: June 15, 2012

Sean P. Reis

SEAN P. REIS (SBN 184044)
(sreis@edelson.com)
EDELSON MCGUIRE LLP
30021 Tomas Street, Suite 300
Rancho Santa Margarita, California 92688
Telephone: (949) 459-2124

JAY EDELSON*
(jedelson@edelson.com)
RAFEY S. BALABANIAN*
(rbalabanian@edelson.com)
ARI J. SCHARG*
(ascharg@edelson.com)
CHRISTOPHER L. DORE*
(cdore@edelson.com)
EDELSON MCGUIRE LLC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Telephone: (312) 589-6370

**Motion for admission pro hac vice to be filed*