Eric H. Gibbs (State Bar No. 178658)
ehg@girardgibbs.com
Dylan Hughes (State Bar No. 209113)
dsh@girardgibbs.com
Geoffrey A. Munroe (State Bar No. 228590)
gam@girardgibbs.com
Amy M. Zeman (State Bar No. 273100)
amz@girardgibbs.com
GIRARD GIBBS LLP
601 California Street, 14th Floor
San Francisco, California 94104
Telephone: (415) 981-4800
Facsimile: (415) 981-4846

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

CV 12 4034

Jeff Allan, on behalf of himself and all others similarly situated,

Plaintiff,

vs.

YAHOO! INC.,

Defendant.

Case No. [redacted]

CLASS ACTION COMPLAINT FOR:

(1) Negligence

DEMAND FOR JURY TRIAL

HRL

SUMMARY OF THE CASE

1. Yahoo! Inc. is a leading Internet company that provides Internet based services to millions of users on a monthly basis and yet failed to deploy even the most rudimentary of protections for certain users' personal information. Consequently, a group of hackers, in the name of publicly humiliating Yahoo for it lax security measures, infiltrated a Yahoo database and publicly posted login credentials from over 450,000 accounts.

2. Plaintiff Jeff Allan is one of the approximately 450,000 users whose information was posted online for the world to see and use. Within days of the breach, Mr. Allan received an alert of account fraud on his eBay account, which used the same login credentials as disclosed in the Yahoo breach. Mr. Allan does not know what other information the hackers and others have gathered about him.

3. Plaintiff Allan brings this class action lawsuit against Yahoo for failing to adequately safeguard his and others' personal information. Mr. Allan seeks an order requiring Yahoo to remedy the harm caused by its negligent security, which may include compensating Plaintiff and class members for resulting account fraud and for all reasonably necessary measures Plaintiff and class members have had to take in order to identify and safeguard the accounts put at risk by Yahoo's negligent security.

PARTIES

4. Plaintiff Jeff Allan is a resident of the State of New Hampshire. Mr. Allan is one of approximately 450,000 people whose e-mail address and password were publicly disclosed on the internet because Yahoo did not take reasonable measures in securing them.

5. Defendant Yahoo! Inc. is a Delaware corporation with its principal place of business at 701 First Avenue, Sunnyvale, California 94089. Yahoo does business throughout the State of California and the United States. Yahoo maintains a substantial portion of its computer systems in California.

JURISDICTION AND VENUE

6. This Court has original jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 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, exclusive of interest and costs, (c) the proposed class consists of more than 100 class members, and (d) none of the exceptions under the

subsection apply to this action.

7. Venue is proper in this District under 28 U.S.C. § 139l(b) 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.

INTRADISTRICT ASSIGNMENT

8. Assignment is proper to the San Jose division of this District under Local Rule 3-2(c), as a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in Santa Clara County.

COMMON FACTUAL ALLEGATIONS

Associated Content and the Yahoo! Contributor Network

9. Yahoo is a Delaware corporation that operates a host of Internet websites and services, including a web portal, search engine, and e-mail service. Roughly 700 million people visit Yahoo websites every month, making them among the most popular on the internet.

10. In 2010, Yahoo paid $100 million for Associated Content, a company that published text, image, and video media contributed by freelancer authors registered with the company. To contribute material before the Yahoo purchase, users had to establish an account with Associated Content, using an e-mail address as the login name and creating a password. Some or all of these login credentials were obtained by Yahoo when it acquired Associated Content.

11. In November 2010, Yahoo launched the Yahoo! Contributor Network, calling it "an evolution of the Associated Content platform" that would "bring contributions from more than 450,000 writers, photographers, and videographers to the Internet's largest media destinations, including Yahoo! News, Yahoo! Finance, Yahoo! Sports, and even the Yahoo! Homepage, among many others." In December 2011, Yahoo also announced Yahoo! Voices, a new digital library for content published by the Yahoo! Contributor Network, including content acquired with Associated Content. Registered users of the Yahoo! Contributor Network can contribute content and, in some cases, earn money if Yahoo publishes their content.

The Security Breach

12. On July 11, 2012, a group of hackers reportedly based in Eastern Europe and known as

"the D33Ds Company" breached Yahoo's security measures and extracted e-mail addresses and passwords that were stored unencrypted within a Yahoo database. D33Ds then posted these login credentials, which were associated with roughly 453,000 Associated Content users, online in a plaintext file, stating that they did so in order to provide a "wake-up" call to Yahoo about its lack of proper security.

13. The hackers used a technique known as a "SQL injection attack," which works by "injecting" malicious commands into the stream of commands between a website application and the database software feeding it. If the database does not properly screen these inputs for signs of attack, the attackers can acquire information from the database that they would otherwise be barred from accessing. In essence, a SQL injection attack exploits the way in which a website communicates with back-end databases, allowing an attacker to issue commands (in the form of specially crafted SQL statements) to a database that contains information used by the website application, such as users' login credentials.

14. Reasonable information security measures include protecting personal information by securing the data server containing that information from SQL injection attacks, encrypting critical data (such as login credentials) contained in the database, and monitoring network activity to identify suspicious amounts of out-bound data. Proper encryption often includes salting and hashing passwords, which refers to adding strings of random characters to the passwords and then obscuring the data with a cryptography algorithm.

15. Yahoo, however, failed to employ these basic security measures to protect the personal information obtained and posted by D33Ds. Yahoo does employ these measures to safeguard other data in its possession, but did not do so with respect to the login credentials obtained from Associated Content and affected by the July 11 data breach.

16. Yahoo's servers should not have been vulnerable to a SQL injection attack. When interviewed about the Yahoo breach, Randy Abrams, research director at NSS Labs, a technology security research and testing company, stated that "[t]he only place we should be seeing SQL injection attacks today is in the classroom, as IT professionals are being trained to prevent such attacks."

17. Jason Rhykerd, an IT security expert with SystemExperts, estimates that the hackers captured more than 2,000 database tables and column names, along with 298 MySQL variables. Mr.

Rhykerd stated that "[t]he amount of network traffic this attack would have generated should of set off the lightest of [intrusion detection system] rules."

18. Anders Nilsson, security expert and chief technology officer of security company Eurosecure, points out that "[w]ith the security policies [Yahoo] has in place for its other sites, it should have known to at least put up a firewall to detect these kind of things."

19. The SQL injection technique used against Yahoo has been known for over a decade and had already been used for massive data thefts against Heartland Payment Systems and others. As far back as 2003, the Federal Trade Commission considered SQL injection attacks to be well-known and foreseeable events that can and should be taken into account through routine security measures. As the FTC stated in a complaint filed against a company who claimed but failed to use reasonable internet security measures:

> The risk of web-based application attacks is commonly known in the information technology industry, as are simple, publicly available measures to prevent such attacks. Security experts have been warning the industry about these vulnerabilities since at least 1997; in 1998, at least one security organization developed, and made available to the public at no charge, security measures which could prevent such attacks; and in 2000, the industry began receiving reports of successful attacks on web-based applications.

20. Yahoo also should have maintained Plaintiff's and class members' critical login credentials in encrypted form, which would have made them unusable in the event of a security breach. Instead, Yahoo stored this personal information in an unencrypted format that could be read by anyone who obtained access to the database, including Yahoo employees.

21. Had Yahoo encrypted the data using standard salting and hashing techniques, the data stolen from Yahoo would have been prohibitively difficult to utilize, as each password would have to be cracked individually. For example, another Internet company (social Q&A website Formspring) whose data was recently stolen appears to have successfully protected its user's personal information with such encryption.

22. As a result of Yahoo's negligent security practices, D33Ds was able to post online the critical login credentials associated with roughly 453,000 Associated Content accounts. Unauthorized individuals could use this information to login into an affected user's Associated Content or Yahoo!

Contributor Network account, and access the personal information contained within the account—including, for instance, the accountholder's PayPal ID.

23. Yahoo's failure to protect the critical login credentials it acquired with Associated Content also put users' accounts with other online service providers at risk because many people use the same login credentials across multiple Internet sites. For instance, a user might use the same e-mail address and password to access a PayPal, Amazon, or internet banking account.

24. In its Yahoo Security Center, Yahoo itself cautions users to protect their login credentials, answering its own question "Why should I worry about my privacy on the Internet?" as follows:

> You could be locked out of your online account and be unable to access your e-mail. But there can be even greater consequences. You could be the victim of identity theft.
>
> Once identity thieves have your personal information, the results can be far-reaching, difficult to rectify, and financially devastating.
>
> Armed with your credit card information, fraudsters could charge thousands of dollars to your account before you ever see a statement from your credit card company. They can open new credit card accounts in your name.
>
> Using your identity, they can open a bank account and write bad checks on that account. They can authorize electronic transfers in your name, draining your bank account. To avoid legal action against debts they've incurred using your identity, they might even file for bankruptcy under your name.
>
> They can take out a loan, buy a car, and get a driver's license — all in your name. They may use your name to get a job or file fraudulent tax returns. And if they're arrested, they may give your name to the police and fail to show up for their court date. Then, a warrant for an arrest is issued — in your name.

25. SQL injection attacks are well-understood in the Internet Technology industry, having taken place for over a decade, and techniques to resist such attacks are both well-known and in common use by all major Internet businesses. Yahoo failed to use industry standard SQL database protections, monitoring techniques, and encryption practices to protect the user data contained within its database. In particular, Yahoo failed to secure its data server containing Plaintiff's and class members' information from SQL injection attacks, encrypt the critical login credentials contained in the database, and monitor its network activity to identify suspicious amounts of out-bound data. In so doing, Yahoo

violated its duty to reasonably secure the personal information it acquired with Associated Content, resulting in unauthorized persons having access to those critical login credentials and thus access to affected users' Associated Content or Yahoo! Contributor Network accounts and other Internet accounts containing personal information.

PLAINTIFF'S EXPERIENCE

26. Mr. Allan opened an account with Associated Content in November 2009 and published articles through the network. Mr. Allan's Content Network account contained personal information, including his full name, e-mail address, PayPal e-mail address, date of birth, residency/citizenship, physical address, telephone number, biography, interests and area of expertise, and education. Associated Content also had Mr. Allan's social security number. All of this information was solicited when Mr. Allan opened his account with Associated Content.

27. On the morning of July 14, 2012, Mr. Allan received e-mails from two online services that he used, informing him of the Yahoo breach. Both services had identified him as a user with breached account information and proactively disabled his passwords.

28. Mr. Allan then changed the passwords for all of the online accounts he could think of. Mr. Allan has been writing content for a variety of websites for several years and many of the accounts he has established to contribute content have personal information related to tax reporting and associated with financial accounts, as well as his social security number.

29. Mr. Allan next attempted to access his Associated Content account through Yahoo! Contributor Network but was unable to do so. Later that afternoon, Mr. Allan received an e-mail from Yahoo informing him of the breach and suggesting that he contact his e-mail service provider to secure his account and monitor activity on all of his online accounts.

30. Mr. Allan used the same login credentials that were stolen and posted online in the security breach to access his eBay account. On the afternoon of July 20, 2012, Mr. Allan received an e-mail from eBay informing him that someone had accessed his account without his permission and that the e-mail address associated with the account may have been changed. Mr. Allan had not used his eBay account since 2010.

31. Concerned about unauthorized access to his online accounts, Mr. Allan purchased an

Experian credit monitoring service for $14.95/month.

CLASS ACTION ALLEGATIONS

32. Plaintiff Jeff Allan brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and a class preliminarily defined as:

> All persons whose personal information was accessed and subsequently disclosed following a data breach of Yahoo! Contributor Network on or about July 11, 2012.

Excluded from the class are Yahoo; any agent, affiliate, parent, or subsidiary of Yahoo; any entity in which Yahoo has a controlling interest; any officer or director of Yahoo; any successor or assign of Yahoo; and any Judge to whom this case is assigned, as well as his or her staff and immediate family.

33. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy prerequisites for suing as a representative party pursuant to Rule 23.

34. **Numerosity**. The proposed class consists of approximately 450,000 persons—far too many to join in a single action.

35. **Commonality**. Plaintiff's and class members' claims raise predominantly common factual and legal questions that can be answered for all class members through a single class-wide proceeding. For example, to resolve any class member's claims, it will be necessary to answer the following questions. The answer to each of these questions will necessarily be the same for each class member.

a. Did Yahoo have a legal duty to use reasonable security measures to protect class members' personal information?

b. Did Yahoo breach its legal duty by failing to secure the data server containing Plaintiff's and class members' information from SQL injection attacks, encrypt the personal information contained in the database, and monitor its network activity to identify suspicious amounts of out-bound data?

c. Did any breach by Yahoo of its legal duty to use reasonable security measures cause Plaintiff and class members legally-cognizable damages?

36. **Typicality.** Plaintiff's claims are typical of class members' claims as each arises from the same data breach and the same alleged negligence on the part of Yahoo in handling class member's

personal information.

37. **Adequacy**. Plaintiff will fairly and adequately protect the interests of the class. His interests do not conflict with class members' interests and he has retained counsel experienced in complex class action litigation and data privacy to vigorously prosecute this action on behalf of the class.

38. In addition to satisfying the prerequisites of Rule 23(a), Plaintiff satisfies the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual members and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing Yahoo's conduct economically feasible in the absence of the class action procedure.

39. In the alternative, class certification is appropriate under Rule 23(b)(2) because Defendant has acted or refused to act on grounds generally applicable to the class, thereby making final injunctive relief appropriate with respect to the members of the class as a whole.

FIRST CAUSE OF ACTION

(For Negligence)

40. Plaintiff incorporates the above allegations by reference.

41. By maintaining their personal information in a database that was accessible through the Internet, Yahoo owed Plaintiff and class members a duty to employ reasonable Internet security measures to protect that information.

42. Yahoo failed to secure the data server containing that information from SQL injection attacks, encrypt the personal information contained in the database, and monitor its networks to identify suspicious amounts of out-bound data. In failing to employ these basic and well-known internet security measures, Yahoo departed from the reasonable standard of care and violated its duty to protect Plaintiff's and class members' personal information.

43. As a direct and proximate result of Yahoo's failure to exercise reasonable care and use commercially reasonable Internet security measures, its databases were accessed by unauthorized individuals who obtained and disclosed the unencrypted personal information of Plaintiff and class

members.

44. The unauthorized access to Plaintiff's and class members' personal information was reasonably foreseeable by Yahoo, particularly considering that the method of access is widely known in the computer and data security industry, and that it has long been standard practice in the Internet technology sector to encrypt personal information, including critical login credentials.

45. Neither Plaintiff nor other class members contributed to the security breach or Yahoo's employment of insufficient security measures to safeguard personal information.

46. As a direct and proximate result of Yahoo's negligence, Plaintiff and class members suffered injury through the public disclosure of their personal information, the unauthorized access to Internet accounts containing additional personal information, and through the heightened risk of unauthorized persons stealing additional personal information. Plaintiff and class members have also incurred the cost of taking measures to identify and safeguard accounts put at risk by disclosure of the personal information stolen from Yahoo, including by purchasing credit monitoring services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, requests that the Court:

a. Certify this case as a class action on behalf of the class defined above, appoint Jeff Allan as class representative, and appoint his counsel as class counsel;

b. Award injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and other class members;

c. Award damages to Plaintiff and class members in an amount to be determined at trial;

d. Award Plaintiff and class members their reasonable litigation expenses and attorneys' fees;

e. Award Plaintiff and class members pre- and post-judgment interest, to the extent allowable; and

f. 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.

Dated: July 31, 2012

GIRARD GIBBS LLP

By: ____________________
Dylan Hughes

Eric H. Gibbs
Geoffrey A. Munroe
Amy M. Zeman
601 California Street, 14th Floor
San Francisco, CA 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846

Attorneys for Plaintiff