

FILED
09 DEC 23 11:10:47
FUGARONE, BECKING, HARRIS & ASSOCIATES
310 PARK BLVD, SUITE 200
MORRISTOWN, NJ 07960

Handwritten signature

ORIGINAL BY FAX

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DAVID C. PARISI (SBN 162248)
(dparisi@parisihavens.com)
SUZANNE HAVENS BECKMAN (SNB 188814)
(shavens@parisihavens.com)
PARISI & HAVENS LLP
15233 Valleyheart Drive
Sherman Oaks, California 91403
Telephone: (818)990-1299
dcparisi@msn.com

JAY EDELSON
(jedelson@kamberedelson.com)
MICHAEL J. ASCHENBRENER
(maschenbrener@kamberedelson.com)

CHRISTOPHER L. DORE
(cdore@kamberedelson.com)
BENJAMIN H. RICHMAN
(brichman@kamberedelson.com)

E-filing

KAMBEREDELSON, LLC
350 North LaSalle Street
Suite 1300
Chicago, Illinois 60654
Telephone: (312) 589-6370
Fax: (312) 589-6378

ATTORNEYS FOR PLAINTIFF AND THE PUTATIVE CLASS

B7

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

C 09 6032

ALAN CLARIDGE, an individual, on behalf
of himself and all others similarly situated,

) Case No.

Plaintiff,

) **CLASS ACTION COMPLAINT FOR:**

v.

ROCKYOU, INC., a Delaware corporation,

Defendant.

- (1) Violations of Cal. Bus. & Prof. Code § 17200
- (2) Violations of Cal. Penal Code § 502
- (3) Violations of Cal. Civ. Code § 1798.80
- (4) Violations of Cal. Civ. Code § 1750
- (5) Breach of Contract
- (6) Breach of Implied Contracts
- (7) Breach of the Implied Covenant of Good Faith and Fair Dealing
- (8) Negligence
- (9) Negligence Per Se

) **DEMAND FOR JURY TRIAL**

COMPLAINT

1 Plaintiff, by and through his attorneys, upon personal knowledge as to himself and his
2 own acts, and upon information and belief as to all other matters, alleges as follows:

3 **NATURE OF THE ACTION**

4 1. Plaintiff, Alan Claridge (“Claridge”), brings this class action complaint
5 against RockYou, Inc. (“RockYou”) for failing to secure and safeguard its users’ sensitive
6 personally identifiable information (“PII”), including e-mail addresses and passwords, as
7 well as login credentials for social networks such as MySpace and Facebook. RockYou
8 knowingly stored Plaintiff and the Class members’ PII in an unprotected format and in a
9 manner easily accessible to malicious intruders, in violation of its own Privacy Policy and
10 accepted industry standards.

11 2. RockYou is a publisher and developer of popular online applications and
12 services for use with social networking sites such as Facebook, MySpace, hi5 and Bebo.

13 3. RockYou stored users’ PII in an unencrypted database with poor network
14 security. RockYou’s willful failure to secure its users’ sensitive PII led to multiple security
15 breaches that exposed 32 million users to identity theft and other malicious conduct. While
16 some security threats are unavoidable in a rapidly developing technological environment,
17 RockYou recklessly and knowingly failed to take even the most basic steps to protect its
18 users’ PII by leaving the data entirely unencrypted and available for any person with a basic
19 set of hacking skills to take the PII of at least 32 million consumers.

20 **PARTIES**

21 4. Plaintiff Alan Claridge is a resident of Evansville, Indiana. He is a registered
22 user of RockYou, Inc.’s services.

23 5. Defendant RockYou, Inc. is a California corporation headquartered in San
24 Mateo County, California, at 585 Broadway Street, #A, Redwood City, California 94063.
25 RockYou does business throughout the State of California and the nation.

1 **JURISDICTION AND VENUE**

2 6. This Court has original jurisdiction over this action pursuant to 28 U.S.C. §
3 1332(d), because (a) at least one member of the putative class is a citizen of a state different
4 from Defendant, (b) the amount in controversy exceeds \$5,000,000, exclusive of interest and
5 costs, and (c) none of the exceptions under the subsection apply to this action.

6 7. Personal jurisdiction and Venue are proper because RockYou is a corporation
7 headquartered in San Mateo County and/or because the improper conduct alleged in the
8 Complaint occurred in, was directed from, and/or emanated or exported from California.

9 **INTRADISTRICT ASSIGNMENT**

10 8. Pursuant to Local Civil Local Rule 3-2(d), this case shall be assigned to either
11 the San Francisco or Oakland Division.

12 **FACTS**

13 9. RockYou offers a variety of products for use through online social networks
14 such as Facebook and MySpace. These products include applications to share photos, write
15 special text on a friend's page, or play games with other users. Once a user begins operating
16 a RockYou application on a social network site, RockYou utilizes that application as a
17 platform to display paid advertisements. RockYou claims to be the leading provider of social
18 networking application-based advertising services, with more than 130 million unique
19 customers using its applications on a monthly basis.

20 10. A customer may sign up to use RockYou's applications through rockyou.com
21 by providing a valid e-mail address and a registration password. RockYou then stores this e-
22 mail address and password in a database. Additionally, and depending upon which online
23 social network a customer chooses to utilize RockYou's products, a user may be required to
24 provide RockYou with a username and password for accessing that network. RockYou also
25 stores this information in its database.

1 11. RockYou asserts through its website that it will safeguard its users sensitive
2 PII. RockYou's Privacy Policy specifically states:

3
4 Our Commitment To Data Security: RockYou! uses
5 commercially reasonable physical, managerial, and technical
6 safeguards to preserve the integrity and security of your
7 personal information. We cannot, however, ensure or warrant
8 the security of any information you transmit to RockYou! and
9 you do so at your own risk. Once we receive your transmission
10 of information, RockYou! makes commercially reasonable
11 efforts to ensure the security of our systems....

12 12. Plaintiff and the Class agreed to RockYou's Terms of Use and Privacy Policy
13 in order to register and use RockYou's products.

14 **RockYou's Unencrypted and Unprotected Storage of PII**

15 13. Under its user agreements, RockYou collects and stores millions of users' PII
16 on a large-scale commercial database, claiming to use "commercially reasonable" methods of
17 data protection. However, until approximately December 5, 2009, RockYou's database
18 stored users' PII in "clear" or "plain" text, meaning there was no form of encryption
19 preventing an intruder from easily reading and removing the sensitive PII. Under widely
20 accepted standards, storing users' PII in clear text is fundamentally outside the bounds of
21 modern database security and a significant risk to the integrity of a user's PII.

22 14. Clear text passwords are not stored in a cryptographically protected form, and
23 therefore are readily accessible to anyone with access to the database. This means that once
24 a hacker gains access to a network or database system, there is no further barrier or
25 protection to removing e-mail addresses and passwords as they are presented without
26 encryption or additional security. Those with access – authorized or unauthorized – may
27 read the passwords as easily as one can read the words in this Complaint.

28 15. By way of analogy, a properly protected database could be compared to the
safety deposit box room at a bank. At any major bank, the hundreds of safe deposit boxes are

1 found inside a walk-in-safe, but then additionally protected by individual two-key locked
2 doors. In the website context, the outer safe door represents basic network security that
3 prevents a hacker from getting anywhere close to a database. However, in the event that a
4 thief is able to bypass the outer safe door, he will encounter a significant second layer (or
5 more) of security to thwart his intentions. RockYou not only left the outer safe door entirely
6 open (as detailed below), but also, left the individual safety deposit boxes open with their
7 contents on display.

8 16. Among the options available to protect its customers' PII, RockYou could
9 have followed a commonly used method of protecting sensitive data that requires conversion
10 and storage of a "hashed" form of a plain text password.¹ A properly designed hash function
11 will make it virtually impossible to decipher the original plain text password.

12 17. RockYou failed to use hashing, salting, or any other common and reasonable
13 method of data protection and therefore drastically exacerbated the consequences of a hacker
14 bypassing its outer layer of web security.

15 **Consumers' E-Mail and Password Unlocks Endless Amounts of Sensitive PII**

16
17 18. The information stored in RockYou's user database is a very powerful set of
18 PII, including email login credentials, that may be used for damaging and malicious
19 purposes.

20 19. By failing to secure its users' PII, RockYou made all of this data available to
21 even the least capable hacker.

22
23
24 ¹ Under this method, when a user inputs a password, the software runs through a
25 cryptographic hash algorithm, and if the hash value generated from the user's input matches
26 the hash stored in the database, access is permitted. A hash value is created by applying a
27 hash function to a string consisting of the submitted password and another value known as a
28 "salt." The salt prevents attackers from easily building a list of hash values for common
passwords.

1 20. Because a majority of internet users utilize identical passwords across a wide
2 range of websites, gaining access to a user's e-mail account name and password has a high
3 likelihood of providing access to a users' personal and/or work e-mail account.²

4 21. Because a person's e-mail account acts as a modern day file cabinet for a
5 variety of interactions, transactions, and correspondence, and is fully searchable, even a
6 cursory review of personal e-mails can provide a litany of valuable and compromising
7 information.

8 22. For example, once a hacker accesses a users' e-mail account, he may be able
9 to take any of the following actions:

10 a. Extract private information from the e-mail inbox including credit card
11 numbers, confidential business information, bank account numbers, etc.;

12 b. Easily see where that person transacts business online (*e.g.*, purchases from
13 online retailers such as Amazon.com or e-mails from a person's bank). Once a person can
14 see where a consumer transacts business, it allows them to (1) attempt to use the e-mail and
15 password already in their possession to sign into that account; or (2) utilize a website's built
16 in "forgotten password" reset mechanism to send a new password to the now accessible e-
17 mail account. Once signed into an online retailer, a consumer's credit card is often pre-
18 stored and may be used for a purchase;

19 c. Access an online payment service such as PayPal, which allows a person to
20 make purchases through a pre-linked credit card;

21 d. Achieve a full scale identify theft by accessing a consumer's social security
22 number, phone number, home address, tax information, bank or credit card account number,
23 birth date, etc.;

24 e. Access health insurance information (including account numbers and
25 _____

26 ² See Rob Leathern, *FTC Security Workshop, Security and Privacy Data*, May 20, 2002
27 (finding that over fifty percent of web users use identical passwords across all websites and
28 applications).

1 passwords), medical records, and otherwise private and confidential medical information;

2 f. Harvest the consumer's contact list for spam. Assuming that each of the
3 exposed 32 million e-mail accounts has only 10 unique contacts (a dramatically conservative
4 estimate), a spammer will have 300 million live e-mail addresses to spam, as well as any
5 phone numbers contained in a user's contact information to use for spam text messages or for
6 use in illegal phone bill cramming.

7 **The Attack on RockYou's Database**

8 23. On December 4, 2009, the online security firm Imperva, Inc. notified
9 RockYou of a security problem with its SQL database.³ Imperva specifically informed
10 RockYou that it had become aware of a SQL injection flaw⁴ as a result of monitoring
11 underground hacker forums. According to Imperva, hackers were regularly discussing
12 RockYou's SQL injection vulnerability and the fact that it was being actively exploited.

13 24. SQL injection flaws have consistently been among the top online security
14 problems of the past decade. For example, in 2007 and 2008, hackers took advantage of a
15 SQL injection flaw to steal 130 million credit card numbers stored on the databases of
16 Heartland Payment Systems, 7-Eleven, and Hannaford Brothers. The attack was widely
17 publicized and is regarded as the largest case of identity theft in American history, re-
18 emphasizing the danger SQL injection attacks pose to commercial database security.

19 25. Because knowledge and understanding of SQL injection flaws has been
20 widespread for more than a decade, measures for protection have become readily available.

21 ³ Like thousands of commercial website operators who collect user information, RockYou
22 utilizes a Structured Query Language ("SQL" (pronounced "sequel")) database. SQL is
23 a database computer language designed for storing data in relational database management
24 systems such as when a company needs to store and manage millions of e-mail accounts and
passwords.

25 ⁴ A SQL injection flaw allows a hacker to take advantage of improperly coded web software
26 to introduce malicious code into a company's network. A hacker may capitalize on the
improperly coded software to send a malformed SQL query to the underlying database to
27 break into it, plant malicious code or access other systems on the network.
28

1 SQL injections flaws, therefore, are relatively easy to prevent and are well known to any web
2 developer handling a large-scale commercial website.

3 26. Based on its own findings, Imperva believed that prior to warning RockYou, it
4 was likely that breaches had already occurred through RockYou's SQL injection flaw.
5 Additionally, Imperva informed RockYou that its researchers were aware that RockYou
6 users' webmail accounts had been accessed as a result of prior breaches.

7 27. The SQL injection flaw was disproportionately hazardous to RockYou's users
8 because RockYou had failed to encrypt its users' PII. Therefore, once a hacker got inside
9 RockYou's network, there was no further deterrent or obstacle to stealing RockYou's users'
10 PII.

11 28. Had RockYou properly secured its database through known and available
12 encryption methods, and even if a hacker were able to enter the network, he would be limited
13 in his ability to inflict harm. For example, a hacker still might be able cause temporary
14 internal havoc in the operation of the site, or "vandalize" the appearance of the site by
15 altering its code, but under the appropriate and necessary security, a hacker would not be able
16 to steal 32 million sets of user PII because the data would be encrypted and indecipherable.

17 29. However, because RockYou did not have this security in place, RockYou's
18 security flaw was being actively exploited and the contents of its database were known and
19 made public through underground hacker forums on or before November 29, 2009

20 30. In a December 15, 2009, interview conducted by SCMagazineUS.com,
21 Imperva's chief technology officer, Amichai Shulman, reports:

22
23 Others probably hacked into the database even earlier,
24 Shulman said. Imperva researchers initially discovered the
25 vulnerability after coming across a thread on a hacking forum,
26 where hackers discussed the flaw and said it was being actively
27 exploited.

28 "It was probably compromised before we warned them about
it," Shulman said. He added that Imperva researchers are

1 certain that some webmail accounts have been accessed as a
2 result of the breach.

3 “I can tell you for sure that some of them have been accessed,”
4 Shulman said. “We know that for a fact. We looked at some of
5 those accounts and they were already flagged as abused by the
6 webmail providers.”

7 “SQL injection is one of the oldest tricks in the book of
8 application-level hacking and it allows direct access to the
9 database through the web app,” Shulman said.⁵

10 31. Based on RockYou’s own press release, after Imperva warned it of the SQL
11 injection vulnerability and the high likelihood of prior breaches, RockYou “immediately
12 brought down the site and kept it down until a security patch was in place.”⁶

13 32. However, RockYou did not in fact respond immediately to the warning and
14 waited at least one day to take action to repair the SQL vulnerability. According to an
15 interview conducted by NetworkWorld.com with Imperva’s chief technology officer,
16 Amichai Shulman, “RockYou did not respond to Imperva, nor did it appear to immediately
17 take down its site as it claimed in its statement to Tech Crunch, Shulman said. The flaw was
18 present for a day or more after Imperva informed RockYou of the issue before it was
19 addressed he said.”⁷

20 33. In the time prior to RockYou fixing the SQL vulnerability, at least one
21 confirmed hacker known by the moniker “igigi” accessed RockYou’s database and removed
22 the e-mails and passwords of approximately 32 million registered RockYou users.

23 34. This hacker accessed and removed the user information prior to Imperva’s
24 warning, and therefore entered RockYou’s database without detection. Further, by entering
25 the database prior to Imperva’s warning, the hacker acted with separate and independent
26 knowledge of RockYou’s vulnerability.

27 ⁵ [http://www.scmagazineus.com/rockyou-hack-compromises-32-million-
28 passwords/article/159676/](http://www.scmagazineus.com/rockyou-hack-compromises-32-million-passwords/article/159676/)

⁶ <http://www.techcrunch.com/2009/12/14/rockyou-hacked/>

⁷ [http://www.networkworld.com/news/2009/121509-rockyou-hack-exposes-names-
passwords.html?page=1](http://www.networkworld.com/news/2009/121509-rockyou-hack-exposes-names-passwords.html?page=1)

1 35. In an interview with RockYou's Chief Technology Officer, Jia Shen, Digital
2 Beat reported that after Imperva notified RockYou of its security vulnerability, "the company
3 began poring through its databases to find any evidence of attack. Shen said the company
4 doesn't know exactly what the hacker did in the attack. The company is in contact with law
5 enforcement but isn't saying more. 'But we are assuming the worst,' Shen said. 'We checked
6 the activity and it looked like it had been going on a couple of days before we were warned.'
7 Mr. Shen continued, 'We started off as a small company and today we have a different
8 engineering structure,' he said. 'But shame on us. If you make a mistake, then people can get
9 in and it is a big hole.'"⁸

10 36. On information and belief, the "activity" referred to by Mr. Shen was in fact
11 not the individual hacker known as "igigi" who publically claimed to have accessed the
12 database, but one or more different individuals.

13 37. On information and belief, RockYou did not utilize any software designed to
14 identify actual or potential attacks, forcing RockYou to manually search for attacks after they
15 had occurred.

16 38. In a statement issued after RockYou publically announced the security breach,
17 RockYou stated that "one or more individuals illegally breached one of our databases that
18 contained the usernames and passwords for about 32 million users in an unencrypted
19 format." While RockYou indicated that updates and increased security were put in place
20 following the breach, it acknowledged that at the time of the breach, the hacked database had
21 not been up-to-date with regard to "industry standard security protocols."⁹

22 39. Implicit in RockYou's statement is the admission that the security methods it
23 utilized to protect user PII did not meet even the most basic industry standards and recklessly
24 exposed its users' information to attack and theft.

25 _____
26 ⁸ [http://digital.venturebeat.com/2009/12/15/rockyou-explains-how-a-hacker-stole-32-million-
passwords-and-what-its-doing-about-it/](http://digital.venturebeat.com/2009/12/15/rockyou-explains-how-a-hacker-stole-32-million-passwords-and-what-its-doing-about-it/)

27 ⁹ <http://www.rockyou.com/help/securityMessage.php>

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FACTS RELATING TO PLAINTIFF

40. During the relevant time period, Alan Claridge was a registered account holder with RockYou. He registered with RockYou on August 13, 2008.

41. In signing up to utilize a photo sharing application offered by RockYou, Claridge submitted his e-mail address and a password to RockYou.

42. On December 16, 2009, Claridge received an e-mail from RockYou informing him that his sensitive PII stored with RockYou may have been compromised through a security breach.

CLASS ALLEGATIONS

43. Plaintiff Alan Claridge brings this action pursuant to Fed. R. Civ. P. 23(b)(2) and (3) on behalf of himself and a Class of similarly situated individuals, defined as follows:

All individuals and entities in the United States who registered an account with RockYou, Inc.

Excluded from the Class are Defendant, its legal representatives, assigns, and successors, and any entity in which Defendant has a controlling interest. Also excluded is the judge to whom this case is assigned and the judge's immediate family, as well as any individual who contributed to the unauthorized access of RockYou's database.

44. The Class consists of millions of individuals and other entities, making joinder impractical.

45. Plaintiff's claims are typical of the claims of all of the other members of the Class.

46. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the

1 financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to
2 those of the other members of the Class.

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

8 48. RockYou has acted and failed to act on grounds generally applicable to
9 Plaintiff and the other members of the Class, requiring the Court's imposition of uniform
10 relief to ensure compatible standards of conduct toward the members of the Class.

11 49. The factual and legal bases of RockYou's liability to Plaintiff and to the other
12 members of the Class are the same and resulted in injury to Plaintiff and all of the other
13 members of the Class. Plaintiff and the other members of the Class have all suffered harm as
14 a result of RockYou's wrongful conduct.

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

- 19 (a) whether RockYou failed to use reasonable care and utilized
20 commercially reasonable methods to secure and safeguard its users' sensitive
21 PII;
 - 22 (b) whether storing user e-mails and passwords in an unencrypted format
23 was commercially reasonable;
 - 24 (c) whether RockYou's conduct described herein violated the Unfair
25 Competition Law (Cal. Bus. & Prof. Code § 17200, *et seq.*);
- 26
27
28

- 1 (d) whether RockYou’s conduct described herein violated California’s
- 2 Computer Crime Law (Cal. Penal Code § 502);
- 3 (e) whether RockYou’s conduct described herein violated the California
- 4 Security Breach Information Act (Cal. Civ. Code § 1798.80, *et seq.*);
- 5 (f) whether RockYou’s conduct describe herein violated the California
- 6 Legal Remedies Act (Cal. Civ. Code § 1750);
- 7 (g) whether RockYou’s conduct described herein constitutes a breach of
- 8 contract;
- 9 (h) whether RockYou’s conduct described herein constitutes breach of the
- 10 implied covenants of good faith and fair dealing;
- 11 (i) whether RockYou’s conduct described herein constitutes breach of
- 12 implied contracts;
- 13 (j) whether RockYou’s conduct described herein was negligent and/or
- 14 grossly negligent;
- 15 (k) whether RockYou’s conduct described herein constitutes negligence
- 16 per se;

17 51. Plaintiff reserves the right to revise these definitions based on facts learned in
 18 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)

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

22 53. California’s Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code §
 23 17200, *et seq.*, protects both consumers and competitors by promoting fair competition in
 24 commercial markets for goods and services.

25 54. The UCL prohibits any unlawful, unfair or fraudulent business act or practice.
 26 A business practice need only meet one of the three criteria to be considered unfair

27
 28

1 competition. An unlawful business practice is anything that can properly be called a business
2 practice and that at the same time is forbidden by law.

3 55. As described herein, Defendant's failure to safeguard and secure its users'
4 sensitive PII and permit it to be stolen is a violation of the UCL.

5 56. Commonly accepted and widely practiced industry standards provide that
6 sensitive PII stored in a commercial database should be not be accessible to theft or
7 manipulation through a SQL injection attack, and commercially reasonable methods to
8 prevent such attacks are widely known throughout the security industry. Further, commonly
9 accepted and widely practiced industry standards provide that sensitive PII stored in a
10 commercial database, especially user passwords, should be not be stored in "clear" text, but
11 rather encrypted to provide a barrier to removal or manipulation.

12 57. RockYou failed to expend the resources necessary to protect the sensitive data
13 entrusted to it by Plaintiff and the Class in clear contradiction of accepted industry standards
14 for database security. In creating the perception that it followed industry standards for
15 database protection, RockYou gained an unfair advantage over its competitors.

16 58. Additionally, RockYou deceived consumers by providing in its Terms of Use
17 that it "uses commercially reasonable physical, managerial, and technical safeguards to
18 preserve the integrity and security of your personal information....Once we receive your
19 transmission of information, RockYou! makes commercially reasonable efforts to ensure the
20 security of our systems."

21 59. RockYou's failure to develop its online software applications in a manner
22 resistant to SQL injection attacks, and/or monitor its database systems for SQL injection
23 flaws, is not a "commercially reasonable" method of preserving the integrity of user
24 information.

25 60. RockYou's failure to maintain an encrypted database of user e-mails and
26 passwords is not a "commercially reasonable" method of preserving the integrity of user
27

1 information. Storing sensitive PII in clear text provides no level of data security and
2 significantly increases the likelihood of data theft.

3 61. Maintaining sensitive PII with substandard security, when reasonable
4 additional security is not only available, but allegedly in use within other parts of RockYou's
5 computer system, is not a "commercially reasonable" method of preserving the integrity of
6 user information.

7 62. Defendant has violated the "unlawful" prong of the UCL in that Defendant's
8 conduct violated the Consumer Legal Remedies Act (Cal. Civ. Code § 1750 *et seq.*), the
9 California Computer Crime Law (Cal. Penal Code § 502), and the California Security Breach
10 Information Act (Cal. Civ. Code § 1798.80, *et seq.*).

11 63. Defendant has violated the fraudulent prong of the UCL in that Defendant
12 misrepresented to its users that it would use commercially reasonable methods to safeguard
13 and secure their PII and induce them to use its services and entrust it with their sensitive data.

14 64. Defendant has violated the unfair prong of the UCL in that Defendant
15 operated a business that induced consumers to submit PII with the written assurance that it
16 would be protected through commercially reasonable methods. Defendant knowingly failed
17 to provide any commercially reasonable security methods and allowed its users' PII to be
18 stolen by malicious third parties.

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

24 66. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiff seeks an order of this
25 Court permanently enjoining Defendant from continuing to engage in the unfair and unlawful
26 conduct described herein. Plaintiff seeks an order requiring Defendant to (1) immediately
27
28

1 stop the unlawful practices stated in this Complaint; (2) pay attorney’s fees, and costs
2 pursuant to Cal. Code Civ. Proc. § 1021.5.

3 **SECOND CAUSE OF ACTION**
4 **Violation of California’s Computer Crime Law (“CCCL”)**
5 **Cal. Penal Code § 502,**
6 **(On Behalf of Plaintiff and the Class)**

7 67. Plaintiff incorporates the foregoing allegations as if fully set forth herein.
8 RockYou knowingly and without permission provided a means for a malicious third party to
9 access its database and alter, damage, delete, destroy, steal, copy or otherwise use its users’
10 data in violation of Cal. Penal Code § 502(c)(6).

11 68. RockYou knowingly and intentionally failed to follow even the most basic
12 database security protocols and thereby failed to safeguard and secure its users’ sensitive PII,
13 allowing that information to be manipulated and stolen by a third party.

14 69. RockYou’s reckless indifference to the proper security measures necessary to
15 protect its users’ sensitive PII created the gaping security hole necessary for a malicious third
16 party to directly access its database. Without RockYou’s reckless and/or gross negligence
17 and unwillingness to follow industry standards for data security, a third party hacker could
18 not have stolen Plaintiff and the Class’s sensitive PII.

19 70. As a direct and proximate result of RockYou’s violation of § 502, RockYou
20 caused loss to Plaintiff and the Class members in an amount to be proven at trial. Plaintiff
21 and the Class are entitled to the recovery of attorneys’ fees pursuant to § 502(e).

22 71. Plaintiff and Class members have also suffered irreparable injury as a result of
23 Defendant’s unlawful conduct, including the harvesting of their personal information.
24 Additionally, because the stolen information cannot be returned, the harm from the security
25 breach is ongoing and compounding. Accordingly, Plaintiff and the Class have no adequate
26 remedy at law, entitling them to injunctive relief.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

THIRD CAUSE OF ACTION
Violation of the California Security Breach Information Act
Cal. Civ. Code § 1798.80, et seq.
(On Behalf of Plaintiff and the Class)

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

73. From 2006 through the present, RockYou conducted business in the State of California and maintained a database of computerized data that included sensitive PII.

74. As of December 4, 2009, at the very latest, RockYou was notified and given substantial grounds to reasonably believe that its database was the subject of a substantial security breach that resulted in an unauthorized third party acquiring its users' personal information. RockYou did not give complete and proper notice of any security breach until 10-12 days later, and only after significant media attention.

75. By waiting at least 10 to 12 days to provide notice of the breach to its users, RockYou failed to act in a timely fashion, thereby delaying Plaintiff and the Class's ability to protect their personal information from the multiple security breaches, including but not limited to the security breach perpetrated by the hacker known as "igigi," and all other security breaches Imperva warned RockYou about. Because of RockYou's willful ignorance and unwillingness to provide even the most basic forms of database and network security, it failed to detect any type of security breaches and/or SQL injection attacks until after it was informed of its vulnerabilities, and even then, failed to take timely action to protect its users' information.

76. RockYou did not give notice of any potential security breach in the most expedient time frame possible and was unreasonably delayed responding to the breach.

77. Separate from any unidentified security breaches, RockYou did not publicly post a warning notice on its website regarding the vulnerability and possible attacks on December 15, 2009, even though it was given a warning and aware of its issues on December 4, 2009 at the latest. The public notice only appeared after significant media coverage and a

1 direct threat from the hacker known as “igigi.” The public notice only appears on
2 RockYou’s front page, and not on an individual’s profile page, the actual web page that
3 registered users use to create and manage RockYou products.

4 78. Likewise, RockYou failed to individually give notice to all of its users until at
5 least December 15 or 16, 2009, when it sent the following e-mail to its users:

6 Dear RockYou user,

7 As you know, RockYou takes our users privacy very seriously.
8 We take a lot of effort to protect user data from security
breaches and attacks.

9 Unfortunately, RockYou has very recently learned that it
10 encountered a security breach. As part of this breach, it is
11 possible that someone may have accessed at least your email
12 address and password for the RockYou system. We felt it was
important to notify you of this immediately so that you could
take any action you feel necessary to protect your privacy.

13 As a precaution, we strongly recommend you change any
14 passwords for other online websites that have the same login
and password immediately in order to protect your security.

15 If you have any questions, please feel free to contact
16 security@rockyou.com. We are sorry for any problems this has
caused you.

17 The RockYou team

18 79. This e-mail was therefore issued at least 12 days after RockYou was notified
19 of the security vulnerability, and only after receiving significant media attention and
20 pressure.

21 80. This notice fails to conclusively inform its users that their data has been stolen
22 as a result of the breach, which RockYou was more than aware of by this time. Therefore,
23 the notice is not only untimely, but insufficient.

24 81. Under Cal. Civ. Code § 1798.84, Plaintiff and the Class seek damages, all
25 applicable civil penalties, and reasonable attorneys’ fees and costs.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

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

83. The Consumers Legal Remedies Act 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.

84. As described within, Defendant has engaged in deceptive practices, unlawful methods of competition, and/or unfair acts as defined by Cal. Civ. Code §§ 1750, *et seq.*, to the detriment of Plaintiff and the Class.

85. Defendant, acting with knowledge, intentionally and unlawfully brought harm upon Plaintiff and the Class by deceptively inducing Plaintiff and the Class to register with RockYou based upon deceptive and misleading representations that it would take commercially reasonable steps to safeguard its users' sensitive PII. Specifically, Defendant violated Cal. Civ. Code § 1750 in at least the following respects:

- (a) In violation of § 1770(5) by representing that goods or services have characteristics and benefits, which they do not have;
- (b) In violation of § 1770(a)(19) by inserting an unconscionable provision in the offer for Defendant's goods and services.

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

87. 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.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

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

89. In order to use its social-networking applications, Defendant required that Plaintiff and the Class affirmatively assent to its Terms of Use Agreement (the “Agreement”).

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

91. Under the Agreement, in order to use Defendant’s social networking applications, Plaintiff and the Class 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 “RockYou! uses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your personal information.” Defendant further promised that it would provide Plaintiff and the Class with prompt and sufficient notice if their sensitive PII was compromised.

92. 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. Defendant further materially breached the terms of the Agreement by failing to promptly and sufficiently notify Plaintiff and the Class that their sensitive personal information had been compromised.

93. As a result of Defendant’s misconduct and breach of the Agreement described herein, Plaintiff and the Class suffered injury.

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

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

1 95. In order to use Defendant’s social-networking applications, Plaintiff and the
2 Class affirmatively assented to Defendant’s Terms of Use Agreement.

3 96. The Agreement’s provisions constitute a valid and enforceable contract
4 between Plaintiff and the Class on the one hand, and Defendant on the other.

5 97. Implicit in the Agreement were contract provisions that prevented Defendant
6 from engaging in conduct that frustrated or injured Plaintiff’s and the Class’s rights to
7 receive the benefits of the Agreement.

8 98. Defendant’s obligation to take commercially reasonable steps to safeguard
9 and secure Plaintiff’s and the Class’s sensitive PII from unauthorized access and theft was a
10 material term of the Agreement. Equally material was Defendant’s obligation to provide
11 prompt and sufficient notice to Plaintiff and the Class in the event that their sensitive PII had
12 been compromised.

13 99. Furthermore, implicit in the terms of the Agreement was Defendant’s
14 obligation to comply with Cal. Bus. & Prof. Code §§ 17200, *et seq.*, Cal. Penal Code § 502,
15 Cal. Civ. Code §§ 1798.80, *et seq.*, and Cal. Civ. Code §§ 1750, *et seq.*

16 100. Defendant breached the implied covenant of good faith and fair dealing by
17 failing to safeguard and secure Plaintiff’s and the Class’s sensitive PII from unauthorized
18 access and theft, failing to promptly and sufficiently notify Plaintiff and the Class that their
19 sensitive PII had been compromised, and further by failing to fully comply with the
20 proscriptions of applicable statutory law.

21 101. Defendant’s misconduct and breach of the implied covenant of good faith and
22 fair dealing as described herein resulted in injury to Plaintiff and the Class.

23 **SEVENTH CAUSE OF ACTION**
24 **Breach of Implied Contracts**
(On Behalf of Plaintiff and the Class)

25 102. Plaintiff incorporates the foregoing allegations as if fully set forth herein.
26
27
28

1 112. Defendant failed to protect its databases against SQL injection attacks and
2 other security vulnerabilities, failed to encrypt Plaintiff's and the Class's passwords, and
3 failed to provide Plaintiff and the Class with prompt and sufficient notice that their sensitive
4 PII had been compromised, thereby breaching its duties to Plaintiff and the Class.

5 113. By failing to take proper security measures to protect Plaintiff's and the
6 Class's sensitive PII as described herein, Defendant's conduct was grossly negligent and
7 departed from all reasonable standards of care.

8 114. As a direct and proximate result of Defendant's failure to exercise reasonable
9 care and use commercially reasonable security measures, its databases were accessed without
10 authorization and Plaintiff's and the Class's sensitive PII was compromised.

11 115. That security breach and resulting unauthorized access to Plaintiff's and the
12 Class's sensitive PII was reasonably foreseeable by Defendant, particularly in light of the fact
13 that the method used to access Defendant's databases—an SQL injection attack—was well-
14 known within the industry and had been successfully guarded against by companies similar
15 to Defendant for approximately a decade prior to the instant breach.

16 116. Neither Plaintiff nor the other members of the Class contributed to the security
17 breach described herein or to the unauthorized access of their sensitive PII.

18 117. As a direct and proximate result of Defendant's misconduct described herein,
19 Plaintiff and the Class were injured.

20 **NINTH CAUSE OF ACTION**
21 **Negligence Per Se**
22 **(On behalf of Plaintiff and the Class)**

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

24 119. Defendant's violations of Cal. Bus. & Prof. Code §§ 17200, *et seq.*, Cal. Penal
25 Code § 502, Cal. Civ. Code §§ 1798.80, *et seq.*, and Cal. Civ. Code §§ 1750, *et seq.*, resulted
26 in injury to Plaintiff and the Class.
27
28


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

JURY TRIAL

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

Respectfully submitted,

Dated: December 28, 2009

By: 
David Parisi
One of the Attorneys for Plaintiff

JS 44 (Rev. 12/07) (and rev 1-16-08)

CIVIL COVER SHEET

603262 (99)

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON PAGE TWO OF THE FORM.)

I. (a) PLAINTIFFS: ALAN CLARIDGE, an individual, on behalf of himself and all others similarly situated. DEFENDANTS: ROCKYOU, INC., a Delaware corporation. (b) County of Residence of First Listed Plaintiff Vanderburgh (EXCEPT IN U.S. PLAINTIFF CASES). (c) Attorney's (Firm Name, Address, and Telephone Number): David C. Parisi (162248) Parisi & Havens LLP 15233 Valleyheart Drive Sherman Oaks, CA 91403. County of Residence of First Listed Defendant San Mateo (IN U.S. PLAINTIFF CASES ONLY). NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE LAND INVOLVED. Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only) and III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant). II includes boxes for U.S. Government Plaintiff/Defendant, Federal Question, Diversity, etc. III includes boxes for Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, etc.

IV. NATURE OF SUIT (Place an "X" in One Box Only). Grid with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

V. ORIGIN (Place an "X" in One Box Only). Includes boxes for Original, Removed from State Court, Remanded from Appellate Court, Reinstated or Reopened, Transferred from another district, Multidistrict Litigation, Appeal to District Judge from Magistrate Judgment.

VI. CAUSE OF ACTION. Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 U.S.C. section 1332. Brief description of cause: Claims based on unlawful and unfair business practices.

VII. REQUESTED IN COMPLAINT: CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23. DEMAND \$: CHECK YES only if demanded in complaint. JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY: PLEASE REFER TO CIVIL L.R. 3-12 CONCERNING REQUIREMENT TO FILE "NOTICE OF RELATED CASE".

IX. DIVISIONAL ASSIGNMENT (CIVIL L.R. 3-2) (PLACE AND "X" IN ONE BOX ONLY). SAN FRANCISCO/OAKLAND SAN JOSE

DATE: Dec. 24, 2009. SIGNATURE OF ATTORNEY OF RECORD: David C. Parisi

ORIGINAL BY FAX

JS 44 Reverse (Rev. 12/07)

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44**Authority For Civil Cover Sheet**

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. (a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.C.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.

United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; federal question actions take precedence over diversity cases.)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerks in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the seven boxes.

Original Proceedings. (1) Cases which originate in the United States district courts.

Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.

Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.

Appeal to District Judge from Magistrate Judgment. (7) Check this box for an appeal from a magistrate judge's decision.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553

Brief Description: Unauthorized reception of cable service

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.

Demand. In this space enter the dollar amount (in thousands of dollars) being demanded or indicate other demand such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.