Scott A. Kamber (*pro hac vice*)
skamber@kamberlaw.com
David A. Stampley (*pro hac vice*)
dstampley@kamberlaw.com
KAMBERLAW, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 202-6364

David C. Parisi (SBN 162248)
dcparisi@parisihavens.com
Suzanne Havens Beckman (SBN 188814)
shavens@parisihavens.com
Azita Moradmand (SBN 260271)
amoradmand@parisihavens.com
PARISI & HAVENS LLP
15233 Valleyheart Drive
Sherman Oaks, California 91403
Telephone: (818) 990-1299
Facsimile: (818) 501-7852

Counsel for Plaintiffs

(Additional counsel listed on signature page)

THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

JOSEPH GARVEY, *et al.*,

Plaintiffs,

v.

KISSMETRICS and HULU, LLC,

Defendants.

LEAD CASE NO. 4:11-cv-03764-LB
consolidated with
CASE NO. 4:11-cv-05606-LB

JURY DEMAND

FIRST AMENDED, CONSOLIDATED CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. Video Privacy Protection Act, 18 U.S.C. § 2710;
2. Trespass to Personal Property/Chattel;
3. Computer Crime Law, Cal. Penal Code § 502;
4. Computer Fraud and Abuse Act, 18 U.S.C. § 2710
5. Unfair Competition Law, Cal. Bus. and Prof. Code § 17200
6. Right to Privacy, Cal. Const., Art. I, Sec. § 1;
7. Negligence

Plaintiffs, on behalf of themselves and all others similarly situated (each, a "Class Member" and, collectively, the "Class") allege as follows based on personal knowledge and on information and belief based on investigation of counsel.

PARTIES

1. Plaintiffs are individuals residing in the United States and each of whom, during the Class Period (as defined herein), used his or her Internet-connected computer and Web-browsing software ("browser") installed on that computer to visit the website of Defendant Hulu, LLC at http://www.hulu.com.

2. Plaintiff Joseph Garvey is a resident of Kings County, New York.

3. Plaintiff Stacey Tsan is a resident of Los Angeles County, California.

4. Plaintiff Susan Couch is a resident of Ector County, Texas.

5. Plaintiff Cristina Garza is resident of Dallas County, Texas.

6. Plaintiff Concepcion Jauregui is a resident of Dallas County, Texas.

7. Plaintiff Silviano Moncada is a resident of Dallas County, Texas.

8. Defendant Hulu, LLC ("Hulu" or "Defendant") is a Delaware corporation with headquarters at 12312 West Olympic Boulevard, Los Angeles, California 90064, doing business throughout the United States and, in particular, in the State of California and County of San Mateo.

INTRADISTRICT ASSIGNMENT

9. Intra-district assignment to the San Francisco Division is proper inasmuch as the first complaint in this matter named as a defendant Space Pencil, Inc. d/b/a/ KISSmetrics ("Kissmetrics"), a company with principal executive offices and headquarters in this District on Morning Lane in Redwood Shores, California.

JURISDICTION AND VENUE

10. This Court has diversity jurisdiction in this case under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). This complaint states claims on behalf of a national class of con-

sumers who are minimally diverse from Defendant. The Class (as defined herein) consists of more than one hundred members. In addition, the amount in controversy exceeds $5 million, exclusive of interest and costs.

11. This Court has federal question jurisdiction under 28 U.S.C. § 1331 as this action arises in part under federal statutes, specifically, the Video Privacy Protection Act and the Computer Fraud and Abuse Act.

12. This Court has supplemental jurisdiction with respect to the pendent state law claims under 28 U.S.C. § 1367.

13. This Court has personal jurisdiction over Defendant because some of the acts alleged herein were committed in the state of California and because Defendant Hulu is registered to do business in this state and Defendant systematically and continuously conduct business in this state.

14. Venue in this District under 28 U.S.C. § 1391(b) is appropriate in that the first complaint in this matter named as a defendant Space Pencil, Inc. d/b/a/ KISSmetrics ("Kissmetrics"), a company with principal executive offices and headquarters in this District on Morning Lane in Redwood Shores, California.

GENERAL ALLEGATIONS

A. Plaintiffs' and Class Members' Interest in Privacy and Integrity of their Software

15. Plaintiffs and Class Members value their privacy while Web-browsing.

16. Plaintiffs and Class Members have a reasonable expectation of privacy while Web-browsing.

17. Plaintiffs and Class Members do not want to be tracked online.

18. Plaintiffs and Class Members believe their Web-browsing is private and not the business of anyone except the Website with which they choose to communicate.

19. Plaintiffs' and Class Members' online communications—*i.e.*, their web browsing activities, including their video viewing choices – involve their personal information of a private, confidential, sensitive, and intimate nature.

20. Plaintiffs and Class Members believe their decisions to disclose or not disclose in-

formation when they view a particular Web page, select content or options on the page, or enter information on the page, is their decision to make.

21. Plaintiffs and Class Members believe the information they disclose online is an asset they possess and to which online third parties have no presumptive right of access.

22. Plaintiffs and Class Members believe their computers, Internet connectivity through their ISPs, and software installed on their computers ("Computer Assets")—are theirs to use and control, to preserve their privacy and for other reasons, such as preventing unwanted communications from diminishing the speed of their Internet connections.

23. Plaintiffs and Class Members believe their Computer Assets are assets they pay for, possess, and/or to which they enjoy a right of possession and use.

24. Plaintiffs and Class Members believe online parties with whom they have not chosen to communicate have no presumptive right to access or use Plaintiffs' and Class Members' Computer Assets.

25. Plaintiffs' and Class Members' reasonably expect that the code transmitted by the websites they patronize and the third parties utilized by those websites will activate intended software functions on Plaintiffs' and Class Members' computers—that is, the websites and third parties will use web page display code to display web pages and will use graphics code to display images.

26. Plaintiffs and Class Members reasonably expect that the websites they patronize and the third parties utilized by those websites will not transmit code that repurposes web page display software and graphics software to perform unintended functions, such as tracking and circumvention of privacy protection mechanisms in Plaintiffs' and Class Members' software.

27. The aforementioned expectations are material to Plaintiffs and Class Members in protecting their privacy interests and keeping their Computer Assets from being used in ways Plaintiffs' and Class Members' do not want their Computer Assets used, including to cause unexpected software operation and to diminish and invade their privacy interests.

28. The aforementioned expectations are material to Plaintiffs and Class Members in their decisions to patronize websites.

B. Hulu's Tracking Exploits[1]

29. Plaintiffs and Class Members share reasonable expectations about tracking of their online activities and limits of that tracking, relating to who will be tracking, what will be tracked, and how tracking will be done.

30. Plaintiffs and Class Members reasonably expect that websites performing tracking do so by storing information in cookies on the computers of visitors to their websites.

31. Hulu and Kissmetrics created several shadow mechanisms for tracking, using software on Plaintiff and Class Members' computers in ways the software was not designed to be used and that Plaintiff and Class Members would not reasonably expect it to be used.

32. Hulu and Kissmetrics engage in these tracking activities regardless of any visitor's browser privacy controls over accepting, blocking, or deleting cookies.

Hulu's exploits of browser cache

33. The purpose of a browser cache is to store, on a user's computer, copies of web pages viewed by the user. The next time the user visits the web page, if it has not changed, the page can simply be loaded from the browser cache instead of being downloaded from the Internet, which would take more time.

34. Hulu, however, repurposed the browser cache of Plaintiffs' and Class Members' browser software. Hulu coordinated with Kissmetrics so that Kissmetrics stored coded information, specific to each individual Plaintiff and Class Member, in the code used to display Hulu web pages. The code had nothing to do with what the user viewed. Like cookies, the code contained tracking identifiers.

35. When a Plaintiff or Class Member returned to a Hulu web page, the browser automatically retrieved its cached copy of the web page, which activated the embedded Kissmetrics scripts that retrieved previously set tracking codes embedded in that page.

[1] As used in this complaint, "exploit" is a computer technology term of art that means computer code, computer commands, or electronic data that interacts with computer software in a way that causes the software to function in a manner not expected or intended by its owner/user, for the advantage or benefit of the party deploying the code, commands, or data. When used as a verb, "exploit" means to engage in the activity described in the preceding sentence.

36. Using the tracking codes stored in the cached page, Kissmetrics respawned its own and Hulu's tracking cookies.

Defendant's exploit of HTML5 storage

37. For those Plaintiffs and Class Members using recent browser versions enabled with HTML5, Hulu stored tracking information in storage area referred as "DOM local storage."

38. Hulu used DOM local storage to store unique identifiers, identified by the label, "ai," assigned to Plaintiffs and Class Members.

39. Hulu shared these unique identifiers with Kissmetrics, such that the identical value was stored in Kissmetrics' "km_cid" cookie.

40. The coordinating and respawning (or "resurrecting") of cookies using Hulu's DOM local storage values was performed by Kissmetrics-provided code that Hulu embedded in its web pages.

41. It is contrary to Internet standards, for privacy reasons, for two websites to share common identifiers.

42. It is contrary to Internet standards to use alternative mechanisms to cookies, respawn cookies, and bypass a user's cookie controls by using DOM local storage, in which the information never expires, without first obtaining user consent.

Hulu's exploit of Adobe Flash LSOs

43. Adobe Flash Player software is installed on the majority of U.S. consumers' computers, including those of Plaintiffs and Class Members.

44. LSOs were designed to store information such as users' volume control settings for videos, game score for multi-session video games, and other user preferences for playing content using their Flash players—not as an alternative to browser cookies to track users. [2]

---

[2] Adobe Systems Incorporated has stated:

> Adobe does not support the use of our products in ways that intentionally ignore the user's expressed intentions.
> . . .
> In every case where rich Internet applications are possible, Local Storage is available (and necessary). The Local Storage capability in Adobe Flash Player is equivalent in concept to the emerging Local Storage capabilities in *i.e.* HTML5 and Silverlight. The fact that Local Storage in these technologies is distinct from the existing

45. Unlike cookies, for which commercial browsers provide consumers some measure of control, consumers have no reasonable means to block, detect, or delete LSOs and are burdened by other, material differences between cookies and LSO. See Figure 1, below.

46. Hulu repurposed the Adobe Flash software installed on Plaintiffs' and Class Members' computers: Hulu used Adobe Flash local shared objects (LSOs) on Plaintiffs' and Class Members' computers as an alternative mechanism in which to store the same information it was storing in cookies, including a Flash LSO named "guid" (a term that typically means "global unique identifier") that Hulu uses to respawn a cookie of the same name.

47. Similarly, Kissmetrics repurposed the Adobe Flash software installed on Plaintiffs' and Class Members' computers: Kissmetrics used Adobe Flash local shared objects (LSOs) on Plaintiffs' and Class Members' computers as an alternative mechanism in which to store tracking information in Adobe Flash LSOs.

48. Kissmetrics was able to do so because Hulu, by embedding Kissmetrics' code on its web pages, gave Kissmetrics access to Plaintiffs' and Class Members' computers.

---

browser cookie system and treated as such by the browsers today underscores the need for responsible use of Local Storage in modern Web applications.

Responses to Adobe's small step forward on Flash-cookie control, posted by Wiebke Lips, Adobe Systems Inc., Jan. 29, 2010, available at http://blog.privacychoice.org/2010/01/29 adobes-small-step-forward-on-flash-cookie-control; see also Letter to FTC, Adobe Systems Inc., Jan. 27, 2010, p. 9, available at http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf.

Figure 1. *Comparison of cookies and LSOs*

	Cookies	*Adobe Flash LSOs*
	Characteristics and Operation	
[a]	subject to global standards	subject to Adobe specifications
[b]	set/used only by originating Website	set/used by multiple Websites*
[c]	4 kilobytes	No limit; up to 100 KB by default
[d]	expires when user exits browser, by default	persistent by default
	User Controls	
[e]	can control through browser	cannot control through browser**
[f]	can identify originating Website	originating Website easily obscured*
[g]	can view cookie contents	cannot reasonably view LSO contents
[h]	relatively apparent and usable	not reasonably apparent and usable

* Adobe Flash permits cross-domain LSO creation and use, *i.e.*, a Website can set an LSO for another Website, or read another Website's LSO; Adobe Flash also permits cross-site scripting, allowing for privacy-invasive and security threatening exploits.

** User must be aware of and use proprietary Adobe tools available on Adobe Website.

49. The Adobe Flash LSOs were not used by Defendant for purposes of retaining user preferences for the display of Flash-based video content.

50. On Plaintiffs' and Class Members' computers, Hulu's and Kissmetrics' LSOs remain stored and available to Hulu and Kissmetrics for their own commercial uses.

51. Plaintiffs and Class Members did not expect that, instead of using Plaintiffs' and Class Members' Adobe Flash software to display rich media content, Hulu would repurpose Plaintiffs' and Class Members' software to assign persistent, unique, identifying codes that evaded browser controls and were effectively undeletable.

C. Hulu's Unauthorized Sharing of Users' Video Viewing Details

52. As Plaintiffs and Class Members viewed video content on Hulu's website, Hulu transmitted their viewing choices to a number of third parties, including Scorecard Research, an online market research company; Facebook, an online social network website; DoubleClick, an online ad network; Google Analytics, an online web analytics company (performing analysis of

web traffic); and QuantCast, an online ad network and web analytics company.

53. Hulu's transmissions of video viewing information to Scorecard Research and Facebook included information that personally identified Plaintiffs and Class Members.

54. In the case of Scorecard Research, Hulu also provided Scorecard Research with Plaintiffs' and Class Members' Hulu profile identifiers linked to Plaintiffs' and Class Members' individual Hulu profile pages that included name, location, preference information designated by the user as private, and Hulu username (which, in the case of many individuals, is the same screen name used in other online environments).

55. Scorecard Research stored the Hulu ID information in a cookie named "b.scorecardresearch.com" and stored the video information in a cookie named "beacon.scorecardresearch.com." In addition, Scorecard Research set its own unique identifier tied to the two previously mentioned cookies.

56. Further, Scorecard Research's cookies were unencrypted, so that any intruder that gained access to the computer of a Plaintiff or Class Member could engage in a trivial exploit to view the profile and perform a "screen scrape" copy of that person's profile page.

57. Hulu and Scorecard Research's practice of sharing user profile IDs and storing them in cookies constitutes a severe failure to observe basic security standards in the handling of user information.

58. In the case of Facebook, Hulu included Plaintiffs' and Class Members' Facebook IDs, connecting the video content information to Facebook's personally identifiable user registration information.

59. Plaintiffs and Class Members reasonably expected that Hulu would not disclose their video and/or video services requests and their identities to social networks and online ad/metrics networks.

60. Plaintiffs and Class Members did not authorize or otherwise consent to Hulu's disclosure of their video and/or video services requests and their identities to social networks and online ad/metrics networks.

D. Hulu's Misleading Privacy Statements

Online Privacy Policy

61. Hulu's online privacy policy is misleading in that it does not disclose its use of aggressive, rogue exploits of Plaintiffs' and Class Members' computer software to engage in widespread tracking and information sharing.

62. In addition, Hulu's online privacy policy is misleading in that it represents that Hulu uses DOM storage to hold "complex data," when, in fact, it only uses DOM storage to store that same data that it stores in cookies; Hulu uses DOM storage solely as a surreptitious backup for cookies, should users delete them. Both purposes constitute circumventions of user privacy controls and basic Internet standards.

P3P Compact Policy

63. For Plaintiffs and Class Members using the Microsoft Internet Explorer ("IE") browser, the privacy controls rely in part on the browser's examination of coded privacy policies on websites, referred to as P3P (Platform for Privacy Preferences) Compact Policies.

64. The purpose of the Compact Policy is to permit Plaintiffs and Class Members using IE to rely on their browsers to automatically read privacy policies before actually having to visit a site and be served its cookies.

65. Hulu's P3P Compact Policy is misleading in that it states that Hulu does not share personally identifiable information with third parties.

E. Harm

66. Plaintiffs and other members of the Class seek to maintain privacy and confidentiality of their unique, personal, and individual information assets, including PII and details of their browsing and online viewing activities.

67. The private and confidential character of Plaintiffs' and Class Members' personal information is further demonstrated by Defendant's use of surreptitious and deceptive methods to deposit unconsented to cookies and exploits of Plaintiffs' and Class Members' Flash software, browser HTML5 storage, browser cache functionality, and browser P3P filters described herein on Plaintiffs' and Class Members' computers.

68. Defendant's attempts to hide its practices included code obfuscation, that is, it developed tracking code using programming and command statements designed to obscure the purpose and function of those statements.

69. Further, the Kissmetrics code Hulu embedded in its web pages operated so as to be inescapable, cycling through tracking data stored in cookies, browser cache files, HTML5 DOM local storage, and Adobe Flash LSOs, so that Plaintiffs' and Class Members' tracking data could be retained by one means or another, so they could be tracked over long periods of time and across multiple websites, regardless of whether they were registered or logged in.

70. Plaintiff and Class Members had no reasonable means to detect or control these tracking activities.

71. Defendant's exploits of Plaintiffs' and Class Members' HTML5 DOM storage and browser cache functionality are so outside the boundaries of reasonable expectations that even industry experts had not previously observed these exploits "in the wild," that is, in actual use on websites available to the public.

72. Defendant acquired personal information to which it was not entitled and without Plaintiffs' and Class Members' consent, and enabled Kissmetrics to do likewise.

73. Defendant's conduct in acquiring such information without authorization or consent has caused and causes economic loss to Plaintiffs and Class Members in that the personal information acquired by Defendant has economic value to Plaintiffs and Class Members.

74. In addition, Defendant's conduct in acquiring such information without authorization or consent has caused economic loss to Plaintiffs and Class Members in that such information has economic value to Plaintiffs and Class Members as an asset they exchange for valuable content and services provided by websites; Plaintiffs and Class Members would have blocked Defendant's exploits of Plaintiffs' and Class Members' Flash software, browser HTML5 storage, browser cache functionality, and browser P3P filters described herein, would not have patronized Defendant's website, and would have avoided websites utilizing Defendant's exploitative repurposing of Plaintiffs' and Class Members' Flash software, browser HTML5 storage, browser cache functionality, and browser P3P filters described herein; Defendant's conduct has thus im-

posed opportunity costs on Plaintiffs and Class Members, depriving them of the opportunity to exchange their valuable information for the content and services of websites engaging in practices that comported with Plaintiffs' and Class Members' reasonable privacy expectations.

75. Defendant's conduct in using Plaintiffs' and Class Members' Computer Assets to exploit Plaintiffs' and Class Members' Flash software, browser HTML5 storage, browser cache functionality, and browser P3P filters for tracking Plaintiffs and Class Members constituted the unconsented use of Plaintiffs' and Class Members' Computer Assets, including Internet connectivity, for which Plaintiffs and Class Members paid, and so Defendant acquired the use of such assets without payment and thus subjected Plaintiffs and Class Members to economic loss.

76. Defendant's unconsented use of Plaintiffs' and Class Members' Computer Assets, for which Plaintiffs and Class Members paid, diminished the performance of Plaintiffs' and Class Members' computers and Internet connectivity, in that LSO-based methods of information collection require the transfer of larger files using more resource-intensive computer processes that must be completed in sequence during the download of Web pages, causing Web pages to load more slowly than Web pages involving the transfer of cookie values; such diminution in performance of Computer Assets constituted an economic loss to Plaintiffs and Class Members.

77. The consequences of the aforementioned conduct also constitute an interruption in service in that they were recurrent, through the Class Period, affecting Plaintiffs' and Class Members' experiences on numerous websites.

78. Defendant's use of Plaintiffs' and Class Members' Computer Assets and collection and use of their personal information in a nontransparent manner, which cannot reasonably be detected at the time or later discovered, has deprived Plaintiffs and Class Members of the ability to protect their privacy and Computer Assets, assess the effects of Defendant's actions on their privacy and Computer Assets, and reasonably undertake self-help measures.

79. Defendant's use of exploits of Plaintiffs' and Class Members' Flash software, browser HTML5 storage, browser cache functionality, and browser P3P filters described herein subjects and/or has subjected Plaintiffs and Class Members to additional harm in that, in further circumvention of their browser settings, Defendant has re-spawned cookies that Plaintiffs and

Class Members deleted, and/or Plaintiffs and Class Members face the imminent harm of such re-spawning through the various exploit methods described herein.

80. Hulu can compete and thrive only if maintains a sufficient traffic volume to attract merchants and advertisers.

81. Plaintiffs and Class Members, through their patronage, provide that traffic and so barter for their ability to access the content and services they buy with that patronage.

82. Defendant, through its conduct, deprives Plaintiffs and Class Members of the opportunity to use their information to purchase from and promote the continued availability of websites that conform to their reasonable expectations, that is, online merchants that deal honestly in the content and services offered to consumers and their related privacy disclosures.

83. Plaintiffs and Class Members incorporated privacy considerations into their online viewing decisions when they visited Hulu's website. Plaintiffs and Class Members made their viewing selection purchases on Hulu's website, and not another competitor's website, because they trusted that Hulu's privacy practices comported with their privacy preferences, as expressed through their browser's privacy controls.

84. Had Plaintiffs and Class Members known that Defendant's privacy practices were not as represented, *i.e.*, that Defendant used unauthorized, persistent cookies and other devices for tracking browsing activities, which Defendant accomplished by exploiting Plaintiff and Class Members' Adobe Flash software, browser HTML5 storage, browser cache functionality, and browser P3P filters, Plaintiffs and Class Members would not have engaged in viewing video content or in visiting Hulu's website.

85. Plaintiffs' and Class Members' experiences are consistent with and borne out by research showing that consumers purchase from online retailers who better protect their privacy and who prominently display their privacy practices; and that once privacy information is more salient, consumers are willing to pay a premium to purchase from more privacy protective websites. See J. Tsai, S. Egelman; L. Cranor; A. Acquisiti [Carnegie Mellon Univ.], "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study" (June 2011), Information Systems Research, Vol. 22:2 at 254–268.

86. Finally, the personal information Defendant wrongfully obtained from Plaintiffs and Class Members constitutes valuable data in the advertising-related market for consumer information. Plaintiff and Class Members are presently harmed or face imminent harm from Defendant's wrongful acquisition and use of their information, preempting Plaintiffs and Class Members from realizing for themselves the full value of their own information.

87. The costs and harms described above are aggravated by Defendant's continued retention and commercial use of the improperly acquired user data; by reducing the scarcity of Plaintiffs' and Class Members' valuable information, Defendant has further reduced the economic value of such information, causing Plaintiffs and Class Members economic harm.

88. Thus, Defendant's unauthorized taking of Plaintiffs' and other Class Members' personal information therefore imposes financial harm on them and constitutes an unwanted cost incurred by them for accessing Defendant's website.

89. Plaintiffs and other Class Members' information acquired by Defendant had and has discernible value to them; the extent of Defendant's acquisition and its facilitation of others' acquisition of personal information and the value of that information can be established through discovery of information that is in Defendant's possession, combined with data available in the market expert analysis..

90. Plaintiffs and Class Members have suffered loss and/or damages that exceed five thousand dollars ($5,000.00) in costs to mitigate Defendant's invasive actions by expending time, money, and resources, to investigate and repair their computers, in that Defendant's conduct described herein has resulted in the storage on their computers of LSOs, HTML5 storage objects, and browser cookies that continue to be available to Hulu and Kissmetrics, and that Plaintiffs and Class Members do not want stored on their computers; based on evaluation by computer forensics experts, Plaintiffs estimate that remediating each computer would cost, at a conservative minimum, $500 to $1,000 per computer.

91. The average computer ranges in cost from $150 to $1,500. Plaintiffs and Class Members use computers to conduct both personal and commercial business. Any interference of any kind to such devices would interfere with their personal enjoyment and/or commercial use.

Plaintiffs and Class Members were harmed due to any impediment to use once the Defendant's actions became known, delay in time to investigate and repair any loss and/or damage.

92. Moreover Plaintiffs' and Class Members' losses potentially include the purchase of new computer hardware and operating systems.

93. Plaintiffs and Class Members purchased computers with consideration for costs, speed and security features. The cost of the hardware and software necessary for the security features were factored into the total price of the computer, thus a specific sum was allocated to the cost of including the security features. As such, Defendant's circumvention of their computers' security mechanisms rendered such hardware and software protections purchased within the computer worthless.

94. Native security software was provided to Plaintiffs and Class Members within their computers when purchased for use on a trial basis, generally an average 60-day trial period. Common native security software is a Norton or McAfee product. Once the trial period expired, the Plaintiffs and Class Members download software or purchased such at an electronic store. Security Software costs averages approximately $75.00 to $150 per computer to provide continued security protection. Such security software purchased was rendered ineffective against the intrusion of Defendants' activities made the basis of this action.

CLASS ALLEGATIONS

95. The "Class Period" is defined as the period from March 4, 2011 through July 28, 2011, inclusive.

96. Pursuant to Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, Plaintiffs brings this action pursuant to on behalf of themselves and the following Class:

> All individuals and entities in the United States who visited Hulu.com during the Class Period.

97. The Class includes individuals who are members of the following subclass (the "Video Subclass"):

> All individuals and entities in the United States who visited Hulu.com during the Class Period and viewed video content.

98. Excluded from the Class and the Video Subclass are Defendant, and its assigns, successors, and legal representatives, and any entities in which Defendant has controlling interests.

99. Also excluded from the Class are the judge to whom this case is assigned and members of the judge's immediate family.

100. Plaintiffs reserve the right to revise the definition of the Class based on facts they learn in the course of litigation.

101. The Class consists of millions of individuals, making joinder impractical. During the Class Period, on a monthly basis, as many as 50 million individuals viewed Defendant's content and were subjected to Defendant's exploits of Plaintiffs' and Class Members' Flash software, browser HTML5 storage, browser cache functionality, and browser P3P filters.

102. Plaintiffs' claims are typical of the claims of all other members of the Class.

103. Plaintiffs will fairly and adequately represent the interests of the Class. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions, including privacy cases.

104. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Class and have the financial resources to do so.

105. Plaintiffs and their counsel do not have any interests adverse to those of the Class.

106. Absent a class action, most Class Members would find the cost of litigating their claims to be prohibitive and would have no effective remedy.

107. The class treatment of common questions of law and fact in this matter is superior to multiple individual actions or piecemeal litigation, in that it conserves the resources of the Court and litigants and promotes consistency and efficiency of adjudication.

108. Defendant has acted and failed to act on grounds generally applicable to Plaintiffs and the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class.

109. The factual and legal bases of Defendant's liability to Plaintiffs and Class Members are the same, resulting in injury to Plaintiffs and all other Class Members. Plaintiffs and

Class Members have all suffered harm and damages as a result of Defendant's wrongful conduct.

110. There are many questions of law and fact common to Plaintiffs and the Class and which predominate over any questions that may affect only individual Class Members. Common and predominant questions for the Class include but are not limited to the following:

a. whether Defendant circumvented Plaintiffs' and Class Members' browser and software control in exploiting Plaintiffs' and Class Members' Flash software, browser HTML5 storage, browser cache functionality, and browser P3P filters described herein on Plaintiffs' and Class Members' computers;

b. whether Defendant's exploits of Plaintiffs' and Class Members' Flash software, browser HTML5 storage, browser cache functionality, and browser P3P filters described herein was without consent, without authorization, and/or exceeding authorization;

c. whether Defendant obtained and shared, or caused to be obtained and shared, Plaintiffs' and Class Members' personal information through tracking using exploits of Plaintiffs' and Class Members' Flash software, browser HTML5 storage, browser cache functionality, and browser P3P filters described herein that Defendant placed on their computers;

d. what personal information of Plaintiffs and Class Members was obtained and continues to be retained and used by Defendant;

e. what are the identities of third parties that obtained Plaintiffs' and Class Members' personal information as a result of Defendant's conduct;

f. whether Defendant's conduct described herein violates the statutory and common-law bases alleged in the Claims for Relief, below;

g. whether Defendant's acquisition of Plaintiffs' and Class Members' personal information and use of Plaintiffs' and Class Members' Computer Assets harmed Plaintiffs and Class Members;

h. whether Defendant's' use of Plaintiffs' and Class Members' Computer Assets damaged and/or diminished the utility and/or value of those Computer Assets;

i. whether, as a result of Defendant's' conduct, Plaintiffs and Class Members are entitled to equitable relief and/or other relief, and if so the nature of such relief; and

j. whether, as a result of Defendant's' conduct, Plaintiffs and Class Members are entitled to damages, including, statutory, punitive, liquidated and/or treble damages.

111. The questions of law and fact common to the Class predominate over any questions affecting only individual members and a class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

112. Plaintiffs' claims for relief include those set forth below.

CLAIMS FOR RELIEF

COUNT ONE

VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

TITLE 18 UNITED STATES CODE, SECTION 2710, ***et seq.***

(VIDEO PRIVACY PROTECTION ACT)

BY THE VIDEO SUBCLASS

113. Plaintiffs incorporate the above allegations by reference as if here fully set forth.

114. Defendant Hulu is and was throughout the Class Period engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials in that Hulu offered to online consumers prerecorded video programs, including previously released and posted, and originally developed news, entertainment, educational, and general interest video programs, and so was, throughout the Class Period, a video tape service provider as defined in the Video Privacy Protection Act.

115. Plaintiffs and Class Members were renters, purchasers, and/or subscribers of goods and/or services from Hulu and so were consumers as defined in the Video Privacy Protection Act.

116. Hulu knowingly and without Plaintiffs' and Class Members' consent disclosed to third parties, including online ad networks, metrics companies, and social networks, Plaintiffs' and Class Members' video viewing selections and personally identifiable information, knowing that such disclosure included the disclosure of personally identifying information of Plaintiffs and Class Members and their requests for and/or obtaining of specific video materials and/or services from Hulu.

117. Hulu's actions were therefore in violation of the Video Privacy Protection Act, 18 U.S.C. § 2710(b)(1).

118. Plaintiffs and Class Members, as to each of them, are entitled to $2,500 in liquidated damages.

119. Plaintiffs and Class Members are entitled to equitable relief that includes Hulu's cessation of the conduct alleged herein.

120. Plaintiffs and Class Members are entitled to equitable relief that includes an accounting of what records regarding their video materials requests and services were disclosed and to whom.

121. Plaintiffs and Class Members are entitled to equitable relief that includes an accounting of Hulu's compliance 18 U.S.C. § 2710(e), regarding its destruction of personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected.

122. Plaintiffs and Class Members seek punitive damages.

123. Plaintiffs and Class Members are entitled reasonable attorneys' fees and other litigation costs reasonably incurred.

124. Plaintiffs and Class Members request such other preliminary and equitable relief, as the Court deems appropriate.

COUNT TWO

TRESPASS TO CHATTEL

125. Plaintiffs incorporate the above allegations by reference as if here fully set forth.

126. Plaintiffs and Class Members were, during the Class Period, the owners and/or possessors of computers on which Defendant, surreptitiously and without consent, used Plaintiff and Class Members' own Computer Assets to exploit Plaintiffs' and Class Members' Flash software, browser HTML5 storage, browser cache functionality, and browser P3P filters, to circumvent privacy controls and collect Plaintiff and Class Members' personal information.

127. Defendant dispossessed Plaintiffs and Class Members of the use of their computers, software, and Internet connectivity by commandeering those resources for Defendant's' own

purposes.

128. Defendant materially impaired the condition, quality, and value of Plaintiffs' and Class Members' computers by their exploits of Plaintiffs' and Class Members' Flash software, browser HTML5 storage, browser cache functionality, and browser P3P filters and their circumvention of Plaintiffs' and Class Members' browser and software controls to collect and/or cause the collection of Plaintiffs' and Class Members' personal information.

129. Defendant's' conduct constituted an ongoing and effectively permanent, material impairment of Plaintiffs' and Class Members' computers in that Defendant's' conduct affected Plaintiffs and Class Members in a substantial amount of their Web-browsing, throughout the Class Period, through the use of LSOs and the artifacts of other exploits described herein that continue to reside on Plaintiffs' and Class Members' computers, and through which Defendant obtained information the use of which they continue to enjoy.

130. Plaintiffs and Class Members each had and have legally protected, privacy and economic interests in their Computer Assets and their personal information.

131. Plaintiffs and Class Members sustained harm as a result of Defendant's' actions, in that the expected operation and use of their Computer Assets were altered and diminished on an ongoing basis.

132. As a direct and proximate result of Defendant's' trespass to chattels and interference, unauthorized access, intermeddling conduct affecting Plaintiffs' and Class Members' Computer Assets, Plaintiffs and Class Members have been injured, as described above.

133. Plaintiffs, individually and on behalf of the Class, seeks injunctive relief restraining Defendant from further such trespass to chattels and requiring Defendant to account for their use of Plaintiffs' and Class Members' Computer Assets, account for the personal information they have acquired, purge such data, and pay damages in an amount to be determined.

COUNT THREE

VIOLATION OF THE COMPUTER CRIME LAW

CALIFORNIA PENAL CODE, SECTION 502

134. Plaintiffs incorporate the above allegations by reference as if here fully set forth.

135. Defendant violated California Penal Code section 502 by knowingly accessing, copying, using, made use of, interfering, and/or altering, data belonging to Plaintiffs and Class Members: (1) in and from the State of California; (2) in the home states of the Plaintiffs and Class Members; and (3) in the state in which the servers that provided the communication link between Plaintiffs and Class Members and the websites they interacted with were located.

136. Defendant violated California Penal Code section 502(c)(1) by knowingly accessing and without permission altering and making use of data from Plaintiffs' and Class Members' computers in order to devise and execute business practices to deceive Plaintiffs and Class Members into surrendering private electronic communications and activities for Defendant's' financial gain, and to wrongfully obtain valuable private data from Plaintiffs.

137. Defendant violated California Penal Code section 502(c)(2) by knowingly accessing and without permission taking, or making use of data from Plaintiffs' and Class Members' computers.

138. Defendant violated California Penal Code section 502(c)(3) by knowingly and without permission using and causing to be used Plaintiffs' and Class Members' computer services.

139. Defendant violated California Penal Code section 502(c)(4) by knowingly accessing and, without permission, adding and/or altering the data from Plaintiffs' and Class Members' computers.

140. Defendant violated California Penal Code section 502(c)(5) by knowingly and without permission disrupting or causing the disruption of Plaintiffs' and Class Members' computer services or denying or causing the denial of computer services to Plaintiffs and the Class.

141. Defendant violated California Penal Code section 502(c)(6) by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiffs' and Class Members' computers, computer system, and/or computer network.

142. Defendant violated California Penal Code section 502(c)(7) by knowingly and without permission accessing or causing to be accessed Plaintiffs' and Class Members' computers, computer systems, and/or computer networks.

143. Defendant violated California Penal Code section 502(c)(8) by knowingly introducing a computer contaminant into the Plaintiffs' and Class Members' computers, computer systems, and/or computer networks, and doing so to obtain data regarding Plaintiffs' and Class Members' electronic communications.

144. Plaintiffs and Class Members have suffered irreparable injury from these unauthorized acts of disclosure in that their information has been harvested, retained, and used by Defendant, and continues to be retained and used by Defendant; due to the continuing threat of such injury and, in addition, the threat that Defendant will transfer Plaintiffs' and Class Members' information to yet other third parties, Plaintiffs and Class Members have no adequate remedy at law, entitling them to injunctive relief.

145. Plaintiffs and Class Members have suffered loss by reason of these violations, including, without limitation, violation of the right of privacy.

146. As a direct and proximate result of Defendant's' unlawful conduct within the meaning of California Penal Code section 502, Defendant has caused loss to Plaintiffs and Class Members in an amount to be proven at trial. Plaintiffs and Class Members are also entitled to recover their reasonable attorneys' fees pursuant to California Penal Code section 502(e).

147. Plaintiffs and the Class Members seek compensatory damages, in an amount to be proven at trial, and injunctive or other equitable relief.

148. Plaintiffs and Class Members have suffered irreparable and incalculable harm and injuries from Defendant's' violations. The harm will continue unless Defendant is enjoined from further violations of this section. Plaintiffs and Class Members have no adequate remedy at law.

149. Plaintiffs and Class Members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code section 502(e)(4) because Defendant's violation was willful and, on information and belief, Defendant is guilty of oppression, fraud, or malice as defined in Cal. Civil Code section 3294.

150. Defendant's unlawful access to Plaintiffs' and Class Members' computers and electronic communications has caused them irreparable injury. Unless restrained and enjoined, Defendant will continue to commit such acts. Plaintiffs' and Class Members' remedy at law is

not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiffs and Class Members to remedies including injunctive relief as provided by California Penal Code section 502(e).

COUNT FOUR

VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT

TITLE 18 UNITED STATES CODE, SECTION 1030, *et seq.*

151. Plaintiffs incorporate the above allegations by reference as if here fully set forth.

152. Plaintiffs and the Class Members' computers are computers used in and affecting interstate commerce and communication and are therefore "protected computers" as defined in the Computer Fraud and Abuse Act (the "CFAA"), 18 U.S.C. § 1030(e)(2).

153. Defendant violated the CFAA, 18 U.S.C. § 1030(a)(4) in that it knowingly and with intent to defraud, accessed the protected computers of Plaintiffs and the Class without authorization, or exceeding authorized access, and by means of such conduct, furthered the intended fraud and obtained things of value.

154. Defendant violated the CFAA, 18 U.S.C. § 1030(a)(5)(A) in that it knowingly caused the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage without authorization, to the protected computers of Plaintiffs and the Class.

155. Defendant violated the CFAA, 18 U.S.C. § 1030(a)(5)(B) in that it intentionally accessed the protected computers of Plaintiffs and Class Members without authorization, and as a result of such conduct, recklessly caused damage.

156. Defendant violated the CFAA, 18 U.S.C. § 1030(a)(5)(C) in that it intentionally accessed the protected computers of Plaintiffs and Class Members without authorization and knowingly transmitted and/or caused the transmission of commands to Plaintiffs' and Class Members' computers in the form JavaScript and other code that effected exploits of Plaintiffs' and Class Members' Flash software, browser HTML5 storage, browser cache functionality, and browser privacy filters based on P3P Compact Policies; Defendant intended that these commands be transmitted to and processed by Plaintiffs' and Class Members' computers and the commands

were, in fact, transmitted to and processed by Plaintiffs' and Class Members' computers.

157. Defendant obtained personal information from Plaintiffs' and Class Members' computers, including information about their web browsing activities and including video viewing selections.

158. Defendant caused damage to Plaintiffs and Class Members computers in that it circumvented their browser privacy controls, effectively rendering those controls non-operational for all of Plaintiff and Class Members' web-browsing on its website and other websites on it serves ad and/or delivers content.

159. Defendant intended to cause such damage in that Defendant's personal information harvesting and tracking technologies were designed to disable Plaintiffs' and Class Members' browser privacy controls.

160. Defendant's access to Plaintiff and Class Members' computers, disabling of browser privacy controls, and taking of information, was without authorization and exceeding authorization in that it circumvented Plaintiffs' and Class Members' express prohibition against tracking.

161. Defendant's unlawful access to Plaintiff and Class Members' computers, use of their Computer Assets, interruption of their services, and taking of their personal information was carried out through the same automated process, which caused the losses alleged in section E, "Harm," above, resulting in an aggregated loss to Plaintiffs and Class Members of at least $5,000 within a one-year period.

162. Defendant acted without authorization or exceeding authorization in that Plaintiffs and the Class Members did not give Defendant permission or consent to exploit the software on Plaintiffs' and Class Members' computers, circumvent their browser privacy controls, store persistent identifiers, and collect personal information using those identifiers.

163. Defendant also acted without authorization or exceeding authorization in that Plaintiffs and the Class Members did not give Defendant permission or consent to place repurposed LSO files or other repurposed storage objects or elements.

164. Defendant's conduct was knowing and with intent to defraud in that, contrary to

the privacy policy representations available to Plaintiffs and Class Members, Defendant affirmatively implemented code designed to circumvent Plaintiffs and Class Members privacy controls without detection and, further, was obfuscated to evade even more sophisticated detection efforts than would typically be exercised by Plaintiffs and Class Members.

165. Defendant furthered its intended fraud, placing persistent identifiers and other storage objects on Plaintiffs' and Class Members' computers to collect and maintain Plaintiffs' and Class Members' PII and to share that information with third parties without the knowledge and consent, and authorization of Plaintiffs and Class Members.

166. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered harms and losses and incurred costs that include those described above.

167. Defendant's unlawful access to Plaintiffs' and Class Members' computers through the use of an invalid P3P Compact Policy, repurposed LSOs and other tracking exploits described herein, resulted in an aggregated loss to Plaintiffs and the Class of at least $5,000 within a one-year period.

168. Therefore, Plaintiffs and the Class are entitled to compensatory damages and equitable relief.

169. Defendant's unlawful access to Plaintiffs' and Class Members' computers has caused Plaintiffs' and Class Members' irreparable injury. Unless restrained and enjoined, Defendant will continue to commit such acts. Plaintiffs' and Class Members' remedy at law is not adequate to compensate them for these inflicted, imminent, threatened, and continuing injuries, entitling Plaintiffs and the Class to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

COUNT FIVE

VIOLATION OF THE UNFAIR COMPETITION LAW ("UCL")

CALIFORNIA BUSINESS AND PROFESSIONS CODE, SECTION 17200, *et seq.*

170. Plaintiffs incorporate the above allegations by reference as if here fully set forth.

171. By engaging in the above-described acts and practices, Defendant has committed one or more acts of unfair competition within the meaning of the UCL and, as a result, Plaintiffs

and the Class have suffered injury-in-fact and have lost money and/or property—specifically, personal information and the full value of their computers.

172. Defendant's actions described above, including False Advertising, are in violation of California Business and Professions Code section 17500, *et seq.* and violations of the right of privacy enshrined in Article I, Section 1 of the Constitution of the State of California.

173. In addition, Defendant's business acts and practices are unlawful, because they violate California Business and Professions Code section 17500, *et seq.*, which prohibits false advertising, in that they were untrue and misleading statements relating to Defendant's performance of services and with the intent to induce consumers to enter into obligations relating to such services, and regarding statements Defendant knew were false or by the exercise of reasonable care Defendant should have known to be untrue and misleading.

174. Defendant's business acts and practices are also unlawful in that they violate the above-mentioned statutes, including California Penal Code, section 502 and Title 18, United States Code, Section 1030. Defendant is therefore in violation of the "unlawful" prong of the UCL.

175. Defendant's business acts and practices are unfair because they cause harm and injury-in-fact to Plaintiffs and Class Members and for which Defendant has no justification other than to increase, beyond what Defendant would have otherwise realized, its profit in fees from advertisers and its information assets through the acquisition of consumers' personal information. Defendant's conduct lacks reasonable and legitimate justification in that Defendant has benefited from such conduct and practices while Plaintiffs and the Class Members have been misled as to the nature and integrity of Defendant's services and have, in fact, suffered material disadvantage regarding their interests in the privacy and confidentiality of their personal information. Defendant's conduct offends public policy in California tethered to the right of privacy set forth in the Constitution of the State of California, and California statutes recognizing the need for consumers to obtain material information with which they can take steps to safeguard their privacy interests, including California Civil Code, Section 1798.80.

176. In addition, Defendant's *modus operandi* constituted a sharp practice in that De-

fendant knew or should have known that consumers care about the status of personal information and its privacy but were unlikely to be aware of the manner in which Defendant failed to fulfill its obligation to observe consumers' privacy expressed in their browser settings. Defendant is therefore in violation of the "unfair" prong of the UCL.

177. Defendant's acts and practices were fraudulent within the meaning of the UCL because they are likely to mislead the members of the public to whom they were directed.

178. As a result, Plaintiffs and the Class have suffered and will continue to suffer damages.

COUNT SIX

VIOLATION OF RIGHT TO PRIVACY

ARTICLE I, SECTION 1 OF THE CALIFORNIA CONSTITUTION

179. Plaintiffs incorporate the above allegations by reference as if here fully set forth.

180. Plaintiffs have a legally protected privacy interest in their electronic communications and in the highly detailed and confidential personal information concerning them that Defendant tracked and shared with third parties over a substantial period of time, without their knowledge or consent.

181. The right of Plaintiffs and Class Members to use their computers without having their web browsing, including the video content viewed by them, tracked and used by Defendant for Defendant's and other third parties' own commercial and advertising purposes constitutes a significant right relating to the use of specific personal property, without interference by Defendant through deception and unauthorized access.

182. Under the circumstances here, where Hulu provided no notice of its clandestine tracking activities and published a misleading privacy policy and P3P Compact policy, where the Internet is used in all facets of Plaintiffs and Class Members lives (for *e.g.*, for family, health, education, religion, politics, finance, and assembly), and in consideration of the highly detailed and confidential nature of, and in some instances, personally identifiable nature of the information taken by Defendant, Plaintiffs and Class Members had an objectively reasonable expectation of privacy from being electronically tracked by Hulu and from the disclosure of their

personal information to the third parties.

183. Hulu's conduct, which by design, allowed third parties to obtain Plaintiffs' and Class Members' personal information (and in some instances, store such information in unencrypted cookies), is not a standard, legitimate commercial practice. Rather it is an egregious breach of industry standards, social norms, and is prohibited by law. Hulu has and continues to commit these serious invasions of Plaintiffs and the Class' privacy.

184. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and Class Members have suffered harm as a result of their personal information being acquired and disseminated without consent.

185. There are no competing or countervailing interests that outweigh the privacy interests at stake. Accordingly, Plaintiffs and Class Members seek declaratory and injunctive relief to prevent Defendant from continuing to track and expose their personal information.

COUNT SEVEN

NEGLIGENCE

186. Plaintiffs incorporate the above allegations by reference as if here fully set forth.

187. Hulu owed a duty to Plaintiffs and Class Members to protect their personal information and data property, and take reasonable steps to protect them from the wrongful taking of such information and the wrongful invasion of their privacy.

188. This duty is not based on any contractual obligation, but arises as a matter of law because at all times, Hulu knew or should have known of the likelihood of harm that would occur should it fail to act reasonably under the circumstances described above.

189. Hulu also has a duty as the proprietor of an website that provides consumers with video content, to protect its consumers from or, at least, refrain from participation in and facilitation of harm from third parties that it reasonably foresees or should foresee, by its incorporation of third-party code—particularly where the harm is not evident to Plaintiffs and the Class. Such a duty arises out of the special relationship between Hulu and Plaintiffs.

190. Hulu had an obligation to use reasonable care to prevent such harm or to adequately warn Plaintiffs and Class Members of such harm.

191. Hulu breached its duty by:

a. capturing and transmitting Plaintiffs' and Class Members' personal information, including specifics of video content they viewed, associated with their personal identifiers, to third parties, without Plaintiffs' and Class Members' knowledge or consent;

b. repurposing Plaintiffs' and Class Members' browser cache, HTML5 storage, and Adobe LSOs and coordinating with Kissmetrics in such exploits;

c. sharing user profile IDs with certain third parties that store such data in unencrypted cookies; and

d. publishing a materially misleading online privacy policy and P3P Compact Policy.

192. As a direct and proximate result of Hulu's breaches of its duties, Plaintiffs and Class Members suffered the harms described more fully in section "E" entitled "Harm" above, each of which were a reasonably foreseeable result of Hulu's negligence.

VII. PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all others similarly situated, pray for the following relief:

A. Certify this matter as a class action.

B. Enter judgment in favor of Plaintiffs and Class Members.

C. Enter injunctive and/or declaratory relief as is necessary to protect the interests of Plaintiffs and Class Members, including reformation of practices and an accounting and purging of wrongfully obtained personal information;

D. Award statutory damages to Plaintiffs and Class Members.

E. Award compensatory damages to Plaintiffs and Class Members in amounts to be proved at trial.

F. Award restitution against Defendant in amounts to be proved at trial.

G. Award increased and/or treble damages in amounts to be proved at trial.

H. Award liquidated damages in amounts to be proved at trial.

I. Award punitive damages in the interest of justice.

J. Award disgorgement of monies obtained through and as a result of unfair and/or deceptive acts and/or practices and/or unjust enrichment, in amounts to be proved at trial.

K. Award Plaintiffs and Class Members pre- and post-judgment interest to the extent allowable.

L. Make such orders or judgments as may be necessary to restore to Plaintiffs and Class Members any money and property acquired by Defendant through wrongful conduct.

M. Award Plaintiffs and Class Members reasonable litigation expenses and attorneys' fees.

N. Award such other and further relief as equity and justice may require or allow.

Dated: February 15, 2012

Respectfully submitted,

s/David C. Parisi

By: David C. Parisi

Scott A. Kamber (*pro hac vice*)
skamber@kamberlaw.com
David A. Stampley (*pro hac vice*)
dstampley@kamberlaw.com
KAMBERLAW, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 202-6364

Deborah Kravitz (SBN 275661)
dkravitz@kamberlaw.com
KAMBERLAW LLP
141 North Street
Healdsburg, CA 95448
Telephone: (707) 820-4247
Facsimile: (212) 920-3081

David C. Parisi (SBN 162248)
dcparisi@parisihavens.com
Suzanne Havens Beckman (SBN 188814)
shavens@parisihavens.com
Azita Moradmand (SBN 260271)
amoradmand@parisihavens.com
PARISI & HAVENS LLP
15233 Valleyheart Drive
Sherman Oaks, California 91403
Telephone: (818) 990-1299

Facsimile: (818) 501-7852

Counsel for Plaintiffs Joseph Garvey and Stacey Tsan

Brian R. Strange (Cal. Bar. No. 103252)
LACounsel@earthlink.net
STRANGE & CARPENTER
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
Telephone: (310) 207-5055
Facsimile: (310) 826-3210

Joseph A. Malley (*pro hac vice*)
malleylaw@gmail.com
LAW OFFICE OF JOSEPH A. MALLEY
1045 North Zang Blvd.
Dallas, Texas 75208
Telephone: (214) 943-6100
Facsimile: (310) 943-6170

Counsel for Plaintiffs Susan Couch, Cristina Carza, Concepcion Jauregui, and Silviano Moncada

JURY TRIAL DEMAND

Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated: February 15, 2012

Respectfully submitted,

s/David C. Parisi

By: David C. Parisi

Scott A. Kamber (*pro hac vice*)
skamber@kamberlaw.com
David A. Stampley (*pro hac vice*)
dstampley@kamberlaw.com
KAMBERLAW, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 202-6364

Deborah Kravitz (SBN 275661)
dkravitz@kamberlaw.com
KAMBERLAW LLP
141 North Street
Healdsburg, CA 95448
Telephone: (707) 820-4247
Facsimile: (212) 920-3081

David C. Parisi (SBN 162248)
dcparisi@parisihavens.com
Suzanne Havens Beckman (SBN 188814)
shavens@parisihavens.com
Azita Moradmand (SBN 260271)
amoradmand@parisihavens.com
PARISI & HAVENS LLP
15233 Valleyheart Drive
Sherman Oaks, California 91403
Telephone: (818) 990-1299
Facsimile: (818) 501-7852

Counsel for Plaintiffs Joseph Garvey and Stacey Tsan

Brian R. Strange (Cal. Bar. No. 103252)
LACounsel@earthlink.net
STRANGE & CARPENTER
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
Telephone: (310) 207-5055
Facsimile: (310) 826-3210

Joseph A. Malley (*pro hac vice*)
malleylaw@gmail.com
LAW OFFICE OF JOSEPH A. MALLEY
1045 North Zang Blvd.
Dallas, Texas 75208
Telephone: (214) 943-6100
Facsimile: (310) 943-6170

Counsel for Plaintiffs Susan Couch, Cristina Carza, Concepcion Jauregui, and Silviano Moncada