KRONENBERGER ROSENFELD, LLP
Karl S. Kronenberger (CA Bar No. 226112)
(Application for admission Pro Hac Vice pending)
Jeffrey M. Rosenfeld (CA Bar No. 222187)
(Application for admission Pro Hac Vice pending)
Virginia A. Sanderson (CA Bar No. 240241)
(Application for admission Pro Hac Vice pending)
150 Post Street, Suite 520
San Francisco, CA 94108
Telephone: (415) 955-1155
Facsimile: (415) 955-1158
karl@KRInternetLaw.com
jeff@KRInternetLaw.com
ginny@KRInternetLaw.com

Attorneys for Plaintiffs
John Doe 1, John Doe 2, and John Doe 3

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

John Doe 1, an individual; **John Doe 2**, an individual; and **John Doe 3**, an individual;

Plaintiffs,

v.

GoDaddy.com, LLC, a Delaware corporation; **Amazon Web Services, Inc.**, a Delaware corporation; **John Roe 1**, d/b/a <ashleymadisonpowersearch.com> and <adulterysearch.com>; **John Roe 2**, d/b/a <ashleymadisoninvestigations.com>; **John Roe 3**, d/b/a <greyhatpro.com>; and **Roes 4–20**, inclusive,

Defendants.

Case No.

COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs John Doe 1, John Doe 2, and John Doe 3 (collectively, "Plaintiffs"), by and through their undersigned counsel, hereby allege as follows:

NATURE OF THE ACTION

1. Plaintiffs' claims arise out of the recent theft of massive amounts of private consumer data, including private stored communications, from the adultery website and dating service known as "Ashley Madison" by anonymous hackers. Due to the salacious nature of Ashley Madison, this Internet crime has been widely reported in the media, both in the United States and internationally.

2. While at least one class action has been filed by users against Ashley Madison for its failure to property secure the hacked information, this action deals with a different injury inflicted upon Ashley Madison users by persons and entities who have obtained the stolen data, repurposed it such that it is more readily accessible and searchable by the media and curious Internet users, and actively distributed it for their own gain. While these persons and entities may labor under the belief that their actions are entrepreneurial rather than criminal, the fact remains that they are in willful possession of stolen property.

3. Indeed, in recognition of the fact that Ashley Madison data contains confidential information and constitutes stolen property, a Canadian court, the Ontario Superior Court of Justice, issued a restraining order requiring several websites and Internet service providers to immediately disable the Ashley Madison data, deeming it "offence-related property in respect of which order of forfeiture may be made under the [Ontario] Criminal Code."

4. By continuing to host and publish the stolen data despite their knowledge of the pain and damage it is causing to those involved, these bad actors are intentionally inflicting emotional distress upon Ashley Madison users. Two suicides have already been attributed to the public dissemination of the Ashley Madison data.

5. Plaintiffs, who are proceeding anonymously in this action, are all former users of Ashley Madison who have been gravely affected by the stolen data and are now

subject to threats and extortion. The defendants are the website operators and Internet Service Providers who are hosting the stolen data to facilitate public searches, often for a fee. Through this action, Plaintiffs allege civil receipt of stolen property under California law, violation of California's Unfair Competition Law, intentional and negligent infliction of emotional distress, and violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 on behalf of Plaintiffs John Doe 1 through 3 and against GoDaddy.com, LLC ("GoDaddy"), Amazon Web Services, Inc. ("Amazon"), and Roes 1 through 20 (collectively, the "Roe Defendants").

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction over Plaintiffs' federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

7. This Court has supplemental jurisdiction of Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367(a) in that these state law claims are so related to the Computer Fraud and Abuse Act claim raised in this Complaint that they form part of the same case or controversy under Article III of the United States Constitution.

8. Alternatively, this Court has subject matter jurisdiction under 28 U.S.C. § 1332 because the matter in controversy exceeds the sum or value of $75,000, exclusive of interest and costs, and the action is between citizens of different states. To wit, Plaintiffs are citizens of and domiciled in California, New Jersey, and Maryland, while Defendants are citizens of and domiciled in Delaware and Arizona.

9. Venue is proper under 28 U.S.C. § 1391 because many of the incidents, events, or omissions complained of and giving rise to the instant claims and controversy occurred within the State of Arizona and this District.

10. This Court has personal jurisdiction over Defendants because Defendants, and each of them, do substantial business in Arizona and purposefully direct substantial activities as the residents of Arizona by means of the Internet services and websites described herein. Defendants, and each of them, have done substantial and continuous business with Arizona residents and have purposefully directed substantial and pervasive

activities at the residents of Arizona such that each can and should reasonably expect to be haled into the courts of Arizona.

PARTIES

11. Plaintiff John Doe 1 is an individual who, at all relevant times, was a citizen and resident of the state of California.

12. Plaintiff John Doe 2 is an individual who, at all relevant times, was a citizen and resident of the state of New Jersey.

13. Plaintiff John Doe 3 is an individual who, at all relevant times, was a citizen and resident of the state of Maryland.

14. If required, Plaintiffs will move for an order from this Court to proceed anonymously. The judicial use of "Doe" plaintiffs to protect legitimate privacy rights has gained wide currency, particularly given the rapidity and ubiquity of disclosures over the World Wide Web, so long as the opposing parties' rights are not prejudiced thereby. Here, Plaintiffs' anonymity is necessary to preserve privacy in a matter of sensitive and highly personal nature—namely, the issue of extra-marital affairs. Plaintiffs can proceed in all aspects of this litigation without prejudicing the rights of Defendants, or any of them.

15. Defendant GoDaddy.com, LLC ("GoDaddy") is a Delaware corporation with its principal place of business located in this state and District at 14455 North Hayden Road, Scottsdale, Arizona. GoDaddy has registered with the Arizona Corporation Commission as a foreign entity doing business in Arizona.

16. Defendant Amazon Web Services, Inc. ("Amazon") is a Delaware corporation doing business within this state and District. Amazon has registered with the Arizona Corporation Commission as a foreign entity doing business in Arizona.

17. Because GoDaddy and Amazon are both Internet Service Providers, or ISPs, they are, at times, referred to collectively herein as the "ISP Defendants."

18. Defendant John Roe 1 ("Roe 1") is the owner and operator of the websites located at <ashleymadisonpowersearch.com> and <adulterysearch.com>.

19. Defendant John Roe 2 ("Roe 2") is the owner and operator of the website

located at <ashleymadisoninvestigations.com>

20. Defendant John Roe 3 ("Roe 3") is the owner and operator of the website located at <greyhatpro.com>.

21. Defendants Roes 4 through 20 are unknown at this time, but are believed to be, among other persons or entities, additional Internet service providers and website operators trafficking in the Stolen Data, as that term is described below.

22. The names and identities of the Roe Defendants, and each of them, are presently unknown to Plaintiffs. Plaintiffs will amend this Complaint to allege the names and identities of said Roe Defendants when they become known to Plaintiffs. Plaintiffs may seek leave to conduct early discovery for the limited purpose of ascertaining the identities of the Roe Defendants.

FACTUAL ALLEGATIONS

The Ashley Madison Internet Dating Service

23. Ashley Madison is the brand name of an Internet dating website and service specializing in adulterous affairs.

24. Ashley Madison is owned and operated by Canadian corporation Avid Life Media, Inc. For purposes of this Complaint, Avid Life Media, the website located at <ashleymadison.com>, and the services provided thereon are collectively referred to as "Ashley Madison."

25. According to the footer on Ashley Madison's homepage, "Ashley Madison is the most famous name in infidelity and married dating…. Ashley Madison is the most successful website for **finding an affair** and cheating partners. Have an Affair today on Ashley Madison. Thousands of **cheating wives** and cheating husbands signup everyday looking for an affair [all sic]." As of the date of this Complaint, the homepage further boasts a roster of "Over **40,330,000** anonymous members!"

26. Indeed, anonymity is one of the promises repeatedly made by Ashley Madison to its members and prospective members. The homepage features the now-iconic picture of a woman, wearing a wedding band and holding a finger to pursed lips in a

"Shhh…" fashion. Directly beneath her are the following attestations that the Ashley Madison service is both private and secure:

- A badge featuring four stars and the text "100% Like-minded people";
- The text "**As see on:** Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today";
- The text "**Ashley Madison** is the world's leading married dating service for ***discreet*** encounters";
- A graphic featuring a gold medal next to the text "Trusted Security Award";
- A badge featuring the text "100% DISCREET SERVICE"; and
- A graphic featuring a lock with a green check on it and the text "**SSL Secure Site**."

27. In order to use the Ashley Madison dating service, "Users" must register by inputting the following personal information, which is used to populate the user's Ashley Madison profile: a username and password, a personalized "greeting," a country, zip code, date of birth, email address, and physical attributes, such as height and weight.

28. To further populate their profiles, Users are permitted to input additional "Preferences," such as personal interests, qualities of a good match, and "Intimate Desires," which is a polite means of describing what can be graphic sexual interests. Users also provide other intimate details and data with an expectation of complete privacy within the membership base of Ashley Madison's secure and controlled environment in which personal identities were never disclosed.

29. While a User may create an Ashley Madison profile for free, payment is required in order to use any of the services. Standard information is collected to process credit and debit card payments, such as credit card number, cardholder name, and associated billing address.

Plaintiffs' Registration With Ashley Madison

30. At various times since 2008, but before July 2015, Plaintiffs, and each of them, registered as Users of Ashley Madison and provided personal and financial

information to Ashley Madison in the process.

31. At the time of registration, each Plaintiff reasonably expected that the data provided to Ashley Madison would be managed with sufficient security protocols to prevent hacking or other disclosure.

Theft and Dissemination of the Ashley Madison Data

32. The crime colloquially referred to as "hacking" is the unauthorized access of a computer system without authorization and is a violation of federal law as well as that of each of the fifty states. Hacking is the electronic equivalent of breaking and entering, and any data acquired through such unlawful acts constitutes stolen property.

33. In or around July 2015, a group of hackers, who self-identify as The Impact Team (the "Hackers"), released snippets of confidential User information stolen from Ashley Madison's servers, and publicly threatened to release much more if Ashley Madison did not cease operation of its website and dating service.

34. When Ashley Madison refused to cave to the Hackers' demands, on or about August 18, 2015, the Hackers began a rolling release of User data stolen by the Hackers from Ashley Madison.

35. In a README file appended to the Hackers' first data dump, the Hackers admitted that the released data was stolen from Ashley Madison's servers through unlawful hacking:

> We are the Impact Team. We have hacked [Ashley Madison] completely, taking over their entire office and production domains and thousands of systems, and over the past few years have taken all customer information databases, complete source code repositories, financial records, documentation, and emails, as we prove here. And it was easy. For a company whose main promise is secrecy, it's like you didn't even try, like you thought you had never pissed anyone off.

36. The data stolen and released by the Hackers includes names, passwords, addresses, phone numbers, and Preferences submitted by users when they registered for the site.

37. The data stolen and released by the Hackers also includes records of millions

of credit card transactions going back to 2008, including the cardholder names, billing addresses, associated email addresses, and the last four digits of the credit card number(s) used to pay for the User's account. The release of this payment information has been integral to public identification of Users in that, while Users could falsify personal information, such as by using a fake name, payment information cannot be falsified without the use of a stolen credit card number.

38. The data stolen and released by the Hackers also includes private stored communications, such as chat logs and private messages exchanged between Users, many of which include photographs or other identifying information.

39. The whole of the data stolen and released by the Hackers is collectively referred to herein as the "Stolen Data."

40. The Stolen Data includes data pertaining to Plaintiffs, and each of them.

41. The Stolen Data was obtained by the Hackers without the authorization or consent of either Ashley Madison or the Users. Plaintiffs, specifically, did not authorize or consent to any access of their personal data.

42. The Hackers' release of the Stolen Data ignited media frenzy, with news outlets across the globe reporting on it and speculating about politicians and celebrities that could be included within the User ranks.

43. However, the Stolen Data, as posted by the Hackers, is not easily accessed or navigated by the average Internet user. The files containing the Stolen Data are each several gigabytes in size, are comprised of massive strings of plain text, and are posted to the so-called "Dark Web" at an address that is only accessible through the Tor browser.[1]

44. This inaccessibility, coupled with public interest, resulted in the immediate creation of a cottage industry of websites that took the Stolen Data and parsed it into databases that could be searched for specific names, email addresses, billing addresses, or

[1] At the risk of oversimplification, content located on the Dark Web is located on the World Wide Web, but is not indexed by search engines and is not accessible through the same means as the public Internet. Instead, content on the Dark Web can only be accessed through specific software, browsers, or networks, such as Tor.

other User information.

45. Roe 1, Roe 2, and Roe 3 each own and/or operate a website within this cottage industry, wherein the Roe Defendant has copied a portion and/or all of the Stolen Data and made it searchable through the Roe Defendant's website (collectively, the "Roe Websites"). As such, each of these Roe Defendants is in willful and knowing possession of stolen property—namely, the Stolen Data.

46. On information and belief, Roe 1, Roe 2, and Roe 3 each employ the services of an ISP Defendant to host its Roe Website. This means that the Stolen Data, as obtained by the Roe Defendant, is located on the servers belonging to and in the possession of the corresponding ISP Defendant.

47. Because the theft of the Stolen Data has been widely reported in the media, both in the United States and internationally, each of the Roe Defendants and ISP Defendants has actual notice that the Stolen Data is stolen property.

48. Indeed, each of the Roe Defendants admits on their website that they know the Stolen Data they possess was procured through criminal hacking.

49. Moreover, as detailed below, Plaintiffs have provided written notice to each of the ISP Defendants that the Stolen Data is (a) stolen property and (b) located on the ISP Defendant's servers at the Roe Website.

50. Because the ISP Defendants and Roe Defendants each have actual notice and knowledge that the Stolen Data is (a) stolen property and (b) within their possession, each Defendant is in willful and knowing possession of stolen property in violation of California Penal Code section 496(a).

51. Because the ISP Defendants and Roe Defendants have each received, possessed, stored, or sold the Stolen Data, knowing the same to have been unlawfully taken, each Defendant has violated 18 U.S.C. § 2315.

52. Like most users, Plaintiffs have suffered damages, including severe emotion distress, due to the ability of Plaintiffs' spouses, children, family members, community connections, business associates, and the public at large to identify Plaintiffs as Users of of

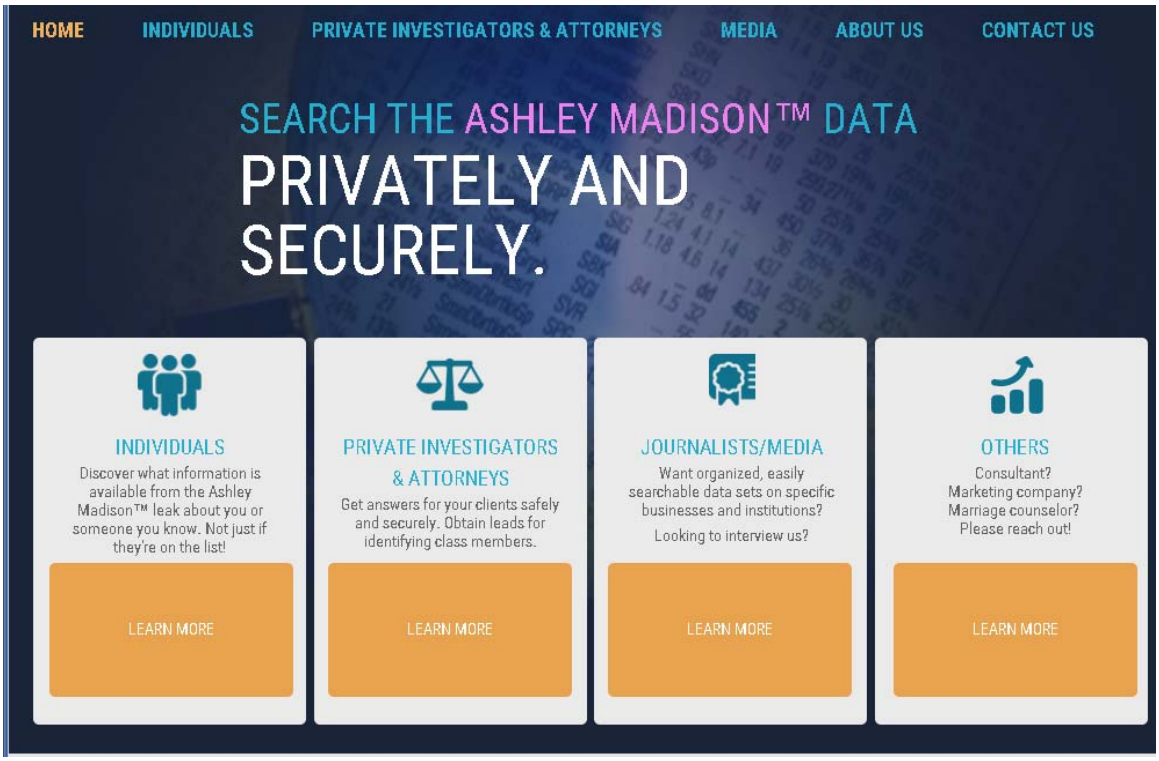
Ashley Madison. By this action, Plaintiffs seek compensatory damages in an amount to be proven at trial, but not less than three million dollars ($3,000,000).

Defendants GoDaddy and Roes 1 and 2

53. Roe 1 is the owner and operator of the Roe Websites located at <ashleymadisonpowersearch.com> and <adulterysearch.com> (the "Roe 1 Websites"). Aside from their domain names, the Roe 1 Websites are identical to one another and, on information and belief, an Internet user who visits <adulterysearch.com> is redirected to <ashleymadisonpowersearch.com>.

54. By their own terms, the Roe 1 Websites enable Internet users to "Search the Ashley Madison™ Data PRIVATELY AND SECURELY." Different price packages are provided for individuals, private investigators, attorneys seeking "leads for identifying class members," journalists and members of the media, marketing consultants, and marriage counselors.

55. The following is a screenshot taken on September 1, 2015 of the homepage of the Roe 1 Websites:



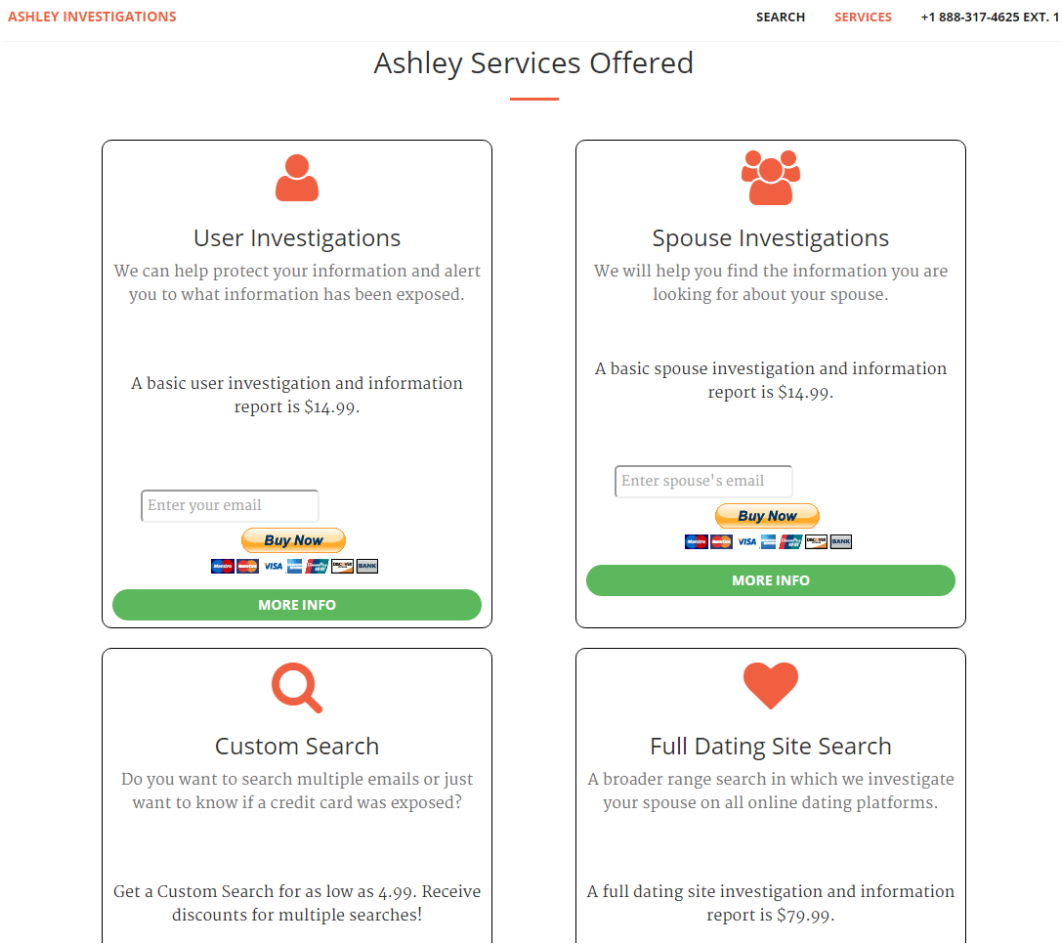
56. According to WHOIS records, the Roe 1 websites are hosted by ISP

Defendant GoDaddy. Accordingly, the Stolen Data obtained by Roe 1 and made available on the Roe 1 Websites is located on the servers of GoDaddy.

57. Roe 2 is the owner and operator of the Roe Website located at <ashleymadisoninvestigations.com> (the "Roe 2 Website").

58. The Roe 2 Website purports that "We will protect you from the hackers and people trying to disseminate negative information about you on the world wide web." At the same time, the Roe 2 Website sells several packages that enable such dissemination, such as a "Spouse Investigation" package to "help you find the information you are looking for about your spouse."

59. The following is a screenshot taken on September 3, 2015 of the homepage of the Roe 2 Website:



60. According to WHOIS records, the Roe 2 website is also hosted by GoDaddy. Accordingly, the Stolen Data obtained by Roe 2 and made available on the Roe 2 Websites

is located on the servers of GoDaddy.

61. On August 31, 2015, Plaintiffs sent written notice to GoDaddy of the existence of stolen property—namely the Stolen Data—on its servers at these Roe Websites and demanded its removal. As of the filing of this Complaint, GoDaddy has not acted upon Plaintiffs' demands and the Stolen Data remains accessible through these Roe Websites.

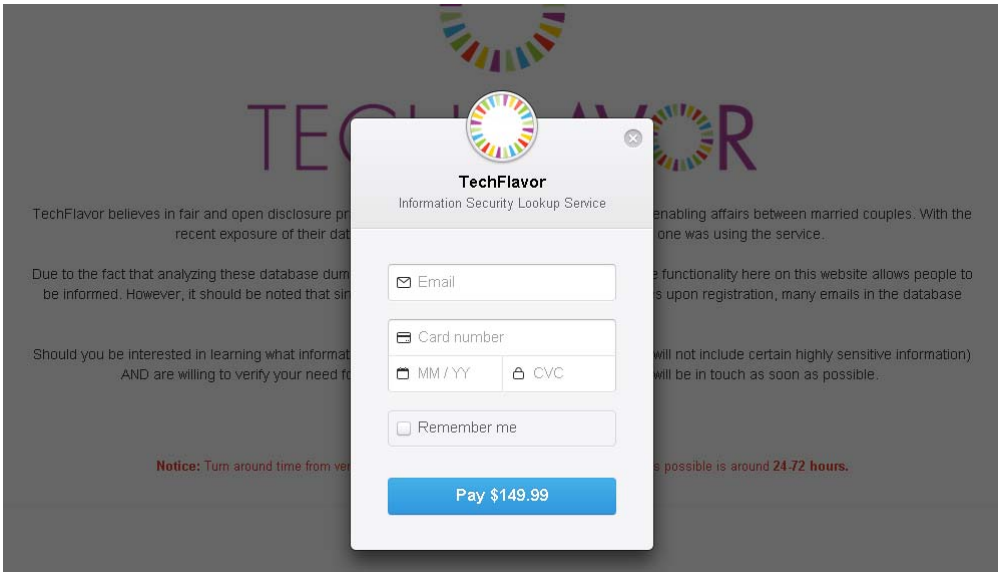
62. GoDaddy, Roe 1, and Roe 2 are each in willful, knowing possession of the Stolen Data.

Defendants Amazon and Roe 3

63. Roe 3 is the owner and operator of the Roe Website located at <greyhatpro.com> (the "Roe 3 Website").

64. By its own terms, the Roe 3 Website enables Internet users to search the Stolen Data for a fee, stating that "Due to the fact that analyzing these database dumps requires a bit of technical savvy, providing the functionality here on this website allows people to be informed." The Roe 3 Website further promises that "Turn around time from verified payment to information delivered as discretely as possible is around 24-72 hours." The fee for conducting a search on the Roe 3 Website is $149.99.

65. The following is a screenshot taken on September 2, 2015 of the "About" page of the Roe 3 Website, including the payment popup window:



66. According to WHOIS records, the Roe 3 Website is hosted by ISP Defendant Amazon. Accordingly, the Stolen Data obtained by Roe 3 and made available on the Roe 3 Website is located on the servers of Amazon.

67. On August 31, 2015, Plaintiffs sent written notice to Amazon of the existence of stolen property—namely the Stolen Data—on its servers at the Roe 3 Website and demanded its removal. As of the filing of this Complaint, GoDaddy has not acted upon Plaintiffs' demands and the Stolen Data remains accessible through the Roe 3 Website.

68. Both Amazon and Roe 3 are in willful, knowing possession of the Stolen Data.

FIRST CLAIM FOR RELIEF

(Violation of California Penal Code § 496—Receipt of Stolen Property By John Doe 1 Against All Defendants)

69. Plaintiff John Doe 1 incorporates by reference the allegations contained in Paragraphs 1 through 68.

70. The Stolen Data procured and posted by the Hackers is stolen property in that it was obtained in a manner constituting theft.

71. Defendants, and each of them, have obtained or received stolen property—namely, the Stolen Data.

72. Defendants, and each of them, know the Stolen Data to be stolen or obtained in a manner constituting theft.

73. By receiving and possessing the Stolen Data, knowing it to be stolen or obtained in a manner constituting theft, Defendants, and each of them, have violated California Penal Code section 496(a).

74. Plaintiff John Doe 1 has been damaged by Defendants' receipt and use of the Stolen Data in an amount to be proven at trial, but not less than $3,000,000.

75. Pursuant to California Penal Code section 496(c), Plaintiff John Doe 1 is entitled to three times the amount of actual damages sustained by Plaintiff, costs of suit,

and reasonable attorneys' fees for prosecuting this action.

76. There is no adequate remedy at law, and enjoining Defendants' unlawful possession and publication of the Stolen Data is necessary and in the public interest.

SECOND CLAIM FOR RELIEF

(Violation of California Business & Professions Code § 17200

By John Doe 1 Against All Defendants)

77. Plaintiff John Doe 1 incorporates by reference the allegations contained in Paragraphs 1 through 68.

78. Plaintiff John Doe 1 asserts this Second Cause of Action for violation of California's Unfair Competition Law.

79. Defendants, and each of them, have engaged in a pattern of unlawful conduct directed at Plaintiff by receiving, possessing, storing and selling the Stolen Data, which they know to be stolen property that has been transmitted across state and United States boundaries.

80. Defendants' above-described misconduct is an unlawful business practice, as that term is used in Business and Professions code section 17200, because Defendants' conduct violates California Penal Code section 496(a) and 18 U.S.C. § 2315, as well as other state and federal laws prohibiting hacking and theft.

81. As a result of Defendants' misconduct, Plaintiff John Doe has been damaged in an amount to be proven at trial, but not less than $3,000,000.

82. Plaintiff John Doe hereby seeks a judicial order of an equitable nature against Defendants including, but not limited to, enjoining Defendants and their agents, employees, representatives, and successors and predecessors in interest from possessing, hosting, publishing, or otherwise making available the Stolen Data.

THIRD CLAIM FOR RELIEF

(Intentional Infliction of Emotional Distress

By All Plaintiffs Against Roes 1–20, Inclusive)

83. Plaintiffs incorporate by reference the allegations contained in Paragraphs 1

through 68.

84. By making the Stolen Data available and searchable through the Roe Websites with an eye toward profiting off the implication that Plaintiffs and other Users are adulterers, the Roe Defendants engaged in outrageous misconduct. Indeed, the Roe Defendants' misconduct was so extreme that it went beyond all possible bounds of decency and a reasonable person would regard the Roe Defendants' misconduct as intolerable in a civilized community.

85. In engaging in their misconduct, the Roe defendants intended to cause Plaintiffs emotional distress and/or acted with reckless disregard of the probability that Plaintiffs would suffer emotional distress, knowing that Plaintiffs would be directly affected by their misconduct.

86. On information and belief, the Roe Defendants engaged in this misconduct willfully and maliciously.

87. As a result of the Roe Defendants' misconduct, Plaintiffs have suffered severe emotional distress.

88. The Roe Defendants' misconduct was a substantial factor in causing Plaintiffs' severe emotional distress.

FOURTH CLAIM FOR RELIEF

(Negligent Infliction of Emotional Distress

By All Plaintiffs Against All Defendants)

89. Plaintiffs incorporate by reference the allegations contained in Paragraphs 1 through 68.

90. As to the Roe Defendants only, Plaintiffs allege this cause of action in the alternative to their Second Claim for Relief for Intentional Infliction of Emotional Distress.

91. Defendants, and each of them, owed Plaintiffs a general duty of care to avoid taking actions that would injure Plaintiffs.

92. Defendants, and each of them, breached their duty of care to Plaintiffs by

making the Stolen Data available and searchable through the Roe Websites, knowing that it would imply that Plaintiffs and other Users are adulterers.

93. As a result of Defendants' negligence, Plaintiffs have suffered severe emotional distress.

94. Defendants' negligence was a substantial factor in causing Plaintiffs' severe emotional distress.

FIFTH CLAIM FOR RELIEF

(Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030

By All Plaintiffs Against All Defendants)

95. Plaintiffs incorporate by reference the allegations contained in Paragraphs 1 through 68.

96. Ashley Madison's server constitutes a "protected computer," as that term is defined in 18 U.S.C. §1030(e)(2).

97. The Hackers, without authorization, intentionally accessed Ashley Madison's server and thereby obtained confidential information about Plaintiffs, in violation of 18 U.S.C. §1030(a)(2)(C).

98. Thereafter, the Hackers publicly threatened on multiple websites to publish and expose the confidential information about Plaintiffs unless Ashley Madison ceased operation of its website.

99. In making these threats, the Hackers, with the intent to extort a thing of value, threatened to impair the confidentiality of the information obtained from a protected computer without authorization, in violation of 18 U.S.C. §1030(a)(7)(B).

100. Moreover, in making these threats, the Hackers, with the intent to extort a thing of value, demanded the thing of value in exchange for not causing further damage, in violation of 18 U.S.C. §1030(a)(7)(C).

101. The Hackers provided the unlawfully-obtained confidential information about Plaintiffs to the Roe Defendants.

102. The Roe Defendants accepted the unlawfully obtained information from the

Hackers and published that information on the publicly-viewable Roe Websites.

103. The Roe Defendants engaged in this conduct knowing that the Hackers had obtained the information through the unlawful means described herein and had made the threats described herein.

104. The Roe Defendants thereby conspired to commit and attempted to commit violations of 18 U.S.C. §1030(a)(7)(B) and (C) in violation of 18 U.S.C. §1030(b).

105. The Roe Defendants provided the unlawfully obtained confidential information about Plaintiffs to the ISP Defendants to host on the ISP Defendants' servers and to display on the publicly-viewable Roe Websites.

106. The ISP Defendants accepted the unlawfully obtained information from the Roe Defendants and assisted the Roe Defendants in displaying that information on publicly-viewable Internet websites.

107. The ISP Defendants engaged in this conduct knowing that the Hackers had obtained the information through the unlawful means described herein and had made the threats described herein.

108. The ISP Defendants thereby conspired to commit and attempted to commit violations of 18 U.S.C. §1030(a)(7)(B) and (C) in violation of 18 U.S.C. §1030(b).

109. Defendants' conduct described herein has caused loss to 1 or more persons during any 1-year period aggregating at least $5,000.

110. As a result of these violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, Plaintiffs have suffered damage or loss in an amount to be determined at trial, but not less than $3,000,000.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request judgment in their favor and against Defendants on each and every claim in this Complaint and for relief as follows:

1. That the Court preliminarily and permanently enjoin Defendants and their agents, employees, representatives, and successors and predecessors in interest from possessing, hosting, publishing, or otherwise making available the Stolen Data.

2. That the Court award damages and monetary relief as follows:

a. Plaintiffs' actual damages in an amount to be determined at trial, but not less than three million dollars ($3,000,000);

b. Treble damages, where applicable;

c. Punitive and exemplary damages, where applicable;

d. Plaintiffs' attorneys fees pursuant to Cal. Penal Code § 496(c); and

e. Plaintiffs' costs and applicable interest.

3. Such other relief that the Court determines is just and proper.

Respectfully submitted,

DATED: September 3, 2015

KRONENBERGER ROSENFELD, LLP

By: s/ Karl S. Kronenberger
Karl S. Kronenberger

Attorneys for Plaintiffs

REQUEST FOR JURY TRIAL

Plaintiffs hereby demand a trial of this action by jury.

Respectfully Submitted,

DATED: September 3, 2015

KRONENBERGER ROSENFELD, LLP

By: s/ Karl S. Kronenberger
Karl S. Kronenberger

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Civil Cover Sheet

This automated JS-44 conforms generally to the manual JS-44 approved by the Judicial Conference of the United States in September 1974. The data is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. The information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is authorized for use only in the District of Arizona.

The completed cover sheet must be printed directly to PDF and filed as an attachment to the Complaint or Notice of Removal.

Plaintiff(s): **John Doe 1 ; John Doe 2 ; John Doe 3**	**Defendant**(s): **GoDaddy.com, LLC ; Amazon Web Services, Inc. ; John Roe 1 ; John Roe 2 ; John Roe 3 ; Roes 4 - 20**
County of Residence: Outside the State of Arizona	County of Residence: Maricopa
County Where Claim For Relief Arose: Maricopa	

Plaintiff's Atty(s):

Karl Stephen Kronenberger , Attorney
Kronenberger Rosenfeld, LLP
150 Post St.
San Francisco, California 94108
4159551155

Virginia Anne Sanderson , Attorney
Kronenberger Rosenfeld, LLP
150 Post St.
San Francisco, California 94108
4159551155

Jeffrey Michael Rosenfeld , Attorney
Kronenberger Rosenfeld, LLP
150 Post St.
San Francisco, California 94108
4159551155

Defendant's Atty(s):

II. Basis of Jurisdiction: **3. Federal Question (U.S. not a party)**

III. Citizenship of Principal

Parties **(Diversity Cases Only)**

Plaintiff:- **N/A**

Defendant:- **N/A**

IV. Origin : **1. Original Proceeding**

V. Nature of Suit: **890 Other Statutory Actions**

VI.Cause of Action: **18 USC § 1030**

VII. Requested in Complaint

Class Action: **No**

Dollar Demand: **3,000,000**

Jury Demand: **Yes**

VIII. This case **is not related** to another case.

Signature: Karl S. Kronenberger

Date: 09/03/2015

If any of this information is incorrect, please go back to the Civil Cover Sheet Input form using the *Back* button in your browser and change it. Once correct, save this form as a PDF and include it as an attachment to your case opening documents.

Revised: 01/2014