

1 Eric H. Gibbs (State Bar No. 178658)
 ehg@girardgibbs.com
 2 Matthew B. George (State Bar No. 239322)
 mbg@girardgibbs.com
 3 Caitlyn D. Finley (State Bar No. 286242)
 cdf@girardgibbs.com
GIRARD GIBBS LLP
 4 601 California Street, 14th Floor
 San Francisco, California 94108
 5 Telephone: (415) 981-4800
 Facsimile: (415) 981-4846

6 *Attorneys for Plaintiff*

7
 8 **UNITED STATES DISTRICT COURT**
 9 **NORTHERN DISTRICT OF CALIFORNIA**
 10 **SAN JOSE DIVISION**

11
 12 CHRISTINA HALPAIN, on behalf of herself and
 13 all others similarly situated,

14
 15 Plaintiff,

16 vs.

17
 18 ADOBE SYSTEMS, INC.,

19
 20 Defendant.

Case No.

CLASS ACTION

COMPLAINT FOR RELIEF BASED ON:

- 1. **VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW**
- 2. **VIOLATION OF CALIFORNIA DATA BREACH ACT**
- 3. **BREACH OF CONTRACT**
- 4. **BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING**
- 5. **MONEY HAD AND RECEIVED**

DEMAND FOR JURY TRIAL

1 Plaintiff Christina Halpain, on behalf of herself and all others similarly situated, alleges as
2 follows:

3 **NATURE OF THE CASE**

4 1. Plaintiff Christina Halpain (“Plaintiff”) brings this complaint against Adobe Systems, Inc.
5 (“Adobe”) for unlawfully failing to properly secure and protect its users’ sensitive personally
6 identifiable information (“PII”), including e-mail addresses, passwords, credit and debit card numbers,
7 expiration dates, and mailing and billing addresses. Adobe promises its users that it will provide
8 “reasonable administrative, technical, and physical security controls” to protect their PII and represents
9 that it uses industry-leading security practices to do so, but Adobe’s actual security practices are
10 substandard in the industry and continue to result in breaches of Adobe’s networks and software.

11 2. On October 3, 2013, Adobe publically announced its largest security breach to date, in
12 which hackers stole approximately 3 million credit and debit card records as well as login data for an
13 undetermined number of Adobe users. Adobe later confirmed that the data breach was thirteen times
14 larger than initially reported, with approximately 38 million active Adobe users impacted. The massive
15 breach did not come as a surprise to industry experts familiar with Adobe’s security practices who
16 warned that Adobe’s shoddy security protocols and track record of previous breaches made it
17 susceptible to massive hack of the scope and depth that resulted.

18 3. Plaintiff and the Class she seeks to represent have been damaged by Adobe’s
19 misrepresentations and non-disclosure of its substandard security practices because they purchased and
20 used Adobe products and services of a quality different than they were promised and which they
21 contracted for. Plaintiff therefore brings this action on behalf of a proposed class of Adobe users whose
22 personal information was compromised as a result of the data breach that occurred on or around
23 September 2013.

24 **PARTIES**

25 4. Plaintiff Christina Halpain is citizen and resident of Huntington Beach, California.

26 5. Defendant Adobe Systems, Inc. is a corporation organized under the laws of the State of
27 Delaware with its principal place of business in San Jose, California.

28 //

1 **JURISDICTION AND VENUE**

2 6. This Court has jurisdiction over this action under the Class Action Fairness Act, 28
3 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed the sum value of
4 \$5,000,000, exclusive of interest and costs, and this is a class action in which more than two-thirds of
5 the proposed plaintiff class, on the one hand, and Defendant Adobe, on the other, are citizens of
6 different states.

7 7. This Court has jurisdiction over Adobe because it maintains its principal headquarters in
8 California, is registered to conduct business in California, has sufficient minimum contacts in California,
9 or otherwise intentionally avails itself of the markets within California, through the promotion, sale,
10 marketing and distribution of its products in California, to render the exercise of jurisdiction by this
11 Court proper and necessary. Moreover, Adobe's wrongful conduct (as described below) emanates from
12 California.

13 8. Venue is proper in this District under 28 U.S.C. § 1391 because Adobe resides in this
14 District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this
15 District.

16 **INTRADISTRICT ASSIGNMENT**

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

20 **FACTUAL ALLEGATIONS**

21 **Adobe's Products and Services Require Storage of Sensitive Consumer Data**

22 10. Adobe is a multinational computer software company that sells and licenses printing,
23 publishing, multimedia, and graphics software products to consumers, professionals, publishers,
24 developers, businesses and organizations.

25 11. Some of Adobe's most popular software products and services include, among others,
26 Illustrator, Photoshop, Acrobat Reader, InDesign, Dreamweaver, Muse, ColdFusion, and Creative Suite,
27 a software bundle that includes some of Adobe's most popular graphic design software applications.
28

1 Adobe's ubiquitous Acrobat Reader and Flash Player are commonly used by consumers on their
2 computers or smart phones to simply view documents, videos or other graphic Internet content.

3 12. Adobe has sold and continues to sell licenses for its software for prices ranging from
4 several hundred dollars for software upgrades to several thousand dollars for initial purchases of
5 software licenses for applications like ColdFusion or Photoshop.

6 13. In April 2012, Adobe announced the introduction of the Adobe Creative Cloud, a
7 subscription based offering of Adobe's popular Creative Suite software bundle with design, web, video
8 and digital imaging tools such as Photoshop, Illustrator and other products. The move was part of
9 Adobe's shift from traditional desktop software to a subscription-based model or "Software as a Service
10 (SAAS)". Instead of consumers paying a one-time price for a software license, consumers who wanted
11 an upgraded version of Creative Suite or another Adobe software product would now have to pay
12 monthly subscription payments. Adobe's Creative Cloud "complete plan" for individual membership
13 typically costs consumers \$49.99 a month with an annual commitment. Customers who elect for the
14 year-long Adobe subscription are subject to a penalty if they cancel their subscription before the end of
15 their contract and must pay the difference between the monthly and yearly commitment pricing for the
16 months their accounts were active.

17 14. Adobe's Creative Cloud and other software subscriptions rely on reoccurring monthly
18 payments that require customers to keep an active credit card on file with Adobe. Adobe stores
19 consumers' credit or debit card information so it can automatically charge customers without sending a
20 traditional bill and without having to wait for payment. Monthly-billed services, like Adobe's
21 subscription services, require companies to store a massive number of active debit and credit cards and
22 thus have long been a target for cyber criminals. Since its launch in April 2012, Adobe's Creative Cloud
23 service has amassed over 1 million subscribers.

24 15. In May 2013, Adobe announced that its popular Creative Suite software bundle and other
25 popular software products would only be available by subscription through Adobe's Creative Cloud
26 service. Adobe would no longer offer upgrades or updates to customers with its traditional desktop
27 software for Adobe's Creative Suite and other applications.

28 //

1 **Adobe Misrepresents That It Uses Industry-Leading Security Practices**

2 16. Adobe offers its software products and services to consumers as a license to use the
3 software, content and services in accordance with certain terms and conditions set out in an End-User
4 License Agreement (“EULA”). As a condition of using Adobe’s software, content or services,
5 customers must agree to the EULA.

6 17. Adobe’s EULA and General Terms of Use state that if a customer resides in North
7 America, or a customer's business is headquartered in North America, then Adobe’s terms “shall be
8 governed and construed pursuant to the laws of California, regardless of conflict of law principles.”
9 Adobe also states that customers irrevocably consent to the exclusive jurisdiction and venue of the
10 courts in Santa Clara County, California.

11 18. Both Adobe’s General Terms of Use and the EULAs for Adobe software products
12 incorporate Adobe’s Privacy Policy as a term of the contract. According to Adobe’s Privacy Policy,
13 when consumers register to use an Adobe application or website, create an Adobe ID, or contact Adobe
14 for customer support or other offerings, Adobe collects identifying information, which may include a
15 person’s name, company name, email address, and/or payment information.

16 19. According to Adobe’s Privacy Policy, Adobe understands that the security of consumers’
17 personal information is “important” and states that Adobe will “provide reasonable administrative,
18 technical, and physical security controls” to protect consumers personal information. According to
19 Adobe’s Safe Harbor Privacy Policy, which supplements Adobe’s Privacy Policy, “Adobe Systems
20 Incorporated uses reasonable physical, electronic, and administrative safeguards to protect your personal
21 information from loss; misuse; or unauthorized access, disclosure, alteration, or destruction.”

22 20. In addition to the terms of the Privacy Policy, Adobe has additional webpages dedicated
23 to explaining and describing Adobe’s purportedly industry-leading security practices to consumers.
24 According to Adobe’s website:

25
26 “At Adobe, the security of your digital experiences is our priority. From
27 our rigorous internal software development process and tools to our cross-
28 functional incident response team, we strive to be proactive, nimble, and

1 accurate in all aspects of security. *What's more, our collaborative work*
2 *with partners, researchers, and other industry organizations helps*
3 *ensure the latest security best practices are built into every product and*
4 *service we offer."*

5 (emphasis added).

6 21. Throughout its website, Adobe consistently and uniformly represents to consumers that
7 Adobe employs "best" practices and works with industry leaders when it comes to data security:

8
9 "Adobe believes it can achieve the *best security* through ongoing
10 proactive measures and deployment of multiple in defense-in-depth
11 methods. *We take pride in the company-wide best practices, processes*
12 *and tools that help ensure your information is safe whenever you use*
13 *Adobe products and services."*

14
15 "Adobe is proud of our work with partners, researchers, and other
16 industry-leading companies and security organizations to share ideas for
17 building more secure software, useful global threat data, and *operational*
18 *best practices*. We believe this collaboration results in better security for
19 both our customers and others in the computing community."

20 (emphasis added).

21 22. Adobe's website also touts that members of Adobe Secure Software Engineering Team
22 (or "ASSET") actively participate in several cyber-security industry organizations including the Open
23 Web Application Security Project ("OWASP"), an open-source web application security project and an
24 emerging standards body. The OWASP Top Ten project raises awareness about application security by
25 identifying some of the most critical risks facing organizations. The Top 10 project is referenced by
26 many standards, books, tools, and organizations including Payment Card Industry Data Security
27 Standard (PCI DSS), Defense Information Systems Agency (DISA), the Federal Trade Commission
28 (FTC) and many more.

1 23. With the launch of Adobe's new subscription cloud services, Adobe acknowledged that
2 one of its customers' principal concerns was security. Adobe reassured consumers and businesses that
3 Adobe uses industry-leading security practices. According to Adobe, security, privacy and compliance
4 policies are some of the most common questions Adobe receives about Creative Cloud. In an
5 informational document for IT Security Staff, Adobe stated that "Organizations using Creative Cloud
6 are concerned about the safety of their data and that access to their data is reliable."

7 24. On a FAQ page for Adobe's Creative Cloud service on its website, Adobe repeatedly
8 emphasizes Adobe's use of industry-leading security practices:

9
10 **"How secure is the storage space on Creative Cloud?"**

11 Adobe uses *industry-leading security engineering processes* to build its
12 products. With Creative Cloud, security is considered at every level, from
13 applications to networks to physical facilities. In addition to the latest
14 technologies, *Adobe adheres to the latest best-practice policies regarding*
15 *online security.*

16
17 **What security is used at the application level? What security**
18 **measures are in place during file transfer, and are stored files**
19 **encrypted?**

20 *Creative cloud uses industry-leading encryption technology to protect*
21 *our members' data* [...] For stored Creative Cloud assets, users benefit
22 from *industry-leading security* and certifications provided by Amazon
23 Web Services."

24 (emphasis added).

25 25. Several other of Adobe's FAQs and marketing materials emphasize that Adobe works
26 with industry researchers and organizations to "understand the latest security best practices and trends
27 and continue to build security into the products and services we offer."

28 //

Adobe's Abysmal Security Record

1
2 26. Despite Adobe's many claims and representations about its use of industry-best practices,
3 Adobe has consistently struggled with security problems for the past decade and has been an easy target
4 for cyber criminals.

5 27. Adobe's security problems are not limited to the most recent security breach, or even
6 limited to just one or two bad years or incidents. In seven years Adobe has had at least eight different
7 security breaches impacting its networks and software:

- 8 a) In 2007, an Adobe Reader bug allowed hackers access to all the files on people's
9 computers.
- 10 b) In 2008, more than 1,000 hacked websites infected computers by delivering fake Adobe
11 Flash Player updates that posed as CNN news notifications.
- 12 c) In 2009, a vulnerability in Adobe's Reader let hackers open back doors into people's
13 computers.
- 14 d) In 2010, attackers created malicious Adobe PDF attachments to hack into several
15 companies, including Adobe.
- 16 e) In 2011, yet another bug gave hackers remote access to people's computers – this time in
17 Adobe's commonly used Flash Player.
- 18 f) In 2012, hackers gained access to Adobe's security system by tapping into its internal
19 servers.
- 20 g) In early February 2013, Adobe issued an emergency update to its Flash Player for two
21 previously unknown security holes that were being exploited by hackers. Less than a
22 month later, Adobe was forced to issue another security patch for its vulnerable Flash
23 Player plug-in.
- 24 h) In June 2013, less than 24-hours after Adobe's Creative Cloud went live the software
25 was hacked causing versions of Adobe's Creative Cloud to appear on pirating websites.

26 28. Adobe's security practices were so bad that in 2010, former Apple CEO Steve Jobs
27 blamed Adobe's commonly used Flash Player Plug-In for being "the number one reason Macs crash"
28 and cited Flash Player for having "one of the worst security records in 2009."

1 29. In 2009, Adobe's Flash Player and Acrobat Reader tied for second place on Symantec's
2 annual list of vulnerable plug-in programs. In 2010 and 2012, Adobe's Acrobat Reader and Flash Player
3 took the top spots on that list, respectively.

4 **The Data Breach and Adobe's Failure to Reasonably Notify Consumers of the Breach**

5 30. According to Adobe, sometime between mid-August and mid-September 2013, hackers
6 broke into an Adobe network that handled credit card transactions for Adobe's customers and also
7 illegally accessed an Adobe source code repository.

8 31. Adobe later confirmed that it was aware of the breach as early as September 17, 2013.
9 But Adobe did not promptly notify Adobe customers about the breach or that customers' PII was
10 compromised.

11 32. Adobe remained silent even as others in the industry became aware of the hack. In late
12 September 2013, two independent Internet security researchers discovered a 40-gigabyte trove of Adobe
13 source code on a server used by the same cyber criminals believed to have hacked into major data
14 aggregators earlier in 2013. Shortly after discovering the stolen source code, the researches shared their
15 discovery with Adobe.

16 33. On October 3, 2013, more than two weeks after discovering the hack, Adobe announced
17 the data breach and informed customers that hackers had accessed customer names, login IDs,
18 passwords, credit and debit card numbers, mailing and billing addresses, and expiration dates, as well as
19 other data for approximately 2.9 million customers worldwide. On top of the PII lost during the breach,
20 Adobe also confirmed that hackers compromised the source code for Adobe Acrobat, ColdFusion,
21 ColdFusion Builder and "other Adobe products."

22 34. On October 29, 2013, Adobe announced that the security breach was much larger than
23 first reported. According to Adobe, hackers had obtained access to Adobe IDs and passwords for
24 approximately 38 million active users. Adobe also announced that hackers stole source code for
25 Adobe's Photoshop software.

26 35. Throughout October 2013, Adobe sent emails to impacted users asking them to reset their
27 login credentials for their Adobe accounts and advised users to monitor their accounts for fraud and
28 identity theft and to regularly review their account statements and credit reports. Although Adobe had

1 publicly announced it would provide impacted users with credit monitoring, the email notification did
2 not mention any offer of credit monitoring services, and it took Adobe several days or weeks after
3 announcing the breach to mail letters containing the activation codes for Adobe's offer of free credit
4 monitoring.

5 **Adobe Failed to Use Industry Best Practices**

6 36. Following the announcement of the breach, researchers revealed, and Adobe later
7 confirmed, that the millions of passwords stolen during the data breach were not originally stored
8 according to industry best practices.

9 37. According to one security website, Adobe's encryption method was so weak that with
10 very little effort researchers were able to recover a lot of information about the compromised data,
11 including identifying the top five passwords precisely, the 2.75% of users who chose them, the
12 compromised accounts' password hints, and the password length of nearly one-third of the nearly 150
13 million user database.

14 38. In the wake of the massive breach, security experts opined that the breach was expected
15 given Adobe's abysmal record when it came to security. According to those experts, Adobe's software
16 is a prime target for hackers because its core code is old and weak by today's standards. Adobe's
17 updates and security patches are built on top of that code but cannot make up for the software's inherent
18 flaws. According to one news article, Adobe's patches are "akin to making repairs to a house with a
19 sinking foundation."

20 39. Security experts further warned that the Adobe's security track record is only going to get
21 worse in the future. According to Kevin Rogers, CEO of the security firm Cypherpath, Adobe's
22 customers will remain at risk of attack until the company completely revamps its software.

23 **The Impact of Adobe's Stolen Source Code**

24 40. When Adobe first announced the security breach on October 3, 2013, it stated that along
25 with stolen PII for several million users, source code for Adobe Acrobat, ColdFusion, ColdFusion
26 Builder and "other Adobe products," was also compromised.

1 41. Many Adobe users became concerned that the stolen source code made their Adobe
2 software products more vulnerable to attack. At that time, however, Adobe would not give any more
3 public information on the scope of the breach.

4 42. On October 29, 2013, after source code for Adobe's Photoshop application appeared
5 online, Adobe confirmed that a portion of Photoshop source code was accessed by the attackers as part
6 of the incident Adobe had disclosed on October 3, 2013.

7 43. Adobe software runs on a closed-source code ecosystem that is not available to the
8 public. One reason companies use this kind of closed-source code is for security. When hackers cannot
9 see the code, it is more difficult to break or exploit. According to security experts, the access to Adobe's
10 closed-source code now makes Adobe's already weak software even easier to infiltrate and more
11 vulnerable to future attacks.

12 44. With deeper access to Adobe's closed-source code, hackers can now better understand
13 the framework of Adobe's security. The stolen source code makes Adobe's software subject to
14 increased vulnerability for widespread attack, which could cover everything from opening PDFs through
15 Adobe's Acrobat Reader to designing web applications through Adobe's ColdFusion software. Some
16 security experts have suggested that Adobe users switch to different software to protect themselves
17 against a future hack.

18 45. Unfortunately, many Adobe users have invested substantial amounts of money in their
19 Adobe software or committed to annual subscriptions for Adobe services under the mistaken belief and
20 understanding that Adobe's software was secure and are now stuck with software products and services
21 that are of less value to them.

22 **Plaintiff Halpain's Experience**

23 46. Ms. Halpain is a graphic and website designer who uses Adobe design software as part of
24 her business creating print graphics and websites for clients.

25 47. Since 2007, Ms. Halpain has purchased several Adobe graphic and website design
26 software products and services.

27 48. In February 2013, Ms. Halpain purchased a year-long Creative Cloud subscription that
28 would give her access to the most up-to-date Adobe graphic and web design software, including Muse,

1 Photoshop, Illustrator, InDesign and Acrobat. Ms. Halpain agreed to a one-year Creative Cloud
2 subscription that would cost her approximately \$29.00 per month.

3 49. Before purchasing her Adobe Creative Cloud subscription, Ms. Halpain agreed to
4 Adobe's End User License Agreement and Adobe's General Terms of Use which incorporated by
5 reference Adobe's Privacy Policy as a term of the contract. Ms. Halpain understood and expected
6 Adobe to use industry best practices to protect her information and to securely build its software
7 products.

8 50. Ms. Halpain agreed to Adobe's Privacy Policy and the representations contained therein
9 before agreeing to purchase her Creative Cloud subscription. Adobe's Privacy Policy promised Ms.
10 Halpain that Adobe would provide "reasonable administrative, technical, and physical security controls"
11 to protect her personal information.

12 51. Because Adobe required her to keep an active credit or debit card on file for her Adobe
13 Creative Cloud subscription, Ms. Halpain believed that Adobe would use reasonable and acceptable
14 methods to secure her personal information in accordance with its representations in its Privacy Policy
15 and in accordance with Adobe's many representations regarding its industry-leading security practices.

16 52. On October 3, 2013, Ms. Halpain received an email from Adobe notifying her of the data
17 breach and advising her to reset her login information and to monitor her accounts and credit report.

18 53. On October 22, 2013, Ms. Halpain received a letter from Adobe with an offer for a credit
19 monitoring service. Ms. Halpain believed that the credit monitoring service was insufficient to meet her
20 needs and decided to buy an alternative credit monitoring service from myfico.com for approximately
21 \$15.00 dollars per month. In addition to purchasing alternative crediting monitoring services Ms.
22 Halpain decided to sign up for a password security service called LastPass which provides password
23 protection beyond the protection Adobe uses.

24 54. Ms. Halpain believed that a portion of the premium she paid for her Adobe Creative
25 Cloud subscription was to provide for adequate security to protect her personal information and the
26 security of the software products she used. Had Ms. Halpain known that Adobe employed substandard
27 security practices, she would not have purchased Adobe products and/or services.
28

1 55. Ms. Halpain remains concerned that Adobe's software and networks remain vulnerable to
2 attack given what she now knows about Adobe's substandard security practices. Ms. Halpain, however,
3 must still keep an active credit or debit card on file with Adobe and pay \$29.00 per month for her
4 Creative Cloud subscription at least until her one-year commitment expires in 2014. Ms. Halpain will
5 be subject to a monetary penalty if she decides to cancel her membership before her one-year contract
6 ends.

7 56. As a result of the breach, Ms. Halpain's Creative Cloud subscription is of less value to
8 her. Ms. Halpain has spent time and money as a result of the breach in order to protect her PII.
9 Additionally, because the source code for the Adobe software that she uses was stolen, Ms. Halpain's
10 Adobe software and the websites that she designs and maintains for her clients with that software are
11 more vulnerable to attack. Consequently, Ms. Halpain has had to notify her clients about potential
12 vulnerabilities in the websites she creates and maintains with Adobe's software. Ms. Halpain now has to
13 work diligently to monitor the security of the websites she maintains for her clients and is looking into
14 alternative and more secure methods for continuing to support and maintain her clients' websites.

15 57. Given its substandard security practices and on-going security problems, Adobe knew or
16 should have known that its networks and software products and services were not secure and left
17 Plaintiff and the other Class members' personal identification vulnerable to attack, theft and misuse.

18 58. Adobe recklessly, or as a matter of gross negligence, failed to provide reasonable and
19 adequate security measures even after repeated hacks to its networks and software over the past seven
20 years.

21 59. Upon learning of the data breach, Adobe failed to notify Plaintiff and the other Class
22 members in a timely manner as required by law.

23 60. As a result of Adobe's practices, Plaintiff and the Class she seeks to represent, have been
24 damaged and have lost money or property as a result of Adobe's misrepresentations, concealments, and
25 non-disclosure of its poor, substandard security practices, because they purchased Adobe products and
26 services of a quality different than they were promised and contracted for, and paid a premium, for what
27 they believed was a superior product, that they otherwise would not have paid.
28

1 **CLASS ACTION ALLEGATIONS**

2 61. Plaintiff brings this action on behalf of herself and a class of persons initially defined as
3 follows:

4 All individuals and entities in the United States who had an Adobe account and whose
5 personal information was compromised as a result of the data breach that occurred on or
6 around September 2013.

7 62. Excluded from the proposed class are Adobe; any affiliate, parent, or subsidiary of
8 Adobe; any entity in which Adobe has a controlling interest, any officer, director, or employee of
9 Adobe; any successor or assign of Adobe; anyone employed by counsel for Plaintiff in this action; and
10 any Judge to whom this case is assigned as well as his or her immediate family.

11 63. This action has been brought and may properly be maintained on behalf of the Class
12 proposed above under the criteria of Rule 23 of the Federal Rules of Civil Procedure.

13 64. Numerosity. Members of the class are so numerous that their individual joinder is
14 impracticable. Upon information and belief there are millions of people in the Class, making joinder of
15 each individual member impracticable. Members of the Class are easily ascertainable through Adobe's
16 own records.

17 65. Existence and Predominance of Common Questions. Common questions of law and fact
18 exist as to all class members and predominate over questions affecting only individual class members.
19 These common questions include the following:

- 20 a. Whether Adobe failed to protect users' PII with industry-standard protocols and
21 technology;
- 22 b. Whether Adobe's practices are false, misleading, or reasonably likely to deceive;
- 23 c. Whether Adobe failed to disclose material facts relating to the character and quality
24 of its securities practices;
- 25 d. Whether Adobe knew that its representations about its security practices were false
26 and misleading but continued to disseminate them;
- 27 e. Whether California law applies to the proposed Class;
- 28 f. Whether Adobe's conduct described herein constitutes a breach of contract;

- 1 g. Whether Adobe's conduct described herein was negligent and/or grossly negligent;
- 2 h. Whether Adobe's conduct described herein constitutes a breach of the covenant of
- 3 good faith and fair dealing;
- 4 i. Whether Adobe's conduct described herein constitutes a claim for money had and
- 5 received;
- 6 j. Whether Adobe violated the California Data Breach Act, Cal. Civ. Code § 1798.80,
- 7 *et. seq.*, as alleged in this complaint;
- 8 k. Whether Adobe violated California' Online Privacy Protection Act, Cal. Bus. & Prof.
- 9 Code § 22576, as alleged in this complaint;
- 10 l. Whether Adobe has engaged in unlawful, unfair, or fraudulent business practices in
- 11 violation of California Business and Professions Code section 17200 *et seq.*, as
- 12 alleged in this complaint;
- 13 m. Whether Plaintiff and the other class members are entitled to equitable relief,
- 14 including, but not limited to a preliminary and/or permanent injunction.

15 66. Typicality. Plaintiff's claims are typical of the claims of the class members because,

16 among other things, Plaintiff and Class members sustained similar damages as a result of Adobe's

17 uniform wrongful conduct and their legal claims all arise from the same core Adobe practice.

18 67. Adequacy of Representation. Plaintiff is an adequate representative of the Class because

19 her interests do not conflict with the interests of the members of the Class she seeks to represent.

20 Plaintiff has retained counsel competent and experienced in complex class action litigation, and Plaintiff

21 intends to prosecute this action vigorously. The interests of members of the Class will be fairly and

22 adequately protected by Plaintiff and her counsel.

23 68. Superiority. The class action is superior to other available means for the fair and efficient

24 adjudication of this dispute. The injury suffered by each Class member, while meaningful on an

25 individual basis, is not of such magnitude as to make the prosecution of individual actions against

26 Adobe economically feasible. Even if Class members themselves could afford such individualized

27 litigation, the court system could not. In addition to the burden and expense of managing numerous

28 actions arising from the headlight assembly defect, individualized litigation presents a potential for

1 inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all
2 parties and the court system presented by the legal and factual issues of the case. By contrast, the class
3 action device presents far fewer management difficulties and provides the benefits of a single
4 adjudication, economy of scale, and comprehensive supervision by a single court.

5 69. In the alternative, the class may be certified because:

- 6 a. the prosecution of separate actions by the individual members of the Class would
7 create a risk of inconsistent or varying adjudication with respect to individual Class
8 members which would establish incompatible standards of conduct for Adobe;
- 9 b. the prosecution of separate actions by individual Class members would create a risk
10 of adjudications with respect to them which would, as a practical matter, be
11 dispositive of the interests of other Class members not parties to the adjudications, or
12 substantially impair or impede their ability to protect their interests; and
- 13 c. Adobe has acted or refused to act on grounds generally applicable to the Class,
14 thereby making appropriate final and injunctive relief with respect to the members of
15 the Class as a whole.

16
17 **FIRST CAUSE OF ACTION**

18 **(For unlawful, unfair, and fraudulent business practices under**
19 **California Business and Professions Code § 17200, et seq.)**

20 70. Plaintiff realleges, as if fully set forth, each and every allegation herein.

21 71. Adobe’s acts and practices, as alleged in this complaint, constitute unlawful, unfair
22 and/or fraudulent business practices, in violation of the Unfair Competition Law, Cal. Bus. & Prof. Code
23 § 17200, et seq.

24 72. Adobe’s acts and practices, as alleged in this complaint, constitute fraudulent practices in
25 that they are likely to deceive a reasonable consumer.

26 73. Adobe’s acts and practices, as alleged in this complaint, constitute unlawful practices in
27 that they violate the California Data Breach Act, Cal. Civ. Code § 1798.80, et. seq.

1 74. Adobe’s acts and practices, as alleged in this complaint, constitute unlawful practices in
2 that they violate California’s Online Privacy Protection Act (“OPPA”), Cal. Bus. & Prof. Code § 22576,
3 which prohibits any company whose website or online service that collects personal identifiable
4 information from California consumers from “knowingly and willfully” or “negligently and materially”
5 breaching its own posted privacy policy.

6 75. Adobe’s acts and practices, as alleged in this complaint, constitute unlawful practices in
7 that they constitute a systematic breach of contract;

8 76. Adobe engaged in unfair business practices by, among other things:

- 9 a. Engaging in conduct where the utility of that conduct is outweighed by the gravity
10 of the consequences to Plaintiff and other members of the class;
- 11 b. Engaging in conduct that is immoral, unethical, oppressive, unscrupulous, or
12 substantially injurious to Plaintiff and other members of the class; and
- 13 c. Engaging in conduct that undermines or violates the stated policies underlying the
14 California’s Online Privacy Act and the California Data Breach Act, which seek
15 to protect consumers and their PII.

16 77. As a direct and proximate result of Adobe’s unlawful, unfair and fraudulent business
17 practices as alleged herein, Plaintiff and Class members have suffered injury in fact and lost money or
18 property, in that they purchased software licenses and software subscriptions they otherwise would not
19 have, paid more for their software licenses and subscriptions than they otherwise would, and paid for
20 alternative credit monitoring services as a result of the breach. Meanwhile, Adobe has sold more
21 software licenses and subscription services than it otherwise could have and charged inflated prices for
22 its services and products, unjustly enriching itself thereby.

23 78. Plaintiff and Class members are entitled to equitable relief, including restitutionary
24 disgorgement of all profits accruing to Adobe because of its unlawful, unfair and fraudulent, and
25 deceptive practices, attorneys’ fees and costs, declaratory relief, and a permanent injunction enjoining
26 Adobe from its unlawful, unfair, fraudulent and deceitful activity.

27 //

28

SECOND CAUSE OF ACTION

(Violation of the California Data Breach Act, Cal. Civ. Code § 1798.80, et. seq.)

79. Plaintiff realleges, as if fully set forth, each and every allegation herein.

80. The September 2013 data breach constituted a “breach of the security system” of Adobe pursuant to Cal. Civ. Code §1798.82(g).

81. Adobe recklessly, or as a matter of gross negligence, failed to provide reasonable and adequate security measures even after repeated hacks to its networks and software over the past seven years.

82. Adobe unreasonably delayed informing Plaintiff and members of the Class about the breach of security of Class members’ confidential and non-public information after Adobe knew the data breach occurred.

83. Adobe failed to disclose to Plaintiff and members of the Class, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, personal information when they knew or reasonably believed such information had been compromised.

84. Upon information and belief, no law enforcement agency instructed Adobe that notification to Plaintiff and Class members would impede investigation.

85. As a result of Adobe’s violation of Cal. Civ. Code § 1798.82, Plaintiff and members of the Class incurred economic damages relating to expenses for credit monitoring and the loss of value in the software licenses and subscriptions provided by Adobe.

86. Plaintiff, individually and on behalf of the members of the Class, seeks all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to: (a) damages suffered by members of the Class; (b) statutory damages for Adobe’s willful, intentional, and/or reckless violation of Cal. Civ. Code § 1798.83; and (c) equitable relief.

87. Plaintiff, individually and on behalf of the members of the Class, also seeks reasonable attorneys’ fees and costs under Cal. Civ. Code § 1798.84(g).

//

THIRD CAUSE OF ACTION

(For Breach of Contract)

1
2
3 88. Plaintiff realleges, as if fully set forth, each and every allegation herein.

4 89. In order to purchase a software license or software license subscription service, Adobe
5 required that Plaintiff, and members of the Class, affirmatively assent to Adobe's End User License
6 Agreements, General Terms of Use, and Privacy Policy which included representations regarding
7 Adobe's security protocols.

8 90. Plaintiff Halpain read and relied on Adobe's Privacy Policy and Adobe's representations
9 regarding privacy and data security before purchasing Adobe's Creative Cloud subscription service.

10 91. Plaintiff and each Class member assented to Adobe's End User License Agreement,
11 General Terms of Use and Privacy Policy when she and they paid for and registered for Adobe products
12 and/or services, and thereafter assented by using Adobe products and/or services.

13 92. As part of Adobe's contracts, Adobe imposed upon itself an obligation to use reasonable
14 and industry-standard security practices and procedures to protect Plaintiff's and Class members' data
15 and personal information.

16 93. Plaintiff expected that Adobe employed industry-leading security practices in accordance
17 with its representations when making her decision to purchase a Creative Cloud subscription with a
18 one-year commitment. Had Adobe represented that it would use substandard security measures or did
19 not use industry-best practices, Plaintiff would not have paid the premium she paid for her Creative
20 Cloud subscription.

21 94. Plaintiff and Class members performed their obligations under the Creative Cloud
22 contract by paying subscription fees and abiding by Adobe's End User License Agreement and General
23 Terms of Use.

24 95. By using substandard security measures for the protection of Adobe users PII, Adobe
25 breached the terms of its contract with Plaintiff and other members of the Class to protect her and the
26 Class members' personal information.

27 96. A software license or cloud service with a substandard security protocol is, in the eyes of
28 the marketplace and consumers such as Plaintiff and members of the Class, a fundamentally less useful

1 and valuable service than a software license or cloud service that uses industry-leading standard security
2 protections. Given the choice between two otherwise identical services or products, consumers and
3 entities will choose the company that uses industry-standard security practices over one that uses
4 substandard security practices.

5 97. Based on Adobe's representations, Plaintiff and members of the Class believed they
6 would receive industry-standard protection for their personal information as part of their Adobe products
7 and/or services, and those security protections were valuable to both Plaintiff and members of the Class.

8 98. Plaintiff and the other Class members paid for, but never received, the valuable security
9 protections to which they were entitled, and which would have made their Adobe products and/or
10 services significantly more useful.

11 99. Accordingly, Plaintiff, on behalf of herself and the other Class members, seeks an order
12 declaring that Adobe's conduct constitutes a breach of contract, and an award to Plaintiff and the Class
13 members' of damages in an amount equal to the difference in the free-market value of the secure
14 services and/or products paid for and the insecure services and/or products they received and for all
15 other damages proximately caused thereby.

16 **FOURTH CAUSE OF ACTION**

17 **(For Breach of Covenant of Good Faith and Fair Dealing)**

18 100. Plaintiff realleges, as if fully set forth, each and every allegation herein.

19 101. The law implies a covenant of good faith and fair dealing in every contract.

20 102. Plaintiff and Class members contracted with Adobe by accepting Adobe's offers and
21 paying Adobe for software products and/or services.

22 103. Plaintiff and the Class members performed all or substantially all of the significant duties
23 under their agreements with Adobe.

24 104. The conditions required for Adobe's performance under the contracts has occurred.

25 105. Adobe did not provide and/or unfairly interfered with and/or frustrated the right of
26 Plaintiff and the Class members to receive the full benefits under their agreements.

27 106. Adobe breached the covenant of good faith and fair dealing implied in its contracts with
28 Plaintiff and Class members by, among other things, failing to use and provide reasonable and industry-

1 leading security practices, an aspect of the parties' course of dealing by which Adobe exercised
2 unilateral discretion and control.

3 107. Plaintiff and the Class members were damaged by Adobe's breach in that Plaintiff and
4 the Class members paid for, but never received, the valuable security protections to which they were
5 entitled, and which would have made their software products and/or services more valuable.

6 **FIFTH CAUSE OF ACTION**

7 **(For Money Had and Received)**

8 108. Plaintiff realleges, as if fully set forth, each and every allegation herein.

9 109. Adobe misrepresented its security practices and procedures to Plaintiff and the Class.

10 110. Adobe received money belonging to Plaintiff and the Class members when it sold them
11 Adobe software products and/or services with substandard security.

12 111. Adobe benefited from the receipt of Plaintiff and the Class members money, and retained
13 it.

14 112. Adobe received money under circumstances that in equity and good conscience it should
15 not be able to retain.

16 113. As a result of Adobe's misconduct, Plaintiff and the other Class members have been
17 harmed and are entitled to relief. Adobe is obligated to make restitution to Plaintiff and the Class
18 members for their purchases of Adobe software products and/or services.

19 **PRAYER FOR RELIEF**

20 WHEREFORE, Plaintiff, on behalf of herself and on behalf of the class, pray for judgment as
21 follows:

- 22 a. For an order certifying the proposed class and appointing Plaintiff and her counsel to
- 23 represent the class;
- 24 b. For an order enjoining Adobe from continuing to engage in unlawful business practices,
- 25 as alleged herein;
- 26 c. For an order declaring that Adobe's acts and practices constitute a breach of contract, as
- 27 alleged herein;
- 28

- d. For an order awarding Plaintiff and the members of the Class actual, statutory and/or punitive damages;
- e. For an order awarding Plaintiff and members of the Class restitution, or any other equitable relief the Court deems proper;
- f. For an order awarding Plaintiff and the members of the Class pre-judgment and post-judgment interest;
- g. For any order awarding Plaintiff and the members of the Class reasonable attorneys' fees and costs of suit, including expert witness fees; and
- h. For an order awarding such other and further relief as this Court may deem just and proper.


DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all claims so triable.

Dated: November 11, 2013

Respectfully Submitted

GIRARD GIBBS LLP

By: 

Eric H. Gibbs
Matthew B. George
Caitlyn D. Finley
601 California Street, 14th Floor
San Francisco, CA 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846

Attorneys for Plaintiff

JS 44 (Rev. 12/12) cand rev (1/15/13)

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS
CHRISTINA HALPAIN

DEFENDANTS
ADOBE SYSTEMS, INC.

(b) County of Residence of First Listed Plaintiff Orange County, California
(EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant Santa Clara, California
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

(c) Attorneys (Firm Name, Address, and Telephone Number)
Eric H. Gibbs, GIRARD GIBBS LLP
601 California Street, 14th Floor, San Francisco, California 94108
Telephone: (415) 981-4800

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff
- 2 U.S. Government Defendant
- 3 Federal Question (U.S. Government Not a Party)
- 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

	PTF	DEF		PTF	DEF
Citizen of This State	<input checked="" type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4
Citizen of Another State	<input type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input checked="" type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS			
<input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding
- 2 Removed from State Court
- 3 Remanded from Appellate Court
- 4 Reinstated or Reopened
- 5 Transferred from Another District (specify)
- 6 Multidistrict Litigation

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
 28 U.S.C. § 1332(d); Cal. Bus. & Prof. Code § 17200, et seq.; Cal. Civ. Code § 1798.80, et seq.
 Brief description of cause:
 Unfair and Deceptive Business Practices

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$ _____ CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
11/11/2013

SIGNATURE OF ATTORNEY OF RECORD

IX. DIVISIONAL ASSIGNMENT (Civil L.R. 3-2)

(Place an "X" in One Box Only) SAN FRANCISCO/OAKLAND SAN JOSE EUREKA

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of California

CHRISTINA HALPAIN

Plaintiff(s)

v.

ADOBE SYSTEMS, INC.

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address) Adobe Systems, Inc.
c/o Karen Robinson
345 Park Avenue
San Jose, California 95110

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Eric H. Gibbs
Matthew B. George
Caitlyn D. Finley
GIRARD GIBBS, LLP
601 California Street, 14th Floor
San Francisco, California 94108

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date:

Signature of Clerk or Deputy Clerk

AO 440 (Rev. 06/12) Summons in a Civil Action (Page 2)

Civil Action No. _____

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____
was received by me on *(date)* _____.

I personally served the summons on the individual at *(place)* _____
_____ on *(date)* _____ ; or

I left the summons at the individual's residence or usual place of abode with *(name)* _____
_____, a person of suitable age and discretion who resides there,
on *(date)* _____, and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* _____, who is
designated by law to accept service of process on behalf of *(name of organization)* _____
_____ on *(date)* _____ ; or

I returned the summons unexecuted because _____ ; or

Other *(specify)*:

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ _____ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc: