

1 Hassan A. Zavareei (CA Bar No. 181547)
Andrea R. Gold*
2 Sarah C. Kohlhofer*
TYCKO & ZAVAREEI LLP
3 1828 L Street, NW, Suite 1000
Washington, D.C. 20036
4 Telephone: (202) 973-0900
Facsimile: (202) 973-0950

5 Sabita Soneji (CA Bar No. 224262)
TYCKO & ZAVAREEI LLP
6 1970 Broadway, Suite 1070
Oakland, CA 94612
7 Telephone: (510) 254-6808
Facsimile: (202) 973-0950
8

9 * *Pro Hac Vice to follow*

10 *Attorneys for Plaintiffs and the Proposed Class*

11
12 **UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

13 AIMEE ABALLO and SETH ZIELICKE,
14 individually on behalf of themselves and all
others similarly situated,

15 Plaintiffs,

16 v.

17 CAPITAL ONE FINANCIAL
18 CORPORATION, CAPITAL ONE, N.A.,
CAPITAL ONE BANK (USA), N.A., and
19 GITHUB, INC.,

20 Defendants.

Case No.: 3:19-cv-4475

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

21 **CLASS ACTION COMPLAINT**

22 1. Plaintiffs Aimee Aballo and Seth Zielicke, individually and on behalf of all others
23 similarly situated, allege the following against Capital One Financial Corporation, Capital One, N.A.,
24 and Capital One Bank (USA), N.A. (collectively “Capital One”) and GitHub, Inc. (“GitHub”) based on
25 personal knowledge with respect to themselves and on information and belief as to other allegations:
26
27

1 **SUMMARY OF THE CASE**

2 2. This is a data breach class action brought on behalf of approximately 100 million people
3 whose personal information—including Social Security numbers, addresses, dates of birth, bank account
4 numbers, and “status data” such as credit scores, credit limits, account balances, and payment histories
5 (collectively “Personal Information”)—was exposed as a result of Defendants’ failure to safeguard
6 Capital One customers’ and potential customers’ privacy. Capital One announced the results of its
7 delinquent behavior on July 29, 2019, when it explained that an “outside individual” had “obtained”
8 customers’ sensitive, Personal Information (the “Capital One Data Breach”) that Capital One had
9 collected and stored.¹ This outside individual (“the hacker”) posted this Personal Information on
10 GitHub.com, GitHub’s website, which encourages (at least friendly) hacking and which is publicly-
11 available. As a result of GitHub’s failure to monitor, remove, or otherwise recognize and act upon
12 obviously-hacked data that was displayed, disclosed, and used on and by GitHub and its website, the
13 Personal Information sat on GitHub.com for *nearly three months*.

14 **JURISDICTION**

15 3. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28
16 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in
17 controversy exceeds \$5,000,000, exclusive of interests and costs, and many members of the class are
18 citizens of states different from Capital One and GitHub. This Court also has supplemental jurisdiction
19 over the state law claims pursuant to 28 U.S.C. § 1367.

20 4. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(c) because GitHub is
21 headquartered in this jurisdiction, and both GitHub and Capital One regularly transact business here, and
22 some of the members of the Class reside in this district. Venue is also proper because a substantial part
23 of the events or omissions giving rise to the claims in this action occurred in this district, including
24

25 _____
26 ¹ *Capital One Announces Data Security Incident*, [http://phx.corporate-](http://phx.corporate-ir.net/mobile.view?c=70667&v=203&d=1&id=2405042)
27 [ir.net/mobile.view?c=70667&v=203&d=1&id=2405042](http://phx.corporate-ir.net/mobile.view?c=70667&v=203&d=1&id=2405042) (last access July 30, 2019).

1 decisions by GitHub’s management that allowed the hacked data to be posted, displayed, used, and/or
2 otherwise available.

3 **INTRADISTRICT ASSIGNMENT**

4 5. Assignment to the San Francisco Division is proper under Civil Local Rules 3-2(c) and 3-
5 2(d) because a substantial part of the events giving rise to Plaintiffs’ claims occurred in San Francisco.

6 **PARTIES**

7 6. Plaintiff Aimee Aballo is a resident of Daytona Beach, Florida who has been a Capital
8 One customer since at least 2010, and whose Personal Information, on information and belief, was
9 compromised in the data breach described herein.

10 7. Plaintiff Seth Zielicke is a resident of Sherman Oaks, California who has been a Capital
11 One customer since at least 2017, and whose Personal Information, on information and belief, was
12 compromised in the data breach described herein.

13 8. Defendant Capital One Financial Corporation is a Delaware corporation with its principal
14 place of business in McLean, Virginia.

15 9. Defendant Capital One, N.A., is a national bank with its principal place of business in
16 McLean, Virginia. Defendant Capital One, N.A. is a wholly-owned subsidiary of Capital One Financial
17 Corporation.

18 10. Defendant Capital One Bank (USA), N.A., is a national bank with its principal place of
19 business in McLean, Virginia. Defendant Capital One Bank (USA), N.A. is a wholly-owned subsidiary
20 of Capital One Financial Corporation.

21 11. Defendant GitHub, Inc. is a Delaware corporation with its principal place of business in
22 San Francisco, California. Defendant GitHub, Inc. (“GitHub”) is a subsidiary of Microsoft Corporation.
23 Github is a software company that owns the website GitHub.com, one of the largest online sources for
24 commercial and open source software.

25 **FACTUAL BACKGROUND**

26 12. Capital One is one of the largest banks and one of the largest credit card issuers by
27 purchase volume in the United States.

1 13. Capital One supports its services by, *inter alia*, renting or contracting for computer servers
2 provided by, among others, Amazon Web Services (“AWS”). AWS, a cloud service, hosted certain
3 Capital One databases that were breached.

4 14. Specifically, dating back to at least March 2019, a former AWS employee (“the hacker”)
5 broke through a Capital One firewall and gained access to Capital One’s AWS-hosted databases and
6 stole customers’ Personal Information. The hacker was able to access Capital One customers’ Personal
7 Information “*because of a security lapse by Capital One.*”²

8 15. While other banks “have moved cautiously to the cloud, partly because of security
9 concerns and the need to keep certain customer and transaction data walled off,” Capital One “has been
10 an enthusiastic adopter of the cloud for data storage,” and has “been public in its embrace of [AWS].”³

11 16. Capital One computer logs demonstrate that Capital One knew or should have known, at
12 least as of March 12, 2019, that its AWS-hosted databases were compromised.⁴

13 17. As evidenced by, *inter alia*, the hacker’s multiple online, publicly-available statements,
14 the hacker “intended” that the breached data “be distributed online.”⁵

15 18. Not surprisingly, therefore, the hacker, a software developer, posted the breached data on
16 GitHub.com, a widely used online software platform acquired by Microsoft for \$7.5 billion in 2018. At

17 ² *Capital One Data Breach Compromises Data of Over 100 Million*, The New York Times,
18 <https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html> (emphasis added).

19 ³ *Id.*

20 ⁴ *United States v. Thompson*, No. MJ19-0344 (W.D. Wa. filed July 29, 2019) (alleging Defendant
21 violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(A) and (C) and (c)(2)(A) and
22 (B)(iii), relating to the Capital One Data Breach).

23 ⁵ *Capital One Reports Data Breach Affecting 100 Million Customers, Applicants*, The Wall Street
24 Journal, <https://www.wsj.com/articles/capital-one-reports-data-breach-11564443355> (last accessed
25 August 1, 2019).
26
27

1 the time of the acquisition, Microsoft’s CEO noted that “[m]ore than 28 million developers already
2 collaborate on GitHub, and it is home to more than 85 million code repositories used by people in nearly
3 every country. From the largest corporations to the smallest startups, GitHub is the destination for
4 developers to learn, share and work together to create software.”⁶

5 19. According to the timestamp on the file containing certain Capital One customers’
6 breached data, the hacker posted the data on GitHub.com on or about April 21, 2019.

7 20. Nevertheless, Capital One did not even *begin* to investigate the data breach until or
8 around July 17, 2019, when it received an email apparently from a GitHub.com user alerting Capital
9 One that there “appear[ed] to be some leaked” customer data publicly available on GitHub.com.⁷

10 21. GitHub, meanwhile, *never* alerted any victims that their highly sensitive Personal
11 Information—including Social Security numbers—was displayed on its site, GitHub.com. Nor did
12 GitHub timely remove the obviously hacked data. Instead, the hacked data was available on
13 GitHub.com for *three months*.

14 22. GitHub apparently did not even suspend the hacker’s GitHub account or access to the
15 site, even though it knew or should have known that the hacker had breached GitHub’s own Terms of
16 Service, which state that: “GitHub has the right to suspend or terminate [a user’s] access to all or any
17 part of the [GitHub.com] Website at any time, with or without cause, with or without notice, effective
18 immediately.”

19 23. On July 29, 2019, Capital One announced that 10 days earlier, Capital One had (finally)
20 determined that:

21 [T]here was unauthorized access by an outside individual who obtained certain types of
22 personal information relating to people who had applied for its credit card products and to
23 Capital One credit card customers. ... Based on our analysis to date, this event affected
24 approximately 100 million individuals in the United States and approximately 6 million
25 in Canada. ... The largest category of information accessed was information on

26 ⁶ <https://blogs.microsoft.com/blog/2018/06/04/microsoft-github-empowering-developers/>.

27 ⁷ This email was sent to a Capital One email address that the company uses to solicit disclosures of
actual or potential vulnerabilities in its computer systems.

1 consumers and small businesses as of the time they applied for one of our credit card
2 products from 2005 through early 2019.⁸

3 24. This Personal Information, Capital One stated, includes information that Capital One
4 “routinely collects at the time it receives credit card applications, including names, addresses, zip
5 codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income. Beyond
6 the credit card application data,” Capital One continued, “the individual also obtained portions of credit
7 card customer data, including: Customer status data, e.g., credit scores, credit limits, balances, payment
8 history, contact information[,] [f]ragments of transaction data from a total of 23 days during 2016, 2017
9 and 2018 ... [and] [a]bout 140,000 Social Security numbers of our credit card customers [and] [a]bout
10 80,000 linked bank account numbers of our secured credit card customers.”

11 25. Capital One had an obligation, arising from, *inter alia*, promises made to its credit card
12 applicants and customers such as Ms. Aballo and Mr. Zielicke and other Class Members, to keep
13 customers’ and applicants’ Personal Information confidential and to protect it from unauthorized
14 disclosures.

15 26. Capital One further had an obligation to keep this Personal Information confidential
16 arising from industry standards.

17 27. GitHub knew or should have known that obviously hacked data had been posted to
18 GitHub.com. Indeed, GitHub actively encourages (at least) friendly hacking as evidenced by, *inter alia*,
19 GitHub.com’s “Awesome Hacking” page.⁹

20 28. GitHub had an obligation, under California law, to keep off (or to remove from) its site
21 Social Security numbers and other Personal Information.

22 29. Further, pursuant to established industry standards, GitHub had an obligation to keep off
23 (or to remove from) its site Social Security numbers and other Personal Information.

24 _____
25 ⁸ *Capital One Announces Data Security Incident*, Capital One, [http://phx.corporate-](http://phx.corporate-ir.net/phoenix.zhtml?c=70667&p=irol-newsArticle_Print&ID=2405042)
26 [ir.net/phoenix.zhtml?c=70667&p=irol-newsArticle_Print&ID=2405042](http://phx.corporate-ir.net/phoenix.zhtml?c=70667&p=irol-newsArticle_Print&ID=2405042) (last accessed July 30, 2019).

27 ⁹ <https://github.com/Hack-with-Github/Awesome-Hacking>.

1 30. Indeed, companies that provide platforms similar to those provided by GitHub spend time
2 and resources monitoring—and removing—such offensive behavior and content. YouTube, Facebook,
3 and Twitter, for example, all train and employ “content moderators” who search for and/or review
4 content that has been flagged as potentially offensive and/or in violation of companies’ respective terms
5 of service.¹⁰

6 31. Moreover, Social Security numbers are readily identifiable: they are nine digits in the
7 XXX-XX-XXXX sequence. Individuals’ contact information such as addresses are similarly readily
8 identifiable.

9 32. Thus, it is *substantially* easier to identify—and remove—such sensitive data. GitHub
10 nonetheless chose not to.

11 33. As a result of GitHub’s failure to monitor its own site—and therefore to keep Social
12 Security numbers and other obviously-hacked Personal Information off its widely-accessed and
13 publicly-available site—the hacked data remained on GitHub.com for *over three months*.

14 34. This is not the first time that Capital One has allowed customer data and Personal
15 Information to be compromised. In fact, in or about November 2014, July 2017, and September 2017,
16 Capital One notified its customers via formal letter that their personal information given—and trusted—
17 to Capital One may have been compromised. In January 2018, Capital One was notified that

18
19
20
21
22
23 ¹⁰ *Content Moderators at YouTube, Facebook and Twitter see the worst of the web—and suffer silently*,
24 The Washington Post, [https://www.washingtonpost.com/technology/2019/07/25/social-media-](https://www.washingtonpost.com/technology/2019/07/25/social-media-companies-are-outsourcing-their-dirty-work-philippines-generation-workers-is-paying-price/?utm_term=.596f8ccc17c2)
25 [companies-are-outsourcing-their-dirty-work-philippines-generation-workers-is-paying-](https://www.washingtonpost.com/technology/2019/07/25/social-media-companies-are-outsourcing-their-dirty-work-philippines-generation-workers-is-paying-price/?utm_term=.596f8ccc17c2)
26 [price/?utm_term=.596f8ccc17c2](https://www.washingtonpost.com/technology/2019/07/25/social-media-companies-are-outsourcing-their-dirty-work-philippines-generation-workers-is-paying-price/?utm_term=.596f8ccc17c2).
27

1 approximately 50GB worth of sensitive data belonging to the bank had been exposed, after a Capital
2 One vendor apparently transferred files destined for the bank’s “unsecured Amazon server.”¹¹

3 35. Since at least 2010, Ms. Aballo has maintained three active accounts with Capital One:
4 (1) a checking account; (2) a Venture One credit card account; and (3) a line of credit.

5 36. In order to obtain these accounts, Capital One required that Ms. Aballo provide Personal
6 Information.

7 37. Since at least 2017, Mr. Zielicke has maintained a Capital One checking account. Since
8 at least 2018, Mr. Zielicke has maintained an overdraft line of credit, and has been an authorized user of
9 a Capital One-issued credit card. In addition, in 2018, Mr. Zielicke applied for at least one credit card
10 with Capital One.

11 38. Ms. Aballo would not have applied for a credit card with—nor provided any Personal
12 Information to—Capital One before and during the period of the Data Breach had Capital One disclosed
13 either that it lacked adequate computer systems and data security practices to safeguard consumers’
14 Personal Information from theft or that it had had multiple incidents in which consumers’ Personal
15 Information in its custody had been compromised.

16 39. Mr. Zielicke would not have applied for an account with—nor provided any Personal
17 Information to—Capital One before and during the period of the Data Breach had Capital One disclosed
18 either that it lacked adequate computer systems and data security practices to safeguard consumers’
19 Personal Information from theft or that it had had multiple incidents in which consumers’ Personal
20 Information in its custody had been compromised.

21
22
23
24 _____
25 ¹¹ *Capital One’s Data Got Exposed, but Don’t Rush Out to Cancel Your Credit Card*,
26 [https://www.creditandcollectionnews.com/rssmodule/capital-ones-data-got-exposed-but-dont-rush-out-](https://www.creditandcollectionnews.com/rssmodule/capital-ones-data-got-exposed-but-dont-rush-out-to-cancel-your-credit-card/)
27 [to-cancel-your-credit-card/](https://www.creditandcollectionnews.com/rssmodule/capital-ones-data-got-exposed-but-dont-rush-out-to-cancel-your-credit-card/) (last accessed July 30, 2019).

CLASS ALLEGATIONS

1
2 40. Plaintiffs bring all of their claims as class claims under Federal Rule of Civil Procedure
3 23. The requirements of Rule 23(b)(2), 23(b)(3) and 23(c)(4) are met with respect to the Class and
4 Subclasses defined below.

5 41. The Class consists of:

6 All persons in the United States who provided personal information to Capital
7 One and whose personal information was accessed, compromised or stolen by an
8 unauthorized individual or individuals in the data breach announced by Capital
One on July 29, 2019.

9 42. The Florida Subclass consists of:

10 All residents of Florida who provided personal information to Capital One and
11 whose personal information was accessed, compromised or stolen by an
12 unauthorized individual or individuals in the data breach announced by Capital
One on July 29, 2019.

13 43. The California Subclass consists of:

14 All residents of California who provided personal information to Capital One and
15 whose personal information was accessed, compromised or stolen by an
16 unauthorized individual or individuals in the data breach announced by Capital
One on July 29, 2019.

17 44. Excluded from the Class and Subclasses are Capital One and any entities in which
18 Capital One or its subsidiaries or affiliates have a controlling interest, and Capital One's officers, agents,
19 and employees. Further excluded from the Class and Subclasses are GitHub and any entities in which
20 GitHub or its subsidiaries or affiliates have a controlling interest, and GitHub's officers, agents, and
21 employees. Also excluded from the Class and Subclasses is the judge assigned to this action, members
of the judge's staff, and any member of the judge's immediate family.

22 45. The Class and Subclasses are so numerous that joinder of all members is impracticable.
23 The Class includes approximately 100 million individuals whose personal information was
24 compromised by the Capital One Data Breach. The names and addresses of Class Members are
25 identifiable through documents maintained by Capital One.

26 46. There are numerous questions of law and fact common to Plaintiffs and the Class and
27 Subclasses, including the following:

- 1 • Whether Capital One and GitHub engaged in the wrongful conduct alleged herein;
- 2 • Whether Class Members' Personal Information was accessed, compromised, or stolen in the
- 3 Capital One Data Breach;
- 4 • Whether Capital One and GitHub owed a duty to Plaintiffs and members of the Class to
- 5 adequately protect their Personal Information and to provide timely and accurate notice of
- 6 the Capital One Data Breach to Plaintiff and members of the Class;
- 7 • Whether Capital One and GitHub breached their duties to protect the Personal Information
- 8 of Plaintiffs and members of the Class by failing to provide adequate data security;
- 9 • Whether Capital One breached its duty to provide timely and accurate notice to Plaintiffs
- 10 and members of the Class each time their data was compromised;
- 11 • Whether Capital One and GitHub, respectively, knew or should have known that their
- 12 computer systems and/or servers were vulnerable to attack and to being the vehicle on which
- 13 to display hacked data;
- 14 • Whether Capital One and GitHub unlawfully failed to inform Plaintiffs and members of the
- 15 Class that they did not maintain security practices adequate to reasonably safeguard Personal
- 16 Information and whether Capital One and GitHub failed to inform Plaintiffs and members of
- 17 the Class of the data breach in a timely and accurate manner;
- 18 • Whether Plaintiffs and members of the Class suffered injury, including ascertainable losses,
- 19 as a result of Capital One's and GitHub's conduct (or failure to act);
- 20 • Whether Capital One and GitHub knew about the Data Breach before it was announced to
- 21 the public, and whether Capital One and GitHub failed to timely notify the public of the
- 22 Capital One Data Breach;
- 23 • Whether Capital One's and GitHub's conduct violated § 5 of the Federal Trade Commission
- 24 Act, 15 U.S.C. § 45, *et seq.*;
- 25 • Whether Capital One's and GitHub's conduct violated Florida and/or California statutory
- 26 law;
- 27

- Whether Plaintiffs and members of the Class are entitled to recover damages; and whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief and/or other equitable relief.

47. Plaintiffs' claims are typical of the claims of the Class in that the representative Plaintiff, like all Class Members, on information and belief, had their Personal Information compromised in the Capital One Data Breach.

48. Plaintiff Aballo's claims are typical of the claims of the Florida Subclass in that Plaintiff Aballo, like all Class Members, on information and belief, had her Personal Information compromised in the Capital One Data Breach.

49. Plaintiff Zielicke's claims are typical of the claims of the California Subclass in that Plaintiff Zielicke, like all Class Members, on information and belief, had his Personal Information compromised in the Capital One Data Breach.

50. Plaintiffs will fairly and adequately protect the interests of the Class and Subclasses. Plaintiffs have retained counsel who is experienced in class action and complex litigation. Plaintiffs have no interests that are adverse to, or in conflict with, other members of the Class or Subclasses.

51. The questions of law and fact common to the Class and Subclass members predominate over any questions which may affect only individual members.

52. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy.

53. The prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Capital One and/or GitHub. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

1 54. Capital One and GitHub have acted on grounds that apply generally to the Class so that
2 injunctive relief under Fed. R. Civ. P. 23(b)(2) is appropriate with respect to the Class as a whole.

3 **CLAIMS**

4 **COUNT I—NEGLIGENCE**
5 **(All Plaintiffs against Capital One)**

6 55. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth
7 herein.

8 56. Plaintiffs allege this claim individually and on behalf of the Class.

9 57. Capital One owed a duty to Plaintiffs and the Class to exercise reasonable care in
10 obtaining, retaining, securing, safeguarding, deleting and protecting the Personal Information in their
11 possession from being compromised, stolen, lost, accessed, misused and/or disclosed to unauthorized
12 recipients. This duty included, among other things, designing, maintaining, and testing Capital One's
13 security systems to ensure that the Personal Information of Plaintiffs and the Class was adequately
14 secured and protected, including using encryption software and technologies. Capital One also had the
15 duty to implement processes that would detect a breach of its security in a timely manner and to timely
16 act upon warnings and alerts.

17 58. Capital One owed a duty to timely disclose the material fact that their computer systems
18 and data security practices were inadequate to safeguard individuals' Personal Information.

19 59. Capital One breached these duties by the conduct alleged in the Complaint, including
20 without limitation: (a) failing to protect the Personal Information; (b) failing to maintain adequate
21 computer systems and data security practices to safeguard the Personal Information; (c) failing to
22 disclose the material fact that Capital One's computer systems and/or servers data security practices
23 were inadequate to safeguard the Personal Information; and (d) failing to disclose in a timely and
24 accurate manner to Plaintiffs and members of the Class the material fact of the Capital One Data Breach.

25 60. The conduct alleged herein caused Plaintiffs and Class Members to be exposed to fraud
26 and be harmed as detailed herein. Plaintiffs and Class Members were foreseeable victims of Capital
27 One's inadequate data security practices and in fact suffered damages caused by Capital One's breaches
of their duties.

1 61. Capital One knew that the Personal Information of Plaintiffs and the Class was sensitive
2 information that is valuable to identity thieves and cyber criminals. Capital One also knew of the serious
3 harms that could result through the wrongful disclosure of the Personal Information of Plaintiffs and the
4 Class.

5 62. Because Plaintiffs and the Class entrusted Capital One with their Personal Information,
6 Capital One had a special relationship with Plaintiffs and the Class. Plaintiffs and the Class signed up
7 and paid for Capital One's banking and credit services and agreed to provide their Personal Information
8 with the understanding that Capital One would take appropriate measures to safeguard it and would
9 timely inform Plaintiffs and the Class of any breaches or other security concerns that might call for
10 action by Plaintiffs and the Class. As alleged herein, Capital One did not. Capital One is morally
11 culpable, given the prominence of security breaches today, particularly in the financial industry, and
12 especially given the admission that their data vulnerability dates back to at least 2014. In light of that
13 history, Capital One had inadequate safeguards to protect Plaintiffs and the Class from breaches or
14 security vulnerabilities.

15 63. Capital One's failure to comply with industry standards and federal regulations further
16 demonstrates its negligence in failing to exercise reasonable care in safeguarding and protecting the
17 Personal Information of Plaintiffs and the Class.

18 64. Capital One's breaches of these duties were not isolated incidents or small mistakes. The
19 breaches set forth herein resulted from long-term Company-wide refusal to acknowledge and correct
20 serious ongoing data security problems dating back to at least 2014.

21 65. But for Capital One's wrongful and negligent breach of its duties owed to Plaintiffs and
22 the Class, their Personal Information would not have been compromised, stolen and accessed by
23 unauthorized persons. Capital One's negligence was a direct and legal cause of the theft of Plaintiffs'
24 and the Class's Personal Information and all resulting damages.

25 66. Capital One knew that their computer systems and/or servers and technologies for
26 processing and securing Personal Information had numerous security vulnerabilities. The injury and
27 harm suffered by Plaintiffs and the Class was a reasonably foreseeable result of Capital One's failure to

1 cure those numerous vulnerabilities or, at a minimum, exercise reasonable care in safeguarding and
2 protecting the Personal Information of Plaintiffs and the other Class Members

3 67. As a result of Capital One's misconduct, the Personal Information of Plaintiffs and the
4 Class was compromised and their Personal Information was disclosed to third parties without their
5 consent, placing them at a greater risk of identity theft. Plaintiffs and the Class have also suffered out of
6 pocket losses from procuring credit protection services, identity theft monitoring, and other expenses
7 related to identity theft losses or protective measures.

8 68. Capital One's misconduct alleged herein was carried out with a willful and conscious
9 disregard of the rights or safety of Plaintiffs and the Class and subjected Plaintiffs and the Class to
10 unjust hardship in conscious disregard of their rights.

11 **COUNT II—NEGLIGENCE**
12 **(All Plaintiffs against GitHub)**

13 69. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth
14 herein.

15 70. Plaintiffs allege this claim individually and on behalf of the Class.

16 71. GitHub owed a duty to Plaintiffs and the Class to exercise reasonable care in maintaining
17 a website that promotes hacking, and in monitoring, securing, safeguarding, deleting and otherwise
18 protecting the Personal Information in its possession from being displayed, misused and/or disclosed to
19 the public and/or unauthorized persons. This duty included, among other things, monitoring with
20 regularity (or at least with more frequency than every three months) its publicly-available website to
21 ensure that individuals' Social Security numbers and other obviously-hacked Personal Information is not
22 available for display, use, and consumption. Because, *inter alia*, GitHub encourages (at least) friendly
23 hacking, GitHub also had the duty to implement processes that would detect when its website publicly
24 displayed sensitive and confidential personal information as a result of (unfriendly) hacking.

25 72. GitHub owed a duty to timely disclose the material fact that its website and data security
26 practices were inadequate to safeguard individuals' Personal Information.

27 73. GitHub breached these duties by the conduct alleged in the Complaint, including without
limitation, (a) failing to protect the Personal Information; (b) failing to maintain adequate data security

1 practices to safeguard the Personal Information; and (c) failing to disclose in a timely and accurate
2 manner to Plaintiffs and members of the Class the material fact that their Social Security numbers and
3 Personal Information was publicly displayed on GitHub's website.

4 74. The conduct alleged herein caused Plaintiffs and Class Members to be exposed to fraud
5 and be harmed as detailed herein. Plaintiffs and Class Members were foreseeable victims of GitHub's
6 enabling the months-long public display of their Personal Information, and in fact suffered damages
7 caused by GitHub's breaches of its duties.

8 75. GitHub knew or should have known that the Personal Information of Plaintiffs and the
9 Class was sensitive information that is valuable to identity thieves and cyber criminals. GitHub also
10 knew of the serious harms that could result through the wrongful disclosure of the Personal Information
11 of Plaintiffs and the Class.

12 76. As an entity that not only allows for such sensitive information to be instantly, publicly
13 displayed, but one that also arguably encourages it, GitHub is morally culpable, given the prominence of
14 security breaches today, particularly in the financial industry.

15 77. GitHub's failure to comply with their own Terms of Service, industry standards, and
16 federal and state regulations further demonstrates its negligence in failing to exercise reasonable care in
17 safeguarding and protecting the Personal Information of Plaintiffs and the Class.

18 78. But for GitHub's wrongful and negligent breach of its duties owed to Plaintiffs and the
19 Class, their Personal Information would not have been publicly displayed and available for access by
20 unauthorized persons. GitHub's negligence was a direct and legal cause of the theft of Plaintiffs and the
21 Class's Personal Information and all resulting damages.

22 79. GitHub knew or should have known that its website allowed for the display of such data
23 and nonetheless failed to monitor it or inform individuals that their Personal Information was displayed
24 and published. The injury and harm suffered by Plaintiffs and the Class was a reasonably foreseeable
25 result of GitHub's failure to cure those numerous vulnerabilities or, at a minimum, exercise reasonable
26 care in safeguarding and protecting the Personal Information of Plaintiffs and the other Class Members.

27 80. As a result of GitHub's misconduct, the Personal Information of Plaintiffs and the Class
was compromised and their Personal Information was disclosed to third parties without their consent,

1 placing them at a greater risk of identity theft. Plaintiffs and the Class have also suffered out of pocket
2 losses from procuring credit protection services, identity theft monitoring, and other expenses related to
3 identity theft losses or protective measures.

4 81. GitHub's misconduct alleged herein was carried out with a willful and conscious
5 disregard of the rights or safety of Plaintiffs and the Class and subjected Plaintiffs and the Class to
6 unjust hardship in conscious disregard of their rights.

7 **COUNT III—NEGLIGENCE *PER SE***
8 **(All Plaintiffs against Capital One)**

9 82. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth
10 herein.

11 83. Plaintiffs allege this claim individually and on behalf of the Class.

12 84. Section 5 of the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45, prohibits
13 "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the
14 unfair act or practice by businesses such as Capital One, of failing to use reasonable measures to protect
15 Personal Information. The FTC publications and orders also form part of the basis for Capital One's
16 duty in this regard.

17 85. Capital One violated Section 5 of the FTC Act by failing to use reasonable measures to
18 protect Personal Information and by otherwise not complying with applicable industry standards. Capital
19 One's conduct was particularly unreasonable given the nature and amount of Personal Information it
20 obtained and stored—that of over 100 million customers—and the foreseeable consequences of a data
21 breach at a financial institution as large as Capital One, including, specifically, the immense damages
22 that would result to Plaintiffs and the Class.

23 86. Capital One's violation of Section 5 of the FTC Act constitutes negligence *per se*.

24 87. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to
25 cover.

26 88. The harm that occurred as a result of the Capital One Data Breach is the type of harm that
27 the FTC Act was intended to protect against. The FTC has pursued enforcement actions against

1 businesses which, as a result of their failure to employ reasonable safeguards to ensure data security and
2 avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

3 89. As a direct and proximate result of Capital One's negligence *per se*, Plaintiffs and the
4 Class have suffered, and will continue to suffer, injuries and damages arising from identity theft.
5 Plaintiffs' and the Class's inability to use their debit or credit cards because those cards were cancelled,
6 suspended or otherwise rendered unusable as a result of the Capital One Data Breach and/or false or
7 fraudulent charges stemming from the Capital One Data Breach, includes but is not limited to: late fees
8 charged and foregone cash back rewards; damages from lost time to mitigate the actual and potential
9 impact of the Capital One Data Breach on their lives such as placing "freezes" and "alerts" with credit
10 reporting agencies, contacting their financial institutions, closing or modifying financial accounts,
11 closely reviewing and monitoring credit reports and accounts for unauthorized access and activity, filing
12 police reports, and damages from identity theft, which may take months if not years to discover and
13 detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of
14 privacy.

15 90. Moreover, as a direct and proximate result of Capital One's negligence *per se*, Plaintiffs
16 and Class Members have suffered and will continue to suffer the risks of exposure of their Personal
17 Information, which remain in Capital One's possession and is subject to further unauthorized disclosures
18 so long as Capital One fails to undertake appropriate and adequate measures to safeguard the Personal
19 Information in its possession.

20 **COUNT IV—NEGLIGENCE *PER SE***
(All Plaintiffs against GitHub)

21 91. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth
22 herein.

23 92. Plaintiffs allege this claim individually and on behalf of the Class.

24 93. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair ... practices in or affecting
25 commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses
26 such as GitHub, of failing to use reasonable measures to protect Personal Information. The FTC
27 publications and orders also form part of the basis for GitHub's duty in this regard.

1 94. GitHub violated Section 5 of the FTC Act by failing to use reasonable measures to
2 protect Personal Information and by otherwise not complying with applicable industry standards.
3 GitHub’s conduct was particularly unreasonable given the nature and amount of Personal Information it
4 displayed, disclosed, used, and stored—that of over 100 million customers—and the foreseeable
5 consequences of a data breach at a hacking-encouraging website as large as GitHub.com, including,
6 specifically, the immense damages that would result to Plaintiffs and the Class.

7 95. GitHub’s violation of Section 5 of the FTC Act constitutes negligence *per se*.

8 96. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to
9 cover.

10 97. The harm that occurred as a result of the Capital One Data Breach is the type of harm that
11 the FTC Act was intended to protect against.

12 98. As a direct and proximate result of GitHub’s negligence *per se*, Plaintiffs and the Class
13 have suffered, and will continue to suffer, injuries and damages arising from identity theft. Plaintiffs’
14 and the Class’s inability to use their debit or credit cards because those cards were cancelled, suspended
15 or otherwise rendered unusable as a result of the Capital One Data Breach and/or false or fraudulent
16 charges stemming from the Capital One Data Breach, includes but is not limited to: late fees charged
17 and foregone cash back rewards; damages from lost time to mitigate the actual and potential impact of
18 the Capital One Data Breach on their lives such as placing “freezes” and “alerts” with credit reporting
19 agencies, contacting their financial institutions, closing or modifying financial accounts, closely
20 reviewing and monitoring credit reports and accounts for unauthorized access and activity, filing police
21 reports, and damages from identity theft, which may take months if not years to discover and detect,
22 given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

23 99. Moreover, as a direct and proximate result of GitHub’s negligence *per se*, Plaintiffs and
24 Class Members have suffered and will continue to suffer the risks of exposure of their Personal
25 Information.
26
27

**COUNT V—BREACH OF CONFIDENCE
(All Plaintiffs against Capital One)**

1
2 100. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth
3 herein.

4 101. Plaintiffs allege this claim individually and on behalf of the Class.

5 102. At all times during Plaintiffs and the Class Members' interactions with Capital One,
6 Capital One was fully aware of the confidential and sensitive nature of the Personal Information that
7 Plaintiffs and the Class Members provided to Capital One.

8 103. As alleged herein, Capital One's relationship with Plaintiffs and the members of the Class
9 was governed by expectations that their Personal Information would be collected, stored, and protected
10 in confidence, and would not be disclosed to unauthorized third parties.

11 104. Plaintiffs and Class Members provided their Personal Information to Capital One with the
12 understanding that Capital One would protect and not allow the Personal Information to be accessed by
13 or disseminated to any unauthorized parties.

14 105. Plaintiffs and Class Members also provided their respective Personal Information to
15 Capital One with the understanding that Capital One would take precautions to protect that Personal
16 Information from unauthorized disclosure, such as following the basic principles of information security
17 practices.

18 106. Capital One required and voluntarily received in confidence the Personal Information of
19 Plaintiffs and the Class with the understanding that it would not be disclosed or disseminated to the
20 public or any unauthorized parties.

21 107. Because of Capital One's failure to prevent, detect, and/or avoid the Capital One Data
22 Breach from occurring by, *inter alia*, failing to follow best information security practices to safeguard
23 the Personal Information of Plaintiffs and the Class, Plaintiffs' and the Class Members' Personal
24 Information was disclosed and misappropriated to unauthorized third parties without their express
25 permission.

26 108. As a direct and proximate cause of Capital One's actions and/or omissions, Plaintiffs and
27 the Class have suffered damages as alleged herein.

1 109. But for Capital One’s disclosure of Plaintiffs’ and Class Members’ Personal Information
2 in violation of the parties’ understanding of confidence, their Personal Information would not have been
3 compromised, stolen, viewed, accessed and used by unauthorized third parties. The Capital One Data
4 Breach was the direct and legal cause of the theft of the Personal Information of Plaintiffs and the Class,
5 as well as of the resulting damages.

6 110. The injury and harm alleged herein was the reasonably foreseeable result of Capital
7 One’s unauthorized disclosure of Plaintiffs’ and Class Members’ Personal Information. Capital One
8 knew that its systems had numerous security vulnerabilities because Capital One failed to follow
9 industry standard information security practices, including Capital One’s inability to prevent historic
10 data breaches as far back as 2014.

11 111. As a direct and proximate result of Capital One’s breaches of confidence, Plaintiffs and
12 the Class have suffered, and will continue to suffer, injuries and damages resulting from identity theft;
13 Plaintiffs’ and members of the Class’s inability to use their debit or credit cards because those cards
14 were cancelled, suspended, or otherwise rendered unusable as a result of the Capital One Data Breach
15 and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees
16 charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and
17 potential impact of the Data Breach on their lives, including, among other things, by placing “freezes”
18 and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying
19 financial accounts, closely reviewing or monitoring their credit reports and accounts for unauthorized
20 activity, filing police reports, and damages from identity theft, which may take months or years to
21 discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and
22 loss of privacy.

23 112. As a direct and proximate result of Capital One’s breaches of confidence, Plaintiffs and
24 Class Members have suffered and will continue to suffer other forms of injury and/or harm, including,
25 but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic
26 loss.
27

**COUNT VI—BREACH OF IMPLIED CONTRACT
(All Plaintiffs against Capital One)**

1
2 113. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth
3 herein.

4 114. Plaintiffs allege this claim individually and on behalf of the Class.

5 115. Capital One solicited and invited Plaintiffs and Class Members to open accounts and
6 apply for credit cards. Plaintiffs and Class Members accepted Capital One's offers and submitted such
7 applications to Capital One.

8 116. When Plaintiffs and Class Members submitted these forms and applications, they were
9 required to—and did—provide their Personal Information to Capital One. In so doing, Plaintiffs and
10 Class Members entered into implied contracts with Capital One pursuant to which Capital One agreed to
11 safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members
12 if their data had been breached or compromised.

13 117. Each application by Plaintiffs and Class Members was made pursuant to mutually
14 agreed-upon implied contracts with Capital One under which Capital One agreed to safeguard and
15 protect Plaintiffs' and Class Members' Personal Information and to provide accurate and timely notice if
16 such information was compromised, lost, or stolen.

17 118. Plaintiffs and Class Members would not have provided their Personal Information
18 to Capital One in the absence of such an implied contract.

19 119. Plaintiffs and Class Members fully performed their obligations under the implied
20 contracts with Capital One.

21 120. Capital One breached the implied contracts it made with the Plaintiffs and Class
22 members by failing to safeguard or protect the Class Members' Personal Information and by
23 failing to provide accurate and timely notice when their Personal Information was compromised.

24 121. As a direct and proximate result of Capital One's breaches of the implied contracts
25 between Capital One and Plaintiffs and Class Members, Plaintiffs and the Class Members sustained
26 actual losses and damages as described herein, and will continue to suffer damages for, potentially, years
27 to come.

1 **COUNT VII—VIOLATION OF FLORIDA’S DECEPTIVE AND UNFAIR TRADE**
2 **PRACTICES ACT, Fla. Stat. §§ 501.201, et seq. 262**
3 **(Plaintiff Aballo against Capital One)**

4 122. Plaintiff Aballo individually and on behalf of the Florida Subclass, repeats and alleges all
5 paragraphs above, as if fully alleged herein.

6 123. Plaintiff Aballo alleges this claim individually and on behalf of the Florida Subclass.

7 124. Plaintiff Aballo and Florida Subclass members are “consumers” as defined by Fla. Stat. §
8 501.203.

9 125. Capital One advertised, offered, or sold goods or services in Florida and engaged in trade
10 or commerce directly or indirectly affecting the people of Florida.

11 126. Capital One engaged in unconscionable, unfair, and deceptive acts and practices in the
12 conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

- 13 a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff
14 Aballo and Florida Subclass members’ Personal Information, which was a direct and proximate
15 cause of the Capital One Data Breach;
- 16 b. Failing to identify foreseeable security and privacy risks, remediate identified security and
17 privacy risks, and adequately improve security and privacy measures following previous
18 cybersecurity incidents, which were a direct and proximate cause of the Capital One Data
19 Breach;
- 20 c. Failing to comply with common law and statutory duties pertaining to the security and privacy of
21 Plaintiffs and Florida Subclass members’ Personal Information, including duties imposed by the
22 FTC Act, 15 U.S.C. § 45, and Florida’s data security statute, F.S.A. § 501.171(2), which was a
23 direct and proximate cause of the Capital One Data Breach;
- 24 d. Explicitly and/or implicitly misrepresenting that it would protect the privacy and confidentiality
25 of Plaintiff Aballo’s and Florida Subclass members’ Personal Information, including by
26 implementing and maintaining reasonable security measures;
- 27 e. Misrepresenting that it would comply with common law and statutory duties pertaining to the
security and privacy of Plaintiff Aballo’s and Florida Subclass members’ Personal Information,

1 including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida’s data security statute,
2 F.S.A. § 501.171(2);

- 3 f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately
4 secure Plaintiff Aballo’s and Florida Subclass members’ Personal Information; and
5 g. Omitting, suppressing, and concealing the material fact that it did not comply with common law
6 and statutory duties pertaining to the security and privacy of Plaintiff Aballo’s and Florida
7 Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. §
8 45, and Florida’s data security statute, F.S.A. § 501.171(2).

9 127. Capital One’s representations and omissions were material because they were likely to
10 deceive reasonable consumers about the adequacy of Capital One’s data security and ability to protect
11 the confidentiality of consumers’ Personal Information.

12 128. Had Capital One disclosed to Plaintiff Aballo and Florida Subclass members that its data
13 systems were not secure and, thus, vulnerable to attack, Capital One would have been unable to continue
14 in such business and it would have been forced to adopt reasonable data security measures and comply
15 with the law. Instead, Capital One maintained customer Personal Information in its databases, where it
16 was insecure, and subject to attack over the course of at least four years. Customers including Plaintiff
17 Aballo and Florida Subclass members would not have provided Capital One with their Personal
18 Information had they known that Capital One was misrepresenting the security of, and omitting the
19 flaws in, its databases. Additionally, Plaintiff Aballo and Florida Subclass members would not have
20 paid as much as they did for Capital One’s services had they known that Capital One would not keep
21 their information secure. Accordingly, Plaintiff Aballo and Florida Subclass members did not receive
22 the benefit of their bargain.

23 129. As a direct and proximate result of Capital One’s unconscionable, unfair, and deceptive
24 acts and practices, Plaintiff Aballo and Florida Subclass members have suffered and will continue to
25 suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages,
26 including from fraud and identity theft; time and expenses related to monitoring their financial accounts
27 for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their
Personal Information; and paying more for Capital One’s services than they otherwise would have.

1 130. Plaintiff Aballo and Florida Subclass members seek all monetary and non-monetary relief
2 allowed by law, including actual or nominal damages under Fla. Stat. § 501.21; declaratory and
3 injunctive relief; reasonable attorneys’ fees and costs, under Fla. Stat. § 501.2105(1); and any other
4 relief that is just and proper.

5 **COUNT VIII—VIOLATION OF THE WIRETAP ACT, 18 U.S.C. § 2511**
6 **(All Plaintiffs Against GitHub)**

7 131. Plaintiffs individually and on behalf of the Class, repeat and allege all paragraphs above,
8 as if fully alleged herein.

9 132. Plaintiffs allege this claim individually and on behalf of the Class.

10 133. Plaintiffs bring this claim pursuant to 18 U.S.C. § 2520, which permits civil recovery for
11 those whose “wire, oral, or electronic communication” has been “intercepted, disclosed, or intentionally
12 used” in violation of, *inter alia*, the Wiretap Act, 18 U.S.C. § 2511. 18 U.S.C. § 2520(a).

13 134. Plaintiffs’ Personal Information constitutes “wire, oral, or electronic communication”
14 within the meaning of the statute.

15 135. By engaging in the conduct alleged herein and/or by failing to act as alleged herein,
16 GitHub has “disclosed” Plaintiffs’ and the Class Members’ Personal Information within the meaning of
17 the statute. Specifically, GitHub “intentionally disclose[d], or endeavor[ed] to disclose, to any other
18 person the contents of any wire, oral, or electronic communication, knowing or having reason to know
19 that the information was obtained through the interception of a wire, oral, or electronic communication”
20 in violation of the Wiretap Act and/or the broader Electronic Communications Privacy Act (“ECPA”),
21 18 U.S.C. §§ 2150, *et seq.*

22 136. Additionally, or alternatively, by engaging in the conduct alleged herein and/or by failing
23 to act as alleged herein, GitHub has “intentionally used” Plaintiffs’ and the Class Members’ Personal
24 Information within the meaning of the statute. Specifically, although GitHub.com is a publicly-available
25 website, it offers a variety of pricing plans and otherwise uses what its customers post and display.

26 137. As a direct and proximate result of GitHub’s having disclosed and/or used Plaintiffs’ and
27 the Class Members’ Personal Information, which was obtained in violation of the ECPA, Plaintiffs and
the Class Members sustained actual losses and damages as described herein, and will continue to suffer
damages for, potentially, years to come.

1
2 **COUNT IX—VIOLATION OF CALIFORNIA CIVIL CODE § 1798.85**
3 **(Plaintiff Zielicke Against GitHub)**

4 138. Plaintiff Zielicke individually and on behalf of the California Subclass, repeats and
5 alleges all paragraphs above, as if fully alleged herein.

6 139. Plaintiff Zielicke alleges this claim individually and on behalf of the California Subclass.

7 140. The California Civil Code § 1798.85 provides, *inter alia*, that an entity may not
8 “[p]ublicly post or publicly display in any manner an individual’s social security number.”

9 141. The statute defines “publicly post” or “publicly display” as “intentionally communicate
10 or otherwise make available to the general public.”

11 142. By engaging in the conduct alleged herein and/or by failing to act as alleged herein,
12 GitHub has publicly posted or publicly displayed Plaintiff Zielicke’s and the California Subclass
13 members’ Social Security numbers within the meaning of the statute.

14 143. As a direct and proximate result of GitHub’s having publicly posted or publicly displayed
15 this Personal Information, Plaintiff Zielicke and the California Subclass members sustained actual losses
16 and damages as described herein, and will continue to suffer damages for, potentially, years to come.

17 **COUNT X—VIOLATION OF CALIFORNIA CIVIL CODE § 1798.82**
18 **(Plaintiff Zielicke Against All Defendants)**

19 144. Plaintiff Zielicke individually and on behalf of the California Subclass, repeats and
20 alleges all paragraphs above, as if fully alleged herein.

21 145. Plaintiff Zielicke alleges this claim individually and on behalf of the California Subclass.

22 146. The California Civil Code § 1798.82 provides that any “business that maintains
23 computerized data that includes personal information that the person or business does not own shall
24 notify the owner or licensee of the information of the breach of the security of the data immediately
25 following discovery, if the personal information was, or is reasonably believed to have been, acquired by
26 an unauthorized person.” Cal. Civ. Code § 1798.82(b).

27 147. Defendant Capital One is a business within the meaning of this statute.

148. Defendant Capital One does not own the Personal Information.

149. Defendant GitHub is a business within the meaning of this statute.

1 150. Defendant GitHub does not own the Personal Information.

2 151. On information and belief, Defendants failed to adequately and appropriately inform
3 Plaintiff Zielicke and the members of the California Subclass that their Personal Information had been
4 acquired by an unauthorized person. *See id.* § 1798.92(d)(1) (providing a template by which covered
5 businesses must inform individuals that their information has been acquired by an unauthorized person).

6 152. Specifically, on information and belief, GitHub never informed Plaintiff Zielicke or any
7 other member of the California Subclass that, for example, their Personal Information was displayed on
8 or otherwise available through GitHub.com.

9 153. Similarly, on information and belief, Capital One issued only a general announcement
10 regarding the Capital One Data Breach, and, therefore, failed to appropriately notify Plaintiff Zielicke
11 and the California Subclass members that their Personal Information had been accessed by an
12 unauthorized person.

13 154. As a direct and proximate result of Defendants' failure to so notify Plaintiffs, Plaintiff
14 Zielicke and the California Subclass members sustained actual losses and damages as described herein,
15 including the potential delay of freezing their credit and monitoring their financial reports, and will
16 continue to suffer damages for, potentially, years to come.

17 **PRAYER FOR RELIEF**

18 WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, respectfully
19 requests that the Court enter judgment against Defendants, as follows:

20 155. That the Court certify this action as a class action, proper and maintainable pursuant to
21 Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives;
22 and appoint the undersigned Class Counsel;

23 156. Finding Defendants' conduct was negligent, deceptive, unfair and unlawful as alleged
24 herein;

25 157. That the Court grant permanent injunctive relief to prohibit Defendants from continuing
26 to engage in the unlawful acts, omissions, and practices described herein;

27 158. That the Court award Plaintiffs and the members of the Class and Subclasses
compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

1 159. That the Court order disgorgement and restitution of all earnings, profits, compensation,
2 and benefits received by Defendants as a result of its unlawful acts, omissions, and practices;

3 160. That the Court award statutory damages, trebled, and punitive or exemplary damages, to
4 the extent permitted by law;

5 161. That the Court award to Plaintiffs the costs and disbursements of the action, along with
6 reasonable attorneys' fees, costs, and expenses;

7 162. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

8 163. Such other or further relief as may be appropriate under the circumstances.

9 **DEMAND FOR JURY TRIAL**

10 Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

11 DATED: August 1, 2019

12 **TYCKO & ZAVAREEI LLP**

13 By: /s/Hassan A. Zavareei
14 Hassan A. Zavareei (CA Bar No. 181547)
15 hzavareei@tzlegal.com
16 Andrea R. Gold*
17 agold@tzlegal.com
18 Sarah C. Kohlhofer*
19 skohlhofer@tzlegal.com
20 **TYCKO & ZAVAREEI LLP**
21 1828 L Street, NW, Suite 1000
22 Washington, D.C. 20036
23 Telephone: (202) 973-0900
24 Facsimile: (202) 973-0950

25 Sabita Soneji (CA Bar No. 224262)
26 ssoneji@tzlegal.com
27 **TYCKO & ZAVAREEI LLP**
1970 Broadway, Suite 1070
Oakland, CA 94612
Telephone: (510) 254-6808
Facsimile: (202) 973-0950

**Pro Hac Vice Applications to be submitted*

*Attorneys for Plaintiffs and the Putative
Classes*