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

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

* *Pro Hac Vice to follow*

*Attorneys for Plaintiffs and the Proposed Class*

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

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

Plaintiffs,

v.

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

Defendants.

Case No.: 3:19-cv-4475

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

## CLASS ACTION COMPLAINT

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

## SUMMARY OF THE CASE

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

## JURISDICTION

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

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

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

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

**INTRADISTRICT ASSIGNMENT**

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

**PARTIES**

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

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

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

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

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

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

**FACTUAL BACKGROUND**

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

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

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

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

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

17. As evidenced by, *inter alia*, the hacker's multiple online, publicly-available statements, the hacker "intended" that the breached data "be distributed online."[5]

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

---

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

[3] *Id*.

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

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

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

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

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

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

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

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

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

[6] https://blogs.microsoft.com/blog/2018/06/04/microsoft-github-empowering-developers/.

[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.

> consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019.[8]

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

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

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

27. GitHub knew or should have known that obviously hacked data had been posted to GitHub.com. Indeed, GitHub actively encourages (at least) friendly hacking as evidenced by, *inter alia*, GitHub.com's "Awesome Hacking" page.[9]

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

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

---

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

[9] https://github.com/Hack-with-Github/Awesome-Hacking.

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

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

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

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

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

[10] *Content Moderators at YouTube, Facebook and Twitter see the worst of the web—and suffer silently*, The Washington Post, 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.

approximately 50GB worth of sensitive data belonging to the bank had been exposed, after a Capital One vendor apparently transferred files destined for the bank's "unsecured Amazon server."[11]

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

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

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

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

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

[11] *Capital One's Data Got Exposed, but Don't Rush Out 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

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

41. The Class consists of:

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

42. The Florida Subclass consists of:

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

43. The California Subclass consists of:

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

44. Excluded from the Class and Subclasses are Capital One and any entities in which Capital One or its subsidiaries or affiliates have a controlling interest, and Capital One's officers, agents, and employees. Further excluded from the Class and Subclasses are GitHub and any entities in which GitHub or its subsidiaries or affiliates have a controlling interest, and GitHub's officers, agents, and 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.

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

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

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

- 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.

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

## CLAIMS

### COUNT I—NEGLIGENCE
### (All Plaintiffs against Capital One)

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

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

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

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

59. Capital One 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 computer systems and data security practices to safeguard the Personal Information; (c) failing to disclose the material fact that Capital One's computer systems and/or servers data security practices were inadequate to safeguard the Personal Information; and (d) failing to disclose in a timely and accurate manner to Plaintiffs and members of the Class the material fact of the Capital One Data Breach.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

124. Plaintiff Aballo and Florida Subclass members are "consumers" as defined by Fla. Stat. § 501.203.

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

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

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Aballo and Florida Subclass members' Personal Information, which was a direct and proximate cause of the Capital One Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which were a direct and proximate cause of the Capital One Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Capital One Data Breach;

d. Explicitly and/or implicitly misrepresenting that it would protect the privacy and confidentiality of Plaintiff Aballo's and Florida Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

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,

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

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Aballo's and Florida Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Aballo's and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

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

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

129. As a direct and proximate result of Capital One's unconscionable, unfair, and deceptive acts and practices, Plaintiff Aballo and Florida Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts 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.

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

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

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

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

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

134. Plaintiffs' Personal Information constitutes "wire, oral, or electronic communication" within the meaning of the statute.

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

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

137. As a direct and proximate result of GitHub's having disclosed and/or used Plaintiffs' and 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.

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

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

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

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

141. The statute defines "publicly post" or "publicly display" as "intentionally communicate or otherwise make available to the general public."

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

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

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

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

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

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

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.

150. Defendant GitHub does not own the Personal Information.

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

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

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

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

**PRAYER FOR RELIEF**

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

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

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

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

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;

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

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

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

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

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

**DEMAND FOR JURY TRIAL**

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

DATED: August 1, 2019

**TYCKO & ZAVAREEI LLP**

By: /s/*Hassan A. Zavareei*

Hassan A. Zavareei (CA Bar No. 181547)
hzavareei@tzlegal.com
Andrea R. Gold*
agold@tzlegal.com
Sarah C. Kohlhofer*
skohlhofer@tzlegal.com
**TYCKO & ZAVAREEI LLP**
1828 L Street, NW, Suite 1000
Washington, D.C. 20036
Telephone: (202) 973-0900
Facsimile: (202) 973-0950

Sabita Soneji (CA Bar No. 224262)
ssoneji@tzlegal.com
**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*