

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON**

MICHAEL FADULLON, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CAPITAL ONE FINANCIAL CORPORATION; AMAZON WEB SERVICES, INC.; PAIGE A. THOMPSON; and DOES 1-10,

Defendants.

Case No. \_\_\_\_\_

**CLASS ACTION COMPLAINT**

**JURY DEMAND**

Plaintiff Michael Fadullon (“Mr. Fadullon,” or “Plaintiff”), individually and on behalf of the proposed Classes defined below, alleges on personal knowledge as to himself and his own experiences and, as to all other matters, upon information and belief including investigation conducted by his attorneys.

**NATURE OF THE CASE**

1  
2 1. Plaintiff brings this class action lawsuit against Capital One Financial Corporation  
3 (“Capital One”), Amazon Web Services, Inc. (“AWS”), and Paige A. Thompson (collectively,  
4 “Defendants”) because of their failure to protect (in the case of Capital One and AWS), or the theft of  
5 (in the case of Ms. Thompson), the confidential information of Plaintiff and many millions of other  
6 consumers—including their names, bank account numbers, Social Security numbers, addresses, phone  
7 numbers, email addresses, dates of birth, income information, banking information, credit scores, credit  
8 limits, contact information, and other private, personal information (collectively, “Personal  
9 Information”). This theft is referred to as the “Data Breach” herein.

10 2. Defendant Capital One is one of the largest banks in the United States, with revenues in  
11 excess of \$28 billion in 2018.<sup>1</sup>

12 3. In order to apply for Capital One’s banking services, an individual must provide his or  
13 her Personal Information.

14 4. Capital One evidently stores this information indefinitely, on the “cloud,” using AWS’s  
15 cloud computing services.

16 5. Defendant Ms. Thompson was able to exploit glaring vulnerabilities in AWS’s systems  
17 to perpetrate the Data Breach at issue.

**PARTIES**

18  
19 6. Plaintiff Michael Fadullon is a resident and citizen of the State of California, who applied  
20 for a Capital One Venture Card on February 2016, and was approved.

21 7. Defendant Capital One is a Delaware Corporation with its headquarters and principal  
22 place of business located in McLean, Virginia.

23 8. Defendant AWS is a Delaware Corporation with its headquarters in Seattle, Washington.

24 9. Defendant Paige A. Thompson is an individual currently incarcerated in the Seattle,  
25 Washington, area.

26 10. Plaintiff is unaware of the true names and capacities of the defendants sued as DOES 1-

27  
28 <sup>1</sup> Capital One, 2018 Annual Report at 2.

1 10, and therefore sues these defendants by fictitious names. Plaintiff will seek leave to amend this  
2 Complaint when and if the true identities of these DOE defendants are discovered. Plaintiff is informed  
3 and believes and thereon alleges that each of the defendants designated as a DOE is responsible in some  
4 manner for the acts and occurrences alleged herein, whether such acts or occurrences were committed  
5 intentionally, negligently, recklessly or otherwise, and that each said DOE defendant thereby  
6 proximately caused injuries and damages to Plaintiff as herein alleged, and is thus liable for the damages  
7 suffered by Plaintiff.

8 **JURISDICTION AND VENUE**

9 11. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2)  
10 because (a) at least one member of the putative Classes is a citizen of a state different from Defendants,  
11 and (b) the amount in controversy exceeds \$5,000,000, exclusive of interest and costs.

12 12. This Court has personal jurisdiction over Defendant Capital One because it regularly  
13 does conduct business in this District, and the unlawful conduct alleged in this Complaint occurred in,  
14 was directed to, and/or emanated, in part, from this District.

15 13. This Court has personal jurisdiction over Defendant AWS because it has headquarters in  
16 this District, and the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or  
17 emanated, in part, from this District.

18 14. This Court has personal jurisdiction over Defendant Thompson because she resides and  
19 is incarcerated in this District and, on information and belief, committed the alleged hacking described  
20 herein in this District.

21 15. Venue is proper under 28 U.S.C. § 1391(b) because a substantial part of the events or  
22 omissions giving rise to the unlawful conduct alleged in this Complaint occurred in, was directed to,  
23 and/or emanated from this District.

24 **FACTUAL BACKGROUND**

25 16. Capital One expressly promises it is “committed to protecting your personal and financial  
26 information. If we collect identifying information from you, we will protect that information with  
27 controls based upon internationally recognized security standards, regulations, and industry-based best  
28

1 practices.”<sup>2</sup>

2 17. AWS similarly promises:

3 At AWS, security is our highest priority. We design our systems with your security and  
4 privacy in mind.

- 5 • We maintain a wide variety of compliance programs that validate our security  
6 controls. . . .
- 7 • We protect the security of your information during transmission to or from AWS  
8 websites, applications, products, or services by using encryption protocols and  
9 software.
- 10 • We follow the Payment Card Industry Data Security Standard (PCI DSS) when  
11 handling credit card data.
- 12 • We maintain physical, electronic, and procedural safeguards in connection with  
13 the collection, storage, and disclosure of personal information. Our security  
14 procedures mean that we may request proof of identity before we disclose  
15 personal information to you.<sup>3</sup>

16 18. On July 29, 2019, it was revealed that AWS’s and Capital One’s failure to protect Capital  
17 One’s customers’ Personal Information resulted in the exposure of over 100 million individuals’  
18 Personal Information. According to Capital One, “[t]he largest category of information accessed was  
19 information on consumers and small businesses as of the time they applied for one of our credit card  
20 products from 2005 through early 2019.”<sup>4</sup>

21 19. In its press release concerning the incident, dated July 29, 2019, Capital One stated: “On  
22 July 19, 2019, we determined there was unauthorized access by an outside individual who obtained  
23 certain types of personal information relating to people who had applied for credit card products and  
24 Capital One credit card customers. This occurred on March 22 and 23, 2019.”<sup>5</sup>

25 20. Capital One admits that “[d]ue to the particular circumstances of this incident, the

---

26 <sup>2</sup> Capital One Online & Mobile Privacy Statement, [https://www.capitalone.com/identity-  
protection/privacy/statement](https://www.capitalone.com/identity-protection/privacy/statement) (last visited July 30, 2019).

27 <sup>3</sup> AWS Privacy Notice, Last Updated: December 10, 2018, <https://aws.amazon.com/privacy/> (last  
visited July 30, 2019).

28 <sup>4</sup> Capital One News Release, July 29, 2019, [phx.corporate-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 visited July 30, 2019).

<sup>5</sup> *Id.*  
CLASS ACTION COMPLAINT - 4

1 unauthorized access also enabled the decrypting of data.”<sup>6</sup>

2 21. Capital One admits that a wide variety of information was compromised:

3 This information included personal information Capital One routinely collects at the time  
4 it receives credit card applications, including names, addresses, zip codes/postal codes,  
5 phone numbers, email addresses, dates of birth, and self-reported income. Beyond the  
6 credit card application data, [an alleged hacker] also obtained portions of credit card  
7 customer data, including:

- 8 • Customer status data, e.g., credit scores, credit limits, balances, payment history,  
9 contact information
- 10 • Fragments of transaction data from a total of 23 days during 2016, 2017 and 2018

11 No bank account numbers or Social Security numbers were compromised, other than:

- 12 • About 140,000 Social Security numbers of our credit card customers
- 13 • About 80,000 linked bank account numbers of our secured credit card customers<sup>7</sup>

14 22. Federal authorities arrested an alleged hacker, Defendant Paige A. Thompson, who has  
15 been charged with perpetrating the Data Breach. *See USA v. Thompson*, Case No. 2:19-mj-00344-MAT  
16 (W.D. Wash., July 29, 2019).

17 23. Defendant Thompson allegedly stole the Personal Information at issue in this District,  
18 and accordingly is being charged here. *See id.*, Dkt. 1 (Complaint) at Count 1.

19 24. According to the Complaint against Defendant Thompson, she stated her intention to  
20 disseminate the Personal Information she stole to others, at least as of June 18, 2019, though she was  
21 not arrested until July 26-29, 2019.

22 25. Accordingly, Defendant Thompson had plenty of time to realize her intention of  
23 distributing the Personal Information at issue before her arrest.

24 26. According to the Complaint against Defendant Thompson, she was able to perpetrate the  
25 Data Breach because Capital One stored the Personal Information at issue on the “cloud,” and Defendant  
26 Thompson was able to exploit vulnerabilities in the cloud services that Defendant utilized, provided by  
27 what the Complaint identifies as the “Cloud Computing Company.” *Id.*

---

28 <sup>6</sup> *Id.*

<sup>7</sup> *Id.*

1 27. The Complaint against Defendant Thompson explains that she “formerly worked at the  
2 Cloud Computing Company,” in Seattle, and additional evidence clearly suggests that this Cloud  
3 Computing Company is AWS. *Id.*<sup>8</sup>

4 28. Fundamentally, Defendants Capital One and AWS failed to provide the level of data  
5 protection that they expressly promised, thus exposing millions of individuals’ Personal Information to  
6 an increased risk of misuse by unauthorized third parties (*e.g.*, identity theft).

7 29. Had Defendant Capital One informed its customers that it would use inadequate security  
8 measures, consumers (like Plaintiff and the members of the Classes) would not have applied for credit  
9 cards with Capital One.

10 30. Capital One’s and AWS’s failure to implement adequate security protocols jeopardized  
11 millions of consumers’ Personal Information, fell well short of its promises, and diminished the value  
12 of the services provided.

13 31. Accordingly, Plaintiff brings suit on behalf of himself and all others similarly situated,  
14 to seek redress for Defendants’ unlawful conduct.

15 **I. Capital One is Subject to the Gramm-Leach-Bliley Act.**

16 32. Capital One is a financial institution, as that term is defined by Section 509(3)(A) of the  
17 Gramm-Leach-Bliley (“GLB”) Act, 15 U.S.C. § 6809(3)(A), and thus is subject to the GLB Act.

18 33. The GLB Act defines a financial institution as “any institution the business of which is  
19 engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company  
20 Act of 1956].” 15 U.S.C. § 6809(3)(A).

21 34. Capital One collects nonpublic personal information, as defined by 16 C.F.R. § 313.3(n).  
22 Accordingly, during the relevant time period Capital One was subject to the requirements of the GLB  
23

---

24 <sup>8</sup> See also, *e.g.*, Brian Krebs, *Capital One Data Theft Impacts 106M People*,  
25 <https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/> (last visited July 30,  
26 2019). Mr. Krebs, a respected blogger on cybersecurity issues, includes links to what appears to be  
27 Defendant Thompson’s resume, which states that she worked for “Amazon Inc. - Simple Storage  
28 Services” from May 2015 - Sep 2016, in Seattle, Washington. See Paige Thompson Resume  
Repository, <https://gitlab.com/netcrave/Resume/blob/master/cv/experience.tex> (last visited July 30,  
2019).

1 Privacy Rule, 16 C.F.R. § 313.1 *et seq.*, and is subject to numerous rules and regulations.

2 35. The GLB Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since  
3 the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing  
4 the Privacy Rule, and accordingly promulgated the Privacy of Consumer Financial Information,  
5 Regulation P, 12 C.F.R. § 1016 (“Regulation P”), which became effective on October 28, 2014.

6 36. Accordingly, Capital One’s conduct is governed by the Privacy Rule prior to October 28,  
7 2014, and by Regulation P after that date.

8 37. Both the Privacy Rule and Regulation P require financial institutions to provide  
9 customers with an initial and annual privacy notice. These privacy notices must be “clear and  
10 conspicuous.” 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. “Clear and conspicuous  
11 means that a notice is reasonably understandable and designed to call attention to the nature and  
12 significance of the information in the notice.” 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These  
13 privacy notices must “accurately reflect[] [the financial institution’s] privacy policies and practices.” 16  
14 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements,  
15 including the categories of nonpublic personal information the financial institution collects and  
16 discloses, the categories of third parties to whom the financial institution discloses the information, and  
17 the security and confidentiality policies of the financial institution. 16 C.F.R. § 313.6; 12 C.F.R. §  
18 1016.6. These privacy notices must be provided “so that each consumer can reasonably be expected to  
19 receive actual notice.” 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Capital One violated  
20 the Privacy Rule and Regulation P.

21 38. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 15 U.S.C.  
22 § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer  
23 information by developing a comprehensive written information security program that contains  
24 reasonable administrative, technical, and physical safeguards, including: (1) designating one or more  
25 employees to coordinate the information security program; (2) identifying reasonably foreseeable  
26 internal and external risks to the security, confidentiality, and integrity of customer information, and  
27 assessing the sufficiency of any safeguards in place to control those risks; (3) designing and  
28 implementing information safeguards to control the risks identified through risk assessment, and

1 regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and  
2 procedures; (4) overseeing service providers and requiring them by contract to protect the security and  
3 confidentiality of customer information; and (5) evaluating and adjusting the information security  
4 program in light of the results of testing and monitoring, changes to the business operation, and other  
5 relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Capital One violated the  
6 Safeguard Rule.

7 39. Capital One failed to assess reasonably foreseeable internal and external risks to the  
8 security, confidentiality, and integrity of customer information.

9 40. Capital One's conduct (and lack thereof), resulted in a variety of failures to follow GLB  
10 mandated rules and regulations, many of which are also industry standard. Among such deficient  
11 practices, the Data Breach demonstrates that Capital One failed to implement (or inadequately  
12 implemented) information security policies or procedures such as effective employee training, adequate  
13 intrusion detection systems, regular reviews of audit logs and records, and other similar measures to  
14 protect the confidentiality of the Personal Information it maintained in its data systems, instead  
15 outsourcing such responsibilities to AWS.

16 41. More specifically, Capital One's security failures demonstrate that it failed to honor its  
17 express and implied promises by failing to:

- 18 a. Maintain an adequate data security system to reduce the risk of data breaches and cyber  
19 attacks;
- 20 b. Adequately protect Plaintiff's and the Classes' Personal Information;
- 21 c. Implement policies and procedures to prevent, detect, contain, and correct security  
22 violations;
- 23 d. Implement procedures to regularly review records of information system activity, such  
24 as audit logs, access reports, and security incident tracking reports;
- 25 e. Protect against any reasonably anticipated threats or hazards to the security or integrity  
26 of Personal Information; and
- 27 f. Effectively train all members of its workforce on the policies and procedures with respect  
28 to Personal Information as necessary and appropriate for the members of its workforce

1 to carry out their functions and to maintain security of Personal Information.

2 42. Had Capital One implemented the above-described data security protocols, the  
3 consequences of the data exposure could have been avoided, or at least significantly reduced (as the  
4 exposure could have been detected earlier, the amount of Personal Information compromised could have  
5 been greatly reduced, and affected consumers could have been notified—and taken protective/mitigating  
6 actions—much sooner).

7 **II. It Is Well Established that Data Breaches Lead to Identity Theft.**

8 43. The United States Government Accountability Office noted in a June 2007 report on Data  
9 Breaches (“GAO Report”) that identity thieves use identifying data such as SSNs to open financial  
10 accounts, receive government benefits and incur charges and credit in a person’s name.<sup>9</sup> As the GAO  
11 Report states, this type of identity theft is the most harmful because it may take some time for the victim  
12 to become aware of the theft and can adversely impact the victim’s credit rating.

13 44. In addition, the GAO Report states that victims of identity theft will face “substantial  
14 costs and inconveniences repairing damage to their credit records” and their “good name.”<sup>10</sup>

15 45. According to the Federal Trade Commission (“FTC”), identity theft victims must spend  
16 countless hours and large amounts of money repairing the impact to their credit.<sup>11</sup> Identity thieves use  
17 stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or  
18 utilities fraud, and bank/finance fraud.<sup>12</sup>

19 \_\_\_\_\_  
20 <sup>9</sup> See *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is*  
21 *Limited; However, the Full Extent Is Unknown* (June 2007) (“GAO Report”), United States  
22 Government Accountability Office, <http://www.gao.gov/new.items/d07737.pdf> (last visited July 30,  
2019).

23 <sup>10</sup> *Id.*

24 <sup>11</sup> See *Identity Theft*, Federal Trade Commission, <http://www.consumer.ftc.gov/features/feature-0014-identity-theft> (last visited July 30, 2019).

25 <sup>12</sup> The FTC defines identity theft as “a fraud committed or attempted using the identifying information  
26 of another person without authority.” 17 C.F.R. § 248.201. The FTC describes “identifying  
27 information” as “any name or number that may be used, alone or in conjunction with any other  
28 information, to identify a specific person,” including, among other things, “[n]ame, Social Security  
number, date of birth, official State or government issued driver’s license or identification number,  
alien registration number, government passport number, employer or taxpayer identification number.”  
*Id.*

1 46. With access to an individual's Personal Information, criminals can do more than just  
2 empty a victim's bank account—they can also commit various types of fraud, including: obtaining a  
3 driver's license or official identification card in the victim's name but with the thief's picture; using the  
4 victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the  
5 victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house,  
6 or receive medical services in the victim's name, and may even give the victim's personal information  
7 to police during an arrest, resulting in an arrest warrant being issued in the victim's name.<sup>13</sup>

8 47. Personal Information is such a valuable commodity to identity thieves that once the  
9 information has been compromised, criminals often trade the information on the "cyber black-market"  
10 for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly  
11 posted stolen credit card numbers, SSNs, and other Personal Information directly on various Internet  
12 websites making the information publicly available.

13 48. There may be a time lag between when Private Information is stolen and when it is used.  
14 According to the U.S. Government Accountability Office ("GAO"):

15 [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to*  
16 *a year or more before being used to commit identity theft.* Further, once stolen data have  
17 been sold or posted on the Web, *fraudulent use of that information may continue for*  
*years.* As a result, studies that attempt to measure the harm resulting from data breaches  
cannot necessarily rule out all future harm.<sup>14</sup>

## 18 CLASS ALLEGATIONS

### 19 A. Class Definitions

20 49. Plaintiff seeks relief in his individual capacity and as a representative of all others who  
21 are similarly situated.

22 50. In accordance with Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiff seeks  
23 certification of the following Class:

24 All persons residing in the United States whose Personal Information was exposed in the  
25

26 <sup>13</sup> See *Warning Signs of Identity Theft*, Federal Trade Commission,  
27 <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last visited July 30, 2019).

28 <sup>14</sup> GAO Report, at 33.

1 Data Breach announced by Capital One on July 29, 2019 (the “Nationwide Class”).

2 51. Plaintiff further seeks certification of the following California Subclass:

3 All persons residing in the State of California whose Personal Information was exposed  
4 in the Data Breach announced by Capital One on July 29, 2019 (the “California Subclass”  
and, together with the Nationwide Class, the “Classes”).

5 52. Excluded from the Classes are: (1) Defendants, any entity or division in which any  
6 Defendant has a controlling interest, and their legal representatives, officers, directors, assigns, and  
7 successors; (2) the Judge to whom this case is assigned and the Judge’s staff; and (3) governmental  
8 entities. Plaintiff reserves the right to amend the Class definitions if discovery and further investigation  
9 reveal that the Classes should be expanded, divided into further subclasses, or modified in any other  
10 way.

11 **B. Certification of the Proposed Class is Appropriate.**

12 53. Each of the proposed Classes meets the certification under Fed. R. Civ. P. 23(a), (b)(1),  
13 (b)(2), and (b)(3).

14 54. **Numerosity:** The exact number of members of the Classes is unknown to Plaintiff at this  
15 time, but on information and belief, there are over 100 million individuals in the Class, making joinder  
16 of each individual member impracticable. Ultimately, members of the Classes will be easily identified  
17 through Capital One’s and AWS’s records.

18 55. **Commonality and Predominance:** There are many questions of law and fact common  
19 to the claims of Plaintiff and the other members of the Classes, and those questions predominate over  
20 any questions that may affect individual members of the Classes. Common questions for the Classes  
21 include:

- 22 a. Whether Defendants Capital One and AWS failed to adequately safeguard Plaintiff’s and  
23 the Classes’ Personal Information;
- 24 b. Whether Defendants Capital One and AWS failed to protect or otherwise keep Plaintiff’s  
25 and the Classes’ Personal Information secure, as promised;
- 26 c. Whether Defendants Capital One and AWS’s failure to secure Plaintiff’s and the Classes’  
27 Personal Information in the manner alleged violated federal, state and local laws, or  
28 industry standards;
- d. Whether Defendant Capital One’s storage of Plaintiff’s and the Classes’ Personal

1 Information in the manner alleged violated the GLB;

2 e. Whether Defendant Thompson distributed Plaintiff's and the Classes' Personal  
3 Information to others;

4 f. Whether Defendants Capital One and AWS engaged in unfair or deceptive practices by  
5 failing to properly safeguard Plaintiff's and the Classes' Personal Information as  
6 promised;

7 g. Whether Defendant Capital One and/or AWS failed to notify Plaintiff and members of  
8 the Classes about the Data Breach as soon as practical and without delay after the breach  
9 was discovered;

10 h. Whether Defendants Capital One and/or AWS acted negligently in failing to properly  
11 safeguard Plaintiff's and the Classes' Personal Information;

12 i. Whether Defendant Capital One's conduct described herein constitutes a breach of its  
13 implied or express contracts with Plaintiff and the members of the Class;

14 j. Whether Defendant Capital One should retain the money paid by Plaintiff and members  
15 of the Classes to protect their Personal Information;

16 k. Whether Defendant AWS should retain the money paid to it by Capital One to protect  
17 the Personal Information at issue; and

18 l. Whether Plaintiff and the members of the Classes are entitled to damages as a result of  
19 Defendants' conduct.

20 56. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class.  
21 Plaintiff and the members of the Class sustained damages as a result of Defendant's uniform wrongful  
22 conduct.

23 57. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the  
24 Classes, and has retained counsel competent and experienced in complex litigation and class actions.  
25 Plaintiff has no interests antagonistic to those of the Classes, and Defendants have no defenses unique  
26 to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of  
27 the members of the proposed Classes, and have the financial resources to do so. Neither Plaintiff nor  
28 their counsel have any interest adverse to those of the other members of the Classes.



1           63.     Capital One utilized AWS’s cloud computing services to store, access, use, and secure  
2 the Personal Information at issue.

3           64.     By collecting, using, storing, and profiting from this data, Defendants Capital One and  
4 AWS each had a duty of care to use reasonable means to secure and safeguard this Personal Information,  
5 to prevent disclosure of the information, and to guard the information from theft.

6           65.     Capital One’s duty included a responsibility to implement a process by which it could  
7 detect a breach of its security systems in a reasonably expeditious period of time and to give prompt  
8 notice in the case of a data breach.

9           66.     As they admit in their respective privacy policies, Defendants Capital One and AWS  
10 each owed a duty to Plaintiff and members of the Classes to provide security consistent with industry  
11 standards and the other requirements discussed herein, and to ensure that their systems and networks—  
12 and the personnel responsible for them—adequately protected Capital One’s customers’ Personal  
13 Information.

14           67.     Capital One further owed a duty to use reasonable security measures as a result of the  
15 special relationship that existed between it and Plaintiff and other members of the Classes. The special  
16 relationship arose because Plaintiff and the members of the Classes entrusted Capital One with their  
17 confidential Personal information in order to acquire and use Capital One’s banking services. Only  
18 Capital One was in a position to ensure that its systems were sufficient to protect against the harm to  
19 Plaintiff and the members of the Classes from such a data breach.

20           68.     Capital One’s duty to use reasonable security measures also arose under GLB, under  
21 which Capital One was required to protect the security, confidentiality, and integrity of customer  
22 information by developing a comprehensive written information security program that contains  
23 reasonable administrative, technical, and physical safeguards.

24           69.     In addition, Defendants Capital One and AWS had a duty to use reasonable security  
25 measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair  
26 . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair  
27 practice of failing to use reasonable measures to protect confidential data.

28           70.     Defendants Capital One and AWS breached their common law, statutory, and other

1 duties by failing to use reasonable measures to protect consumers' Personal Information and by failing  
2 to provide timely notice of the Data Breach. The specific negligent acts and omissions include, but are  
3 not limited to, the following:

- 4 a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's  
5 and members of the Classes' Personal Information;
- 6 b. failing to adequately monitor the security of Capital One's customer data on AWS's networks;
- 7 c. allowing unauthorized access to Plaintiff's and other members of the Classes' Personal  
8 information;
- 9 d. failing to recognize in a timely manner that Plaintiff's and other members of the Classes'  
10 Personal information had been compromised; and
- 11 e. failing to warn Plaintiff and other members of the Classes in a timely manner that their Personal  
12 Information had been compromised.

13 71. It was foreseeable that failure to use reasonable measures to protect this Personal  
14 Information and to provide timely notice of the Data Breach would result in injury to Plaintiff and other  
15 members of the Classes. Further, the breach of security, unauthorized access, and resulting injury to  
16 Plaintiff and other members of the Classes were reasonably foreseeable.

17 72. It was and remains foreseeable that the failure to adequately safeguard Personal  
18 Information will result in one or more of the following injuries to Plaintiff and other members of the  
19 Classes: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse,  
20 resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting  
21 in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; illegal  
22 sale of the compromised data on the deep web black market; expenses and/or time spent on credit  
23 monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements,  
24 and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings;  
25 lost work time; and other economic and non-economic harm.

26 73. Accordingly, Plaintiff, on behalf of himself and other members of the Classes, seeks an  
27 order declaring that Defendants' conduct constitutes negligence, and awarding them damages in an  
28 amount to be determined at trial.

1 **COUNT II**  
2 **Violation of the Washington Consumer Protection Act**  
3 **(On behalf of Plaintiff and the Nationwide Class Against Defendants Capital One and AWS)**

4 74. Plaintiff incorporates the allegations above as if fully set forth here.

5 75. Washington's Consumer Protection Act, RCW §§ 19.86.010, *et seq.* (“CPA”), protects  
6 both consumers and competitors by promoting fair competition in commercial markets for goods and  
7 services.

8 76. To achieve that goal, the CPA prohibits any person from using “unfair methods of  
9 competition or unfair or deceptive acts or practices in the conduct of any trade or commerce. . . .” RCW  
10 § 19.86.020. An unfair or deceptive business practice is one that is likely to deceive a substantial portion  
11 of the public or otherwise affect public interest.

12 77. Defendants Capital One and AWS expressly represented that they would take reasonable  
13 measures to protect the Personal Information compromised in the Data Breach.

14 78. Consistent with their privacy policy representations, Defendants Capital One and AWS  
15 accepted responsibility for securing Plaintiff’s and other Class members’ Personal Information. Given  
16 that it was Defendants’ responsibility for creating, overseeing, maintaining, and otherwise implementing  
17 their own data security practices, Defendants knew (or should have known) that they were not  
18 adequately protecting the compromised Personal Information in accordance with their express  
19 guarantees.

20 79. Defendants’ failure to notify Plaintiff and other Class members promptly about the Data  
21 Breach was both unfair and misleading, because this failure ran contrary to Defendants’ promised  
22 confidentiality practices, and exposed Plaintiff and other Class members to additional (and unnecessary)  
23 harm, and otherwise offended public policy.

24 80. Consumers—like Plaintiff and other Class members—value their privacy. Companies  
25 that offer adequate data security protections are more valuable to consumers than those with substandard  
26 security practices. As such, consumers will, if given the choice between two otherwise identical services,  
27 choose one with adequate security practices over one with substandard security practices.

28 81. Because of this consumer preference for data security, a bank safeguarding and  
protecting Personal Information in accordance with the GLB, other federal, state and local laws, and

1 industry standards—in addition with its own affirmative representations of its data security practices—  
2 commands a higher customer based for its services than a bank with substandard security.

3 82. Similarly, a cloud computing company's services are worth more if it provides adequate  
4 security, as AWS represents it will provide.

5 83. Prior to the Data Breach, neither Plaintiff nor the general public knew that neither  
6 Defendant Capital One nor AWS was implementing the data security and privacy protocols they  
7 promised in their own consumer-facing representations. These Defendants knew that customers would  
8 not give these Defendants their business if customers knew Defendants could not or would not protect  
9 such Personal Information, as they represented they would. And rather than implement the data security  
10 and privacy protocols they promised, Defendants actively concealed their true practices and protocols  
11 (which were of material concern to all of their customers), while at the same time expressly promising  
12 that Personal Information would be protected as described above.

13 84. Had Plaintiff and other Class members known that Defendant Capital One did *not*  
14 actually implement its promised data security and privacy protocols, they would not have been willing  
15 to provide Defendant with their Personal Information.

16 85. Defendants' unfair acts or practices occurred in their trade or business and have  
17 proximately caused injury to Plaintiff and to other Class members. Defendants' general course of  
18 conduct is injurious to the public interest, and such acts are ongoing and/or have a substantial likelihood  
19 of being repeated inasmuch as the long-lasting harmful effects of their misconduct may last for years  
20 (*e.g.*, affected individuals could experience identity theft for years). As a direct and proximate result of  
21 Defendants' unfair acts, Plaintiff and other Class members have suffered actual injuries, including  
22 without limitation investing substantial time or money in monitoring and remediating the harm inflicted  
23 upon them by the Data Breach.

24 86. As a result of Defendants' conduct, Plaintiff and other Class members have suffered  
25 actual damages, including the lost value of their privacy, the lost value of their Personal Information,  
26 and lost property in the form of their breached and compromised Personal Information (which is of great  
27 value to third parties); ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and  
28 abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse,

1 resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data;  
2 the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on  
3 credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card  
4 statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores  
5 and ratings; lost work time; and other economic and non-economic harm.

6 87. Accordingly, Plaintiff, on behalf of himself and members of the proposed Class, seeks to  
7 enjoin further violation and recover actual damages and treble damages (where applicable), together  
8 with the costs of bringing this suit, including reasonable attorneys' fees.

9 88. With respect to injunctive relief, Plaintiff, on behalf of himself and members of the  
10 proposed Class, seeks an Order requiring Defendants to: (1) engage third-party security  
11 auditors/penetration testers as well as internal security personnel to conduct testing, including simulated  
12 attacks, penetration tests, and audits on their systems on a periodic basis, and ordering Defendants to  
13 correct any problems or issues detected by such third-party security auditors promptly; (2) engage third-  
14 party security auditors and internal personnel to run automated security monitoring; (3) audit, test, and  
15 train their security personnel regarding any new or modified procedures; (4) segment data by, among  
16 other things, creating firewalls and access controls so that if one area of Capital One's AWS-maintained  
17 cloud network is compromised, hackers cannot gain access to other portions of either Defendants'  
18 systems; (5) purge, delete, and destroy in a reasonably secure manner Personal Information not  
19 necessary for Capital One's provisions of services to such consumers; (6) conduct regular database  
20 scanning and securing checks; (7) routinely and continually conduct internal training and education to  
21 inform internal security personnel how to identify and contain a breach when it occurs and what to do  
22 in response to a breach; and (8) meaningfully educate all Class members about the threats they face as  
23 a result of the loss of their confidential financial, personal, information to third parties, as well as the  
24 steps affected individuals should take to protect themselves.

25 **COUNT III**  
26 **Violation of Washington Data Breach Disclosure Law**  
**(On behalf of Plaintiff and the Nationwide Class Against Capital One and AWS)**

27 89. Plaintiff incorporates the foregoing allegations as if fully set forth here.

28 90. RCW § 19.255.010(2) provides that "[a]ny person or business that maintains

1 computerized data that includes personal information that the person or business does not own shall  
2 notify the owner or licensee of the information of any breach of the security of the data immediately  
3 following discovery, if the personal information was, or is reasonably believed to have been, acquired  
4 by an unauthorized person.” *See* RCW § 19.255.010(2) (2005).

5 91. The Data Breach described above resulted in an “unauthorized acquisition of  
6 computerized data that compromise[d] the security, confidentiality, [and] integrity of personal  
7 information maintained by” Defendants and, therefore, experienced a “breach of the security of [their]  
8 system[s],” as defined by RCW § 19.255.010(4) (2005).

9 92. Defendants failed to disclose the breach of Capital One’s data on AWS’s systems  
10 immediately after discovering the Data Breach. Defendants unreasonably delayed informing Plaintiff  
11 and other Class members about the Data Breach after they knew or should have known that the Data  
12 Breach had occurred.

13 93. Defendants’ failure to provide notice immediately after discovering the Data Breach is a  
14 violation of RCW § 19.255.010.

15 **COUNT IV**  
16 **Violation of California Data Breach Law**  
17 **(On behalf of Plaintiff and the California Subclass Against Capital One and AWS)**

18 94. Plaintiff incorporates the foregoing allegations as if fully set forth here.

19 95. “[T]o ensure that personal information about California residents is protected,” the  
20 California legislature enacted Cal. Civil Code § 1798.81.5, which requires that any business that “owns  
21 or licenses personal information about a California resident shall implement and maintain reasonable  
22 security procedures and practices appropriate to the nature of the information, to protect the personal  
23 information from unauthorized access, destruction, use, modification, or disclosure.”

24 96. The Private Information taken in the Data Breach fits within the definition of “Personal  
25 Information” in Cal. Civil Code § 1798.80.

26 97. Plaintiff and California Subclass members provided their Personal Information to  
27 Defendant Capital in order to use its banking services, and thus qualify as “Customer[s]” as defined in  
28 Cal. Civil Code § 1798.80.

98. Defendants failed to dispose of Plaintiff’s and others’ Personal Information when it was

1 no longer needed, violating Cal. Civil Code § 1798.81.

2 99. By failing to implement reasonable measures to protect the Personal Information in their  
3 possession, Defendants violated Cal. Civil Code § 1798.81.5.

4 100. In addition, by failing to promptly notify all who were affected by the Data Breach that  
5 their Personal Information had been acquired by hackers, Defendants violated Cal. Civil Code  
6 § 1798.82.

7 101. As a direct or proximate result of Defendants' violations of Cal. Civil Code §§ 1798.81,  
8 1798.81.5, and 1798.82, Plaintiff and California Subclass members were (and continue to be) injured  
9 and have suffered (and will continue to suffer) the damages described in this Class Action Complaint.

10 102. Defendants' violations of Cal. Civil Code §§ 1798.81, 1798.81.5, and 1798.82 were, at a  
11 minimum, reckless.

12 103. In addition, by violating Cal. Civil Code §§ 1798.81, 1798.81.5, and 1798.82, Defendants  
13 may be enjoined under Cal. Civil Code § 1798.84(e).

14 104. Defendants' violations of Cal. Civil Code §§ 1798.81.5 and 1798.82 also constitute an  
15 unlawful acts or practices under California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code  
16 § 17200 *et seq.*, which affords the Court discretion to enter whatever orders may be necessary to prevent  
17 future unlawful acts or practices.

18 105. Plaintiff accordingly requests that the Court enter an injunction requiring Defendants to  
19 implement and maintain reasonable security procedures, including, but not limited to: (1) engage third-  
20 party security auditors/penetration testers as well as internal security personnel to conduct testing,  
21 including simulated attacks, penetration tests, and audits on their systems on a periodic basis, and  
22 ordering Defendants to correct any problems or issues detected by such third-party security auditors  
23 promptly; (2) engage third-party security auditors and internal personnel to run automated security  
24 monitoring; (3) audit, test, and train their security personnel regarding any new or modified procedures;  
25 (4) segment data by, among other things, creating firewalls and access controls so that if one area of  
26 Capital One's AWS-maintained cloud network is compromised, hackers cannot gain access to other  
27 portions of either of Defendants' systems; (5) purge, delete, and destroy in a reasonably secure manner  
28 Personal Information not necessary for Capital One's provisions of services to such consumers; (6)

1 conduct regular database scanning and securing checks; (7) routinely and continually conduct internal  
2 training and education to inform internal security personnel how to identify and contain a breach when  
3 it occurs and what to do in response to a breach; and (8) meaningfully educate all California Subclass  
4 members about the threats they face as a result of the loss of their confidential financial, personal,  
5 information to third parties, as well as the steps affected individuals should take to protect themselves.

6 106. Plaintiff further requests that the Court require Defendants to identify and notify all  
7 members of the California Subclass who have not yet been informed of the Data Breach, and to notify  
8 affected consumers of any future data breaches by email within 24 hours of Defendants' discovery of a  
9 breach or possible breach and by mail within 72 hours.

10 107. Plaintiff and the California Subclass are entitled to actual damages in an amount to be  
11 determined at trial under Cal. Civil Code Section 1798.84.

12 108. Plaintiff and the California Subclass also are entitled to an aware of attorney fees and  
13 costs under Cal. Civil Code Section 1798.84.

14 **COUNT V**  
15 **Conversion**

16 **(On behalf of Plaintiff and the Nationwide Class Against Defendant Thompson)**

17 109. Plaintiff incorporates the foregoing allegations as if fully set forth here.

18 110. By hacking into Defendants Capital One's and AWS's computerized systems to take  
19 Plaintiff's Personal Information, Defendant Thompson eviscerated the confidentiality of that Personal  
20 Information.

21 111. Plaintiff and other Class members did not consent to Defendant Thompson's actions.

22 112. As a result of Defendant Thompson's conduct, Plaintiff and other Class members have  
23 suffered actual damages, including the lost value of their privacy, the lost value of their Personal  
24 Information, and lost property in the form of their breached and compromised Personal Information  
25 (which is of great value to third parties); ongoing, imminent, certainly impending threat of identity theft  
26 crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes,  
27 fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen  
28 confidential data; the illegal sale of the compromised data on the deep web black market; expenses  
and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank

1 statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts;  
2 decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

3 113. Plaintiff seeks damages on behalf of himself and other Class members from Defendant  
4 Thompson compensating them for their injuries.

5 114. Plaintiff further seeks an injunction preventing Defendant Thompson from working in  
6 any capacity in which she again could gain access to knowledge concerning cloud computing industry  
7 vulnerabilities.

8 **COUNT VI**  
9 **Breach of Express Contract**  
10 **(On behalf of Plaintiff and the National Data Breach Class Against Defendant Capital One)**

11 115. Plaintiff incorporates the foregoing allegations as if fully set forth here.

12 116. Plaintiff and members of the Classes entered into valid and enforceable contracts with  
13 Defendant Capital One under which it promised to provide data protection services to them, along with  
14 banking services. Plaintiff and members of the Classes agreed to, among other things, pay money for  
15 such services, and use Defendant's credit cards as opposed to credit cards from other issuers, thereby  
16 generating revenues for Defendant in the form of processing fees charged to merchants and interest  
17 charged to consumers.

18 117. Both aspects of Plaintiff's and the other Class members' agreements with Defendant (*i.e.*,  
19 the provision of banking and data protection services) were material.

20 118. Defendant expressly promised Plaintiff and other Class members to safeguard and protect  
21 the confidentiality of their Personal Information in accordance with GLB regulations; federal, state  
22 and/or local laws; and industry standards.

23 119. Defendant promised to comply with all GLB regulations, federal, state and/or local laws,  
24 and industry standards to make sure that Plaintiff's and the members of the Classes' Personal  
25 Information was protected.

26 120. These contracts required that Defendant protect Plaintiff's and other Class members'  
27 Personal Information and to prevent unauthorized access to such information.

28 121. Unfortunately, Defendant Capital One did not safeguard this Personal Information.  
Specifically, Defendant did not comply with its promises to abide by GLB, federal, state and/or local

1 laws, or industry standards.

2 122. The failure to meet these promises and obligations constitutes a breach of express  
3 contract.

4 123. Because Defendant allowed unauthorized access to Plaintiff's and other Class members'  
5 Personal Information, and otherwise failed to safeguard the Personal Information, as promised,  
6 Defendant breached its contracts with Plaintiff and other Class members.

7 124. A meeting of the minds occurred, as Plaintiff and other Class members agreed to, among  
8 other things, provide Defendant with their accurate and complete information (including their Personal  
9 Information) and to use Defendant's payment cards in exchange for its agreement to, among other things,  
10 protect their Personal Information.

11 125. Defendant breached these contracts by failing to implement (or adequately implement)  
12 sufficient security measures to protect Plaintiff's and other Class members' Personal Information.

13 126. As a result of Defendant's conduct, Plaintiff and members of the Classes have suffered  
14 actual damages.

15 127. Accordingly, Plaintiff, on behalf of themselves and the other members of the Classes  
16 seek an order declaring that Defendant's conduct constitutes breach of express contract, and awarding  
17 them damages in an amount to be determined at trial.

18 **REQUEST FOR RELIEF**

19 Plaintiff, on behalf of themselves and the Classes, respectfully requests that this Court enter an  
20 Order:

21 A. Certifying this case as a class action on behalf of Plaintiff and the Classes defined above,  
22 appointing Plaintiff as representatives of their respective Classes, and appointing their counsel as Class  
23 Counsel;

24 B. Awarding injunctive and other equitable relief as is necessary to protect the interests of  
25 the Classes, including (i) an order prohibiting Defendants from engaging in the wrongful and unlawful  
26 acts described herein, and (ii) requiring Defendants Capital One and AWS to protect all data collected  
27 through the course of their business in accordance with GLB regulations, industry standards, and federal,  
28 state and/or local laws; (iii) requiring Defendants Capital One and AWS to engage third-party security



1 Respectfully submitted,

2 Dated: July 30, 2019

**KELLER ROHRBACK L.L.P.**

3  
4 By: /s/ Cari C. Laufenberg

Cari Campen Laufenberg (WSBA 34354)

Lynn Lincoln Sarko (WSBA 16569)

T. David Copley (WSBA 19379)

5 KELLER ROHRBACK L.L.P.

1201 Third Avenue, Suite 3200

6 Seattle, WA 98101

7 Tel: (206) 623-1900

8 Fax: (206) 623-3384

9 claufenberg@kellerrohrback.com

10 lsarko@kellerrohrback.com

dcopley@kellerrohrback.com

11 Christopher Springer, *pro hac vice forthcoming*

12 KELLER ROHRBACK L.L.P.

801 Garden Street, Suite 301

13 Santa Barbara, CA 93101

14 Tel: (805) 456-1496

15 Fax: (805) 456-1497

cspringer@kellerrohrback.com

**AHDOOT & WOLFSON, PC**

16  
17 /s/ Tina Wolfson

Tina Wolfson, *pro hac vice forthcoming*

18 Theodore Maya, *pro hac vice forthcoming*

19 Bradley K. King, *pro hac vice forthcoming*

Ruhandy Glezakos, *pro hac vice forthcoming*

20 AHDOOT & WOLFSON, PC

10728 Lindbrook Drive

21 Los Angeles, CA 90024

22 Tel: (310) 474-9111

23 Fax: (310) 474-8585

twolfson@ahdootwolfson.com

24 tmaya@ahdootwolfson.com

bking@ahdootwolfson.com

25 rglezakos@ahdootwolfson.com