UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

DEBORAH DAMES, individually and on behalf of all others similarly situated, Plaintiff, v. CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE, N.A., CAPITAL ONE BANK (USA), N.A., Defendants.	Case No. 1:19-cv-1010 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Deborah Dames ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action against Defendants Capital One Financial Corporation, Capital One, N.A., and Capital One Bank (USA), N.A. (collectively, "Capital One," "the Company," or "Defendants"). Plaintiff's allegations are based upon personal knowledge as to her own acts and upon information and belief as to all other matters alleged herein, including the investigation of counsel, publicly available information, news articles, press releases, and additional analysis. Plaintiff believes that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

I. NATURE OF THE ACTION

1. On July 29, 2019, Capital One announced that the personal information of over ***100 million*** credit card applicants and customers had been accessed by a hacker—marking one of the largest data thefts from a financial institution in history.

2. In connection with credit card applications, Plaintiff and members of the Classes (defined below) were required to provide and provided Capital One with highly-sensitive personal

information with the reasonable expectation that Defendants would adequately safeguard and protect that information from unauthorized access and use.

3. Defendants have collected millions of records containing sensitive and personal information, including that of Plaintiff and members of the Classes, and maintain that information on a server, which houses personally identifying information including, *inter alia*: names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, self-reported income, credit scores, credit limits, balances, payment history, contact information, account numbers and information, transaction data, and/or social security numbers ("Personally Identifying Information" or "PII").

4. Capital One assured its credit card applicants and customers that it takes privacy and data security seriously. Specifically, Capital One promised to "make your safety and security a top priority" and informed consumers that the Company is "committed to protecting your personal and financial information . . . with controls based upon internationally recognized security standards, regulations, and industry-based best practices."[1]

5. Yet, Defendants negligently failed to implement, test and maintain reasonable cyber-security measures to safeguard Plaintiff's and Class members' PII.

6. In March 2019, a hacker named Paige Thompson or handle "erratic" accessed the PII of over 100 million consumers and small businesses that applied for Capital One credit cards over the course of a 14 year period—from 2005 through 2019. The Data Breach (defined below) compromised the PII of Plaintiffs and Class members, including 140,000 social security numbers and 80,000 bank account numbers.

[1] *Capital One Online & Mobile Privacy Statement*, CAPITAL ONE, https://www.capitalone.com/identity-protection/privacy/statement.

7. While Amazon Web Services hosted the remote data servers the Company used to store the PII, Capital One built its own web application on top of Amazon's cloud data so it could use the PII in ways specific to its needs; it was this application that was breached.

8. According to the Federal Bureau of Investigation ("FBI"), Ms. Thompson gained access to the PII through a "misconfiguration" of a firewall on a Capital One web application, which allowed her to communicate with the server where Capital One was storing its information and obtain Plaintiff's and Class members' PII.[2]

9. Ms. Thompson posted the hacked PII on her GitHub account on April 21, 2019, allowing other unauthorized users to access and exploit Plaintiff's and Class members' PII.

10. On information and belief, the PII remained exposed until July 17, 2019 when "an unidentified tipster informed Capital One of its existence by emailing the bank's responsible disclosure address with a brief warning about the data and a link to it on GitHub."[3]

11. Capital One has long known that the PII it maintains is highly valuable to hackers and that the Company is susceptible to data breaches if it does not implement proper data security measures. For example, in 2017, "Capital One notified customers that a former employee may have had access for four months to their personal data, including account numbers, telephone numbers, transaction history and Social Security numbers."[4] A similar breach was reported by the Company in 2014.

---

[2] Emily Flitter and Karen Weise, *Capital One Data Breach Compromises Data of Over 100 Million*, N.Y. TIMES (July 29, 2019), https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html (the "N.Y. Times Article").

[3] Lily Hay Newman, *The Alleged Capital One Hacker Didn't Cover Her Tracks*, WIRED, (July 29, 2019, 10:29 PM), https://www.wired.com/story/capital-one-hack-credit-card-application-data/?itm_campaign=TechinTwo (the "Wired Article").

[4] N.Y. Times Article.

12. In this Data Breach, Capital One first failed to maintain adequate safeguards to protect the PII, then failed to discover the unauthorized access to Plaintiff's and Class members' PII for ***almost four months***, and then waited 10 days after discovering the Data Breach to notify Plaintiffs and Class members that their PII had been compromised. During this time, Plaintiff and members of the Classes had no way of knowing of the Data Breach and no ability to mitigate the harm caused by the breach.

13. Contrary to the reasonable expectations of Plaintiff and Class members, Defendants failed to reasonably maintain and protect Plaintiff and Class members' PII in a secure manner, in breach of their implied and express agreements, and in violation of their legal duties and state laws.

14. In addition to Defendants' failure to adequately implement, test and maintain reasonable cyber-security measures to protect against the wrongful disclosure or compromise of the PII, Defendants failed to timely detect and notify Plaintiff and Class members of the Data Breach in violation of their duties and applicable state data protection laws.

15. Plaintiff brings this class action on behalf of herself and the Class against Defendants for negligence, negligence per se, and breach of implied contract, on behalf of herself and the Nationwide Contract Sub-Class (defined below) for breach of express contract, and on behalf of herself and the Missouri Sub-Class (defined below) for violation of The Missouri Merchandising Practices Act, Mo. Rev. Stat. 407.010, *et seq.* (the "MMPA").

16. As a direct and proximate result of Defendants' failure to adequately safeguard and protect Plaintiff's and the Class's PII, Plaintiff and members of the Class have suffered damages and will continue to suffer damages including, but not limited to: (l) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Defendants with the understanding that Defendants would safeguard their PII against theft and not

allow access and misuse of their PII by others; (3) the compromise, disclosure, theft and/or misuse of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of PII; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and/or PII misuse; (6) the continued risk to their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their possession; and (7) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach.

17. As a further result of Defendants' negligence in failing to timely identify a breach and notify Plaintiff and members of the Classes that their PII was compromised, Plaintiff and members of the Classes have been harmed in that they have been unable to take the necessary precautions to mitigate their damages by preventing future identity theft and/or fraud.

II. PARTIES

18. Plaintiff Deborah Dames is Missouri resident whose PII, on information and belief, was compromised in the Data Breach. Plaintiff Dames has three credit card accounts with Capital One: (1) a Platinum MasterCard opened in 2013; (2) a Platinum MasterCard opened in 2014; and (3) a Visa Platinum card opened in 2015. Plaintiff Dames entrusted her PII to Defendants with the reasonable expectation and understanding that Defendants would protect and safeguard that information from compromise, disclosure, and/or misuse by unauthorized users.

19. Defendant Capital One Financial Corporation ("Capital One Financial") is a Delaware corporation headquartered in McLean, Virginia.

20. Defendant Capital One, N.A. is a wholly-owned subsidiary of Capital One Financial and is a national bank headquartered in McLean, Virginia.

21. Defendant Capital One Bank (USA) N.A. is a wholly-owned subsidiary of Capital One Financial and is headquartered in McLean, Virginia.

III. JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this lawsuit has been brought as a class action on behalf of a proposed Class including millions of members, the aggregate claims of the putative Class members exceed $5 million exclusive of interest and costs, and one or more of the members of the putative Class are citizens of a different state than the Defendants.

23. This Court has jurisdiction over Capital One because its principal place of business is located within this District, it conducts significant business in this District, has sufficient minimum contacts with the District, and much of the relevant conduct occurred in this District.

24. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Capital One resides within this District, transacts business, is found, and/or has agents in this District; a substantial part of the events giving rise to Plaintiff's and the Classes' claims arose in the District; and Capital One had sufficient contacts with Virginia and this District.

IV. FACTUAL ALLEGATIONS

A. Capital One Collects and Promises to Safeguard PII

25. Capital One Financial, the tenth-largest bank in the United States and the third-largest credit-card issuer in the nation, derived over 60% of the company's revenues in 2018 from credit cards.

26. In connection with its issuance of credit cards, Capital One collects and maintains highly-sensitive PII from millions of credit card applicants. As required by Defendants, Plaintiff

and members of the Classes provided their PII to Defendants, and that PII was maintained by Defendants.

27. This PII is considered extremely valuable: an individual in possession of this information can determine a given applicant's financial status, creditworthiness, and affluence, and even open credit cards, accounts or loans in an applicant's name.[5]

28. Indeed, bank account information can be sold on the dark web, "the part of the internet that is not catalogued by normal search engines, like Google[,]" for $1000 or more.[6]

29. Plaintiff and Class members provided Defendants their PII with the understanding and reasonable expectation that Defendants would protect and safeguard the PII from compromise, disclosure, and/or misuse by unauthorized users.

30. Contrary to the understanding and reasonable expectations of Plaintiff and Class members, Defendants failed to reasonably maintain Plaintiff's and Class members' PII in a secure manner and failed to safeguard the PII from compromise, disclosure and/or misuse by unauthorized parties, in violation of their legal duties, in breach of their implied and express agreements, and in violation of state laws.

31. Capital One, like any financial institution that collects and stores PII, is charged with safeguarding that information, and makes various representations to those applying for credit cards that it will adequately safeguard and protect their PII.

---

[5] Bourree Lam and Julia Carpenter, *The Capital One Data Breach: What It Means for You*, ST. J. (July 30, 2019, 11:21 AM), https://www.wsj.com/articles/the-capital-one-breach-what-it-means-for-you-11564500086.

[6] Cadie Thompson, *Here's how much thieves make by selling your personal data online*, BUSINESS INSIDER (May 28, 2015, 4:45 PM), https://www.businessinsider.com.au/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5.

32. For example, on its website, Capital One assures credit applicants that it "protects your Social Security Number," and that Capital One's policies and procedures "[p]rohibit the unlawful disclosure of Social Security numbers."[7]

33. Capital One further promises to "make your safety and security a top priority," and that it is "committed to protecting your personal and financial information . . . with controls based upon internationally recognized security standards, regulations, and industry-based best practices.[8]

B. Capital One Announces the Data Breach

34. On July 29, 2019, Capital One issued a press release, publicly revealing for the first time that a hacker accessed Capital One's system remotely and gained access to the PII of more than 100 million individuals and small businesses that used or applied for Capital One credit card products (the "Data Breach").[9]

35. The stolen PII included "names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income," in addition to "credit scores, credit limits, balances, payment history, contact information" and "transaction data from a total of 23 days during 2016, 2017, and 2018."[10] According to the Company, approximately 140,000 Social Security numbers ("SSNs") and approximately 80,000 bank account numbers were compromised in the Data Breach.

36. Capital One admitted that it had discovered the breach 10 days earlier—on July 19, 2019—when it "determined there was unauthorized access by an outside individual who obtained

---

7 *Social Security Number Protections*, CAPITAL ONE, https://www.capitalone.com/identity-protection/privacy/social-security-number.

8 *Capital One Online & Mobile Privacy Statement*, CAPITAL ONE, https://www.capitalone.com/identity-protection/privacy/statement.

9 Capital One Fin. Corp., Current Report (Form 8-K, Ex. No. 99.1) (July 30, 2019).

10 *Id.*

certain types of [P]ersonal [I]nformation relating to people who had applied for its credit card products and to Capital One credit card customers."[11]

37. Despite having knowledge of the Data Breach on July 19, 2019, Capital One waited 10 days to notify Plaintiffs and members of the Classes that their PII had been compromised. During this time, Plaintiff and members of the Classes had no way of knowing of the Data Breach and no ability to mitigate the harm caused by the breach.

38. When announcing the Data Breach, Capital One Chairman and CEO, Richard D. Fairbank, stated "While I am grateful that the perpetrator has been caught, I am deeply sorry for what has happened . . . I sincerely apologize for the understandable worry this incident must be causing those affected and I am committed to making it right."[12] However, Capital One downplayed the gravity of the Data Breach, stating it was unlikely that PII had been misused.

39. The FBI conducted an investigation and subsequently executed a search warrant on the premises of the suspected hacker, later identified as Paige A. Thompson or handle "erratic".[13]

40. According to the criminal complaint against Thompson, Capital One's storage was first accessed, and its firewall first breached, on or about March 22, 2019. A series of commands, believed by the FBI to have been executed by Thompson, first copied the PII on April 21, 2019.[14]

41. Ms. Thompson posted the hacked PII on her GitHub account on April 21, 2019, allowing other unauthorized users to access and exploit Plaintiff's and Class members' PII.

---

11 *Id.*

12 *Id.*

13 Criminal Complaint, *United States v. Thompson*, No. 2:19-mj-00344-MAT, (W.D. Wash. July 29, 2019), ECF No. 1.

14 *Id.*

42. Capital One later revealed that the Data Breach occurred as a result of an unknown "specific configuration vulnerability in [Capital One's] infrastructure.[15]

43. The Data Breach went undetected by Capital One for ***almost four months***—in fact, Capital One's "routine automated scanning" was so ineffective that Capital One only learned about the Data Breach after an anonymous individual relayed a tip indicating that Capital One's servers may have been compromised.[16]

44. Capital One finally realized that its server's firewall had been breached, and that the PII of Plaintiff and Class members had been accessed by unauthorized users, via a message sent through its "Responsible Disclosure" e-mail tip line on July 17, 2019, ***two days prior*** to the Company's "determining" that its server had been breached.[17] Only then, on July 19, 2019, did Capital One contact law enforcement.[18]

45. So complete was Capital One's failure to protect the members of the Class, including Plaintiff, that the same "vulnerability" that allowed Thompson to access the data also allowed anyone who accessed the data to exploit it.

C. Capital One Owes a Duty to Plaintiff and Class Members to Safeguard PII

46. Capital One is well aware of the threat posed by hackers and data breaches, and most banks approach the threat accordingly. For example, JPMorgan Chase Chief Executive

---

15 Capital One Fin. Corp., Current Report (Form 8-K, Ex. No. 99.1) (July 30, 2019).

16 Alexandra Ma, *Capital One found out about its 106-million-customer data breach only because a member of the public emailed it a tip*, BUSINESS INSIDER (July 31, 2019), https://www.businessinsider.com/capital-one-hack-data-breach-email-tip-off-2019-7.

17 *Id.*

18 Press Release, U.S. Dep't of Justice, Seattle Tech Worker Arrested for Data Theft Involving Large Financial Services Company (July 29, 2019), https://www.justice.gov/usao-wdwa/pr/seattle-tech-worker-arrested-data-theft-involving-large-financial-services-company.

Officer Jamie Dimon claims that JPMorgan Chase spends almost $600 million annually, and Bank of America allows a "blank check" for cybersecurity expenses.[19]

47. Capital One was also acutely aware of the threat posed by, and consequences of, cyberattacks, as it experienced data breaches before: for example, in both 2017 and 2014, Capital One reported breaches that occurred when former employees gained access to similarly sensitive personal information.[20]

48. Defendants knowingly collected and maintained the PII of Plaintiff and members of the Class, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties.

49. The Federal Trade Commission ("FTC") has established regulations and guidelines for fundamental data security principles and practices for businesses such as Capital One. These guidelines establish proper procedures for safeguarding PII and implementing intrusion detection systems.[21] Further, Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including the unfair act or practice by businesses of failing to use reasonable measures to safeguard and protect PII.

50. Individual states have also enacted statutes based on the FTC Act that require Capital One to act reasonably in the management of data, to use reasonable security measures to protect such data, and to timely notify consumers of any breach.

---

19 *The New York Times* Article.

20 *Id.*

21 *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

51. Defendants violated Section 5 of the FTC Act (and state statutes) by failing to implement reasonable measures to safeguard and protect the PII of Plaintiff and Class members. Defendants further violated Section 5 of the FTC Act (and state statutes) by failing to comply with industry standards regarding the reasonable protection of PII.

52. Had Defendants taken reasonable steps to protect and maintain the security of Plaintiff's and Class members' PII, they would have quickly detected the intrusion and could have alerted Plaintiff and members of the Classes to the Data Breach.

53. It was foreseeable that if Defendants failed to take reasonable cyber-security measures, the PII of Plaintiff and members of the Class could be stolen, lost, misused, and/or disclosed to unauthorized users. Defendants knew or should have known that Plaintiff's and Class members' PII was an attractive target for cyber attackers, particularly in light of highly-publicized prior data breaches, and Defendants failed to take reasonable precautions to safeguard the PII of credit card applicants, including Plaintiff and members of the Class.

54. By failing to implement necessary cyber-security measures to protect credit card applicants' PII and by failing to timely identify a breach and notify Plaintiff and Class members of the Data Breach, Defendants departed from the reasonable standard of care and breached their duties to Plaintiff and members of the Class.

55. Plaintiff and members of the Classes have suffered harm as a result of the Data Breach, in the form of unauthorized disclosure of their PII in a useable, decrypted format. All members of the Class, including Plaintiff, are subject to unknown third parties phishing, opening and re-opening accounts in their names, stealing their identities, and/or emptying their bank accounts.

56. Furthermore, Capital One's failure to timely identify that its security had been breached and its failure to timely notify Plaintiff and members of the Classes of the Data Breach exacerbated harm to Plaintiff and other members of the Classes, as Thompson posted the PII to her GitHub account for others to view and access and Plaintiff and Class members had no way to mitigate this harm.

57. Due to Defendants' failure to properly safeguard Plaintiff's and Class members' PII and to timely identify a breach and notify credit card applicants of the Data Breach, hackers had access to Plaintiff's and members of the Classes' PII, exposing Plaintiff and members of the Classes to fraud, identity theft, and financial harm, and to a heightened imminent risk of such harm in the future.

58. As a result of Defendants' wrongful conduct, Plaintiff and Class members have suffered and will continue to suffer actual damages, including, *inter alia*, costs associated with mitigating the real and imminent risk of fraud and identity theft, such as costs for effective credit monitoring services and identity theft insurance, and other costs associated with closing accounts and re-issuing credentials.

V. CLASS ACTION ALLEGATIONS

59. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of the following Class and Sub-Classes:

> **Nationwide Class**: All persons and entities whose PII was compromised as a result of the data breach announced by Capital One on or about July 29, 2019 (the "Nationwide Class" or "Class").
>
> **Nationwide Contract Sub-Class:** All persons and entities who entered into customer agreements with Capital One for credit card services and whose PII was compromised as a result of the data breach announced by Capital One on or about July 29, 2019 (the "Nationwide Contract Sub-Class").

> **Missouri Class**: All persons residing in Missouri whose PII was compromised as a result of the data breach announced by Capital One on or about July 29, 2019 (the "Missouri Sub-Class").
>
> **Missouri Contract Sub-Class (in the alternative to the Nationwide Contract Sub-Class)**: All persons and entities who reside or have their principal place of business in Missouri who entered into customer agreements with Capital One for credit card services and whose PII was compromised as a result of the data breach announced by Capital One on or about July 29, 2019 (the "Missouri Contract Sub-Class").

60. Excluded from the proposed Class and Sub-Classes are Defendants, as well as their agents, officers, and directors, and their families, as well as their parent companies, subsidiaries, and affiliates. Any judicial officer assigned to this case is also excluded. Plaintiff reserves the right to revise the definitions of the Class and Sub-Classes based upon subsequently discovered information.

61. The Class and Sub-Classes are referred to herein as the Classes.

62. This action is brought and may be properly maintained as a class action under Federal Rules of Civil Procedure 23(a) and 23(b)(3).

63. The Classes are so numerous that joinder of all members is impracticable. Plaintiff believes that there are millions of proposed Class members throughout the United States.

64. Common questions of law and fact exist as to all members of the Classes and predominate over any issues solely affecting individual members of the Classes. The common questions of law and fact include but are not limited to:

a) whether Defendants failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the PII of Plaintiff and members of the Classes;

b) whether Defendants compromised, disclosed and/or permitted unauthorized access to the PII of Plaintiff and members of the Classes;

c) whether Defendants failed to act reasonably in securing PII of Plaintiff and members of the Classes;

d) whether Defendants failed to timely notify Plaintiff and members of the Class of the Data Breach;

e) whether Defendants' conduct was negligent;

f) whether Defendants' conduct was negligent per se;

g) whether Defendants breached their implied contracts with Plaintiff and Class members by failing to protect the PII of Plaintiff and members of the Class;

h) whether Defendants breached their express contracts with Plaintiff and members of the Nationwide Contract Sub-Class by failing to protect the PII of Plaintiff and members Nationwide Contract Sub-Class;

i) whether Defendants breached their implied covenant of good faith and fair dealing with Plaintiff and members of the Nationwide Contract Sub-Class by failing to protect the PII of Plaintiff and members Nationwide Contract Sub-Class;

j) whether Defendants violated The Missouri Merchandising Practices Act, Mo. Rev. Stat. 407.010 *et seq.*; and

k) whether Plaintiff and members of the Classes are entitled to actual damages, statutory damages, punitive damages, restitution, restitutionary disgorgement, and/or other equitable or declaratory relief.

65. Plaintiff's claims are typical of the claims of the Classes. As alleged herein, Plaintiff and members of the Classes all sustained damages arising out of the same course of unlawful conduct by Defendant.

66. Plaintiff is willing and prepared to serve the Classes in a representative capacity with all of the obligations and duties material thereto. Plaintiff will fairly and adequately protect the interests of the Classes and has no interests adverse to, or which conflict with, the interests of the other members of the Classes.

67. Plaintiff has engaged the services of the undersigned counsel. Counsel is experienced in complex litigation, will adequately prosecute this action, and will assert and protect the rights of, and otherwise represent, Plaintiff and the absent members of the Classes.

68. Plaintiff's interests are co-extensive with, and not antagonistic to, those of the absent members of the Classes. Plaintiff will undertake to represent and protect the interests of the absent members of the Classes.

69. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Plaintiff knows of no difficulty to be encountered in the management of this litigation that would preclude its maintenance as a class action.

70. Class action status is warranted under Rule 23(b)(3) because questions of law or fact common to the members of the Classes predominate over any questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

71. The interest of members of the Classes in individually controlling the prosecution of separate actions is theoretical and not practical. Prosecution of the action through multiple representatives would be objectionable and Plaintiff anticipates no difficulty in the management of this matter as a class action.

VI. CLAIMS

FIRST CLAIM

NEGLIGENCE
AGAINST DEFENDANTS ON BEHALF OF THE NATIONWIDE CLASS

72. Plaintiff incorporates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

73. Plaintiff brings this claim on behalf of herself and members of the Nationwide Class.

74. Defendants knowingly collected and maintained the PII of Plaintiff and members of the Class, and had a duty to exercise reasonable care in safeguarding, securing and protecting

such information from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties.

75. Defendants also had a duty to timely notify Plaintiff and members of the Class of the Data Breach under Va. Code Ann. § 18.2-186.6.

76. Defendants owed Plaintiff and members of the Class a duty to take reasonable steps to maintain and protect against any dangers to Plaintiff's and members of the Class' PII presented by cyber-attackers. This duty included, among other things, maintaining and testing their cyber-security systems, taking other reasonable security measures to protect and adequately secure PII of Plaintiff and members of the Class from unauthorized access, and taking reasonable steps to ensure that hackers did not compromise the systems and/or gain access to credit card applicants' PII.

77. Defendants owed a duty of care to Plaintiff and members of the Class because it was foreseeable that they would be harmed by Defendants' inadequate cyber-security practices. By failing to implement necessary measures to protect the PII of Plaintiff and Class members, Defendants departed from the reasonable standard of care and breached their duties to Plaintiff and members of the Class.

78. It was foreseeable that if Defendants did not take reasonable security measures, the PII of Plaintiff and members of the Class could be stolen, lost, misused, and/or disclosed to unauthorized users. Defendants knew or should have known that Plaintiff's and Class members' PII was an attractive target for cyber attackers, particularly in light of highly-publicized prior data breaches, and Defendants failed to take reasonable precautions to safeguard the PII of their customers, including Plaintiff and members of the Class.

79. As a direct and proximate result of Defendants' failure to exercise reasonable care and deploy reasonable cyber-security measures, the PII of Plaintiff and members of the Class was accessed by a cyber-attacker and can be used to commit identity theft and/or fraud.

80. But for Defendants' failure to implement and maintain adequate cyber-security measures to protect Plaintiff's and member of the Class' PII, Plaintiff's and members of the Class' PII would not have been compromised, stolen, and/or disclosed to unauthorized users, Plaintiff and members of the Class would not have been injured, and Plaintiff and members of the Class would not be at a heightened future risk of identity theft and/or fraud.

81. Defendants had and continue to have a duty to timely identify a breach and disclose that Plaintiff's and Class members' PII within their possession was compromised, lost, stolen, misused and/or disclosed to unauthorized parties and precisely the types of information compromised.

82. Defendants unlawfully breached their duty to timely identify a breach and disclose to Plaintiff and members of the Class the fact that their PII was compromised, lost, stolen, misused and/or disclosed to unauthorized parties and precisely the type of information compromised.

83. As a result of Defendants' negligence, Plaintiff and members of the Class have suffered damages including, but not limited to: (l) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Defendants with the understanding that Defendants would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, disclosure, theft and/or misuse of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of PII; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences

of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and/or PII misuse; (6) the continued risk to their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their possession; and (7) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the data breach.

84. As a further result of Defendants' negligence in failing to timely identify a breach and notify Plaintiff and members of the Class that their PII was compromised, Plaintiff and members of the Class have been harmed in that they have been unable to take the necessary precautions to mitigate their damages by preventing future identity theft and/or fraud.

SECOND CLAIM

NEGLIGENCE PER SE
AGAINST DEFENDANTS ON BEHALF OF THE NATIONWIDE CLASS

85. Plaintiff incorporates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

86. Plaintiff brings this claim on behalf of herself and members of the Nationwide Class.

87. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including the unfair act or practice by businesses of failing to use reasonable measures to safeguard and protect PII. FTC guidelines, publications and consent orders further establish this duty.

88. Individual states have enacted statutes based on the FTC Act that require Capital One to act reasonably in the management of data, and to use reasonable security measures to protect such data that also created a duty.

89. Defendants violated Section 5 of the FTC Act (and state statutes) by failing to implement reasonable measures to safeguard and protect the PII of Plaintiff and Class members. Defendants further violated Section 5 of the FTC Act (and state statutes) by failing to comply with industry standards regarding the reasonable protection of PII.

90. Defendants' violation of Section 5 of the FTC Act (and state statutes) constitutes negligence per se.

91. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

92. The harm that has occurred as a result of the Data Breach is the type of harm the FTC Act intended to guard against. For example, the FTC has pursued numerous enforcement actions against businesses that caused substantially harm to that caused by Capital One as a result of their failure to employ reasonable data security measures and failure to avoid unfair and deceptive practices.

93. Capital One breached its duty and mishandled Plaintiff's and Class members' PII by adopting and maintaining data security measures that the Company knew or should have known were unreasonable and inadequate to protect PII.

94. As a direct and proximate result of Defendants' negligence per se, Plaintiff and Class members have been injured and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

95. As a direct result of Defendants' unlawful conduct, Plaintiff and members of the Class have suffered damages and will continue to suffer damages including, but not limited to: (l) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Defendants with the understanding that Defendants would safeguard

their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, disclosure, theft and/or misuse of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of PII; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and/or PII misuse; (6) the continued risk to their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their possession; and (7) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the data breach.

96. As a further result of Defendants' failure to timely identify a breach and notify Plaintiff and members of the Class that their PII was compromised, Plaintiff and members of the Class have been harmed in that they have been unable to take the necessary precautions to mitigate their damages by preventing future identity theft and/or fraud.

THIRD CLAIM

BREACH OF IMPLIED CONTRACT
AGAINST DEFENDANTS ON BEHALF OF THE NATIONWIDE CLASS

97. Plaintiff incorporates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

98. Plaintiff brings this claim on behalf of herself and members of the Nationwide Class.

99. Plaintiff and members of the Class entered into implied contracts with Defendants under which Plaintiff and members of the Class provided PII in order to apply for credit cards from

Defendants with the understanding that Defendants agreed to safeguard and protect that PII and would timely identify a breach and notify Plaintiff and Class members of any unauthorized access to their PII.

100. Plaintiff and members of the Class would not have provided their PII to Defendants without the understanding that Defendants would protect and safeguard their PII and identify a breach and notify Plaintiff and Class members of any unauthorized access to their PII in a timely manner.

101. Defendants breached their implied contracts with Plaintiff and Class members by failing to safeguard the PII of Plaintiff and members of the Class and by permitting the compromise and/or disclosure of that PII to unauthorized users.

102. Further, Defendants breached their implied contracts with Plaintiff and Class members by failing to timely identify a breach and notify Plaintiff and Class members of the Data Breach and unauthorized access to their PII.

103. As a direct and proximate result of Defendants' breaches of their implied contracts with Plaintiff and members of the Class, Plaintiff and members of the Class have suffered damages and will continue to suffer damages including, but not limited to: (l) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Defendants with the understanding that Defendants would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, disclosure, theft and/or misuse of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of PII; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how

to prevent, detect, contest, and recover from identity theft and/or PII misuse; (6) the continued risk to their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their possession; and (7) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the data breach.

104. As a further result of Defendants' breach of their implied contracts with Plaintiff and Class members by failing to timely identify a breach and notify Plaintiff and members of the Class that their PII was compromised, Plaintiff and members of the Class have been harmed in that they have been unable to take the necessary precautions to mitigate their damages by preventing future identity theft and/or fraud.

FOURTH CLAIM

BREACH OF CONTRACT
AGAINST DEFENDANTS ON BEHALF OF THE NATIONWIDE CONTRACT SUB-CLASS, OR IN THE ALTERNATIVE, THE MISSOURI CONTRACT SUB-CLASS

105. Plaintiff incorporates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

106. Plaintiff brings this claim on behalf of herself and members of the Nationwide Contract Sub-Class, or in the alternative, on behalf of herself and the Missouri Contract Sub-Class.

107. Plaintiff and members of the Nationwide Contract Sub-Class provided PII to Capital One and entered into customer agreements with Capital One to provide credit card services.

108. Capital One's customer agreements incorporate privacy notices into the terms of the agreements.

109. Pursuant to Capital One's privacy notices, Capital One expressly promised Plaintiff and members of the Class to safeguard and protect the confidentiality of their PII in accordance with regulations, federal, state, and/or local laws, and industry standards.

110. Specifically, Capital One informed Plaintiff and members of the Nationwide Contract Class in its Capital One Online & Mobile Privacy Statement that: "Capital One is committed to your privacy. Our goal is to maintain your trust and confidence when handling personal and financial information about you."[22]

111. Capital One further promised: "At Capital One, we make your safety and security a top priority and are committed to protecting your personal and financial information. If we collect identifying information from you, we will protect that information with controls based upon internationally recognized security standards, regulations, and industry-based best practices."[23]

112. Through its Capital One Privacy and Opt-Out Notice, Capital One promised: "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[24]

113. These contracts required that Capital One implement reasonable safeguards to protect Plaintiff's and members of the Nationwide Contract Sub-Class' PII, comply with federal laws, regulations and industry standards regarding the protection of PII, and prevent unauthorized access to PII.

---

[22] *Capital One Online & Mobile Privacy Statement*, CAPITAL ONE, https://www.capitalone.com/identity-protection/privacy/statement.

[23] *Id.*

[24] *Capital One Privacy and Opt-Out Notice*, CAPITAL ONE, https://www.capitalone.com/privacy/notice/en-us/.

114. The promises made by Capital One regarding the safeguard and protection of PII were material to Plaintiff and members of the Nationwide Contract Sub-Class.

115. A meeting of the minds occurred when Plaintiffs and members of the Nationwide Contract Sub-Class agreed to, *inter alia*, provide Defendants with their PII and to use Defendants' credit card services in exchange for Defendants' agreement to, among other things, reasonably protect and safeguard the PII of Plaintiffs and members of the Nationwide Contract Sub-Class.

116. Plaintiff and members of the Nationwide Contract Sub-Class performed their obligations under their contracts with Capital One.

117. Capital One breached its agreements with Plaintiff and members of the Nationwide Contract Sub-Class by failing to implement, test and maintain reasonable cyber-security measures to safeguard Plaintiff's and Nationwide Contract Sub-Class members' PII and failing to comply with federal and state law, regulations and industry standards regarding the reasonable safeguard of PII.

118. Defendants further breached their contracts with Plaintiff and Nationwide Contract Sub-Class members by permitting the compromise and/or disclosure of that PII to unauthorized users.

119. Further, Defendants breached their contracts with Plaintiff and Nationwide Contract Sub-Class members by failing to timely identify a breach and notify Plaintiff and Nationwide Contract Sub-Class members of the Data Breach and unauthorized access to their PII.

120. Defendants further breached their contracts with Plaintiff and members of the Nationwide Contract Sub-Class by breaching the implied covenant of good faith and fair dealing.

121. Defendants breached the implied covenant of good faith and fair dealing by failing to implement, test and maintain reasonable cyber-security measures to safeguard Plaintiff's and

Nationwide Contract Sub-Class members' PII, failing to comply with federal and state law, regulations and industry standards regarding the reasonable safeguard of PII, failing to timely identify the Data Breach and failing to timely notify Plaintiff and Nationwide Contract Sub-Class members of the Data Breach.

122. As a direct and proximate result of Defendants' breaches of their contracts with Plaintiff and members of the Nationwide Contract Sub-Class and breaches of the implied covenant of good faith and fair dealing, Plaintiff and members of the Nationwide Contract Sub-Class have suffered damages and will continue to suffer damages including, but not limited to: (l) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Defendants with the understanding that Defendants would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, disclosure, theft and/or misuse of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of PII; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and/or PII misuse; (6) the continued risk to their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their possession; and (7) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the data breach.

123. As a further result of Defendants' breaches of their contracts with Plaintiff and Nationwide Contract Sub-Class members and breaches of the implied covenant of good faith and

fair dealing by failing to timely identify a breach and notify Plaintiff and members of the Nationwide Contract Sub-Class that their PII was compromised, Plaintiff and members of the Nationwide Contract Sub-Class have been harmed in that they have been unable to take the necessary precautions to mitigate their damages by preventing future identity theft and/or fraud.

FIFTH CLAIM

VIOLATIONS OF THE MISSOURI MERCHANDISING PRACTICES ACT, MO. REV. STAT. § 407.010, *ET SEQ.*
AGAINST DEFENDANTS ON BEHALF OF THE MISSOURI SUB-CLASS

124. Plaintiff incorporates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

125. Plaintiff brings this claim on behalf of herself and members of the Missouri Sub-Class.

126. Plaintiff, members of the Missouri Sub-Class, and Defendants are "persons" within the meaning of Mo. Rev. Stat. § 407.020.

127. Defendants' credit card products and services are "merchandise" within the meaning of Mo. Rev. Stat. § 407.010(4).

128. Defendants were and are engaged in "trade" or "commerce" within the meaning of Mo. Rev. Stat. § 407.010(7).

129. Plaintiff and members of the Missouri Sub-Class applied for Capital One credit cards primarily for personal, family or household purposes.

130. The Missouri Merchandising Practices Act ("MMPA") makes unlawful the "act, use or employment by any person of any deception, fraud, false pretense, misrepresentation, unfair practice, or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise." Mo. Rev. Stat. § 407.020.

131. In the course of Defendants' business, Defendants violated the MMPA by failing to disclose and actively concealing the dangers and risks posed to the security of Missouri Sub-Class members' PII by Capital One's insufficient information security and faulty systems monitoring practices, as described above. Specifically, in advertising, soliciting applications for, and providing their credit card products and services, Defendants engaged in one or more of the following unfair or deceptive acts or practices proscribed by the MMPA, including: representing Capital One's storage and security systems for protecting PII had characteristics or benefits that they do not have; representing that they are of a particular standard and quality when they are not; and/or advertising them with the intent not to provide the level of security and protection advertised.

132. Defendants have long known of security vulnerabilities in their server and storage systems and failed to remedy those vulnerabilities. Defendants also failed to disclose and actively concealed the dangers and risks posed to Missouri Sub-Class members' PII by these vulnerabilities.

133. By failing to disclose and by actively concealing these security vulnerabilities in Capital One's server and storage systems, by marketing the same systems as safe, reliable, and of high quality, and by presenting themselves as reputable financial institutions that value and prioritize privacy, confidentiality and data security, Defendants engaged in unfair or deceptive business practices in violation of the MMPA. Defendants deliberately withheld the information about the vulnerabilities in their security systems, including the propensity of their firewalls to fail to prevent, or of their system checks to timely discover, unauthorized access to customer PII, in order to ensure that consumers, including the Missouri Sub-Class, would apply for and utilize Defendants' credit card products and services.

134. In the course of Defendants' business, they willfully failed to disclose and actively concealed the dangerous risks posed by the security vulnerabilities discussed above. Defendants compounded the deception by failing to timely detect a critical infiltration of their firewall while continuing to represent to consumers that Capital One's information security measures were reliable and of high quality, and by claiming to be reputable financial institutions that value and prioritize privacy, confidentiality and information security.

135. Defendants further violated the MMPA by concealing the Data Breach and failing to timely notify Plaintiff and members of the Missouri Sub-Class that their PII had been compromised.

136. Defendants' unfair or deceptive acts or practices, including these concealments, omissions, and suppressions of material facts, had a tendency or capacity to mislead, tended to create a false impression in consumers, were likely to and did in fact deceive reasonable consumers, including the members of the Missouri Sub-Class, about the true safety and security of PII solicited by and subsequently shared with Capital One and, as a result, of the true value of and risks attendant to applying for Capital One's credit card products and services.

137. Defendants intentionally and knowingly misrepresented material facts regarding the effectiveness and robustness of data protection measures utilized to protect the PII of credit card applicants with an intent to mislead Plaintiff and the members of the Missouri Sub-Class.

138. Defendants knew or should have known that their conduct violated the MMPA.

139. As alleged above, Defendants made material statements about the safety and reliability of the systems Capital One used to prevent unauthorized access to and dissemination of PII that were either false or misleading.

140. Defendants owed the members of the Missouri Sub-Class a duty to disclose the true security risks and known vulnerability of Capital One's information storage systems to unauthorized access because Defendants: (1) possessed exclusive knowledge of the dangers and risks posed by the foregoing; (2) intentionally concealed the foregoing from Missouri Sub-Class; and/or (3) made incomplete representations about the safety and reliability of the foregoing generally, while purposefully withholding material facts from the Missouri Sub-Class that contradicted these representations.

141. Plaintiff and members of the Sub-Class would not have provided their PII to Defendants without the understanding that Defendants would protect and safeguard their PII. In violation of the MMPA, Defendants engaged in deception, fraud, false pretense, misrepresentation, unfair practice, or the concealment, suppression, or omission of any material fact concerning their collection and safeguarding of Plaintiff's and Class members' PII.

142. Defendants' misrepresentations and fraudulent omissions were material to Plaintiff and members of the Class. Had Defendants disclosed that the PII was not safeguarded and was subject to access by unauthorized users, Plaintiff and members of the Class would not have provided their PII to Defendants.

143. As a direct and proximate result of Defendants' violations of the MMPA, the members of the Missouri Sub-Class have suffered injury-in-fact and/or actual damage.

144. As a direct and proximate result of Defendants' violations of the MMPA, Plaintiff and members of the Class have suffered damages and will continue to suffer damages including, but not limited to: (l) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Defendants with the understanding that Defendants would safeguard their PII against theft and not allow access and misuse of their PII by others; (3)

the compromise, disclosure, theft and/or misuse of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of PII; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and/or PII misuse; (6) the continued risk to their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their possession; and (7) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the data breach.

145. As a further result of Defendants' violations of the MMPA by failing to timely identify a breach and notify Plaintiff and members of the Class that their PII was compromised, Plaintiff and members of the Class have been harmed in that they have been unable to take the necessary precautions to mitigate their damages by preventing future identity theft and/or fraud.

146. Defendants are liable to members of the Missouri Sub-Class for damages in amounts to be proven at trial, including attorneys' fees, costs, and punitive damages, and any other just and proper relief under Mo. Rev. Stat. § 407.025.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that this Court enter a judgment against Defendants and in favor of Plaintiff and the Class and Sub-Classes, and award the following relief:

a) that this action be certified as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, declaring Plaintiff as the representative of the Class and Sub-Classes, and Plaintiff's counsel as counsel for the Class and Sub-Classes;

b) award Plaintiff and members of the Classes appropriate relief, including actual damages, statutory damages, punitive damages, and restitutionary disgorgement;

c) award equitable and declaratory relief as may be appropriate, including without limitation extended credit monitoring services and identity theft protection for Plaintiff and members of the Classes;

d) award all costs of prosecuting the litigation, including expert fees;

e) award pre- and post-judgment interest;

f) award attorneys' fees; and

g) grant such additional relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff hereby demands a trial by jury.

DATED: August 2, 2019

Respectfully submitted,

/s/ Haley N. Proctor
COOPER & KIRK, PLLC
David H. Thompson*
Haley N. Proctor (Bar No. 84272)
1523 New Hampshire Avenue, N.W.
Washington, D.C. 20036
Tel: (202) 220-9600
Fax: (202) 220-9601
dthompson@cooperkirk.com
hproctor@cooperkirk.com

KESSLER TOPAZ
MELTZER & CHECK LLP
Joseph H. Meltzer*
Naumon A. Amjed*
Melissa L. Troutner*
280 King of Prussia Road
Radnor, PA 19087
Tel: (610) 667-7706
Fax: (610) 667-7056
jmeltzer@ktmc.com
namjed@ktmc.com
mtroutner@ktmc.com

*Applications for admission PHV forthcoming

Attorneys for Plaintiff Deborah Dames and the proposed Classes

JS 44 (Rev 02/19)

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS DEBORAH DAMES, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff St. Louis County, MO.
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Haley N. Proctor, Cooper & Kirk, PLLC
1523 New Hampshire Avenue, N.W., Washington, D.C. 20036
(202) 220-9600

DEFENDANTS
CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE, N.A., CAPITAL ONE BANK (USA), N.A.

County of Residence of First Listed Defendant Fairfax County, VA.
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

Attorneys *(If Known)*

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

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

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*
Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☒ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer w/Disabilities - Employment
- ☐ 446 Amer w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U S Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

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

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
28 U.S.C. 1332(d)
Brief description of cause:
Redress injuries resulting from Defendants' massive data breach.

VII. REQUESTED IN COMPLAINT: ☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.
DEMAND $ In excess of $5 million
CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions)*:
JUDGE See attached list. DOCKET NUMBER 1:19-cv-1010

DATE 08/02/2019
SIGNATURE OF ATTORNEY OF RECORD s/ Haley N. Proctor

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG JUDGE _____

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

DEBORAH DAMES, individually and on behalf of all others similarly situated, Plaintiff, v. CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE, N.A., CAPITAL ONE BANK (USA), N.A., Defendants.	Case No. 1:19-cv-1010

List of Related Cases

Judge	**Docket Number**
Leonie M. Brinkema	1:19-cv-00979
Liam O'Grady	1:19-cv-00984
Claude M. Hilton	1:19-cv-00993
Rossie D. Alston, Jr	1:19-cv-00995
Rossie D. Alston, Jr	1:19-cv-01006
Unassigned	1:19-cv-01008