IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
(Alexandria Division)

RACHEL MCDONOUGH, individually and on behalf of all others similarly situated, Plaintiff, v. CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE BANK (USA), N.A., and CAPITAL ONE, N.A., Defendants.	)	Civil Action No. _____ **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff RACHEL MCDONOUGH, who is a citizen and resident of Wyoming, Rhode Island (Washington County), brings this class action against Defendants CAPITAL ONE FINANCIAL CORPORATION, whose principal place of business is 1680 Capital One Drive, McLean, VA, 22102-3491, Defendant CAPITAL ONE BANK (USA), N.A., whose principal place of business is 1680 Capital One Drive, McLean, VA, 22102-3491, and Defendant, CAPITAL ONE, N.A., whose principal place of business is 1680 Capital One Drive, McLean, VA, 22102-3491 (collectively, "Capital One"), on behalf of herself and others similarly situated to obtain damages, restitution and injunctive relief for the Class, as defined, below, from Defendants. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record:

PARTIES

1. Plaintiff is an individual who resides in Wyoming, Rhode Island (Washington County) in and is therefore a citizen of Rhode Island. Plaintiff has a Capital One® Venture® Rewards Credit Card account with Capital One ("Venture Card"). Plaintiff McDonough applied for a a Venture Card in January of 2019 and was issued a Venture Card shorty thereafter. Capital One collected stored Plaintiff's personal information, including at least her name, address, phone number, email address, birthday, self-reported income, and social security number as part of the application process and process of issuing a Venture Card to Plaintiff McDonough, and of course, they maintained her credit card number with expiration date as part of maintaining her Venture Card account. Plaintiff has made multiple purchases from using her Venture Card and currently is an account holder in good standing.

2. Each of the Defendants are headquartered in McLean, Virginia. Defendants are each therefore citizens of Virginia. Capital One Financial Corporation is a bank holding company specializing in credit cards, auto loans, banking and savings accounts. Defendants Capital One, N.A. and Capital One Bank (USA), N.A offer banking and lending products and services to consumers and businesses, and issue multiple types of credit cards for use by consumers and businesses, including the Venture Card, Capital One® Quicksilver® Cash Rewards Credit Card, Capital One® Spark® Cash for Business, Journey® Student Rewards from Capital One®, Capital One® SavorOne℠ Cash Rewards Credit Card, Capital One® QuicksilverOne® Cash Rewards Credit Card, Capital One® QuicksilverOne® Cash Rewards Credit Card, Capital One Savor® Rewards Credit Card, and Capital One® Secured Mastercard®, among others (the "Credit Cards"). Defendants are headquartered in this District, do business in this District, and issues credit cards, offer and maintain checking and savings

accounts, issue automobile loans, and provide a host of services to businesses from this District. Capital One is one of the largest retail and commercial banks in the U.S., and is ranked 10th on the list of largest banks in the United States by assets and had We posted record revenue of $28.1 billion in revenue in 2018. *See* 2018 Annual Report, p. 3, available at http://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_COF_2018.pdf (last accessed July 30, 2019) ("2018 Annual Report").

JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), the class contains members of diverse citizenship from Defendants, there are more than 100 Class members, and the amount in controversy exceeds $5 million.

4. This Court has personal jurisdiction over Defendants because Defendants are authorized to and conduct substantial business in Virginia, generally, and this District, specifically. Defendants own and operate retail locations within this District and throughout Virginia.

5. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1), because a substantial part of the events and omissions giving rise to this action occurred in this District as Defendants have their center of operations within this District, Plaintiff provided her Personally Identifiable Information, including name, address, phone number, email address, birthday, self-reported income, and social security number to Defendants here ("PII"), and for those applicants that were issued cards, Capital One also maintained the account number, expiration date, and related data for the issued card, and Plaintiff was issued her Credit Card from here.

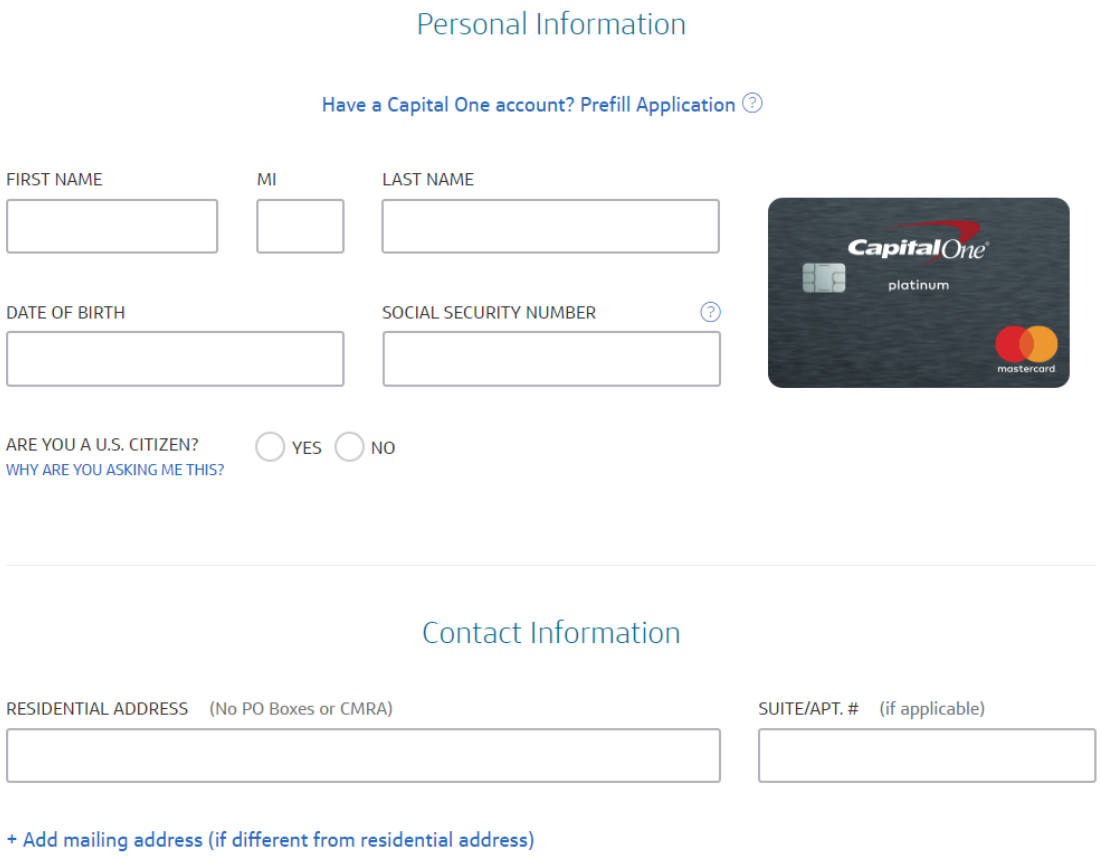
DEFENDANTS' COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION VIA CREDIT CARD APPLICATIONS

6. Defendants proclaim that they are really an information-based technology

company that does banking. According to Defendants, their rallying cry has been, "'Build a technology company that does banking, and compete against banks that use technology.'" 2018 Annual Report, p. 5. "The vast majority of [their] operating and customer-facing applications operate in the cloud," 2018 Annual Report, p. 5, which creates significant exposure to hackers and makes them more easily the subject of other nefarious computer intrusions.

7. Over 100 million Americans have applied for Capital One Credit Cards since 2005. Upon information and belief, over 40 million of those applicants have been issued Credit One Credit Cards.

8. As part of the application process for a Credit Card, consumers are requested to submit a myriad of PII in forms, including the following information:



EMAIL ADDRESS

When you provide your email address, we may use it to send you important information about your application and account(s), as well as other useful products and services.

PRIMARY PHONE NUMBER

MOBILE HOME WORK

Financial Information

DO YOU HAVE ANY BANK ACCOUNTS?

Select a type

EMPLOYMENT STATUS

Select status

TOTAL ANNUAL INCOME

$

Alimony, child support or separate maintenance income need not be revealed if you do not choose to have it considered as a basis for repaying this loan.

MONTHLY RENT/MORTGAGE

$

IF OFFERED, WOULD YOU BE INTERESTED IN BLANK CHECKS TO USE FOR CASH ADVANCES? (Optional)

YES NO

Additional Information

We need your agreement to receive by electronic means only communications regarding your application, including notice of our decision on your application and important account opening information regarding rates, fees and other costs related to the credit card for which you are applying. Please review the terms of our Electronic Communications Disclosure.

I have reviewed and agree to the terms of the Electronic Communications Disclosure. I confirm that I have an active email address and the ability to access, view and print PDF files.

Some of our communications are available in both English and Spanish. Which language would you prefer for future communications?

ENGLISH SPANISH

https://applynow.capitalone.com/?productId=6675. This information is highly sensitive and the

compromise of this PII data creates immense personal damage and exposure to those that accepted Capital One's invitation to submit this information.

9. Defendants collect and retain this information for purposes of approving applications for their Credit Cards. According to Defendants, the information they collect is immensely valuable:

> We were founded on the belief that the banking industry would be revolutionized by information and technology, beginning with credit cards. Back then, credit cards were a onesize-fits-all business that relied on judgmental decision-making by underwriters and marketers. There were few data-driven decisions and a whole lot of conventional wisdom. But we saw credit cards as an information-based technology business rather than a lending business, one powered by worldclass analysts leveraging the latest technology, massive amounts of information, statistical modeling, and the scientific testing of thousands of ideas.

2018 Annual Report, p. 3.

10. Thus, Defendants store massive amounts of PII on their servers, locally and in the cloud, and Capital One utilizes this information to maximize their profits through predictive marketing and other marketing techniques.

VALUE OF PII TO HACKERS AND LACK OF SEGREGATION OF CARD HOLDER DATA

11. It is well known and the subject of many media reports that PII data is highly coveted and a frequent target of hackers.

12. Legitimate organizations and the criminal underground alike recognize the value in PII. Otherwise, they would not pay for it or aggressively seek it.

13. PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of thefts and unauthorized access have been the subject of many media reports. Unfortunately, and as will be alleged below, despite all of this publicly available knowledge of the continued compromises of PII, Defendants' approach at maintaining the privacy of Plaintiff's and Class Members' PII was lackadaisical, illegal, cavalier, reckless, and

negligent.

14. Unlike PII data, payment card data ("PCI") is heavily regulated. The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.

15. "PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data." PCI DSS v. 2 at 5 (2010) (hereafter PCI Version 2).

16. One PCI requirement is to protect stored cardholder data. Cardholder data includes Primary Account Number, Cardholder Name, Expiration Date, and Service Code. *Id*. at 7.

17. "Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement." *Id*. at 10. However, segregation is recommended because, among other reasons, "[i]t's not just cardholder data that's important; criminals are also after personally identifiable information (PII) and corporate data." *See* Verizon 2014 PCI ComplianceReport, available at http://www.nocash.info.ro/wp-content/uploads/2014/02/Verizon_pci-report-2014.pdf (hereafter "2014 Verizon Report"), at 54.

18. As noted in the 2014 Verizon Report, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users." *Id*. Similarly, in the Target data breach, in addition to PCI data pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 customers. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." *Id.* Illicitly obtained PII and PCI, sometimes aggregated from different data breaches, is sold on the black market, including on websites, as a product at a

set price. *See, e.g.*, <http://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth> (last visited March 4, 2014).

19. Moreover, PII of individuals with something in common is extremely valuable to criminals because it can help them perpetrate targeted spear phishing attacks. Spear phishers target select groups with something in common, i.e., they applied for credit cards at Capital One, so that they can send members of the group an email that looks just like an email from Capital One. But once recipients click on a link, they can be tricked into downloading malware on their own computers or deceived into giving up additional confidential information such as new passwords, financial information, personal data and much more.

THE DATA BREACH AFFECTING CAPITAL ONE

20. Plaintiff first became aware that her PII was at risk on July 30, 2019 via several news outlets, which was a day after the FBI charged Paige A. Thompson a/k/a "erratic" with a complaint for violations of 18 U.S.C. § 1030(a)(2). A copy of that criminal complaint is attached as Exhibit A (the "FBI Complaint"). According to news outlets, those that were subject to the hack if they had "applied for one of our credit card products from 2005 through early 2019." *See* http://press.capitalone.com/phoenix.zhtml?c=251626&p=irol-newsArticle&ID=2405043 (last accessed July 30, 2019). Indeed the PII that was stored by Capital One here was even more detailed than most: the PII additionally included customer status data, e.g., credit scores, credit limits, balances, payment history, contact information, among other information. *Id.*

21. Plaintiff McDonough had applied in January of 2019. By Capital One's own admissions, she was affected by the breach at the center of this lawsuit. The actual breach occurred on March 22 and 23, 2019. *Id.*

22. Plaintiff's PII, credit and financial information has been forever adversely

affected by this data breach proximately caused by Defendants.

23. According to Capital One, the hacker "exploit[ed] a specific configuration vulnerability in our infrastructure. When this was discovered, [Capital One] immediately addressed the configuration vulnerability and verified there are no other instances in [their] environment. Among other things, [Capital One] also augmented our routine automated scanning to look for this issue on a continuous basis." *Id.* Unfortunately for Plaintiff McDonough and the putative Class(es), "[d]ue to the particular circumstances of this incident, the unauthorized access also enabled the decrypting of data." *Id.*

24. Capital One claims "[t]he configuration vulnerability was reported to [them] by an external security researcher through our Responsible Disclosure Program on July 17, 2019." *Id.*

25. Nevertheless, the hacker infiltrated Capital One's deficient systems on March 22 and 23, 2019 and Defendants did not even know about it until a third party notified Capital One of the vulnerability.

26. By Defendants' own admission, the hacker(s) had access to Defendants' information systems, including Plaintiff's and the Class' PII, for four months without any detection of the infiltration.

27. Hacking is often accomplished in a series of phases to include reconnaissance, scanning for vulnerabilities and enumeration of the network, gaining access, escalation of user, computer and network privileges, maintaining access, covering tracks and placing backdoors. According to the FBI Complaint, the hacker "intentionally accessed a computer without authorization, to wit, a computer containing information contained in a financial record or a financial institutions and of a card issuer[.]" *See* Ex. A, p. 1. According to the FBI Complaint,

"[a] firewall misconfiguration permitted commands to reach and be executed by [a] server, which enabled access to folders or buckets of data in Capital One's storage space at the Cloud Computing Company." *See* Ex. A, p. 6. The factual allegations regarding the method, manner, and techniques used in the hack from the FBI Complaint are incorporated herein by reference, including those specifically outlined on pages 6-8 of the FBI Complaint.

28. It was Defendants duty to protect Plaintiff's PII and PCI data, and Defendants failed to do so. They unreasonably permitted her PII and PCI to be stored and in a manner that caused it to be publicly accessible which ultimately caused her damages. Defendants had highly deficient security measures in place that left Plaintiff and Class(es) members exposed in the cloud to the public through a fairly simple intrusion routine. No reasonable holder of PII and PCI data would have maintained such deficient and easily accessed systems for the public to access with the simple intrusion routine outlined in the FBI Complaint.

CONSEQUENCES OF DEFENDANTS' CONDUCT

29. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach.

30. The ramifications of Defendants' failure to keep class members' data secure are severe.

31. The information Defendants lost, including Plaintiff's identifying information and other financial information, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC"). FTC Interactive Toolkit, *Fighting Back Against Identity Theft*, available at <http://www.a2gov.org/government/safetyservices/Police/Documents/FTC%20identity%20theft%20guide.pdf> (last visited Jan. 27, 2014). Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address,

credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes. *Id.* The FTC estimates that as many as 10 million Americans have their identities stolen each year. *Id.*

32. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance." FTC, Signs of Identity Theft, available at <http://www.consumer.ftc.gov/articles/0271-signs-identity-theft> (last visited Jan. 21, 2014).

33. According to Javelin Strategy and Research, "1 in 4 data breach notification recipients became a victim of identity fraud." *See* 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available at <www.javelinstrategy.com/brochure/276 >(last visited Mar. 4, 2014) ("2013 Identity Fraud Report"). 46% of consumers with a breached debit card became fraud victims within the same year. *Id.*

34. Identity thieves can use personal information such as that pertaining to the Class, which Defendants failed to keep secure, to perpetrate a variety of crimes that harm the victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years.

35. In addition, identity thieves may get medical services using consumers' lost information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

36. It is incorrect to assume that reimbursing a consumer for fraud makes that

individual whole again. On the contrary, after conducting a study the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems." Victims of Identity Theft, 2012 (Dec. 2013) at 10, available at <http://www.bjs.gov/content /pub/pdf/vit12.pdf> (last visited Mar. 5, 2014). In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*. at 11.

37. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2008:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

The President's Identity Theft Task Force Report at p.21 (Oct. 21, 2008), available at <http://www.idtheft.gov/reports/StrategicPlan.pdf>.

38. Javelin Strategy and Research reports that those losses increased to $21 billion in 2013. *See* 2013 Identity Fraud Report.

39. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or payment card data is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a

> year or more before being used to commit identity theft. Further, once stolen data have 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.

GAO, *Report to Congressional Requesters*, at p.33 (June 2007), available at <http://www.gao.gov/new.items/d07737.pdf> (emphasis added).

40. The injuries Plaintiff and the Class(es) suffered as a direct result of the Data Breach include: (i) theft of personal and financial information; (ii) costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts; (iii) damages arising from the inability to use debit or credit card accounts because accounts were suspended or otherwise rendered unusable as a result of fraudulent charges, including but not limited cash back rewards; (iv) damages arising from the inability to withdraw or otherwise access funds because accounts were suspended, restricted, or otherwise rendered unusable as a result of the data breach, including, but not limited to, missed bill and loan payments, late-payment charges, and lowered credit scores and other adverse impacts on credit; (v) costs associated with spending time to address and mitigate the actual and future consequences of the breach such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, including, but not limited to, lost productivity, opportunities, and the inconvenience, nuisance and annoyance of dealing with all issues resulting from the Data Breach; (vi) the imminent and certainly impending injury resulting from the potential fraud and identity theft posed by PII and PCI being exposed for theft and sale on the internet; (vii) damages to and diminution in value of PII and PCI entrusted to Capital One for the sole purpose of purchasing products and services from Capital One; (viii) the loss of Plaintiffs and Class members' privacy; and (ix) other as yet unidentified harms.

CLASS ACTION ALLEGATIONS

41. Plaintiff seeks relief in her individual capacity and seeks to represent a class consisting of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiff seeks certification of classes initially defined as follows:

THE NATIONWIDE CLASS:

> All persons whose personal and/or financial information was disclosed in the data incursion affecting Capital One in 2019. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff (the "Class").

THE RHODE ISLAND SUBCLASS:

> All persons residing in Rhode Island whose personal and/or financial information was disclosed in the data incursion affecting Capital One in 2019. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff (the "Rhode Island Subclass," and collectively with the Class, the "Classes").

42. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class(es) are so numerous that the joinder of all members is impractical. While the exact number of Class(es) members is unknown to Plaintiff at this time, based on Capital One's admissions, it is over 10 million persons.

43. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost or disclosed Class(es) members' personal and/or financial information;

b. Whether Defendants unreasonably delayed in notifying affected customers of the data breach;

c. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach.

d. Whether Defendants' conduct was negligent;

e. Whether Defendants' negligence caused harm to Plaintiff and the Class(es); and

f. Plaintiff and the Class(es) are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

44. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class members because Plaintiff's information, like that of every other Class(es) member, was misused and/or disclosed by Defendants.

45. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the members of the Class(es). Plaintiff's Counsel are competent and experienced in litigating class actions.

46. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class(es) is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

47. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' violations of law

inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

48. Defendants have acted or refused to act on grounds that apply generally to the class, as alleged above, and certification is proper under Rule 23(b)(2).

FIRST COUNT
Negligence
(On Behalf of the Nationwide Class and the New Jersey Subclass)

49. Plaintiff incorporates the substantive allegations contained in all previous paragraphs as if fully set forth herein.

50. Plaintiff brings this claim individually and on behalf of the Class and the Rhode Island Subclass.

51. Defendants knowingly collected, came into possession of and maintained Plaintiff's PII and PCI (the "Private Information"), and had a duty to exercise reasonable care in safeguarding and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

52. Defendants had a duty to timely disclose that Plaintiff's Private Information within their possession might have been compromised.

53. Defendants had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's Private Information. It was Defendants duty to protect Plaintiff's Private Information, and Defendants failed to do so.

54. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff by failing to exercise reasonable care in protecting and safeguarding Plaintiff's Private Information within Defendants' possession. They unreasonably permitted her Private Information to be stored and in a manner that caused it to be publicly accessible. Defendants had

highly deficient security measures in place that left Plaintiff and Class(es) members exposed in the cloud to the public through a fairly simple intrusion routine. No reasonable holder of such Private Information, much less a bank, would have maintained such deficient and easily accessed systems for the public to access with the simple intrusion routine outlined in the FBI Complaint.

55. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's Private Information.

56. Defendants, through their actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and class members the fact that their Private Information within their possession might have been compromised.

57. Defendants' negligent and wrongful breach of their duties owed to Plaintiff and the Class proximately caused Plaintiff's and Class members' Private Information to be compromised.

58. Defendants' breach caused Plaintiff to suffer damages, including the need to set us monitoring services for her credit, loss of time and money monitoring her finances for future fraud, and caused her Private Information to be available on the internet and accessed by those with nefarious intent.

59. Plaintiff seeks the award of actual damages on behalf of the Class.

SECOND COUNT
Violations of State Data Breach Notice Statutes
(For the Class)

60. Plaintiff incorporates the substantive allegations contained in all previous paragraphs as if fully set forth herein.

61. Plaintiff brings this claim individually and on behalf of the Class and the Rhode Island Subclass.

62. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally require that any person or business conducting business within the state that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system to any resident of the state whose personal information was acquired by an unauthorized person, and further require that the disclosure of the breach be made in the most expedited time possible and without unreasonable delay.

63. Defendants' data breach constituted breach of Capital One's security system within the meaning of the below state data breach statutes and the data breached was protected and covered by the below breach statutes.

64. Plaintiff and Class(es) members' Private Information constitute personal information under and subject to the below state data breach statutes.

65. Defendants unreasonably delayed in informing the public, including Plaintiff and Class(es) members, about the breach of security of Plaintiff and Class members' confidential and Private Information after Defendants knew or should have known that the data breach occurred.

66. Defendants failed to disclose or notify the public of the data breach when, on or about late March of 2019, the hacker(s) gained access to Defendants data, which contained information including Plaintiff and Class members' Private Information.

67. As a direct and proximate result of Defendants' failure to provide, and the delay in providing, timely and accurate notice as required by the below state data breach statutes, Plaintiff and Class(es) members suffered harm. Had Defendants provided timely and accurate notice of the data breach, Plaintiff and Class members would have been able to

avoid, and/or attempt to ameliorate or mitigate the damages and harm resulting from Defendants' unreasonable delay to provide notice.

68. Defendants' failure to protect Plaintiff and Class(es) members' Private Information, and Defendants' failure to provide timely and accurate notice of the data breach violated the following state data breach statutes (including any revisions, modifications, and additions to these statutes):

a. Alaska Stat.§ 45.48.010(a), *et seq.;*

b. Ark. Code§ 4-110-105(a), *et seq.;*

c. Cal. Civ. Code § 1798.83(a), *et seq.;*

d. Colo. Rev. Stat.§ 6-1-716(2), *et seq.;*

e. Conn. Gen. Stat.§ 36a-701b(b), *et seq.;*

f. Del. Code Tit. 6 § 12B-102(a), *et seq.;*

g. D.C. Code§ 28-3852(a), *et seq.;*

h. Fla. Stat. § 501.171 (4), *et seq.;*

1. Ga. Code§ 10-1-912(a), *et seq.;*

j. Haw. Rev. Stat. § 487N-2(a), *et seq.;*

k. Idaho Code§ 28-51-105(a), *et seq.;*

I. 815 ILCS 530/1, *et seq.;*

m. Iowa Code § 715C.2(1), *et seq.;*

n. Kan. Stat.§ 50-7a02(a), *et seq.;*

o. Ky. Rev. Stat. § 365. 735(2), *et seq.;*

p. La. Rev. Stat.§ 51:3074(A), *et seq.;*

q. Md. Code, Commercial Law § 14-3504(b), *et seq.;*

r. Mass. Gen. Laws Ch. 93H § 3(a), *et seq.;*

s. Mich. Comp. Laws§ 445.72(a), *et seq.;*

t. Minn. Stat.§ 325E.61(1)(a), *et seq.;*

u. Mont. Code§ 30-14-1704(a), *et seq.;*

v. Neb. Rev. Stat.§ 87-803(a), *et seq.;*

w. Nev. Rev. Stat. § 603A.220(1), *et seq.;*

x. N.H. Rev. Stat.§ 359-C:20(1)(a), *et seq.;*

y. N.J. Stat.§ 56:8-163(a), *et seq.;*

z. N.C. Gen. Stat. § 75-65(a), *et seq.;*

aa. N.D. Cent. Code§ 51-30-02, *et seq.;*

bb. Okla. Stat. Tit. 24 § 163(A), *et seq.;*

cc. Or. Rev. Stat. § 646A.604(1), *et seq.;*

dd. R.I. Gen. Laws§ 11-49.3-4, *et seq.;*

ee. S.C. Code§ 39-1-90(A), *et seq.;*

ff. Tenn. Code§ 47-18-2107(b), *et seq.;*

gg. Tex. Bus. & Com. Code § 521.053(b), *et seq.;*

hh. Utah Code § 13-44-202(1), *et seq.;*

n. Va. Code§ 18.2-186.6(B), *et seq.;*

jj. Wash. Rev. Code§ 19.255.010(1), *et seq.;*

kk. Wis. Stat. § 134.98(2), *et seq.;*

11. Wyo. Stat. § 40-12-502(a), *et seq.*

69. Plaintiff and Class members seek all remedies available under their respective state data breach statutes, including but not limited to a) damages suffered by Plaintiff and Class(es) members as alleged above, (b) equitable relief, including injunctive relief, and c) reasonable

attorney fees and costs, as provided by law.

THIRD COUNT
Violation of Rhode Island Deceptive Trade Practices Act
(For the Rhode Island Subclass)

70. Plaintiff incorporates the substantive allegations contained in all previous paragraphs as if fully set forth herein.

71. Plaintiff brings this claim individually and on behalf of the Class and the Rhode Island Subclass.

72. Plaintiff, each Rhode Island Subclass Member, and Defendants are "persons" within the meaning of R.I.G.L. § 6-13.1-1.

73. The actions of Defendants, as alleged herein, constituted unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade and commerce in relation to the sale of credit card services within the meaning of R.I.G.L. § 6-13.1-2 and under the Rhode Island Deceptive Trade Practices Act ("RIDTPA").

74. Rhode Island law provides that Defendants have a duty to notify consumers subject to a data breach in the "most expedient time possible, but no later than forty-five (45) calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements contained in subsection (d) of this section[.]" R.I.G.L. § 11-49.3-4. Based upon public information, Defendants knew or should have known of the breach as of late March but waited until an unknown person emailed them to take any action on the breach.

75. Rhode Island law also provides "[i]n the event that more than five hundred (500) Rhode Island residents are to be notified, the municipal agency, state agency, or person shall notify the attorney general and the major credit reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals. Notification to

the attorney general and the major credit reporting agencies shall be made without delaying notice to affected Rhode Island residents." *Id.*

76. Defendants failed to so notify as they were required and thus they breached Rhode Island law related to data breach notices.

77. Had Defendants properly notified Plaintiff as they are required to do, at least some of Plaintiff's injuries could have been reduced as she would have been able to notify the appropriate authorities in a timely manner.

78. Rhode Island law also provides that Defendants "implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure and to preserve the confidentiality, integrity, and availability of such information" and "shall not retain personal information for a period longer than is reasonably required to provide the services requested; to meet the purpose for which it was collected; or in accordance with a written retention policy or as may be required by law" and "shall destroy all personal information, regardless of the medium that such information is in, in a secure manner, including, but not limited to, shredding, pulverization, incineration, or erasure." R.I.G.L. § 11-49.3-2.

79. Defendants failed to maintain the security required above, to preserve the confidentiality, integrity, and availability of it, and failed to destroy it when unneeded as required above, and instead, allowed it to be used against Plaintiff and the Rhode Island Subclass in violation of the RIDTPA.

80. Defendants have engaged in unconscionable commercial practices or deceptive

acts or practices when they obtained Plaintiff's and the Rhode Island Subclass's Private Information by false pretenses and failed to secure their Private Information as required and promised.

81. Plaintiff and the Rhode Island Subclass suffered damage and/or loss because Defendants' actions and inactions lacked honesty in fact, fair dealing, and good faith and because they had the capacity to deceive consumers acting reasonably, did deceive consumers acting reasonably, used deceptive representations, represented that the Private Information of Plaintiff and Rhode Island Subclass members was secure when it was not, . As such, their conduct violates the RIDTPA.

82. Defendants also knowingly omitted material facts to Plaintiff and the Rhode Island Subclass when they obtained their Private Information, promised to keep it securely, yet failed to keep it securely.

83. Due to Defendants' violation of the RIDTPA, Plaintiff and the Rhode Island Subclass have suffered ascertainable losses, and unless restrained, Rhode Island Subclass Members and others in the future will continue to suffer injury and harm.

JURY DEMAND

Plaintiff demands a trial by jury of all claims in this Complaint so triable.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class and the Rhode Island Subclass, respectfully request that the Court enter judgment in her favor and against Defendants, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her Counsel to represent the Class and the Rhode Island Subclass;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff and Class members; and to do whatever is necessary to correct the harm befallen Plaintiff and Class members;

C. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

D. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined;

E. For an award of punitive damages;

F. For an award of costs of suit and attorneys' fees, as allowable by law; and

G. Such other and further relief as this court may deem just and proper.

Dated: July 30, 2019

Respectfully submitted,

/s/ Steven T. Webster

Steven T. Webster
VSB No. 31975
WEBSTER BOOK LLP
300 N. Washington St., Suite 404
Alexandria, Virginia 22314
Telephone: (888) 987-9991
Facsimile: (888) 987-9991
swebster@websterbook.com

Of Counsel:

HENINGER GARRISON DAVIS, LLC
W. Lewis Garrison, Jr. (AL Bar No. ASB-3591-N74W)
Email: lewis@hgdlawfirm.com
Taylor C. Bartlett (AL Bar No. ASB-2365-A51B)
Email: taylor@hgdlawfirm.com
Christopher B. Hood (AL Bar No. ASB-2280-S35H)

2224 1st Avenue North
Birmingham, Alabama 35203
Telephone: (205) 326-3336
Facsimile: (205) 326-3332

James F. McDonough, III (GA Bar No. 117088)
Email: jmcdonough@hgdlawfirm.com
Jonathan R. Miller (GA Bar No. 507179)
Email: jmiller@hgdlawfirm.com
Travis E. Lynch (GA Bar No. 162373)
Email: tlynch@hgdlawfirm.com
3621 Vinings Slope, Suite 4320
Atlanta, Georgia 30339
Telephone: (404) 996-0869, -0863, -0867
Facsimile: (205) 326-5502, -5506, -5515

Attorneys for Plaintiff Rachel McDonough and the putative class