THE ROSEN LAW FIRM, P.A.
Phillip Kim, Esq. (PK 9384)
Laurence M. Rosen, Esq. (LR 5733)
275 Madison Ave., 40th Floor
New York, New York 10016
Telephone: (212) 686-1060
Fax: (212) 202-3827
Email: pkim@rosenlegal.com
lrosen@rosenlegal.com

Counsel for Plaintiff

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MARCUS MINSKY, Individually and On Behalf of All Others Similarly Situated, Plaintiff, v. CAPITAL ONE FINANCIAL CORPORATION, RICHARD FAIRBANK, and R. SCOTT BLACKLEY, Defendants.	Case No: CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS JURY TRIAL DEMANDED

Plaintiff Marcus Minsky ("Plaintiff"), individually and on behalf of all other persons similarly situated, by Plaintiff's undersigned attorneys, for Plaintiff's complaint against Defendants (defined below), alleges the following based upon personal knowledge as to Plaintiff and Plaintiff's own acts, and information and belief as to all other matters, based upon, inter alia, the investigation conducted by and through Plaintiff's attorneys, which included, among other things, a review of Defendants' public documents, conference calls and announcements made by Defendants, United States Securities and Exchange Commission ("SEC") filings, wire and press releases published by and regarding Capital One Financial Corporation ("Capital One" or the "Company"), analysts' reports and advisories about the

Company, and information readily obtainable on the Internet. Plaintiff believes that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

NATURE OF THE ACTION

1. This is a federal securities class action on behalf of a class consisting of all persons other than Defendants who purchased or otherwise acquired Capital One securities between February 2, 2018 and June 29, 2019, both dates inclusive (the "Class Period"). Plaintiff seeks to recover compensable damages caused by Defendants' violations of the federal securities laws and to pursue remedies under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the "Exchange Act") and Rule 10b-5 promulgated thereunder.

JURISDICTION AND VENUE

2. The claims asserted herein arise under and pursuant to Sections 10(b) and 20(a) of the Exchange Act (15 U.S.C. §§ 78j(b) and 78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17 C.F.R. § 240.10b-5).

3. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331, and Section 27 of the Exchange Act (15 U.S.C. §78aa).

4. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) and Section 27 of the Exchange Act (15 U.S.C. § 78aa(c)) as the alleged misstatements entered and the subsequent damages took place in this judicial district.

5. In connection with the acts, conduct and other wrongs alleged in this complaint, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including but not limited to, the United States mails, interstate telephone communications and the facilities of the national securities exchange.

PARTIES

6. Plaintiff, as set forth in the accompanying Certification, purchased Capital One securities at artificially inflated prices during the Class Period and was damaged upon the revelation of the alleged corrective disclosure.

7. Defendant Capital One operates as the bank holding company for the Capital One Bank (USA), National Association and Capital One, National Association, which provides various financial products and services in the United States, the United Kingdom, and Canada. Capital One is incorporated in Delaware, and its principal executive offices are located in Virginia. Capital One's common stock trades on the New York Stock Exchange ("NYSE") under the ticker symbol "COF."

8. Defendant Richard Fairbank ("Fairbank") founded the Company and served as the Company's Chief Executive Officer ("CEO") and President during the Class Period.

9. Defendant R. Scott Blackley ("Blackley") has served as the Company's Chief Financial Officer ("CFO") during the Class Period.

10. Defendants Fairbank and Blackley are collectively referred to herein as the "Individual Defendants."

11. Each of the Individual Defendants:

(a) directly participated in the management of the Company;

(b) was directly involved in the day-to-day operations of the Company at the highest levels;

(c) was privy to confidential proprietary information concerning the Company and its business and operations;

(d) was directly or indirectly involved in drafting, producing, reviewing and/or disseminating the false and misleading statements and information alleged herein;

(e) was directly or indirectly involved in the oversight or implementation of the Company's internal controls;

(f) was aware of or recklessly disregarded the fact that the false and misleading statements were being issued concerning the Company; and/or

(g) approved or ratified these statements in violation of the federal securities laws.

12. The Company is liable for the acts of the Individual Defendants and its employees under the doctrine of *respondeat superior* and common law principles of agency because all of the wrongful acts complained of herein were carried out within the scope of their employment.

13. The scienter of the Individual Defendants and other employees and agents of the Company is similarly imputed to the Company under *respondeat superior* and agency principles.

14. The Company and the Individual Defendants are collectively referred to herein as "Defendants."

SUBSTANTIVE ALLEGATIONS

Materially False and Misleading Statements Issued During the Class Period

15. Capital One's Online & Mobile Privacy Statement (the "Privacy Statement"), last updated May 1, 2014 and found on its website throughout the Class Period at

https://www.capitalone.com/identity-protection/privacy/statement, advised Capital One users, in part, the following regarding information security:

> 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.***

(Emphasis added).

16. The Class Period beings on February 21, 2018, when Capital One filed an annual report on Form 10-K with the SEC, announcing the Company's financial and operating results for the year ended December 31, 2017 (the "2017 10-K"). The 2017 10-K was signed by Defendant Fairbank and Blackley. The 2017 10-K contained signed certifications pursuant to the Sarbanes-Oxley Act of 2002 ("SOX") by Defendants Fairbank and Blackley, attesting to the accuracy of financial reporting, the disclosure of any material changes to the Company's internal control over financial reporting and the disclosure of all fraud.

17. The 2017 10-K stated, in relevant part, the following regarding information security:

> ***We safeguard our customers' and our own information and technology, implement backup and recovery systems, and generally require the same of our third-party service providers. We take measures that mitigate against known attacks and use internal and external resources to scan for vulnerabilities in platforms, systems, and applications necessary for delivering Capital One products and services.***
>
> * * *
>
> Our products and services involve the gathering, authentication, management, processing, storage and transmission of sensitive and confidential information regarding our customers and their accounts, our employees and third parties with which we do business. Our ability to provide such products and services, many of which are web-based, depends upon the management and safeguarding of information, software, methodologies and business secrets. To provide these products and services to, as well as communicate with, our customers, we rely on

information systems and infrastructure, including digital technologies, computer and email systems, software, networks and other web-based technologies, that we and third-party service providers operate. We also have arrangements in place with third parties through which we share and receive information about their customers who are or may become our customers.

Like other financial services firms, technologies, systems, networks and devices of Capital One or our customers, employees, service providers or other third parties with whom we interact continue to be the subject of attempted unauthorized access, mishandling or misuse of information, denial-of-service attacks, computer viruses, website defacement, hacking, malware, ransomware, phishing or other forms of social engineering, and other forms of cyber-attacks designed to obtain confidential information, destroy data, disrupt or degrade service, sabotage systems or cause other damage, and other events. These threats may derive from human error, fraud or malice on the part of our employees, insiders or third parties or may result from accidental technological failure. Any of these parties may also attempt to fraudulently induce employees, customers, or other third-party users of our systems to disclose sensitive information in order to gain access to our data or that of our customers or third parties with whom we interact. Further, cyber and information security risks for large financial institutions like us have generally increased in recent years in part because of the proliferation of new technologies, the use of the internet and telecommunications technologies to conduct financial transactions, and the increased sophistication and activities of organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments and other external parties. In addition, our customers access our products and services using computers, smartphones, tablets, and other mobile devices that are beyond our security control systems.

The methods and techniques employed by perpetrators of fraud and others to attack, disable, degrade or sabotage platforms, systems and applications change frequently, are increasingly sophisticated and often are not fully recognized or understood until after they have occurred, and some techniques could occur and persist for an extended period of time before being detected. As a result, we and our third-party service providers and partners may be unable to anticipate or identify certain attack methods in order to implement effective preventative measures or mitigate or remediate the damages caused in a timely manner. We may also be unable to hire and develop talent capable of detecting, mitigating or remediating these risks. Although we believe we have a robust suite of authentication and layered information security controls, including our cyber threat analytics, data encryption and tokenization technologies, anti-malware defenses and vulnerability management program, any one or combination of these controls could fail to detect, mitigate or remediate these risks in a timely manner. We may face an increasing number of attempted cyber-attacks as we expand our mobile- and other internet-based products and services, as well as our usage of

> mobile and cloud technologies and as we provide more of these services to a greater number of retail clients.
>
> A disruption or breach, including as a result of a cyber-attack, or media reports of perceived security vulnerabilities at Capital One or at third-party service providers, could result in significant legal and financial exposure, regulatory intervention, remediation costs, card reissuance, supervisory liability, damage to our reputation or loss of confidence in the security of our systems, products and services that could adversely affect our business. We and other U.S. financial services providers continue to be targeted with evolving and adaptive cybersecurity threats from sophisticated third parties. Although we have not experienced any material losses relating to cyber incidents, there can be no assurance that unauthorized access or cyber incidents will not occur or that we will not suffer such losses in the future. Unauthorized access or cyber incidents could occur more frequently and on a more significant scale. If future attacks like these are successful or if customers are unable to access their accounts online for other reasons, it could adversely impact our ability to service customer accounts or loans, complete financial transactions for our customers or otherwise operate any of our businesses or services. In addition, a breach or attack affecting one of our third-party service providers or partners could harm our business even if we do not control the service that is attacked.
>
> (Emphasis added.)

18. On February 20, 2019, Capital One filed an annual report on Form 10-K with the SEC, announcing the Company's financial and operating results for the year ended December 31, 2018 (the "2018 10-K"). The 2018 10-K was signed by Defendants Fairbank and Blackley. The 2018 10-K contained signed SOX certifications by Defendants Fairbank and Blackley, attesting to the accuracy of financial reporting, the disclosure of any material changes to the Company's internal control over financial reporting and the disclosure of all fraud.

19. The 2018 10-K stated, in relevant part, the following regarding information security:

> ***We safeguard our customers' and our own information and technology, implement backup and recovery systems, and generally require the same of our third-party service providers. We take measures that mitigate against known attacks and use internal and external resources to scan for vulnerabilities in platforms, systems, and applications necessary for delivering Capital One products and services.***

* * *

Our products and services involve the gathering, authentication, management, processing, storage and transmission of sensitive and confidential information regarding our customers and their accounts, our employees and third parties with which we do business. Our ability to provide such products and services, many of which are web-based, depends upon the management and safeguarding of information, software, methodologies and business secrets. To provide these products and services to, as well as communicate with, our customers, we rely on information systems and infrastructure, including digital technologies, computer and email systems, software, networks and other web-based technologies, that we and third-party service providers operate. We also have arrangements in place with third parties through which we share and receive information about their customers who are or may become our customers.

Like other financial services firms, technologies, systems, networks and devices of Capital One or our customers, employees, service providers or other third parties with whom we interact continue to be the subject of attempted unauthorized access, mishandling or misuse of information, denial-of-service attacks, computer viruses, website defacement, hacking, malware, ransomware, phishing or other forms of social engineering, and other forms of cyber-attacks designed to obtain confidential information, destroy data, disrupt or degrade service, sabotage systems or cause other damage, and other events. These threats may derive from human error, fraud or malice on the part of our employees, insiders or third parties or may result from accidental technological failure. Any of these parties may also attempt to fraudulently induce employees, customers, or other third-party users of our systems to disclose sensitive information in order to gain access to our data or that of our customers or third parties with whom we interact. Further, cyber and information security risks for large financial institutions like us have generally increased in recent years in part because of the proliferation of new technologies, the use of the internet and telecommunications technologies to conduct financial transactions, and the increased sophistication and activities of organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments and other external parties. In addition, our customers access our products and services using computers, smartphones, tablets, and other mobile devices that are beyond our security control systems.

The methods and techniques employed by perpetrators of fraud and others to attack, disable, degrade or sabotage platforms, systems and applications change frequently, are increasingly sophisticated and often are not fully recognized or understood until after they have occurred, and some techniques could occur and persist for an extended period of time before being detected. As a result, we and our third-party service providers and partners may be unable to anticipate or identify certain attack methods in order to implement effective preventative measures or mitigate or remediate the damages caused in a timely manner. We may also be unable to hire and develop talent capable of detecting, mitigating or

> remediating these risks. Although we believe we have a robust suite of authentication and layered information security controls, including our cyber threat analytics, data encryption and tokenization technologies, anti-malware defenses and vulnerability management program, any one or combination of these controls could fail to detect, mitigate or remediate these risks in a timely manner. We may face an increasing number of attempted cyber-attacks as we expand our mobile- and other internet-based products and services, as well as our usage of mobile and cloud technologies and as we provide more of these services to a greater number of retail clients.
>
> A disruption or breach, including as a result of a cyber-attack, or media reports of perceived security vulnerabilities at Capital One or at third-party service providers, could result in significant legal and financial exposure, regulatory intervention, remediation costs, card reissuance, supervisory liability, damage to our reputation or loss of confidence in the security of our systems, products and services that could adversely affect our business. We and other U.S. financial services providers continue to be targeted with evolving and adaptive cybersecurity threats from sophisticated third parties. Although we have not experienced any material losses relating to cyber incidents, there can be no assurance that unauthorized access or cyber incidents will not occur or that we will not suffer such losses in the future. Unauthorized access or cyber incidents could occur more frequently and on a more significant scale. If future attacks like these are successful or if customers are unable to access their accounts online for other reasons, it could adversely impact our ability to service customer accounts or loans, complete financial transactions for our customers or otherwise operate any of our businesses or services. In addition, a breach or attack affecting one of our third-party service providers or partners could harm our business even if we do not control the service that is attacked.
>
> (Emphasis added.)

20. The statements contained in ¶¶15-20 were materially false and/or misleading because they misrepresented and/or failed to disclose the following adverse facts pertaining to the Company's business, operational and financial results, which were known to Defendants or recklessly disregarded by them. Specifically, Defendants made false and/or misleading statements and/or failed to disclose that: (1) the Company did not maintain robust information security protections, and its protection did not shield personal information against security breaches; (2) such deficiencies heightened the Company's exposure to a cyber-attack; and (3) as

a result, Capital One's public statements were materially false and misleading at all relevant times.

THE TRUTH EMERGES

21. On July 29, 2019, after the market closed, Capital One announced in a press release that on July 19, 2019, Capital One suffered a data breach affecting over 106 million individuals in the United States and Canada. The Company stated, in pertinent part:

> MCLEAN, Va., July 29, 2019 /PRNewswire/ -- Capital One Financial Corporation (NYSE: COF) announced today that ***on July 19, 2019, it determined there was unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for its credit card products and to Capital One credit card customers.***
>
> Capital One immediately fixed the configuration vulnerability that this individual exploited and promptly began working with federal law enforcement. The FBI has arrested the person responsible and that person is in custody. Based on our analysis to date, we believe it is unlikely that the information was used for fraud or disseminated by this individual. However, we will continue to investigate.
>
> "While I am grateful that the perpetrator has been caught, I am deeply sorry for what has happened," said Richard D. Fairbank, Chairman and CEO. "I sincerely apologize for the understandable worry this incident must be causing those affected and I am committed to making it right."
>
> ***Based on our analysis to date, this event affected approximately 100 million individuals in the United States and approximately 6 million in Canada***.
>
> Importantly, no credit card account numbers or log-in credentials were compromised and over 99 percent of Social Security numbers were not compromised.
>
> The largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019. This information included personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income. Beyond the credit card application data, the individual also obtained portions of credit card customer data, including:

> • Customer status data, e.g., credit scores, credit limits, balances, payment history, contact information
>
> • Fragments of transaction data from a total of 23 days during 2016, 2017 and 2018
>
> No bank account numbers or Social Security numbers were compromised, other than:
>
> • About 140,000 Social Security numbers of our credit card customers
>
> • About 80,000 linked bank account numbers of our secured credit card customers
>
> For our Canadian credit card customers, approximately 1 million Social Insurance Numbers were compromised in this incident.
>
> We will notify affected individuals through a variety of channels. We will make free credit monitoring and identity protection available to everyone affected.
>
> Safeguarding our customers' information is essential to our mission and our role as a financial institution. We have invested heavily in cybersecurity and will continue to do so. We will incorporate the learnings from this incident to further strengthen our cyber defenses.
>
> (Emphasis added.)

22. According to the criminal complaint brought by the Federal Bureau of Investigation against Paige A. Thompson, the purported hacker, though some of the data was tokenized or encrypted, "data including applicants' names, addresses, dates of birth and information regarding their credit history ha[d] not been tokenized." *United States of America v. Paige A. Thompson, a/k/a "erratic"*, Case No. MJ19-0344 (W.D. Wash. Jul. 29, 2019) (Compl. at 8).

23. On this news, shares of Capital One fell $5.71 or nearly 5.9% over to close at $91.21 on July 30, 2019.

24. As a result of Defendants' wrongful acts and omissions, and the precipitous decline in the market value of the Company's securities, Plaintiff and other Class members have suffered significant losses and damages.

PLAINTIFF'S CLASS ACTION ALLEGATIONS

25. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of a Class, consisting of all those who purchased or otherwise acquired Capital One securities traded on the NYSE during the Class Period (the "Class"); and were damaged upon the revelation of the alleged corrective disclosures. Excluded from the Class are Defendants herein, the officers and directors of the Company, at all relevant times, members of their immediate families and their legal representatives, heirs, successors or assigns and any entity in which Defendants have or had a controlling interest.

26. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, Capital One securities were actively traded on the NYSE. While the exact number of Class members is unknown to Plaintiff at this time and can be ascertained only through appropriate discovery, Plaintiff believes that there are hundreds or thousands of members in the proposed Class. Record owners and other members of the Class may be identified from records maintained by Capital One or its transfer agent and may be notified of the pendency of this action by mail, using the form of notice similar to that customarily used in securities class actions.

27. Plaintiff's claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by defendants' wrongful conduct in violation of federal law that is complained of herein.

28. Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class and securities litigation. Plaintiff has no interests antagonistic to or in conflict with those of the Class.

29. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the questions of law and fact common to the Class are:

- whether the Exchange Act were violated by Defendants' acts as alleged herein;
- whether statements made by Defendants to the investing public during the Class Period misrepresented material facts about the financial condition and business of Capital One;
- whether Defendants' public statements to the investing public during the Class Period omitted material facts necessary to make the statements made, in light of the circumstances under which they were made, not misleading;
- whether the Defendants caused Capital One to issue false and misleading SEC filings during the Class Period;
- whether Defendants acted knowingly or recklessly in issuing false and SEC filing
- whether the prices of Capital One securities during the Class Period were artificially inflated because of the Defendants' conduct complained of herein; and
- whether the members of the Class have sustained damages and, if so, what is the proper measure of damages.

30. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as

the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

31. Plaintiff will rely, in part, upon the presumption of reliance established by the fraud-on-the-market doctrine in that:

- Capital One shares met the requirements for listing, and were listed and actively traded on NYSE, a highly efficient and automated market;
- As a public issuer, Capital One filed periodic public reports with the SEC and NYSE;
- Capital One regularly communicated with public investors via established market communication mechanisms, including through the regular dissemination of press releases via major newswire services and through other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services; and
- Capital One was followed by a number of securities analysts employed by major brokerage firms who wrote reports that were widely distributed and publicly available.

32. Based on the foregoing, the market for Capital One securities promptly digested current information regarding Capital One from all publicly available sources and reflected such information in the prices of the shares, and Plaintiff and the members of the Class are entitled to a presumption of reliance upon the integrity of the market.

33. Alternatively, Plaintiff and the members of the Class are entitled to the presumption of reliance established by the Supreme Court in *Affiliated Ute Citizens of the State of Utah v. United States*, 406 U.S. 128 (1972), as Defendants omitted material information in their Class Period statements in violation of a duty to disclose such information as detailed above.

COUNT I

For Violations of Section 10(b) And Rule 10b-5 Promulgated Thereunder Against All Defendants

34. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

35. This Count is asserted against Defendants is based upon Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the SEC.

36. During the Class Period, Defendants, individually and in concert, directly or indirectly, disseminated or approved the false statements specified above, which they knew or deliberately disregarded were misleading in that they contained misrepresentations and failed to disclose material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

37. Defendants violated §10(b) of the 1934 Act and Rule 10b-5 in that they:

- employed devices, schemes and artifices to defraud;
- made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or
- engaged in acts, practices and a course of business that operated as a fraud or deceit upon plaintiff and others similarly situated in connection with their purchases of Capital One securities during the Class Period.

38. Defendants acted with scienter in that they knew that the public documents and statements issued or disseminated in the name of Capital One were materially false and misleading; knew that such statements or documents would be issued or disseminated to the investing public; and knowingly and substantially participated, or acquiesced in the issuance or dissemination of such statements or documents as primary violations of the securities laws. These defendants by virtue of their receipt of information reflecting the true facts of Capital One, their control over, and/or receipt and/or modification of Capital One's allegedly materially misleading statements, and/or their associations with the Company which made them privy to confidential proprietary information concerning Capital One, participated in the fraudulent scheme alleged herein.

39. Individual Defendants, who are the senior officers and/or directors of the Company, had actual knowledge of the material omissions and/or the falsity of the material statements set forth above, and intended to deceive Plaintiff and the other members of the Class, or, in the alternative, acted with reckless disregard for the truth when they failed to ascertain and disclose the true facts in the statements made by them or other Capital One personnel to members of the investing public, including Plaintiff and the Class.

40. As a result of the foregoing, the market price of Capital One securities was artificially inflated during the Class Period. In ignorance of the falsity of Defendants' statements, Plaintiff and the other members of the Class relied on the statements described above and/or the integrity of the market price of Capital One securities during the Class Period in purchasing Capital One securities at prices that were artificially inflated as a result of Defendants' false and misleading statements.

41. Had Plaintiff and the other members of the Class been aware that the market price of Capital One securities had been artificially and falsely inflated by Defendants' misleading statements and by the material adverse information which Defendants did not disclose, they would not have purchased Capital One securities at the artificially inflated prices that they did, or at all.

42. As a result of the wrongful conduct alleged herein, Plaintiff and other members of the Class have suffered damages in an amount to be established at trial.

43. By reason of the foregoing, Defendants have violated Section 10(b) of the 1934 Act and Rule 10b-5 promulgated thereunder and are liable to the plaintiff and the other members of the Class for substantial damages which they suffered in connection with their purchase of Capital One securities during the Class Period.

COUNT II
Violations of Section 20(a) of the Exchange Act
Against the Individual Defendants

44. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

45. During the Class Period, the Individual Defendants participated in the operation and management of Capital One, and conducted and participated, directly and indirectly, in the conduct of Capital One's business affairs. Because of their senior positions, they knew the adverse non-public information about Capital One's misstatement of revenue and profit and false financial statements.

46. As officers and/or directors of a publicly owned company, the Individual Defendants had a duty to disseminate accurate and truthful information with respect to Capital One's financial condition and results of operations, and to correct promptly any public statements issued by Capital One which had become materially false or misleading.

47. Because of their positions of control and authority as senior officers, the Individual Defendants were able to, and did, control the contents of the various reports, press releases and public filings which Capital One disseminated in the marketplace during the Class Period concerning Capital One's results of operations. Throughout the Class Period, the Individual Defendants exercised their power and authority to cause Capital One to engage in the wrongful acts complained of herein. The Individual Defendants therefore, were "controlling persons" of Capital One within the meaning of Section 20(a) of the Exchange Act. In this capacity, they participated in the unlawful conduct alleged which artificially inflated the market price of Capital One securities.

48. By reason of the above conduct, the Individual Defendants are liable pursuant to Section 20(a) of the Exchange Act for the violations committed by Capital One.

PRAYER FOR RELIEF

WHEREFORE, plaintiff, on behalf of himself and the Class, prays for judgment and relief as follows:

(a) declaring this action to be a proper class action, designating plaintiff as Lead Plaintiff and certifying plaintiff as a class representative under Rule 23 of the Federal Rules of Civil Procedure and designating plaintiff's counsel as Lead Counsel;

(b) awarding damages in favor of plaintiff and the other Class members against all defendants, jointly and severally, together with interest thereon;

awarding plaintiff and the Class reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

(d) awarding plaintiff and other members of the Class such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury.

Dated: October 2, 2019

Respectfully submitted,

THE ROSEN LAW FIRM, P.A.

By:/s/Phillip Kim
Phillip Kim, Esq. (PK 9384)
Laurence M. Rosen, Esq. (LR 5733)
275 Madison Avenue, 40th Floor
New York, NY 10016
Telephone: (212) 686-1060
Fax: (212) 202-3827
Email: pkim@rosenlegal.com
lrosen@rosenlegal.com

Counsel for Plaintiff