UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KEVIN ZOSIAK, individually and on behalf of all those similarly situated, Plaintiffs, v. CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE, N.A., and CAPITAL ONE BANK (USA), N.A., Defendants.	Civil Action No. 19-2265 **COMPLAINT and DEMAND FOR JURY TRIAL**

Plaintiff Kevin Zosiak ("Plaintiff"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following, against Defendants Capital One Financial Corporation, Capital One, N.A., and Capital One Bank (USA), N.A. (collectively, "Capital One" or "Defendants"). Based upon personal knowledge, information, belief, and investigation of counsel, Plaintiff specifically alleges as follows:

SUMMARY OF THE CASE

1. Plaintiff brings this action on behalf of a nationwide class against Defendants because of their failure to protect the confidential information of millions of consumers and small businesses – including financial information (*e.g.*, bank account numbers, fragments of transaction history, self-reported income, and credit scores), and/or personal information (*e.g.*, Social Security Numbers, names, addresses, phone numbers, email addresses, and dates of birth) (collectively, their "Sensitive Information"). Defendants' wrongful disclosure has harmed Plaintiff and the Class, believed to include approximately 106 million card customers and applicants.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) in that: (1) this is a class action involving more than 1,000 class members; (2) minimal diversity is present as Plaintiff is a citizen of Connecticut (and the proposed class members are from various states), while Defendants are citizens of Virginia; and (3) the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs.

3. This Court has personal jurisdiction over Defendants because Defendants conduct business in and throughout the District of Columbia, and the wrongful acts alleged in this Complaint were committed in the District of Columbia, among other venues.

4. Venue is proper in this District pursuant to: (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, and (2) 28 U.S.C. § 1391(b)(3) in that Defendants are subject to personal jurisdiction in this District.

PARTIES

5. Plaintiff Kevin Zosiak is an individual residing in Stamford, Connecticut, who has been a credit card customer for Capital One and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

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

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

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

FACTUAL BACKGROUND

9. Defendant Capital One Financial Corporation, through its subsidiaries, including Defendants Capital One, N.A., and Capital One Bank (USA), N.A., is one of the largest credit-card issuers in the United States, and one of the top 10 largest banks based on deposits, serving approximately 45 million customer accounts.

10. On July 29, Capital One publicly announced the following:

> [O]n 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 . . . . Based on our **analysis to date**, this event affected approximately 100 million individuals in the United States and approximately 6 million in Canada.
> . . .
> The largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019.[1]

11. Capital One further disclosed that the breached Sensitive Information included:

a. Personal information, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self reported income;

b. Customer status data, *e.g.*, credit scores, credit limits, balances, payment history, contact information;

[1] *Capital One Announces Data Security Incident*, Capital One, http://phx.corporate-ir.net/phoenix.zhtml?c=70667&p=irol-newsArticle_Print&ID=2405042 (emphasis added).(last accessed July 29, 2019).

c. Fragments of transactional data from a total of 23 days during 2016, 2017, and 2018;

d. About 140,000 Social Security numbers of its credit card customers; and

e. About 80,000 linked bank account numbers of its secured credit card customers.

12. The Data Breach that had occurred on March 22 and 23, 2019, was discovered by Defendants only in July 19, 2019 and publicly disclosed on July 29, 2019, over four months after the Sensitive Information of over 100 million customers and credit card applicants were breached. Defendants apparently continued to allow the hacker to intrude their systems at least until April 21, 2019.

13. Defendants only discovered the Data Breach after an individual previously unknown to Capital One sent the following email to Capital One providing a link to a file containing the leaked Sensitive Information. The file provided in the link, which was timestamped April 21, 2019, also contained code for commands used in the intrusion, as well as a list of more than 700 folders or buckets of data.

Capital One

Responsible Disclosure (Shared) <responsiblediscloure@capitalone.com>

[External Sender] Leaked s3 data

[redacted] Wed, Jul 17, 2019 at 1:25 AM

To: "responsiblediscloure@capitalone.com" <responsiblediscloure@capitalone.com>

Hello there,

There appears to be some leaked s3 data of yours in someone's github / gist:

https://gist.github.com/[redacted]

Let me know if you want help tracking them down.

Thanks,

[redacted]

14. Defendants had obligations, arising from promises made to its credit card applicants and customers like Plaintiff and other Class Members, and based on industry standards, to keep the Sensitive Information confidential and to protect it from unauthorized

disclosures. Class Members provided their Sensitive Information to Capital One with the understanding that Capital One and any business partners to whom Capital One disclosed the Sensitive Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

15. Capital One promises customers that it will keep their Sensitive Information confidential, assuring customers on its credit card applications explicitly that "Capital One uses 256-bit Secure Sockets Layer (SSL) technology. This means that when you are on our website, the data transferred between Capital One and you is encrypted and **cannot be viewed by any other party.**"[2]

16. Defendants' security failures demonstrate that they failed to honor their duties and promises by not:

a. maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. adequately monitoring its system to identify the data breaches and cyber-attacks; and

c. adequately protecting Plaintiff's and the Class's Sensitive Information.

17. Plaintiff and other Class Members have been injured by the disclosure of their Sensitive Information in the Data Breach.

18. Defendants' data security obligations and promises were particularly important given the substantial increase in data breaches, which were widely known to the public and to anyone in Defendants' industries.

[2] *See e.g.,* Application for Venture Credit Card, https://applynow.capitalone.com/?productId=6691 (last visited July 29, 2019) (emphasis added).

19. Defendants had ample warnings of weaknesses and risks to its systems, as they have had multiple security breaches in the past. On or about January 2018, Capital One suffered a data breach that compromised 50GB worth of sensitive data that contained highly sensitive information that put Capital One's network at significant risk. In addition, Defendants have issued formal letters to an undisclosed number of their customers informing that their personal information may have been breached, in numerous other occasions including the letters issued on or about November 2014, July 28, 2017, July 31, 2017, and September 12, 2017.

20. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in a person's name.[3] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

21. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[4]

22. Identity theft victims frequently are required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information such as social security numbers ("SSNs") for a variety of crimes, including credit card fraud, phone or utilities fraud, and/or bank/finance fraud.

[3] *See* U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (2007).
[4] *Id.*, at 2, 9.

23. There may be a time lag between when Sensitive Information is stolen and when it is used. According to the GAO Report:

> [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.[5]

24. With access to an individual's Sensitive Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name. Identity thieves may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[6]

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

[5] *Id.*, at 29 (emphasis added).
[6] *See Warning Signs of Identity Theft*, Federal Trade Commissions, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed July 29, 2019).

26. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole. Financial databases are especially valuable to identity thieves.

CLASS ALLEGATIONS

27. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiff brings this case as a class action on behalf of a Class defined as follows:

> All persons in the United States whose Sensitive Information was maintained on the servers of Capital One and the cloud computing company used by Capital One that were compromised as a result of the breach announced by Capital One on or around July 29, 2019.

28. The Class is so numerous that joinder of all members is impracticable. On information and belief, the Class has more than 106 million members. Moreover, the disposition of the claims of the Class in a single action will provide substantial benefits to all parties and the Court.

29. There are numerous questions of law and fact common to Plaintiff and Class Members. These common questions of law and fact include, but are not limited to, the following:

a. Whether Defendants' data security systems prior to the Data Breach complied with all applicable legal requirements;

b. Whether Defendants' data security systems prior to the Data Breach met industry standards;

c. Whether Plaintiff's and other Class members' Sensitive Information was compromised in the Data Breach; and

d. Whether Plaintiff's and other Class members are entitled to damages as a result of Defendant's conduct.

30. Plaintiff's claims are typical of the claims of the Class's claims. Plaintiff suffered the same injury as Class Members – *i.e.* upon information and belief, Plaintiff's Sensitive information was compromised in the Data Breach.

31. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel have interests that are contrary to or that conflict with those of the proposed Class.

32. Defendants have engaged in a common course of conduct toward Plaintiff and other Class Members. The common issues arising from this conduct that affect Plaintiff and Class Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

33. A class action is the superior method for the fair and efficient adjudication of this controversy. Class Members' interests in individually controlling the prosecution of separate actions are low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendants. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Defendants' records and the records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove Plaintiff's claims.

34. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendants have acted or refused to act on grounds that apply generally to Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class Members.

FIRST COUNT
Negligence

35. Plaintiff realleges and incorporates by reference all preceding factual allegations.

36. Capital One required Plaintiff and Class Members to submit non-public Sensitive Information to apply for a credit card.

37. By collecting and storing this data, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard this Sensitive Information, to prevent disclosure of the information, and to guard the information from theft.

38. Defendants' duty included a responsibility to implement a process by which they could detect a breach of their security systems in a reasonably expeditious period of time and give prompt notice to those affected in the case of a data breach.

39. Defendants also owed a duty of care to Plaintiff and members of the Class to provide security consistent with industry standards and the other requirements discussed herein, and to ensure that their systems and networks—and the personnel responsible for them adequately protected their potential customers' and customers' Sensitive Information.

40. Only Defendants were in a position to ensure that their systems were sufficient to protect against the harm to Plaintiff and the members of the Class from a data breach.

41. Defendants breached their duty by failing to use reasonable measures to protect Plaintiff's and Class Members' Sensitive Information.

42. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Sensitive Information;

b. failing to adequately monitor the security of their networks and systems;

c. allowing unauthorized access to Plaintiff's and Class Members' Sensitive Information; and

d. failing to recognize in a timely manner that Plaintiff's and other Class Members' Sensitive Information had been compromised.

43. It was foreseeable that Defendants' failure to use reasonable measures to protect and monitor the security of Sensitive Information would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

44. It was therefore foreseeable that the failure to adequately safeguard Sensitive Information would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

45. Accordingly, Plaintiff, individually and on behalf of all those similarly situated, seeks an order declaring that Defendants' conduct constitutes negligence and awarding damages in an amount to be determined at trial.

SECOND COUNT
Negligence Per Se

46. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

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

48. Capital One violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and not complying with industry standards.

49. Capital One's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

50. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

51. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

52. As a direct and proximate result of Capital One's negligence, 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.

THIRD COUNT
Breach of Implied Contract

53. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

54. When Plaintiff and Class members paid money and provided their Sensitive Information to Defendants in exchange for services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

55. Defendants solicited and invited prospective clients and other consumers to provide their Sensitive Information as part of its regular business practices. These individuals accepted Defendants' offers and provided their Sensitive Information to Defendants. In entering into such implied contracts, Plaintiff and the Class assumed that Defendants' data security practices and policies were reasonable and consistent with industry standards, and that Defendants would use part of the funds received from Plaintiff and the Class to pay for adequate and reasonable data security practices.

56. Plaintiff and the Class would not have provided and entrusted their Sensitive Information to Defendants in the absence of the implied contract between them and Defendants to keep the information secure.

57. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendants.

58. Defendants breached their implied contracts with Plaintiff and the Class by failing to safeguard and protect their Sensitive Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data breach.

59. As a direct and proximate result of Defendants' breaches of their implied contracts, Plaintiff and the Class sustained actual losses and damages as described herein.

WHEREFORE, Plaintiff and Class Members demand judgment as follows:

A. Certification of the action as a Class Action pursuant to Federal Rule of Civil Procedure 23, and appointment of Plaintiff as Class Representative and his counsel of record as Class Counsel;

B. That acts alleged herein be adjudged and decreed to constitute negligence and amount to violations of the consumer protection laws of Connecticut, and other states;

C. Judgment against Defendants for the damages sustained by Plaintiff and the Class defined herein, and for any additional damages, penalties, and other monetary relief provided by applicable law;

D. By awarding Plaintiff and Class Members pre-judgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of the Complaint in this action;

E. The costs of this suit, including reasonable attorney fees; and

F. Such other and further relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of all those similarly situated, hereby requests a jury trial, pursuant to Federal Rule of Civil Procedure 38, on any and all claims so triable.

Dated: July 30, 2019

Respectfully submitted,

/s/ Linda P. Nussbaum

Linda P. Nussbaum
Bart D. Cohen
NUSSBAUM LAW GROUP, P.C.
1211 Avenue of the Americas, 40th Floor
New York, NY 10036-8718
(917) 438-9189
lnussbaum@nussbaumpc.com
bcohen@nussbaumpc.com

Adam Frankel
GREENWICH LEGAL ASSOCIATES, LLC
881 Lake Avenue
Greenwich, CT 06831
(203) 622-6001
adam@grwlegal.com

Counsel for Plaintiff and the Proposed Class