IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

CHRISTI J. HILKER, individually and on behalf of all others similarly situated, Plaintiff, v. CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE, N.A., and CAPITAL ONE BANK (USA), N.A., Defendants.	Case No.: 19-cv-995 **Jury Trial Demanded**

CLASS ACTION COMPLAINT

Plaintiff, Christi J. Hilker, individually and on behalf of all persons similarly situated, makes the following allegations based upon information and belief, except as to allegations specifically pertaining to her, which are based on personal knowledge.

INTRODUCTION

1. On July 29, 2019, Capital One Financial Corporation, Capital One N.A., and Capital One Bank (USA), N.A. (collectively, "Capital One" or "Defendants"), one of the largest banks and credit card issuers in the United States, announced it had experienced a data breach that affected over 100 million people in the United States and six million people in Canada (the "Data Breach").[1]

2. The approximately 106 million individuals affected were largely consumers and small businesses who applied for credit card products between 2005 and 2019. The stolen data

[1] Capital One Form 8-K (July 29, 2019) ("July 29 Form 8-K"), https://bit.ly/2ymc729.

included names, addresses, zip codes, phone numbers, email addresses, dates of birth, self-reported income, approximately 140,000 Social Security Numbers, 80,000 bank account numbers, credit scores, credit card limits, credit card balances, credit card payment history, and fragments of transaction data from 23 days during 2016, 2017, and 2018 (collectively, "Personal Information").

3. The massive breach went undiscovered by Capital One despite the fact that the hacker had posted publicly about the breach on Twitter and other social medial sites over the course of several months and Capital One had records of the unauthorized intrusion.[2] Moreover, Capital One – which has infinite resources to protect the vulnerable data entrusted to it – was fully aware of the perils of a data breach and its legal responsibility to protect against a data breach, acknowledging in a recent public filing that "[s]afeguarding our customers' information is essential to our mission as a financial institution."[3]

4. Capital One announced that it was able to "immediately address[] the configuration vulnerability" that allowed the malicious and unauthorized access of over 100 million consumers' Personal Information, but it is too little too late for the millions of Americans whose privacy has been invaded and who now must contend with the resultant and imminent identity theft and fraud.

[2] Krebs on Security, *Capital One Data Theft Impacts 106M People* (July 30, 2019), https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/.

[3] July 29 Form 8-K.

PARTIES

5. Plaintiff Christi J. Hilker is a resident and citizen of Overland Park, Kansas, whose Personal Information, upon information and belief, was compromised in the Data Breach described herein.

6. Defendant Capital One Financial Corporation is a bank holding company that specializes in credit cards, auto loans, and banking and savings accounts. It is headquartered in McLean, Virginia, and incorporated under the laws of the State of Delaware.

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.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000.00 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Capital One. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Capital One resides in this District, transacts business in this District, and its principal place of business is located in this district.

11. This Court has personal jurisdiction over Capital One because it conducted substantial business in this District, and Capital One's corporate headquarters are located within this District.

STATEMENT OF FACTS

A. The Data Breach

12. Capital One, a Fortune 100 company, is one of the largest banks and credit card issuers in the United States, with over $28 Billion in revenue for fiscal year 2018.[4] It has over 39,000 automated teller machines (ATMs) in its network, hundreds of banking locations, and millions of customers who use its credit card and banking services.

13. On July 29, 2019, Capital One announced in a filing with the Securities Exchange Commission ("SEC") that it had experienced a data breach affecting "approximately 100 million individuals in the United States and approximately 6 million in Canada."[5]

14. In the filing, Capital One stated that the information breached was largely derived from consumers and small businesses who had applied for Capital One credit card products between the years 2005 through early 2019. The stolen information includes names, addresses, zip codes, phone numbers, email addresses, dates of birth, self-reported income, approximately 140,000 Social

[4] Capital One 2018 Form 10-K ("2018 Form 10-K) at 41, https://bit.ly/2K53e3w.

[5] July 29 Form 8-K.

Security Numbers, 80,000 bank account numbers, credit scores, credit limits, credit card balances, credit card payment history, and fragments of transaction data from 23 days during 2016, 2017, and 2018. Capital One represented that the data was encrypted but that the unauthorized access "also enabled the decrypting of [the] data."[6]

15. Capital One learned about the breach via an anonymous tip sent to it on July 17, 2019, which informed it that the stolen data was being stored publicly on Github, a software development platform where users can share information or collaborate on open source code projects.[7] After receiving the tip, Capital One commenced an investigation.

16. As detailed in the Federal Bureau of Investigation ("FBI")'s criminal complaint against the alleged hacker Paige A. Thompson (a/k/a "erratic"), Capital One's investigation, revealed that Thompson, a systems engineer and former employee of Amazon, posted the stolen data publicly on Github in a file time-stamped April 21, 2019,[8] – three months prior to Capital One's discovery and disclosure of the breach.

17. As alleged in the criminal complaint, the file posted by Thompson contained the IP address for a server at Amazon Web Services, which provides cloud computing services to Capital One. The file also contained command information that enabled access to folders and buckets of data in Capital One's storage space at the cloud computing company. A firewall misconfiguration

[6] *Id.*

[7] *See United States v. Paige A. Thompson, a/k/a "erratic,"* Complaint, Case No. 2:19-mj-00344-MAT, at ¶¶ 9, 15-16 (filed July 29, 2019) (the "Thompson Complaint"), https://www.justice.gov/usao-wdwa/press-release/file/1188626/download.

[8] *Id.*

permitted the commands to reach and be executed by the server, thereby enabling unauthorized access to the Capital One data.[9]

18. Specifically, the file posted by Thompson contained "700 folders or buckets of data," as well as code for three commands that could be used to extract data. The three commands, when executed, accomplished the following:

- The first command obtained security credentials for an account known as WAF-Role that enabled access to certain of Capital One's folders at the cloud computing company;
- The second command used the WAF-Role account to list the names of folders or buckets of data in Capital One's storage space at the cloud computing company (the "List Buckets Command"); and,
- The third command then used the same account the extract or copy data from the folders or buckets in Capital One's storage space for which the account had permissions (the "Sync Command").[10]

19. Capital One tested the three commands and confirmed that the commands functioned to obtain Capital's One credentials and could be used to extract data.[11]

20. Further, as alleged in the criminal complaint, Capital One's logs show a number of connections or attempted connections to Capital One's server from an Onion Router (or "TOR"), an anonymity tool used by individuals to conceal their identities and the origin of their internet

[9] *Id.* at ¶¶ 7-10.

[10] *Id.* at ¶ 11.

[11] *Id.* at ¶ 12.

connection (i.e. IP address), and a number of connections from a specific IP address beginning with 46.246, all of which Capital One believes relate to activity conducted by the same person involved in the April 21, 2019 intrusion. Capital One's logs show the following connections or attempted connections:

- On or about March 12, 2019, IP address 46.246.35.99 attempted to access Capital One's data. According to the FBI, this IP address is controlled by IPredator, a company that provides virtual private network ("VPN") services designed to mask users' IP addresses.[12]
- On or about March 22, 2019, the WAF-Role account was used to execute the List Buckets Command several times. The FBI believes the commands were executed from IP addresses concealed by a TOR, and Capital One reported to the FBI that the WAF-Role account does not, in the ordinary course of business, invoke the List Buckets Command.
- Also on or about March 22, 2019, the WAF-Role account was used to execute the Sync Command a number of times to obtain data from Capital One's data folders and buckets, including files that contained credit card application data. A number of those commands were executed from IP address 46.246.38.224, which the FBI found is controlled by IPredator.

[12] VPN services is a secure connection over a less secure network, such as a public network. A VPN uses shared public infrastructure but maintains privacy by employing security procedures and tunneling protocols. For example, a VPN encrypts data at the sending end, decrypts it at the receiving end, and sends the data through a "tunnel" that cannot be entered by data that is not properly encrypted.

21. In Capital One's Form 8-K disclosing the Data Breach, Capital One confirmed that unauthorized activity occurred on March 22 and 23, 2019.

22. The FBI's investigation revealed that after effectuating the hack, Thompson created a Meetup group with a Slack invitation for a public Slack channel. Meetup is an internet-based platform designed to let people find and build local communities, and Slack is a cloud-based team-collaboration software tool where users can establish "channels" in which they can then share messages, tools, and files.[13]

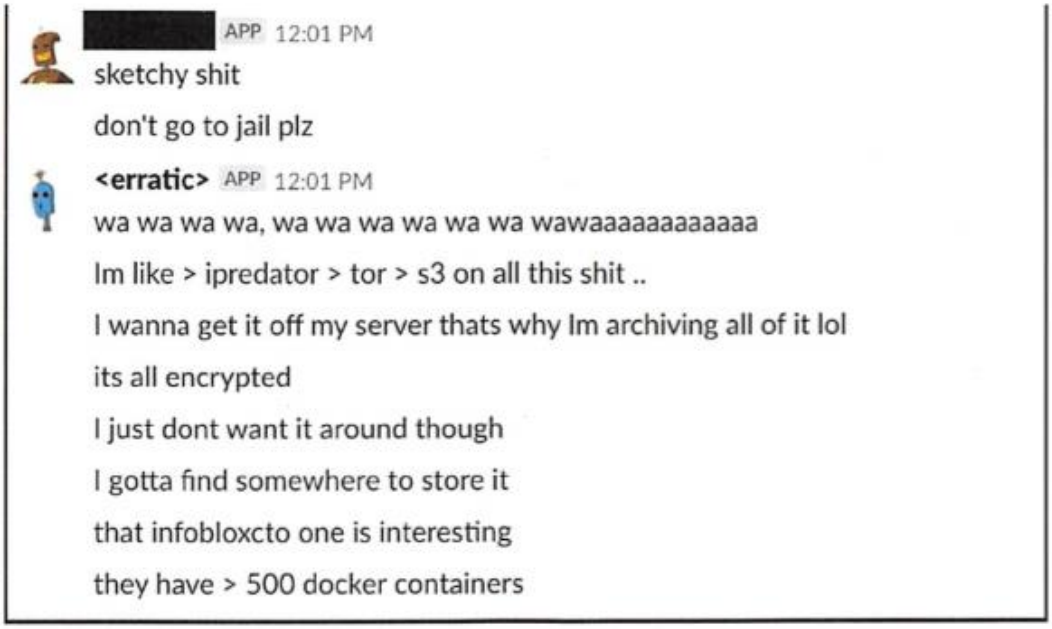
23. On the publicly-accessible Slack channel created by Thompson, a user named "erratic" – which the FBI alleges is Thompson – posted a list of files the user claimed to possess, which included files that were extracted using the commands set forth in the April 21st Github file posted by Thompson.[14]

24. On or about June 27, 2019, according to the FBI, "erratic posted [on the Slack channel] about several companies, government entities, and educational institutions, and included in the post references to the April 21st Github files associated with Capital One. After this posting, another user posted "don't go to jail plz" to which "erratic" responded "Im like > ipredator > tor > s3 on all this shit." The FBI interpreted this response to be detailing the method "erratic" used to commit the intrusion (*i.e.* that Ms. Thompson used IPredator and TOR to conceal her IP address).[15] The exchange between "erratic" and the other user was as follows:

[13] Thompson Compl. at ¶ 17.

[14] *Id*. at ¶ 18.

[15] *Id*. at ¶¶ 19-20.

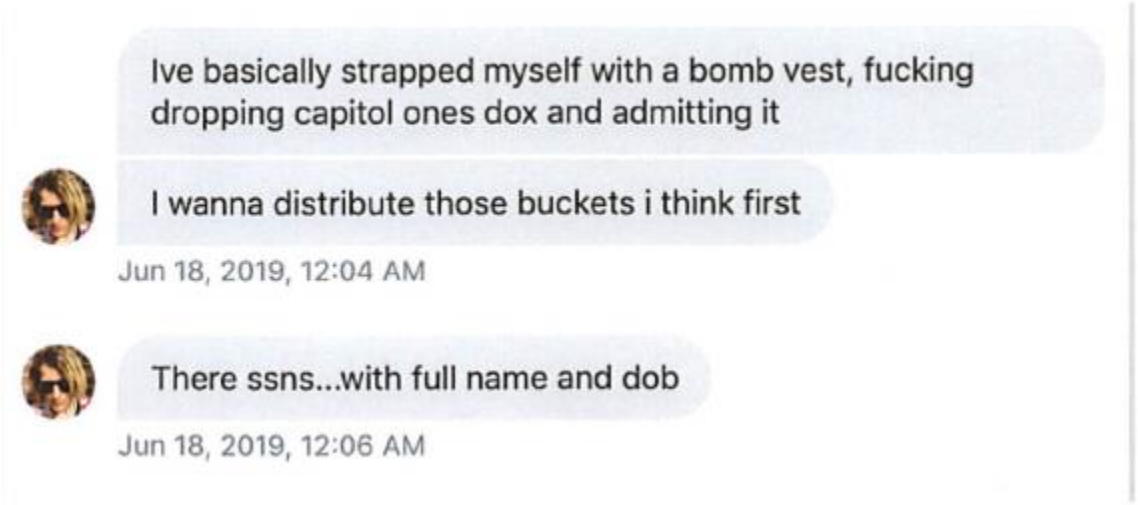


25. Capital One also provided the FBI with another screenshot from the Slack channel dated June 27, 2019, in which a user containing the name "paige" posted: "I've also got a leak proof IPredator router setup in anyone nneds [sic] it." In the screenshot, the same user posted a Github link that included "paige" and "thompson" in the link. The FBI was subsequently unable to locate the post, possibly because it has since been deleted.[16]

26. In addition to the Slack channel, the government further alleges that Thompson operated a Twitter account name @0xA3A97B6c with the username "ERRATIC." Capital One provided the FBI with a screenshot from Thompson's Twitter in which she sent a direct message on June 18, 2019 to the person who ultimately tipped off Capital One on July 17, 2019. In the message, Thompson relayed that she had "basically strapped myself with a bomb vest, fucking

[16] *Id.* at ¶ 21.

dropping capital ones dox and admitting it. I wanna distribute those buckets i think first" – indicating Thompson planned to disseminate the stolen data from Capital One:[17]



27. Investigative Reporter, Brian Krebs, who operates the website Krebs on Security, reported that Thompson spoke openly on her Twitter account over the course of several months about finding huge stores of data intended to be secured on various Amazon cloud servers – the servers from which (he suggested) Thompson likely stole the Capital One data:[18]

[17] *Id.* at ¶¶ 24-25.

[18] Krebs on Security, *Capital One Data Theft Impacts 106M People* (July 30, 2019),https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/.

28. Capital One's failure to detect the breach sooner is shocking given the public nature of Thompson's disclosures. As noted by Krebs, "[i]ncredibly, much of this breach played out publicly over several months on social media and other open online platforms" such as Twitter, Meetup, and Slack. And, for months beginning in April 2019, Capital One's stolen data and the means to steal data were stored in the open on Github for untold numbers of malicious actors to access.

29. Moreover, Capital One did not have reasonable safeguards and controls in place to detect the unauthorized activity as soon as it occurred. According to its investigation, Capital One's own records reflected that an unauthorized individual accessed and attempted to access Capital One's system multiple times in March 2019. Yet the breach went undiscovered for over four months. This suggests that Capital One did not have adequate Security Incident & Event Management ("SIEM") policies in place requiring IT-security events to be logged and reported to a centralized location and monitored in real time.

30. In fact, Capital One's security systems never detected the intruder; only when Capital One received the anonymous tip on July 17, 2019 did it realize its systems had been breached.

31. In its filing with the SEC disclosing the Data Breach, Capital One admitted the hacker "was able to exploit a specific configuration vulnerability in our infrastructure," which once discovered was "immediately addressed." The vulnerability at issue was "common to both cloud and on-premises data center environments." In addition to fixing the vulnerability, Capital One "augmented [its] routine automated scanning to look for this issue on a continuous basis."[19]

32. The criminal complaint specifies that the vulnerability was a misconfigured firewall.[20]

33. Amazon Web Services reiterated the FBI's allegation in a public statement regarding the Data Breach: "[Amazon Web Services] was not compromised in any way and functioned as designed. The perpetrator gained access through a misconfiguration of the web application and not the underlying cloud-based infrastructure. As Capital One explained clearly in its disclosure, this type of vulnerability is not specific to the cloud."[21]

B. Plaintiff's Individual Allegations

34. In or around August 2016, Plaintiff Hilker applied for a credit card with Capital One.

---

[19] July 29 Form 8-K.

[20] Thompson Compl. ¶ 10.

[21] Newsweek, *Amazon Refuses Blame for Capital One Data Breach* (July 30, 2019), available at https://www.newsweek.com/amazon-capital-one-hack-data-leak-breach-paige-thompson-cybercrime-1451665

35. Based upon Capital One's announcement that consumers who applied for credit cards between the years 2005-2019 were affected, and upon information and belief, Plaintiff Hilker's Personal Information was compromised as a result of the Data Breach.

36. As a result of the Data Breach, Plaintiff has spent and time and effort monitoring her financial accounts to detect fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Hilker remains at a substantial and imminent risk of future harm.

C. Capital One's Privacy Practices and Capital One's Knowledge That It Was a Target of Cyber Threats

37. Capital One was fully aware that it was a prime target of cyber threats. In its 2018 Form 10-K, Capital One discussed the threat of cyber-attacks at length, including acknowledging that it is a target: "cyber and information security risks for large financial institutions like us have generally increased in recent years" and that "[w]e and other U.S. financial services providers continue to be targeted with evolving and adaptive cybersecurity threats from sophisticated third parties."[22]

38. Capital One itself acknowledges that "[s]afeguarding our customers' information is essential to our mission and our role as a financial institution."[23]

39. With respect to cyber-security threats, Capital One specifically noted that it may "face an increasing number of attempted cyber-attacks as we expand . . . our usage of mobile and cloud technologies and as we provide more of these services to a greater number of retail clients."[24]

[22] 2018 Form 10-K at 24.

[23] July 29 Form 8-K.

[24] 2018 Form 10-K at 24.

40. To protect against these risks, Capital One touted its "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[.]"[25] Yet Capital One's supposedly robust systems did not detect the repeated unauthorized access and access attempts of its system.

41. Capital One's Privacy Notice promises its customers, a term defined to include applicants, current customers, and former customers of Capital One and its affiliates, that it will protect the "personal information [the customers or prospective customers provide in order to obtain the services] from unauthorized access and use [by employing] security measures that comply with federal law."[26]

42. Capital One's website also represents that "security is a top priority," specifying that it "prohibit[s] the unlawful disclosure of [applicant's] Social Security number[s]" and that is uses "some of the strongest forms of encryption commercially available for use on the Web today."[27]

43. Yet, despite these acknowledgments of the severity of the treat and promises to protect its customers' Personal Information, an unauthorized individual was able to exploit a vulnerability that Capital One's systems failed to detect.

44. Further, Capital One has experienced data breaches before. For example, in July 2017, Capital One disclosed to customers that a former employee had accessed customer

---

[25] *Id.*

[26] Capital One, *Privacy and Opt-Out Notice*, https://www.capitalone.com/privacy/notice/en-us/ (last visited July 30, 2019).

[27] Capital One, *Bank Securely*, https://www.capitalone.com/applications/identity-protection/commitment/ (last visited July 30, 2019).

information over a three-month period. The customer information accessed in that data breach included names, account numbers, telephone numbers, transaction history, dates of birth, and Social Security Numbers.[28]

45. Capital One has also observed numerous, well-publicized data breaches involving other types of major corporations who were also targeted given the sensitive consumer information they retained.

46. For example, through a series of data breaches extending back to 2013, more than three billion Yahoo! user accounts were compromised when account-holders' names, addresses, and dates of birth were stolen. The hackers also stole users' passwords, both encrypted and unencrypted, and security questions and answers.[29]

47. In separate incidents in 2013 and 2014, hundreds of millions of retail customers were victimized by hacks of payment card systems at Target and the Home Depot. Both breaches led to rampant payment card fraud and other damages both to consumers and to the card-issuing banks.[30]

48. In early 2015, Anthem, Inc., the second-largest health insurer in the United States, suffered a data breach that exposed the names, addresses, Social Security numbers, dates of birth,

[28] July 2017 Capital One Data Breach Notice, https://dojmt.gov/wp-content/uploads/Capital-One-1.pdf (last visited July 31, 2019).

[29] S. Larson, *Every Single Yahoo Account was Hacked – 3 Billion in All*, CNN (OCT. 4, 2017), https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html (last visited July 30, 2019).

[30] B. Krebs, *Home Depot Hit By Same Malware as Target*, KREBS ON SECURITY (Sept. 14, 2014), https://krebsonsecurity.com/tag/home-depot-databreach/ (last visited July 30, 2019).

and employment histories of nearly 80 million current and former plan members.[31] Other health care providers like, Premera and Excellus BlueCross BlueShield, reported similar breaches.[32]

49. In September 2017, credit reporting agency Equifax announced that hackers stole the personal and financial information of nearly 150 million Americans between May and July 2017.[33]

50. Despite being the holder of Personal Information for millions of individuals and businesses worldwide, Capital One failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to their highly-sensitive databases. Capital One had the resources to prevent a breach and made significant expenditures to market their credit card and banking services, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches affecting the financial industry and similar industries.

D. Capital One Failed to Comply with Regulatory Guidance

51. Federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance

[31] C. Riley, *Insurance Giant Anthem Hit by Massive Data Breach*, CNN (Feb. 6, 2015), https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/ (last visited July 30, 2019).

[32] *Cyber Breach Hits 10 Million Excellus Healthcare Customers*, USA TODAY (Sept. 10, 2015), https://www.usatoday.com/story/tech/2015/09/10/cyber-breach-hackers-excellus-blue-cross-blue-shield/72018150/ (last accessed July 22, 2019).

[33] https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last visited July 30, 2019).

of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[34]

52. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[35] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[36]

53. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[37]

---

[34] Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 30, 2019).

[35] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 30, 2019).

[36] *Id*.

[37] FTC, *Start With Security*, *supra* note 34.

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[38]

55. In this case, Capital One was fully aware of its obligation to use reasonable measures to protect the personal information of its customers, acknowledging as much in its own privacy policies. Capital One also knew it was a target for hackers. But despite understanding the consequences of inadequate data security, Capital One failed to comply with industry-standard data security requirements.

56. Capital One's failure to employ reasonable and appropriate measures to protect against unauthorized access to its customers' information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

E. The Effect of the Data Breach on Impacted Customers

57. Capital One's failure to keep Plaintiff's and Class Members' Personal Information secure has severe ramifications. Given the sensitive nature of the Personal Information stolen in the Data Breach – names, addresses, zip codes, phone numbers, email addresses, dates of birth, self-reported income, Social Security Numbers, bank account numbers, credit scores, credit limits, credit balances, payment history, and fragments of transaction data – hackers have the ability to

[38] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited July 30, 2019).

commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future.

58. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person." *Id*.

59. The Personal Information exposed in the Data Breach is highly-coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web" – exposing consumers to identity theft and fraud for years to come. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits or medical treatment; (f) file a fraudulent tax return using the victim's information; (g) commit espionage; or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

60. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017, fraudsters stole $16.8 billion from consumers in the United States, which includes $5.1 billion stolen through bank account take-overs.[39]

[39] Javelin, *2018 Identity fraud: Fraud Enters A New Era of Complexity*, https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-

61. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cybercrime is $445 billion a year.[40]

62. For class members who had their Social Security Numbers exposed, the unauthorized disclosure can be particularly damaging because, unlike a credit card, Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[41]

---

complexity (last visited July 30, 2019).

[40] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited July 30, 2019).

[41] Social Security Administration, *Identity Theft and Your Social Security Number* (June 2017),

63. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of a Social Security Number, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[42]

64. And, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[43] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

65. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey[44] evidences the emotional suffering experienced by victims of identity theft:

---

http://www.ssa.gov/pubs/10064.html (last visited July 30, 2019).

[42] U.S. Department of Justice, *Victims of Identity Theft, 2014* (Revised November 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 30, 2019).

[43] Identity Theft Resource Center, *The Aftermath 2017*, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited July 30, 2019).

[44] *Id.*

- 75% of respondents reported feeling severely distressed
- 67% reported anxiety
- 66% reported feelings of fear related to personal financial safety
- 37% reported fearing for the financial safety of family members
- 24% reported fear for their physical safety
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft
- 7% reported feeling suicidal.

66. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances
- 37.1% reported an inability to concentrate / lack of focus
- 28.7% reported they were unable to go to work because of physical symptoms
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues)
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[45]

67. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

[45] *Id.*

> [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.[46]

68. Despite Capital One's clear awareness of the cyber-security threat posed to financial institutions, such as itself, Capital One failed to properly safeguard Plaintiff's and the Class Members' Personal Information as required by various state and federal regulations, industry practices, the common law, and its own promises. The Data Breach was a direct and proximate result of Capital One's failure.

69. As the result of the Data Breach, Plaintiff and Class Members have suffered and/or will suffer or continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

- purchasing goods and services they would not have otherwise paid for and/or paying more for good and services than they otherwise would have paid, had they known the truth about Defendants' substandard data security practices;
- losing the inherent value of their Personal Information;
- losing the value of Capital One's explicit and implicit promises of adequate data security;
- identity theft and fraud resulting from the theft of their Personal Information;
- costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;
- unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being

[46] U.S. Government Accountability Office, *Report to Congressional Requesters* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited July 30, 2019).

limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

- lowered credit scores resulting from credit inquiries following fraudulent activities;
- costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and
- the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

70. Additionally, Plaintiff and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[47]

71. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like Capital One would have no reason to tout their data security efforts to their actual and potential customers.

[47] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited July 30, 2019).

72. Consequently, had consumers known the truth about Capital One's data security practices – that the company would not adequately protect and store their data – they would not have applied for a Capital One credit card or remained a Capital One customer. As such, Plaintiff and Class Members did not receive the benefit of their bargain with Capital One because they paid for the value of services they expected but did not receive.

CLASS ALLEGATIONS

73. Plaintiff seeks relief on behalf of herself and as a representative of all others who are similarly situated. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3) and/or (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons in the United States whose Personal Information was compromised as a result of the data breach announced by Capital One on July 29, 2019 (the "Class" or "Nationwide Class").

74. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims under the law of the state of Kansas on behalf of a separate statewide class, defined as follows:

> All persons in the State of Kansas whose Personal Information was compromised as a result of the data breach announced by Capital One on July 29, 2019 (the "Kansas Subclass").

75. Excluded from each of the above Classes are Capital One, any entity in which Capital One has a controlling interest, and Capital One's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded are all persons who make a timely election to be excluded from the Class; government entities; and any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

76. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

77. Each of the proposed Classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

78. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class Members is unknown to Plaintiff at this time, Capital One has acknowledged that the Personal Information of over 100 million persons have been compromised. Those persons' names and addresses are available from Capital One's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include electronic mail, U.S. Mail, internet postings, and/or published notice.

79. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

- Whether Capital One knew or should have known that its computer systems were vulnerable to attack;
- Whether Capital One failed to take adequate and reasonable measures to ensure its data systems were protected;
- Whether Capital One failed to take available steps to prevent and stop the breach from happening;

- Whether Capital One owed a duty to Plaintiff and Class Members to protect their Personal Information;
- Whether Capital One breached its duty to protect the Personal Information of Plaintiff and Class Members by failing to provide adequate data security;
- Whether Capital One's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unauthorized access to and/or theft of Plaintiff's and Class Members' Personal Information;
- Whether Capital One has a contractual obligation to use reasonable security measures and whether it complied with such contractual obligation;
- Whether Capital One's conduct amounted to violations of state consumer protection statutes, and/or state data breach statutes;
- Whether, as a result of Capital One's conduct, Plaintiff and Class and Subclass members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and
- Whether, as a result of Capital One's conduct, Plaintiff and Class and Subclass members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

80. **Typicality. Fed. R. Civ. P. 23(a)(3).** As to the Nationwide Class and the Kansas Subclass, Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way.

81. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed

to pursuing this matter against Capital One to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

82. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual Plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Capital One, and thus, individual litigation to redress Capital One's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

83. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Capital One, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

84. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- Whether Capital One owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;
- Whether Capital One failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiff and the Class Members; and,
- Whether Capital One's security measures to protect is systems were reasonable in light of known legal requirements.

85. Finally, all members of the proposed Class are readily ascertainable. Capital One has access to information regarding which individuals were affected by the Data Breach. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

86. Plaintiff restates and re-alleges the preceding paragraphs as if fully set forth herein.

87. Capital One owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and

testing Capital One's security systems to ensure that Plaintiff's and Class Members' Personal Information in Capital One's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

88. Capital One had a common law duty to prevent foreseeable harm to its customers. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their Personal Information because hackers routinely attempt to steal such information and use it for nefarious purposes, Capital One knew that it was more likely than not Plaintiff and other Class Members would be harmed.

89. Capital One's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information by companies such as Capital One. Various FTC publications and data security breach orders further form the basis of Capital One's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

90. Capital One breached the duties it owed to Plaintiff and Class Members described above and thus was negligent. Capital One breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices

sufficient to protect the Personal Information of Plaintiff and Class Members; (b) detect the breach while it was ongoing or even promptly after it occurred; and (c) maintain security systems consistent with industry standards.

91. But for Capital One's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Personal Information would not have been compromised.

92. As a direct and proximate result of Capital One's negligence, Plaintiff and Class Members have been injured as described *supra*, and are entitled to damages in an amount to be proven at trial.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

93. Plaintiff restates and re-alleges the preceding paragraphs as if fully set forth herein.

94. 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.

95. 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. Capital One's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of a data breach on its systems.

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

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

98. 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 Class Members.

99. As a direct and proximate result of Capital One's negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages in an amount to be proven at trial.

COUNT III
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

100. Plaintiff restates and re-alleges the preceding paragraphs as if fully set forth herein.

101. Capital One's Privacy and Opt-Out Notice (the "Notice") is an agreement between Capital One and persons who provided their Personal Information to Capital One, including Plaintiff and Class Members.

102. Capital One's Notice states that it applies to customers, applicants, and former customers of Capital One, and it details how Capital One will both protect and use the Personal Information provided by customers and applicants of Capital One's services.

103. The Notice provides detailed information about what types of Personal Information will be shared and with what entities. It further promises that to "protect your personal information from unauthorized access and use, we use security measures that comply with federal law."

104. Plaintiff and Class Members on the one hand and Capital One on the other formed a contract when Plaintiff and Class Members provided Personal Information to Capital One subject to the Notice.

105. Plaintiff and Class Members fully performed their obligations under the contract with Capital One.

106. Capital One breached its agreement with Plaintiff and Class Members by failing to protect their Personal Information. Specifically, Capital One (1) failed to use reasonable measures to protect that information; and (2) disclosed that information to unauthorized third party, in violation of the agreement.

107. As a direct and proximate result of these breaches of contract, Plaintiff and Class Members sustained actual losses and damages as described in detail above, including that they did not get the benefit of the bargain for which they paid.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

108. Plaintiff restates and re-alleges the preceding paragraphs as if fully set forth herein, and asserts this claim in the alternative to their breach of contract claim to the extent necessary.

109. Plaintiff and Class Members also entered into an implied contract with Capital One when they obtained services from Capital One, or otherwise provided Personal Information to Capital One.

110. As part of these transactions, Capital One agreed to safeguard and protect the Personal Information of Plaintiff and Class Members.

111. Plaintiff and Class Members entered into implied contracts with the reasonable expectation that Capital One's data security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class Members believed that Capital One would use part of the monies paid to Capital One under the implied contracts to fund adequate and reasonable data security practices.

112. Plaintiff and Class Members would not have provided and entrusted their Personal Information to Capital One or would have paid less for Capital One's services in the absence of the implied contract or implied terms between them and Capital One. The safeguarding of the Personal Information of Plaintiff and Class Members was critical to realize the intent of the parties.

113. Plaintiff and Class Members fully performed their obligations under the implied contracts with Capital One.

114. Capital One breached its implied contracts with Plaintiff and Class Members to protect their Personal Information when it (1) failed to have security protocols and measures in place to protect that information; and (2) disclosed that information to unauthorized third parties.

115. As a direct and proximate result of Capital One's breach of implied contract, Plaintiff and Class Members sustained actual losses and damages as described in detail above, including that they did not get the benefit of the bargain for which they paid.

COUNT V
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

116. Plaintiff restates and re-alleges the preceding paragraphs as if fully set forth herein, and asserts this claim in the alternative to their breach of contract claim to the extent necessary.

117. Plaintiff and Class Members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by Capital One and that was ultimately stolen in the Data Breach.

118. Capital One was benefitted by the conferral upon it of the Personal Information pertaining to Plaintiff and Class Members and by its ability to retain and use that information. Capital One understood that it was in fact so benefitted.

119. Capital One also understood and appreciated that the Personal Information pertaining to Plaintiff and Class Members was private and confidential and its value depended upon Capital One maintaining the privacy and confidentiality of that Personal Information.

120. But for Capital One's willingness and commitment to maintain its privacy and confidentiality, that Personal Information would not have been transferred to and entrusted with Capital One. Further, if Capital One had disclosed that its data security measures were inadequate, Capital One would not have been permitted to continue in operation by regulators, its shareholders, and its customers.

121. As a result of Capital One's wrongful conduct as alleged in this Complaint (including, among things, its knowing failure to employ adequate data security measures, its continued maintenance and use of the Personal Information belonging to Plaintiff and Class Members without having adequate data security measures, and its other conduct facilitating the

theft of that Personal Information), Capital One has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members. Capital One continues to benefit and profit from its retention and use of the Personal Information while its value to Plaintiff and Class Members has been diminished.

122. Capital One's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class Members' Personal Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

123. Under the common law doctrine of unjust enrichment, it is inequitable for Capital One to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and class members in an unfair and unconscionable manner. Capital One's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

124. The benefit conferred upon, received, and enjoyed by Capital One was not conferred officiously or gratuitously, and it would be inequitable and unjust for Capital One to retain the benefit.

125. Capital One is therefore liable to Plaintiff and class members for restitution in the amount of the benefit conferred on Capital One as a result of its wrongful conduct, including specifically the value to Capital One of the Personal Information that was stolen in the Data Breach and the profits Capital One is receiving from the use of that information

COUNT VI
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

126. Plaintiff restates and re-alleges the preceding paragraphs as if fully set forth herein.

127. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

128. An actual controversy has arisen in the wake of the Capital One Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Capital One is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Personal Information. Plaintiff remains at imminent risk that further compromises of their Personal Information will occur in the future.

129. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Capital One continues to owe a legal duty to secure consumers' Personal Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. Capital One continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Personal Information.

130. The Court also should issue corresponding prospective injunctive relief requiring Capital One to employ adequate security protocols consistent with law and industry standards to protect consumers' Personal Information.

131. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Capital One. The

risk of another such breach is real, immediate, and substantial. If another breach at Capital One occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

132. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Capital One if an injunction is issued. Among other things, if another massive data breach occurs at Capital One, Plaintiff and Class Members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Capital One of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Capital One has a pre-existing legal obligation to employ such measures.

133. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Capital One, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose Personal Information would be further compromised.

COUNT VII
KANSAS CONSUMER PROTECTION ACT, Kan. Stat. Ann. §§ 50-623, *et seq.*
(ON BEHALF OF PLAINTIFF AND THE KANSAS SUBCLASS)

134. Plaintiff Hilker ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and alleges the preceding paragraphs as if fully set forth herein.

135. K.S.A. §§ 50-623, *et seq.* is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

136. Plaintiff and Kansas Subclass members are "consumers" as defined by K.S.A. § 50-624(b).

137. The acts and practices described herein are "consumer transactions," as defined by K.S.A. § 50-624(c).

138. Capital One is a "supplier" as defined by K.S.A. § 50-624(l).

139. Capital One advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

140. Capital One engaged in deceptive and unfair acts or practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kansas Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b, which non-compliance was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Kansas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Kansas Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b.

141. Capital One's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Capital One's data security and ability to protect the confidentiality of consumers' Personal Information.

142. Capital One intended to mislead Plaintiff and Kansas Subclass members and induce them to rely on its misrepresentations and omissions.

143. Had Capital One disclosed to Plaintiffs and the Subclass members that its data systems were not secure and, thus, vulnerable to attack, Capital One would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Capital One received, maintained, and compiled Plaintiff's and Class Members' Personal Information as part of the services Capital One provided and for which Plaintiff and Class Members paid without advising Plaintiff and Class Members that Capital One's data

security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Class Members' Personal Information. Accordingly, Plaintiff and the Kansas Subclass members acted reasonably in relying on Capital One's misrepresentations and omissions, the truth of which they could not have discovered.

144. Capital One also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

a. Knowingly taking advantage of the inability of Plaintiff and the Kansas Subclass to reasonably protect their interests, due to their lack of knowledge (see K.S.A. § 50-627(b)(1)); and

b. Requiring Plaintiff and the Kansas Subclass to enter into a consumer transaction on terms that Capital One knew were substantially one-sided in favor of Capital One (see K.S.A. § 50-627(b)(5)).

145. Plaintiff and the Kansas Subclass had unequal bargaining power with respect to their ability to control the security and confidentiality of their Personal Information in Capital One's possession.

146. The above unfair, deceptive, and unconscionable practices and acts by Capital One were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

147. Capital One acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act, and recklessly disregarded Plaintiff and Kansas Subclass members'

rights. Capital One's past data breaches and breaches within the financial industry put it on notice that its security and privacy protections were inadequate.

148. As a direct and proximate result of Capital One's unfair, deceptive, and unconscionable trade practices, Plaintiff and Kansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Capital One as they would not have paid Capital One for goods and services or would have paid less for such goods and services but for Capital One's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; and an increased, imminent risk of fraud and identity theft.

149. Plaintiff and Kansas Subclass members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; restitution; and reasonable attorneys' fees and costs

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class Members proposed in this Complaint, respectfully request that the Court enter judgment in her favor and against Capital One as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiff and her Counsel to represent the Nationwide Class and the Kansas Subclass;

b. For equitable relief enjoining Capital One from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Personal Information;

c. For equitable relief compelling Capital One to use industry-standard security methods and policies with respect to data collection, storage and protection and to dispose of Plaintiff's and Class Members' Personal information in its possession;

d. For an award of damages, including nominal damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

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

Dated: July 31, 2019

Respectfully submitted,

/s/ *John G. Harnishfeger*
William H. Murphy III (*pro hac vice* to be submitted)
Jessica H. Meeder (*pro hac vice* to be submitted)
John G. Harnishfeger (Virginia Bar No. 36878)
MURPHY, FALCON & MURPHY
One South Street, Ste 2300
Baltimore, Maryland 21202
T: (410) 951-8744
F: (410) 539-6599
hassan.murphy@murphyfalcon.com
jessica.meeder@murphyfalcon.com
john.harnishfeger@murphyfalcon.com

Norman E. Siegel (*pro hac vice* to be submitted)
Barrett J. Vahle (*pro hac vice* to be submited)
J. Austin Moore (*pro hac vice* to be submitted)
Jillian R. Dent (*pro hac vice* to be submitted)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Telephone: (816) 714-7100
Facsimile: (816) 714-7101
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com
dent@stuevesiegel.com

Counsel for Plaintiff and the Proposed Class

JURY DEMAND

Plaintiff, on behalf of herself and the Class of all others similarly situated, hereby demands a trial by jury on all issues so triable pursuant to rule 38 of the Federal Rules of Civil Procedure.

/s/ *John G. Harnishfeger*
John G. Harnishfeger (Virginia Bar No. 36878)