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

BRANDI EDMONDSON, BRANDON HAUSAUER, SARA SHARP, CARALYN TADA, and GARY ZIELICKE, Plaintiffs, v. CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE BANK (USA) N.A., CAPITAL ONE, N.A., AMAZON.COM, INC., and AMAZON WEB SERVICES, INC., Defendants.	)	Civil Action No. _____ JURY DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs identified below (collectively, "Plaintiffs"), individually and on behalf of the classes defined below of similarly situated persons, allege the following against Defendants Capital One Financial Corporation, Capital One Bank (USA) N.A., and Capital One, N.A. (collectively, the "Capital One Defendants" or "Capital One"), and against Amazon.com, Inc., and Amazon Web Services, Inc. (collectively, the "Amazon Defendants" or "Amazon"; with the Capital One and Amazon Defendants collectively, "Defendants"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. On July 29, 2019, Capital One, 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 reported 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, "PII").

3. Through their failure to adequately protect Plaintiffs' and class members' PII, the Capital One Defendants and the Amazon Defendants, which hosted the PII on Amazon Web Services ("AWS"), allowed Paige A. Thompson ("Thompson"), a former Amazon employee, to

[1] Capital One Form 8-K (July 29, 2019) ("July 29 Form 8-K"), https://sec.report/Document/0000927628-19-000262/.

obtain access to and to surreptitiously view, remove, and make public Plaintiffs' and class members' PII entrusted to Defendants.

4. The massive breach went undiscovered by Defendants despite the fact that the hacker had posted publicly about the breach on Twitter and other social media sites over the course of several months[2] and despite the fact that Capital One had records of the unauthorized intrusion. Moreover, Capital One—which has almost limitless resources to protect the vulnerable data entrusted to it and in the face of well publicized data breaches sustained by numerous other companies, including financial institutions in the United States—was fully aware of the perils of a data breach and its legal responsibility to protect against a data breach, acknowledging publicly that "[s]afeguarding our customers' information is essential to our mission as a financial institution."[3] And all Defendants knew of the particular security vulnerabilities that permitted the Data Breach, but still failed to protect Plaintiffs' and class members' PII.

5. Capital One claimed that it was able to "immediately address[] the configuration vulnerability" after the Data Breach,[4] but it was too little too late for the millions of Americans whose privacy has been compromised and who now must contend with the loss of this valuable data and resultant and imminent identity theft and fraud. And despite Capital One's assurances, vast amounts of PII belonging to Plaintiffs and class members remains dangerously exposed and vulnerable to theft and fraud as currently maintained and used by Amazon and Capital One for their own profit.

---

[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.
[4] *Id.*

JURISDICTION AND VENUE

6. 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 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 Defendants. 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.

7. This Court has personal jurisdiction over Capital One because it is headquartered in and maintains its principal place of business in this District. Capital One is authorized to and regularly conducts business in Virginia. In this District, Capital One makes decisions regarding corporate governance and management of its credit card business, including decisions regarding the security measures to protect its customers' PII. Capital One intentionally avails itself of this jurisdiction by promoting, selling and marketing its services from Virginia to millions of consumers nationwide.

8. This Court has personal jurisdiction over Amazon because it is authorized to and regularly conducts business in Virginia and has sufficient minimum contacts in Virginia such that Amazon intentionally avails itself of this Court's jurisdiction by conducting operations here and promoting, selling and marketing its services in this District.

9. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Capital One's headquarters and principal place of business are located in this District, Capital One resides in this District, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by Capital One's governance and management personnel or inaction by those individuals that led to misrepresentations, invasions of privacy, and the Data Breach. Moreover, Amazon maintains

physical facilities in this District, conducts business in this District, provided services to Capital One in this District, and is executing plans to build a new headquarters in this District.

DEFENDANTS

10. 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.

11. 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.

12. 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.

13. Defendant Amazon.com, Inc. is a corporation with its headquarters and principal place of business in Seattle, Washington, and incorporated under the laws of the State of Delaware.

14. Defendant Amazon Web Services, Inc. is a corporation with its headquarters and principal place of business in Seattle, Washington, and incorporated under the laws of the State of Delaware. Amazon Web Services, Inc. is a subsidiary of Amazon.com, Inc.

NAMED PLAINTIFFS

15. Plaintiffs are individuals who, upon information and belief, had their PII compromised in the Data Breach, and bring this action on behalf of themselves and all those similarly situated both across the United States and within their State residence. The following allegations are made upon information and belief derived from, among other things, investigation of counsel, public sources, and the facts and circumstances as currently known. Because Defendants have exclusive knowledge of what information was compromised for each individual, Plaintiffs

reserve their right to supplement their allegations with additional facts and injuries as they are discovered.

16. Plaintiffs place significant value in the security of their PII. Plaintiffs entrusted their sensitive PII to Defendants with the understanding, based on Defendants' statements and representations, that Defendants would keep their information secure and employ reasonable and adequate security measures to ensure that it would not be compromised. If Plaintiffs had known of Defendants' lax security practices with respect to Plaintiffs' PII, they would not have done business with Capital One, would not have applied for Capital One credit cards, would not have opened, used, or continued to use Capital One credit cards or banking services at the applicable interest rates and on the applicable terms, or would have paid less because of the diminished value of Capital One's services.

17. Plaintiffs' PII remains at risk because Defendants continue to store and use that data in a manner that unreasonably exposes it to targeting by malicious third parties for identity theft, fraud, and misuse.

CALIFORNIA

18. Plaintiff Brandon Hausauer is a resident and citizen of San Francisco, California. Prior to the Data Breach, Plaintiff Hausauer applied for and used a personal Capital One credit card, a business credit card, and a business checking and savings account, and provided his PII to Capital One in order to do so. On August 7, 2019, he received a letter from Capital One informing him that hackers had obtained his name and Business Tax Identification number, which is also his Social Security Number, as part of the Data Breach. Capital One also stated that the hackers may have obtained his: name, address, zip code/postal code, phone number, email address, date of birth, self-reported income, credit card customer data including customer status data (for example, credit scores, credit limits, balances, payment history and contact information) and fragments of

transactional data from 23 days during 2016, 2017 and 2018. If Plaintiff Hausauer had known that Capital One's data security measures were inadequate to safeguard customers' PII from theft, he would not have applied for or used a Capital One credit card or provided his PII. As a result of the Data Breach, Plaintiff Hausauer spent time and effort regularly monitoring his accounts to detect fraudulent activity in order to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Hausauer remains at a substantial and imminent risk of future harm.

19. Plaintiff Caralyn Tada is a resident and citizen of Los Angeles, California. Prior to the Data Breach, Plaintiff Tada applied for and used a Capital One credit card, and provided her PII to Capital One in order to do so. On or around the end of August 2019, Plaintiff Tada received notice of the Data Breach from Capital One. Plaintiff Tada then spoke by phone to a Capital One representative who confirmed that Ms. Tada's PII had been compromised in the Data Breach. Since the Data Breach, Plaintiff Tada has experienced several incidents of attempted fraud on several of her bank accounts, including at least one large charge, which has caused Plaintiff Tada to expend significant time, effort, and worry. Further, as a result of the Data Breach, Plaintiff Tada spent time and effort regularly monitoring her accounts to detect fraudulent activity in order to mitigate against potential harm. Plaintiff Tada also purchased and continues to pay $25 per month for credit-monitoring due to the Data Breach. If Plaintiff Tada had known that Capital One's data security measures were inadequate to safeguard customers' PII from theft, she would not have applied for or used Capital One credit cards or provided her PII. Given the highly-sensitive nature of the information stolen, Plaintiff Tada remains at a substantial and imminent risk of future harm.

FLORIDA

20. Plaintiff Gary Zielicke is a resident and citizen of Clewiston, Florida. Prior to the Data Breach, Plaintiff Zielicke applied for and used a Capital One credit card, and provided his PII to Capital One in order to do so. After the Data Breach, Plaintiff Zielicke experienced identity theft and fraud, including that his cell phone, a number associated with his Capital One credit card, had been de-activated by an unauthorized individual and large unauthorized charges had been charged to his Capital One credit card. Plaintiff Zielicke was not able to recover control over his cell phone number for several days, during which he expended time and money in his efforts to re-gain control. Plaintiff Zielicke also spent significant time reporting the identity theft to the police and working to resolve it. When Plaintiff Zielicke contacted Capital One about the identity theft of his Capital One card, representatives of Capital One informed him that the identity theft may be related to the Data Breach. In subsequent months, Plaintiff Zielicke has experienced further identity theft wherein an unauthorized individual opened an account in his name and used the account to pay tens of thousands of dollars in his name, which was then registered as a delinquent account in his name resulting in his credit score dropping several hundred points. Because of the multiple incidents of identity theft, Plaintiff Zielicke has frozen his credit. He has also expended significant amounts of time, effort, and money in resolving the issues, including continuing to regularly monitor his accounts to detect any future fraudulent activity. If Plaintiff Zielicke had known that Capital One's data security measures were inadequate to safeguard customers' PII from theft, he would not have applied for or used Capital One credit cards or provided his PII. Given the highly-sensitive nature of the information stolen, Plaintiff Zielicke remains at a substantial and imminent risk of future harm.

TEXAS

21. Plaintiff Brandi Edmondson is a resident and citizen of Dallas, Texas. Prior to the Data Breach, Plaintiff Edmondson applied for and used a Capital One credit card, and provided her PII to Capital One in order to do so. As a result of the Data Breach, Plaintiff Edmondson spent time and effort dealing with these unauthorized account requests and expended further time and effort regularly monitoring her accounts to detect fraudulent activity in order to mitigate against potential harm. If Plaintiff Edmondson had known that Capital One's data security measures were inadequate to safeguard customers' PII from theft, she would not have applied for or used Capital One credit cards or provided her PII. Given the highly-sensitive nature of the information stolen, Plaintiff Edmondson remains at a substantial and imminent risk of future harm.

WASHINGTON

22. Plaintiff Sara Sharp is a resident of Ocean Shores, Washington. Prior to the Data Breach, Plaintiff Sharp applied for and used a Capital One credit card, and provided her PII to Capital One in order to do so. After the Data Breach, Plaintiff Sharp suffered identity theft and fraud in the form of unauthorized charges on her bank account, as well as reports of fraudulent charges made in her name. As a result of this fraud, Plaintiff Sharp spent time investigating the source of the fraud and unauthorized charges. On January 11, 2020, after an inquiry, Capital One sent Plaintiff Sharp an "Update About the Capital One Data Security Incident." If Plaintiff Sharp had known that Capital One's data security measures were inadequate to safeguard customers' PII from theft, she would not have applied for or used a Capital One credit card or provided her PII. As a result of the Data Breach, Plaintiff Sharp spent time and effort regularly monitoring her accounts to detect fraudulent activity in order to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Sharp remains at a substantial and imminent risk of future harm.

FACTUAL ALLEGATIONS

"We're building a technology company that does banking."
Richard D. Fairbank - Chairman, CEO and President of Capital One, February 20, 2019

A. Capital One's Collection and Use of Customer Data

23. Capital One is one of the largest banks and credit card issuers in the United States. In 2018 it recorded over $28 billion in revenues and had $107.35 billion in credit card loans outstanding in the United States, with credit cards representing 47.3% of total loans outstanding. In addition to credit card loans, Capital One offers banking services, including checking accounts, saving accounts, and money market accounts as well as retail and auto loans. As of December 31, 2018, the company had $2.864 billion in retail loans outstanding and $56.341 billion in auto finance loans outstanding, representing 24.1% of total loans outstanding.[5]

24. Capital One routinely collects PII from consumers and small businesses applying for its credit. Applicants are asked for name, date of birth, social security number, address, phone number, annual income, mortgage information, bank account information, and other personal financial information. The PII collected by Capital One is not simply used to process a card or loan application, but is also used to determine credit limits, interest rates, fees, and other terms of credit.

25. In addition to this customary use of PII to make credit decisions, Capital One maintains and mines the data for purposes of product development, targeted solicitation for new products, and target marketing of new partners—all in an effort to boost its profits.

26. From its beginning, Capital One adopted this "Information Based Strategy," or IBS, to obtain a competitive advantage. In its very first Form 10-K in 1996, Capital One explained:

> The Company's IBS is designed to allow the Company to differentiate among customers based on credit risk, usage and other characteristics and to match customer characteristics with appropriate product offerings. IBS

[5] Capital One 2018 Annual Report, at 3, 78, available at https://ir-capitalone.gcs-web.com/static-files/04c57bd9-b351-418c-9f18-ed91d4bfad23.

> involves developing sophisticated models, information systems, well-trained personnel and a flexible culture to create credit card or other products and services that address the demands of changing consumer and competitive markets. By using sophisticated statistical modeling techniques, the Company is able to segment its potential customer lists based upon the integrated use of credit scores, demographics, customer behavioral characteristics and other criteria. By actively testing a wide variety of product and service features, marketing channels and other aspects of its offerings, the Company can design and target customized solicitations at various customer segments, thereby enhancing customer response levels and maximizing returns on investment within given underwriting parameters.[6]

27. In its 2018 Annual Report, Capital One recalled its 25-year history of using technology to advance its business:

> Capital One Was the Original "FinTech." It didn't come easy at first. We had more passion than customers and more belief than believers. The term didn't exist yet, but in the early days of Capital One, we were a FinTech. For a while it was unclear if our little company would get a chance to make a big impact. We were a start-up: recruiting talent, building modern technology from scratch, conducting tests, and incubating results. And all along the way, we worked to keep the dream alive. While the initial idea came quickly, it took five lonely years until we had our first success. Against all odds, it finally worked, and we haven't looked back. We built one of the nation's largest credit card businesses and then did the same thing in auto finance and small business cards.[7]

28. As technology improved throughout the 1990's and 2000's, Capital One's Information Based Strategy moved to a digitally based system. For example, Capital One's 2011 Form 10-K stated that Capital One "leverage[s] information technology to achieve our business objectives and to develop and deliver products and services that satisfy our customers' needs [a key aspect of which is] the development of efficient, flexible computer and operational systems to support complex marketing and account management strategies and the development of new and

---

[6] Capital One Financial Corporation, 1996 Form 10-K, available at http://getfilings.com/o0000950133-97-001012.html.

[7] Capital One 2018 Annual Report, at 3.

diversified products."[8] This strategy also prompted Capital One to utilize artificial intelligence to analyze customer data, which would require Capital One to collect, store, and mine customer data on an unprecedented scale.

29. Machine learning is an application of artificial intelligence through which computer algorithms are given raw data and "learn" on their own to discern patterns and accomplish tasks. As an example, in the financial services industry, machine learning is used to detect unauthorized use of a credit card by analyzing customer data to discern patterns suggestive of unauthorized transactions. Artificial intelligence programs can detect patterns in data that are difficult for humans to perceive.

30. Machine learning requires data. There is a direct correlation between the amount of data provided to the machine learning algorithm and the effectiveness of the machine learning algorithm.[9] Thus, the more data made available to these artificial intelligence programs, the more accurate and useful the programs will be.

31. To store, process, and mine sensitive customer data, banks like Capital One traditionally use a dedicated-server or private-cloud solution for their storage and processing needs. Dedicated servers assign specific hardware and software to perform specific tasks, while private clouds allow hardware and software to be assigned dynamically. In both scenarios, the equipment is dedicated to a single company that exercises control over the infrastructure. And, in both

---

[8] Capital One Financial Corporation, 2011 Form 10-K, available at http://investor.capitalone.com/static-files/9982f071-158b-4ecd-9a42-77200b9d2442.

[9] *See* William Sundblad, *Data is the Foundation For Artificial Intelligence and Machine Learning*, FORBES (Oct. 18, 2018), available at https://www.forbes.com/sites/willemsundbladeurope/2018/10/18/data-is-the-foundation-for-artificial-intelligence-and-machine-learning/#45c9c0551b49.

scenarios, the costs to maintain the needed infrastructure rises with the increase in the amount of data collected.

B. Capital One Partners With AWS For Cloud Computing

32. As the costs of dedicated-servers or private-cloud solutions have increased, public clouds hosted and run by third parties, such as Amazon's AWS, Microsoft's Azure, IBM's Cloud, and Google Cloud, have developed as a cheaper alternative. Those third parties own and maintain the infrastructure, which is then leased on a scalable, dynamic basis to businesses. Because resources can be scaled to meet demand, with server space expanding or contracting based on use, a contracting business using a public cloud service may save money by only paying for the computing power and storage that it needs and not having to pay for the cost of excessive capacity or maintaining the infrastructure required of dedicated servers or a private cloud.

33. The primary downsides of public cloud computing are the increased data security risk inherent in their use,[10] and the related difficulty of meeting regulatory hurdles regarding the security of sensitive information.[11] Accordingly, banks proved to be reticent to use public cloud services, as moving to the public cloud would require addressing access, encryption, and legal and compliance issues.[12]

---

[10] *See, e.g.*, *12 Risks, Threats, & Vulnerabilities in Moving to the Cloud*, CARNEGIE MELLON UNIVERSITY BLOG (March 5, 2018), available at https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html.

[11] Federal Reserve Bank of Atlanta, *Supervisory Considerations in Cloud Computing in the Financial Services Industry* (May 8, 2018), available at https://www.frbatlanta.org/economy-matters/banking-and-finance/viewpoint/2018/05/supervisory-considerations-in-cloud-computing-in-the-financial-services-industry.

[12] *See id.*

34. Despite these inherent security risks, in 2015 Capital One announced that it would move all of its data to the public cloud, and in 2016, Capital One announced that it would make AWS its predominant public cloud provider.

35. Amazon touted the AWS cloud environment as a technology-forward solution for Capital One's aggressive data collection strategy. Partnering with AWS allowed Capital One to use Amazon's data scientists and artificial intelligence tools[13] to analyze the trove of customer data it collected from credit applicants.

36. The strategy was an aggressive move into uncharted territory for a major bank. Migration to AWS's cloud servers would mean that customer data would no longer be in the bank's physical custody; instead, it would be in the hands of a third-party partner, AWS.

37. For this move to work, Capital One would have to convince its present and prospective customers that their information would be safe. With this in mind, both Capital One and AWS charted a course to make deceptive, false, misleading and unfair representations regarding the collection of customer data sitting on the public cloud.

38. For example, in July 2015, Capital One Chief Executive Officer Rich Fairbanks, noting that "increasingly we're focusing on cloud computing," assured customers that "[w]e're investing in cyber security. This is an incredibly important area and we are putting a lot of very top talent and a lot of energy and investment into that."[14]

---

[13] AWS, *AWS Marketplace, Data Science Tools*, available at https://aws.amazon.com/marketplace/solutions/machine-learning/data-science-tools (last visited March 2, 2020).

[14] Sara Hoisington, *Capital One: Banking Is Inherently A Digital Business* (July 24, 2015), available at https://conferencetrackerblog.wordpress.com/2015/07/24/capital-one-banking-is-inherently-a-digital-business/.

39. In October 2015, at an Amazon-sponsored industry event known as "AWS re:Invent 2015," Capital One's Chief Information Officer Rob Alexander used his keynote address to announce that Capital One would be shifting its data to the cloud. In those remarks he stated:

> [S]ecurity is critical for us. The financial services industry attracts some of the worst cyber criminals so we work closely with the Amazon team to develop a security model which we believe enables us to operate more securely in the public cloud than we can even in our own data centers.[15]

40. Despite these public statements suggesting a commitment to data security, including data security in the cloud, Capital One instead undertook a risky move of consumer data to AWS, an environment with well-known data security vulnerabilities.

C. AWS Cloud Computing's Default Settings Have Known Vulnerabilities

41. The AWS cloud environment has long suffered from a widely known flaw. As explained in detail below, AWS servers—unlike those run by its competitors—were not secured against what are known as Server Side Request Forgery ("SSRF") attacks. Simply stated, SSRF attacks allow an intruder to penetrate a firewall and exfiltrate data to a third-party server. Year after year this flaw was the subject of discussion at some of the largest cybersecurity conferences in the United States. Each year, presentations were made expressly calling out the SSRF vulnerability in AWS's cloud computing services.[16]

42. AWS's servers facilitate machine learning by allowing large amounts of data to be collected in a common pool, which is segmented into folders. This AWS configuration allows for

---

[15] Rob Alexander (CIO of Capital One), *AWS re:Invent 2015 Keynote*, available at https://www.youtube.com/watch?v=0E90-ExySb8.

[16] Rob Wright, *Capital One Hack Highlights SSRF Concerns for AWS*, TECHTARGET (Aug. 5, 2019), available at https://searchsecurity.techtarget.com/news/252467901/Capital-One-hack-highlights-SSRF-concerns-for-AWS; *see also*, Sen Ron Wyden and Sen. Elizabeth Warren, Letter to FTC (Oct. 24, 2019), available at https://www.wyden.senate.gov/imo/media/doc/102419%20Wyden%20Warren%20Letter%20to%20FTC%20RE%20Amazon%20Capital%20One%20Hack.pdf.

different web applications to draw from a vast collection of data but also allows for the configuration of access "policies" to allow the application to only pull the data it needs, and nothing more. One way to do this is through Identity and Access Management ("IAM") roles.

43. An IAM role is an identity created in an account that has specific permissions that determines what the identity can or cannot do in AWS. Unlike a username or credential associated with a specific person, an IAM role is intended to be assumable by anyone who needs it. An entity can use IAM roles to delegate access to users, applications, or services that do not normally have access to the restricted AWS data, or resources, stored by the owner of the cloud.[17] These IAM roles are used on AWS to allow various computers access to particular resources on a dynamic basis. For example, a computer on Capital One's system with an IAM role configured to allow broad access, as required to run machine learning algorithms for example, could allow that computer to access the entire data collection while another computer with a more restrictive IAM role may restrict access only to a small subset of consumer data.

44. While the IAM roles work to regulate access to data within the AWS server, the only defense protecting the data from outside penetration is a firewall. A firewall is, in effect, a shield placed between a server and traffic originating from the outside the server. It is designed to block unauthorized access while permitting authorized access and outward communication.

45. A firewall uses programmed rules to distinguish between legitimate access requests, which it permits, and unauthorized and illegitimate access requests, which it denies. If a request is legitimate, then the firewall automatically assigns the requester a "role." These roles establish what

[17] AWS, *AWS Identity and Access Management User Guide*, available at https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html (last visited March 2, 2020).

portions of the server the requester will have access to as well as the conditions of that access. The requester receives temporary credentials assigned to that role.

46. A firewall also, among other purposes, ensures that sensitive resources on a computer network are not exposed directly to the Internet. For web applications that need to pass data to and from a user on the open Internet—such as a credit card application—a Web Application Firewall ("WAF") is used. A WAF filters, monitors, and blocks web traffic to and from a web application.

47. But the firewalls used on the AWS cloud are known to be vulnerable to an SSRF attack. In an SSRF attack, an attacker tricks a server—in this case the WAF—into thinking that the attacker is permitted to request and access data from the server. By tricking a server into thinking that it is receiving a legitimate request for resources from inside the firewall (rather than an illegitimate request from outside), the attacker obtains a foothold inside the targeted network.

48. However, despite this being a well-known problem deployed by hackers, AWS has no protections built into its systems to protect against an SSRF attack. Instead, because Amazon uses IAM roles to control access to sensitive resources, such as data stored on the cloud, an attacker who gains access to a resource behind a firewall can then assume a privileged IAM role and can gain access to whatever data the role can access.

49. This vulnerability to SSRF attacks is a well-known flaw in AWS-based systems. By contrast, Amazon's competitors, such as Google and Microsoft, have built protections against SSRF into their cloud-based products.[18]

[18] *See* Letter from Senators Elizabeth Warren and Ron Wyden to the Federal Trade Commission (Oct. 24, 2019), available at https://www.wyden.senate.gov/imo/media/doc/102419%20Wyden%20Warren%20Letter%20to%20FTC%20RE%20Amazon%20Capital%20One%20Hack.pdf; *see also Is AWS Liable in Capital One Data Breach*, THREATPOST (Oct. 25, 2019), available at

50. According to Evan Johnson, manager of the product security team at Cloudflare, "SSRF has become the most serious vulnerability facing organizations that use public clouds . . . . The impact of SSRF is being worsened by the offering of public clouds, and the major players like AWS are not doing anything to fix it. The problem is common and well-known, but hard to prevent and does not have any mitigations built into the AWS platform."[19]

51. In 2016, Capital One and AWS jointly announced that together they had developed a new product it called Cloud Custodian. Defendants announced that with Cloud Custodian they had solved the security problems inherent in using the AWS cloud for machine learning at scale,[20] and have billed Cloud Custodian as a comprehensive cloud security tool which would automatically detect and fix security flaws.[21]

52. Defendants represented that Cloud Custodian would, among other things, automatically scan Capital One's internal systems to ensure that all of the servers and permissions were set according to defined policies.[22] Additionally, Defendants represented that Cloud Custodian would grant the minimum amount of access necessary to complete a given task.[23]

---

https://threatpost.com/capital-one-breach-senators-aws-investigation/149567/.

[19] *What We Can Learn from the Capital One Hack*, KREBS ON SECURITY (Aug. 2, 2019), available at https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/.

[20] Henrik Johanson and Kapil Thangavlu, *AWS Summit: Protecting Your Data In AWS*, (Apr. 19, 2016), available at https://www.slideshare.net/AmazonWebServices/protecting-your-data-in-aws-61113337 (last visited March 2, 2020); *see also*, AWS, *Announcing Cloud Custodian Integration with AWS Security Hub* (Nov. 29, 2018), available at https://aws.amazon.com/blogs/opensource/announcing-cloud-custodian-integration-aws-security-hub/.

[21] *See* Kapil Thangavelu, *AWS re:Invent 2018: Cloud Custodian- Open Source AWS Security & Governance* (DEM78), available at https://www.youtube.com/watch?v=oY8Nmh6B7P8.

[22] Kapil Thangavelu, *Cloud Custodian A Serverless Rules Engine For the Cloud* (Nov. 2018), available at https://www.youtube.com/watch?v=hm9Bx2MHyNw (last visited March 2, 2020).

[23] *Id.*

53. Moreover, Defendants boasted that Cloud Custodian would automatically encrypt all data on the AWS servers.[24] But encrypting the data stored on the AWS servers did not solve the security vulnerability. Credentials assigned with IAM roles automatically decrypt the data the role is allowed to access. Therefore, if an intruder is able to gain access to an IAM role and get past the firewall, the IAM role will decrypt the data, allowing the unauthorized user access to unencrypted data. In other words, one key unlocks both sets of doors—the firewall and the encryption.

54. At Amazon's yearly re:Invent conference in November 2018, Capital One's Senior Distinguished Engineer Kapil Thangavelu gave a presentation showcasing Cloud Custodian.[25] Several minutes into his presentation, Thangavelu discussed IAM roles and described the precise vulnerability in "S3"[26]—the AWS cloud service—that would result in the Data Breach the next year:

> In the cloud, all these resources are just available via URL so those are part of your network boundary. And those resources that have embedded IAM policies need special care and attention because they can be enabled to be accessible outside of your account. I think everyone's familiar with some of the things around S3 but that extends out to a lot of the other resources I called out a couple here.[27]

55. With S3, IAM roles determine what buckets of data on the server the user is allowed to access. Thus, if a company grants broad permissions to its IAM roles, then an unauthorized user who gains access to an IAM role also gains broad access to all of the now-unencrypted data stored in the cloud environment. With that presentation, Capital One's Senior Distinguished Engineer[28]

---

[24] Kim Nash, *CIO Voices: Capital One's Rob Alexander on How to Win in Banking*, WALL STREET JOURNAL CIO JOURNAL (Nov. 30, 2016), available at https://blogs.wsj.com/cio/2016/11/30/cio-voices-capital-ones-rob-alexander-on-how-to-win-in-banking/.

[25] Kapil Thangavelu, *AWS re:Invent 2018: Cloud Custodian - Open Source AWS Security & Governance* (DEM78), available at https://www.youtube.com/watch?v=oY8Nmh6B7P8

[26] Amazon Simple Storage, known as S3.

[27] *AWS re:Invent 2018: Cloud Custodian¸ supra* n. 27.

[28] In January 2019, approximately one month after his presentation at re:Invent 2018, Thangavelu left Capital One and joined Amazon AWS as a Principal OpenSource Technologist.

acknowledged the known vulnerability in AWS's system that persisted despite the implementation of Cloud Custodian in 2016. And that risk still existed in 2019.

56. Capital One and Amazon appreciated and intentionally assumed a known risk that despite any benefits of Cloud Custodian, a broadly configured IAM role, if assumed from inside the firewall, would grant full access to the data stored on an AWS server. It was this known vulnerability that allowed the theft of Capital One's customer data in March 2019.

D. The Known Vulnerability is Exploited

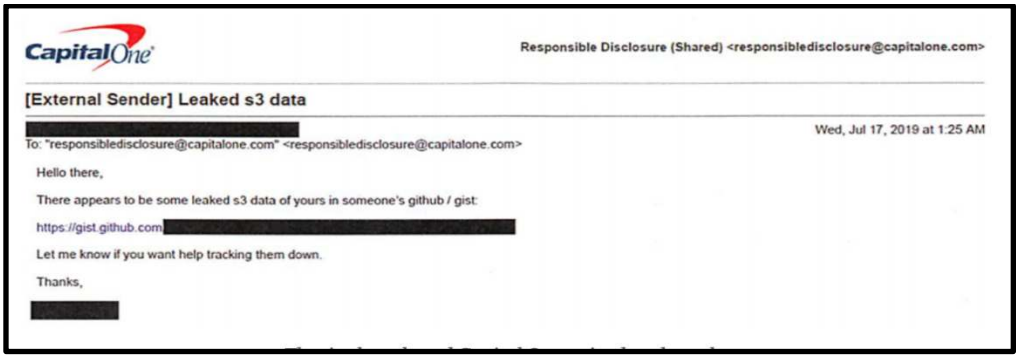
57. On July 29, 2019, Capital One announced in a filing with the Securities Exchange Commission ("SEC") that it had experienced a data breach affecting "approximately 100 million individuals in the United States and approximately 6 million in Canada."[29]

58. As detailed in the criminal complaint filed by the Federal Bureau of Investigation ("FBI") against the alleged hacker, Paige A. Thompson (a/k/a "erratic"), Thompson publicly posted instructions about how to access the stolen data on Github, a software development platform on which users can share information or collaborate on open source code projects, in a file timestamped April 21, 2019.[30] Thompson had previously worked as a "systems engineer" for Defendant Amazon Web Services.

[29] July 29 Form 8-K.

[30] *See United States v. Paige A. Thompson, a/k/a "erratic,"* Complaint at 10, Case No. 2:19-mj-00344 (W.D. Wash.) (filed July 29, 2019) (hereinafter, "Thompson Criminal Complaint"), available at https://www.justice.gov/usao-wdwa/press-release/file/1188626/download. On July 29, 2019, Thompson was arrested by the FBI and charged by federal prosecutors in the United States District Court for the Western District of Washington. The charges included computer fraud and abuse in violation of 18 U.S.C. § 1030(a)(2).

59. Capital One learned about the Data Breach from an anonymous tip sent by email on July 17, 2019.[31] The email advised that data belonging to Capital One had been posted on GitHub and provided the address of the GitHub file containing the data.[32]



Capital One

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

[External Sender] Leaked s3 data

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

To: "responsibledisclosure@capitalone.com" <responsibledisclosure@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]

60. According to Defendants, the intrusion occurred through a misconfigured Web Application Firewall (WAF) that Capital One was using as part of its operations hosted in the cloud with AWS.

61. Capital One had worked closely with multiple groups at Amazon to set up the cloud systems and to migrate the customer data to the cloud.[33]

62. The firewall misconfiguration permitted commands that reached and were executed by a server. The commands executed by the hacker accomplished the following:

a. Obtained security credentials for an account known as WAF-Role that allowed access to Capital One's data folders on the AWS cloud;

b. Used the security credentials to list the names of the Capital One data folders on the AWS cloud ("List Buckets Command"); and,

[31] *Id.* at ¶ 9.
[32] *Id.*
[33] *See, e.g.*, Stephen Orban, Capital One's Cloud Journey Through the Stages of Adoption, MEDIUM (April 5, 2017), available at https://medium.com/aws-enterprise-collection/capital-ones-cloud-journey-through-the-stages-of-adoption-bb0895d7772c.

c. Used the security credentials to extract or copy data from the Capital One data folders on the AWS cloud ("Sync Command").[34]

63. Capital One has confirmed that the commands function to obtain security credentials on the AWS cloud environment and that these commands could be used to extract data.[35]

64. Capital One has confirmed that the List Buckets Command was executed on April 21, 2019, which matches the timestamp of the Github file.[36]

65. While AWS has blamed Capital One for the Data Breach, it has also admitted that the SSRF vulnerability of its cloud environment played a role:

> As Capital One outlined in their public announcement, the attack occurred due to a misconfiguration error at the application layer of a firewall installed by Capital One, exacerbated by permissions set by Capital One that were likely broader than intended. After gaining access through the misconfigured firewall and having broader permission to access resources, we believe a SSRF attack was used (which is one of several ways an attacker could have potentially gotten access to data once they got in through the misconfigured firewall).[37]

66. Online, the hacker publicly exposed the code and processes through which she had discovered the vulnerability in the configuration of the AWS WAF used by Capital One, as well as the code and processes she used to gain access to the stolen data through that misconfiguration.

67. While the intrusion was sophisticated because of the abilities of the hacker and how she performed the hack, the vulnerability of the AWS WAF used by the hacker to infiltrate was, as described *supra*, well known.

---

[34] *Id*. at ¶ 11.
[35] *Id*. at ¶ 12.
[36] *Id.*
[37] AWS Letter to The Honorable Ron Wyden, United States Senate, at 1 (August 13, 2019), available at https://www.wyden.senate.gov/imo/media/doc/081319%20Amazon%20Letter%20to%20Sen%20Wyden%20RE%20Consumer%20Data.pdf.

68. Shortly after the Data Breach, Capital One and AWS worked to fix the WAF configuration to address the known vulnerability.

69. Capital One subsequently determined that 1.75 terabytes of consumer data was downloaded on or about March 22-23, 2019, although the initial hacking began weeks before. Capital One determined that the hacker first scanned its network on March 4, 2019 for vulnerabilities and first accessed its network on March 12, 2019, prior to her March 22-23 access and download. Capital One believes the hacker probed their environment three additional times on April 2, April 19, and May 26, 2019.[38]

70. Capital One's post-breach investigation revealed that the company's logs showed a number of connections or attempted connections to the AWS server from an Onion Router (also known as "TOR"), an anonymity tool used by individuals to conceal their identities and their IP address, and a number of connections from a specific IP address in March and April 2019.[39] During these March and April 2019 connections, the WAF-Role account was used to execute the List Buckets Command as well as the Sync Command to extract or copy data from Capital One's data folders on the AWS cloud environment.[40] Capital One has confirmed that unauthorized activity occurred on its AWS server on March 12, 22 and 23, 2019 and on April 21, 2019.[41]

71. That Capital One's own logs recorded multiple instances of unauthorized access and attempts of unauthorized access during March 2019, yet Capital One only learned of the Data Breach four months later from an anonymous tip, suggests that Capital One did not have adequate

[38] Capital One Defendants' Responses to Plaintiffs' First Interrogatories, at Answer to Interrogatory 9.
[39] Thompson Criminal Complaint at ¶ 13.
[40] *Id*. at ¶¶ 11-13.
[41] *See* July 29 Form 8-K; Thompson Criminal Complaint at ¶ 13.

Security Incident and Event Management ("SIEM") policies in place requiring IT-security events to be logged in a centralized location and monitored in real time.

72. Indeed, the length of time the Data Breach went unnoticed and undetected by Defendants is astonishing, in light of both the public postings made by the alleged hacker Thompson and the activity on the AWS server. Capital One, in its sworn interrogatory answers, admits that it received alerts related to the breach on March 22, April 19, and May 20, 2019, which it purports to have investigated. The May 20, 2019 alert came from Amazon who had received a handwritten note warning Amazon and Capital One that "Open Socks Proxy **.***.**.136 Can Hit IMS – lots of security credentials." Capital One now believes that the hacker stole a valid Capital One AWS Credential for its Instance Metadata Service ("IMS") role – the role mentioned in the anonymous alert.[42]

73. Capital One and Amazon also did not detect the Data Breach despite the fact that the hacker spent months posting publicly about the Data Breach online.

74. On or about June 26, 2019, "erratic" publicly posted on a Slack channel a list of files she claimed to possess, among which two referenced "WAF-Role."[43] The Sync Command placed extracted files in a directory containing the name WAF-Role.

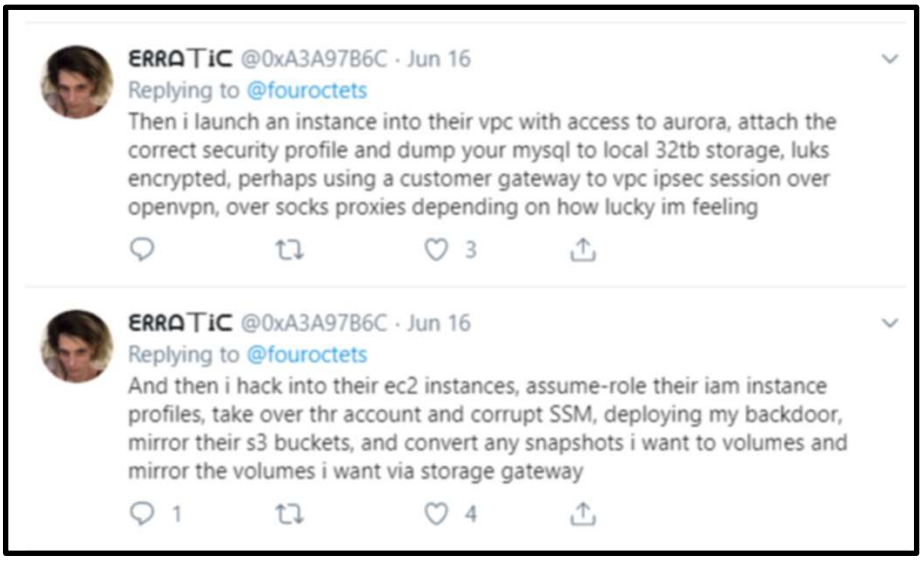
75. On or about June 27, 2019, "erratic" posted about several companies, governmental entities, and education entities, and referred to an account associated with Capital One.[44]

76. On or about July 4, 2019, the alleged hacker Thompson posted a message seeking information about the "Snappy Parquet File" which was a named file in the Capital One directory

[42] Capital One Defendants' Amended Responses to Plaintiffs' First Interrogatories, at Answers to Interrogatories 8-9.
[43] Thompson Criminal Complaint at ¶ 18.
[44] *Id*. at ¶ 19.

on the AWS server and was determined to be one of the files exfiltrated from Capital One on March 22, 2019.[45]

77. Cybersecurity investigative reporter Brian Krebs reported that Thompson posted openly on her Twitter account over the course of several months about finding huge files of data intended to be secured on various AWS cloud servers.[46]



78. The length of time the Github file remained publicly posted without Defendants' knowledge suggests that neither Capital One nor Amazon employed threat intelligence to monitor the dark web for activity involving its data, a standard practice in the financial industry.

79. Because the hacker placed the script and code she used in public areas, the code and processes could have been used by others to gain access to CapitalOne's customer data via the AWS WAF vulnerability.

E. The Scope of the Data Breach

80. The scope of the breach was staggering, with compromised data going back over a decade to 2005.

---

[45] *Id*. at ¶ 22.
[46] *Capital One Data Theft Impacts 106M People*, *supra* n.2.

81. Capital One reported that the Data Breach impacted consumers who applied for Capital One credit card products from 2005 through "early 2019," and that the compromised information included "personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income."[47]

82. In addition, Capital One also admitted the Data Breach included consumers' credit scores, credit limits, balances, payment histories, contact information, and "fragments of transaction data from a total of 23 days during 2016, 2017 and 2018."[48]

83. Capital One further admitted that "about 140,000 Social Security numbers of [its] credit card customers" and "about 80,000 linked bank account numbers of our secured credit card customers" were also disclosed in the Data Breach.[49]

84. Capital One's retention of data far exceeds customers' reasonable expectations of how long their data would be stored and how their data would be used.

F. Defendants' Knowledge of Cyber Security Threats

85. At all relevant times, Defendants were well-aware, or reasonably should have been aware, that the PII collected, maintained, and stored on the cloud is highly sensitive, susceptible to attack, and could be used for malicious purposes by third parties, such as identity theft, fraud and other misuse.

86. Banking repositories and databases are popular and well-known targets for cyberattacks, especially given the extremely sensitive nature of the PII stored on those repositories and databases. The frequency and prevalence of attacks make it imperative that banks such as

[47] July 29 Form 8-K.
[48] *Id.*
[49] *Id.*

Capital One routinely and constantly monitor for exploits and cyberattacks and regularly update their software and security procedures.

87. 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."[50]

88. With respect to cyber-security threats directed at the cloud, 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."[51]

89. Capital One itself acknowledges that "[s]afeguarding our customers' information is essential to our mission and our role as a financial institution."[52] 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[.]"[53] Yet Capital One's supposedly robust systems did not detect the repeated unauthorized access and access attempts of its system.

---

[50] Capital One Financial Corporation, 2018 Form 10-K, at 24 ("2018 Form 10-K"), available at https://www.sec.gov/Archives/edgar/data/927628/000092762819000093/cof1231201810kfinal.pdf.
[51] *Id.*
[52] July 29 Form 8-K.
[53] 2018 Form 10-K, at 24.

90. 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 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.[54]

91. In addition to its appreciation of threats imposed by external attacks, Capital One—and Amazon—were aware, or should have been aware, of security vulnerabilities posed by current and former employees of both Capital One and Amazon, as well as the well-known security vulnerabilities to the cloud, as described *supra*.

92. Despite being the holder of PII 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 invest adequately in data security, despite the growing number of well-publicized data breaches affecting the financial industry and similar industries.

G. The Capital One Defendants Breached Their Promises to Plaintiffs

93. Capital One's Privacy and Opt-Out 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 provide in order to obtain the services] from unauthorized access and use [by employing] security measures that comply with federal law."[55]

[54] July 2017 Capital One Data Breach Notice, available at https://dojmt.gov/wp-content/uploads/Capital-One-1.pdf.

[55] Capital One, *Privacy and Opt-Out Notice*, https://www.capitalone.com/privacy/notice/en-us/ (last visited March 2, 2020).

94. Further, in its Privacy Statement, Capital One advises its customers:

> At Capital One, we make your safety and security a top priority and are committed to protecting your personal and financial information. If we collect identifying information from you, we will protect that information with controls based upon internationally recognized security standards, regulations, and industry-based best practices.[56]

95. 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."[57]

96. Yet, despite these promises to protect its customers' Personal Information, Capital One failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to Plaintiffs' and class members data. 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 its promises to do so. As a result, an unauthorized individual was able to exploit a well-known vulnerability and steal Capital One's customers' unencrypted data.

H. Defendants Failed to Comply with Regulatory Requirements and Industry Practices

97. As Capital One acknowledges in its Privacy Statement, federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. There are a number of state and federal laws and requirements and industry standards governing the protection of PII.

---

[56] Capital One, *Capital One Online & Mobile Privacy Statement*, available at https://www.capitalone.com/bank/mobile-privacy-statement/disclosures/ (last visited March 2, 2020).

[57] Capital One, *Bank Securely*, https://www.capitalone.com/applications/identity-protection/commitment/ (last visited March 2, 2020).

98. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license or maintain personal information, or PII, about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect PII from unauthorized access. California is one such state and requires that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use modification or disclosure." Cal. Civ. Code § 1798.81.5(b).

99. The Federal Trade Commission ("FTC"), which is responsible for enforcing the Safeguards Rule, has issued guidance and published regulatory decisions interpreting the measures financial institutions must take to comply with the Safeguards Rule. The FTC recommends:

- limiting access to customer information to employees who have a business reason to see it;
- keeping customer information in encrypted files provides better protection in case of theft;
- maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information;
- using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information;
- monitoring both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and,
- monitoring activity logs for signs of unauthorized access to customer information.[58]

[58] Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, available at https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (last visited March 2, 2020).

100. The Federal Trade Commission has also issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[59]

101. 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.[60] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of PII 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.

102. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; 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.[61]

103. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

---

[59] Federal Trade Commission, *Start With Security* at 2, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 2, 2020).

[60] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited March 2, 2020).

[61] FTC, *Start With Security*, *supra*.

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 ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

104. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data. The body of law created by the FTC recognizes that failure to restrict access to information[62] and failure to segregate access to information[63] may violate the FTC Act.

105. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data (i.e., PII) constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

106. The PCI (Payment Card Industry) Security Standards Council, of which Capital One is a participant, has published its *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures* ("PCI-DSS"), the latest version of which (3.2.1) is dated May 2018.[64]

107. Capital One violated the mandates of PCI-DSS concerning data retention, encryption, and access.

---

[62] *In the Matter of LabMD, Inc.*, Dkt. No. 9357, Slip Opinion, at 15 ("Procedures should be in place that restrict users' access to only that information for which they have a legitimate need."), available at https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf.

[63] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 258 (3d Cir. 2015) (companies should use "readily available security measures to limit access between" data storage systems).

[64] *Payment Card Industry Data Security Standard* v3.2.1 (May 2018), available at https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1580206053881.

108. In this case, Capital One was at all times fully aware of its obligation to protect the financial data—including PII—of Capital One's applicants because of its status as a one of the United States' largest financial institutions. Capital One was also aware of the significant repercussions if it failed to do so because Capital One collected applicant data from millions of consumers daily and it knew that this data, if hacked, would result in injury to consumers, including Plaintiffs and class members.

I. Capital One is Subject to the Gramm-Leach-Bliley Act

109. Capital One is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

110. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

111. Capital One collects nonpublic PII, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Capital One was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1 *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

112. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

113. Accordingly, Capital One's conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

114. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic PII the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic PII. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Capital One violated the Privacy Rule and Regulation P.

115. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract

to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Capital One violated the Safeguard Rule.

116. Capital One failed to assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information.

117. Capital One's conduct resulted in a variety of failures to follow GLB mandated rules and regulations, many of which are also industry standard. Among such deficient practices, the Data Breach demonstrates that Capital One failed to implement (or inadequately implemented) information security policies or procedures such as effective employee training, adequate intrusion detection systems, regular reviews of audit logs and records, and other similar measures to protect the confidentiality of the PII it maintained in its data systems, instead outsourcing such responsibilities to the Amazon Defendants.

118. More specifically, Capital One's security failures demonstrate that it failed to honor its express and implied promises by failing to:

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

b. Adequately protect Plaintiff's and class members' PII;

c. Implement policies and procedures to prevent, detect, contain, and correct security violations;

d. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;

e. Protect against any reasonably anticipated threats or hazards to the security or integrity of PII; and

f. Effectively train all members of its workforce on the policies and procedures with respect to PII as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PII.

119. Had Capital One implemented the above-described data security protocols, the consequences of the data exposure could have been avoided, or at least significantly reduced as the exposure could have been detected earlier, the amount of PII compromised could have been greatly reduced, and affected consumers could have been notified—and taken protective/mitigating actions—much sooner.

J. Defendants' Delays in Discovery and Notice of the Data Breach

120. It took Defendants approximately four months—from March to July 2019—to realize Capital One's vast collection of customer PII stored on the AWS cloud had been breached. That discovery occurred not because of Defendants' own diligence, but because an unknown third party alerted Capital One.

121. Further compounding the negative consequences of the Data Breach, Defendants then failed to provide timely notice to affected class members. Remarkably, Capital One chose not to directly notify the vast majority of individuals affected by the Data Breach; rather, it merely published a press release, leaving victims in the dark as to whether their information had, in fact, been compromised. Without detailed disclosures to Capital One's customers, many class members are even to this day unknowingly and unwittingly left exposed to continued misuse and ongoing risk of misuse of their PII without being able to take necessary precautions to prevent imminent harm.

122. Defendants' delays in discovering and announcing the breach left all Plaintiffs and class members exposed and unable to take precautions.

K. The Effect of the Data Breach on Impacted Customers

123. Defendants' failure to keep Plaintiffs' and class members' PII secure has severe ramifications. Given the sensitive nature of the PII 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 commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and class members now and into the indefinite future.

124. The PII 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 PII 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.

125. This is especially true for data held by banks, given that the PII compromised in this Data Breach was precisely the PII Capital One used to extend credit to customers, meaning data

thieves had access to a single data set to commit fraud through, for example, opening new lines of credit.

126. PII has significant monetary value in part because criminals continue their efforts to obtain this data.[65] In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. Instead, just the opposite has occurred. For example, the Identity Theft Resource Center reported 1,473 data breaches in 2019, which represents a 17 percent increase from the total number of breaches reported in 2018.[66]

127. The PII of consumers remains of high value to identity criminals, as evidenced by the prices criminals will pay through black-market sources on the dark web. Numerous sources cite dark web pricing for stolen identity credentials, quantifying the loss to victims based on the value of the data itself. For example, a complete set of bank account credentials can fetch a thousand dollars or more.[67]

128. Just as companies like Capital One and Amazon trade on the value of consumers' PII, consumers recognize the value of their PII and offer it in exchange for goods and services. Plaintiffs gave Capital One their PII in exchange for Capital One's services, such as providing or potentially providing credit. Further, the value of PII is key to unlocking many parts of the financial sector for consumers. Whether someone can obtain a mortgage, credit card, business loan, tax

---

[65] *Data Breaches Rise as Cybercriminals Continue to Outwit IT*, CIO MAGAZINE (Sept. 28, 2014), available at http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html.

[66] Identity Theft Center, *2019 End-of-Year Data Breach Report* (2019), available at https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf.

[67] *Here's How Much Thieves Make By Selling Your Personal Data Online,* BUSINESS INSIDER (May 27, 2015), available at http://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5.

return, or even apply for a job depends on the integrity of their PII. Similarly, the businesses that request (or require) consumers to share their PII as part of a commercial transaction do so with the expectation that its integrity has not been compromised.

129. 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.[68]

130. 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.[69]

131. 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:

> Keep in mind that a new number probably won't 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. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

---

[68] Javelin, *2018 Identity fraud: Fraud Enters A New Era of Complexity*, available at https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity (last visited March 2, 2020).

[69] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited March 2, 2019).

> If you receive a new Social Security Number, you shouldn't 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.[70]

132. 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.[71]

133. 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.[72] 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.

---

[70] Social Security Administration, *Identity Theft and Your Social Security Number*, available at http://www.ssa.gov/pubs/10064.html (last visited March 2, 2020).
[71] U.S. Department of Justice, *Victims of Identity Theft, 2014* (Revised November 13, 2017), available at http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited March 2, 2020).
[72] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, available at https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited March 2, 2020).

134. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey[73] evidences the emotional suffering experienced by victims of identity theft:

- 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.

135. 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.[74]

[73] *Id.*
[74] *Id.*

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[75]

137. 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 services they would not have otherwise paid for and/or paying more for services than they otherwise would have paid, had they known the truth about Defendants' substandard data security practices;
- losing the inherent value of their PII;
- 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 PII;
- costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- costs associated with purchasing credit monitoring 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 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;

[75] U.S. Government Accountability Office, *Report to Congressional Requesters* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited March 2, 2020).

- 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 PII being in the possession of one or many unauthorized third parties.

138. 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.[76]

139. 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.

140. Consequently, had consumers known the truth about Defendants' data security practices—that Defendants would not adequately protect and store their data—they would not have entrusted their PII to Capital One, applied for a Capital One credit card or remained a Capital One customer, and would not have been willing to pay as much for Capital One's services. As such,

[76] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited March 2, 2020).

Plaintiffs and class members did not receive the benefit of their bargain with Capital One because they paid for a value of services they expected but did not receive.

CLASS ACTION ALLEGATIONS

141. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Class" or the "Nationwide Class"):

All persons in the United States whose PII was compromised in the Data Breach.

142. The Nationwide Class asserts claims against all Defendants for negligence (Count 1), negligence *per se* (Count 2), unjust enrichment (Count 3), and declaratory judgment (Count 4), and against the Capital One Defendants only for breach of confidence (Count 5), breach of contract (Count 6), and breach of implied contract (Count 7).

143. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of state-by-state claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes (Counts 8 through 15), on behalf of separate statewide subclasses for the States of California, Florida, Texas, and Washington (the "State Subclasses"), defined as follows:

All persons in [name of state] whose PII was compromised in the Data Breach.

144. Excluded from the Nationwide Class and each State Subclass are Defendants, any entity in which any Defendant has a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and each State Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

145. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

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

147. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Nationwide Class and each State Subclass are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of class members is unknown to Plaintiffs at this time, Capital One has acknowledged that the PII of approximately 100 million persons throughout the United States was compromised in the Data Breach. Those persons' names and addresses are available from Capital One's records and in data maintained by Amazon, 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 notice, and/or published notice.

148. **Predominance of Common Issues. 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:

a. Whether Defendants knew or should have known that their computer and data storage systems were vulnerable to attack, including but not limited to, that their web application firewall was vulnerable to attack by an SSRF;

b. Whether Defendants omitted or misrepresented material facts regarding the security of their computer and data storage systems and their inability to protect the vast amounts of consumer data, including Plaintiffs' and class members' PII, hosted by the Amazon Defendants for the Capital One Defendants;

c. Whether Defendants failed to take adequate and reasonable measures to ensure such computer and data systems were protected;

d. Whether Defendants failed to take available steps to prevent and stop the Breach from happening;

e. Whether Defendants owed tort duties to Plaintiffs and class members to protect their PII;

f. Whether Defendants owed a duty to provide timely and accurate notice of the Data Breach to Plaintiffs and class members;

g. Whether Defendants breached their duties to protect the PII of Plaintiffs and class members by failing to provide adequate data security;

h. Whether Defendants' failure to secure Plaintiffs' and class members PII in the manner alleged violated federal, state and local laws, or industry standards;

i. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unauthorized access to and/or theft of Plaintiffs' and class members' PII;

j. Whether Capital One has a contractual obligation to use reasonable security measures and whether it complied with such contractual obligation;

k. Whether Defendants' conduct amounted to violations of state consumer protection statutes, and/or state data breach statutes;

l. Whether, as a result of Defendants' conduct, Plaintiffs and class 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;

m. Whether the Capital One Defendants should retain the money paid by Plaintiffs and class members to protect their PII;

n. Whether Defendants should retain Plaintiffs' and class members' valuable PII;

o. Whether, as a result of Defendants' conduct, Plaintiffs and class members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

149. **Typicality. Fed. R. Civ. P. 23(a)(3).** As to the Nationwide Class and each State Subclass, Plaintiffs' claims are typical of other class members' claims because Plaintiffs and class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

150. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Classes because Plaintiffs are members of the Classes and are committed to pursuing this matter against Defendants to obtain relief for the Classes. Plaintiffs have no conflicts of interest with the Classes. Plaintiffs' Lead Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the interests of all of the Classes.

151. **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 plaintiffs and class members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the class mmbers are relatively small

compared to the burden and expense required to individually litigate their claims against Defendants, and thus, individual litigation to redress Defendants' 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.

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

153. 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.

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

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1

NEGLIGENCE

Against all Defendants, On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the State Subclasses

155. Plaintiffs repeat and allege Paragraphs 1–157, as if fully alleged herein.

156. The Capital One Defendants required Plaintiffs and class members to submit sensitive personal information, including their PII, in order to obtain credit card and banking services. The Capital One Defendants and the Amazon Defendants stored this vast treasure trove of PII on the Amazon Defendants' cloud computing platforms.

157. By collecting, storing, using, and profiting from this data, the Capital One Defendants and the Amazon Defendants each had a duty of care to Plaintiffs and class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting this PII in Defendants' 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 Defendants' security systems and data storage architecture to ensure that Plaintiffs' and class members' PII was adequately secured and protected; (b) implementing processes that would detect an unauthorized breach of Defendants' security systems and data storage architecture in a timely manner; (c) timely acting upon all warnings and alerts, including public information, regarding Defendants' security vulnerabilities and potential compromise of the compiled data of Plaintiffs and millions of class members; and (d) maintaining data security measures consistent with industry standards.

158. The Capital One Defendants and the Amazon Defendants had common law duties to prevent foreseeable harm to Plaintiffs and class members. These duties existed because Plaintiffs and class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendants knew that it was more likely than not Plaintiffs and other class members would be harmed by such theft.

159. Defendants had a duty to monitor, supervise, control, or otherwise provide oversight to safeguard the PII that was collected and stored on the Amazon Defendants' cloud computing platforms.

160. Defendants' duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiffs and class members, on the other hand. The special relationship arose because Plaintiffs and class members entrusted Defendants with their PII as part of the applications for, opening, or use of credit cards or banking services with the Capital One Defendants. Defendants alone could have ensured that their security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

161. Defendants' duties 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 PII. Various FTC publications and data security breach orders further form the basis of Defendants' duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

162. Capital One's duty to use reasonable security measures also arose under the GLBA, under which Capital One was required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

163. Defendants knew or should have known that the Amazon Defendants' cloud computing systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII.

164. Defendants breached the duties they owed to Plaintiffs and class members described above and thus were negligent. Defendants 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 PII of Plaintiffs 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.

165. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and class members, their PII would not have been compromised.

166. As a direct and proximate result of the Capital One Defendants' negligence and the Amazon Defendants' negligence, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT 2

NEGLIGENCE *PER SE*

Against all Defendants, On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the State Subclasses

167. Plaintiffs repeat and allege Paragraphs 1–157, as if fully alleged herein.

168. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

169. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendants' systems.

170. Capital One's duty to use reasonable security measures also arose under the GLBA, under which Capital One was required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

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

172. Capital One's violation of the GLBA and its Safeguards Rule constitutes negligence per se.

173. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes), and the GLBA, were intended to protect.

174. 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 Plaintiffs and class members. The GLBA, with its Safeguards Rule, was similarly intended.

175. As a direct and proximate result of the Capital One Defendants' negligence and the Amazon Defendants' negligence, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT 3

UNJUST ENRICHMENT

Against all Defendants, On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the State Subclasses

176. Plaintiffs repeat and allege Paragraphs 1–157, as if fully alleged herein.

177. Plaintiffs and class members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by Defendants and that was ultimately stolen in the Data Breach.

178. Defendants were benefitted by the conferral upon them of the PII pertaining to Plaintiffs and class members and by their ability to retain, use, and profit from that information. Defendants understood that they were in fact so benefitted.

179. Defendants also understood and appreciated that the PII pertaining to Plaintiffs and class members was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of that PII.

180. But for Defendants' willingness and commitment to maintain its privacy and confidentiality, that PII would not have been transferred to and entrusted with Defendants.

181. Defendants continue to benefit and profit from their retention and use of the PII while its value to Plaintiffs and class members has been diminished.

182. Capital One also benefitted through its unjust conduct by selling credit card and banking services for more than those services were worth to Plaintiffs and class members, who would not have applied for or used Capital One credit cards at all, or at the terms offered by Capital One, had they been aware that Capital One would fail to protect their PII.

183. Capital One also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs' and class members' PII.

184. It is inequitable for Defendants to retain these benefits.

185. As a result of Defendants' wrongful conduct as alleged in this Complaint (including, among things, their knowing failure to employ adequate data security measures, their continued

maintenance and use of the PII belonging to Plaintiffs and class members without having adequate data security measures, and their other conduct facilitating the theft of that PII), Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and class members.

186. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and class members' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

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

188. The benefits conferred upon, received, and enjoyed by Defendants were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendants to retain these benefits.

189. Plaintiffs have no adequate remedy at law.

190. Defendants are therefore liable to Plaintiffs and class members for restitution or disgorgement in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including specifically: the value to Defendants of the PII that was stolen in the Data Breach; the profits Defendants are receiving from the use of that information; the amounts that Capital One overcharged Plaintiffs and class members for use of their credit card and banking services; and the amounts that Capital One should have spent to provide reasonable and adequate data security to protect Plaintiffs' and class members' PII.

COUNT 4

DECLARATORY JUDGMENT

Against all Defendants, On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the State Subclasses

191. Plaintiffs repeat and allege Paragraphs 1–157, as if fully alleged herein.

192. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., the 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.

193. An actual controversy has arisen in the wake of the Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and class members from further data breaches that compromise their PII. Plaintiffs remain at imminent risk that further compromises of their PII will occur in the future.

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

a. Defendants continue to owe a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, the GLBA, and various state statutes;

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

195. The Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

196. If an injunction is not issued, Plaintiffs and class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Capital One or Amazon. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs 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.

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

198. 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 or Amazon, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose PII would be further compromised

COUNT 5

BREACH OF CONFIDENCE

Against the Capital One Defendants, On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the State Subclasses

199. Plaintiffs restate and realleges paragraphs 1–157, as if fully set forth herein.

200. At all times during Plaintiffs' and class members' interactions with Capital One, Capital One was fully aware of the confidential and sensitive nature of Plaintiffs' and class members' PII.

201. As alleged herein and above, Capital One's relationship with Plaintiffs and class members was governed by terms and expectations that Plaintiffs' and class members' protected PII would be collected, stored, and protected in confidence, and would not be disclosed to the public or any unauthorized third parties.

202. Plaintiffs and class members provided their respective PII to Capital One with the explicit and implicit understandings that Capital One would protect and not permit the PII to be disseminated to the public or any unauthorized parties.

203. Plaintiffs and class members also provided their respective PII to Capital One with the explicit and implicit understandings that Capital One would take precautions to protect the PII from unauthorized disclosure, such as following basic principles of encryption and information security practices.

204. Capital One voluntarily received in confidence Plaintiffs' and class members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

205. Due to Capital One's failure to prevent, detect, avoid the Data Breach from occurring by following best information security practices to secure Plaintiffs' and class members' PII, Plaintiffs' and class members' PII was disclosed and misappropriated to the public and unauthorized third parties beyond Plaintiffs' and class members' confidence, and without their express permission.

206. But for Capital One's disclosure of Plaintiffs' and class members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Capital One's Data Breach was the direct and legal cause of the theft of Plaintiffs' and class members' PII, as well as the resulting damages.

207. The injury and harm Plaintiffs and class members suffered was the reasonably foreseeable result of Capital One's unauthorized disclosure of Plaintiffs' and class members' PII. Capital One knew its computer systems and technologies for accepting, securing, and storing Plaintiffs' and class members' PII had serious security vulnerabilities because Capital One failed to observe even basic information security practices or correct known security vulnerabilities.

208. As a direct and proximate result of Capital One's breaches of confidence, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT 6

BREACH OF CONTRACT

Against the Capital One Defendants, On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the State Subclasses

209. Plaintiffs repeat and allege Paragraphs 1–157, as if fully alleged herein.

210. Capital One's Privacy and Opt-Out Notice (the "Notice") is an agreement between Capital One and persons who provided their PII to Capital One, including Plaintiffs and class members.

211. 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 PII provided by customers and applicants of Capital One's services.

212. The Notice provides detailed information about what types of PII 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."

213. Plaintiffs and class members on the one hand and Capital One on the other formed a contract when Plaintiffs and class members provided PII to Capital One subject to the Notice.

214. Plaintiffs and class members fully performed their obligations under the contract with Capital One.

215. Capital One breached its agreement with Plaintiffs and class members by failing to protect their PII. Specifically, Capital One (1) failed to use reasonable measures to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

216. As a direct and proximate result of these breaches of contract, Plaintiffs and class members sustained actual losses and damages as described in detail above, including but not limited to that they did not get the benefit of the bargain for which they paid and were overcharged by Capital One for its services.

COUNT 7

BREACH OF IMPLIED CONTRACT

Against the Capital One Defendants, On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the State Subclasses

217. Plaintiffs repeat and allege Paragraphs 1–157, as if fully alleged herein, and assert this claim in the alternative to their breach of contract claim to the extent necessary.

218. Plaintiffs and class members also entered into an implied contract with Capital One when they obtained services from Capital One, or otherwise provided PII to Capital One.

219. As part of these transactions, Capital One agreed to safeguard and protect the PII of Plaintiffs and class members.

220. Plaintiffs 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. Plaintiffs 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.

221. Plaintiffs and class members would not have provided and entrusted their PII 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 PII of Plaintiffs and class members was critical to realize the intent of the parties.

222. Plaintiffs and class members fully performed their obligations under the implied contracts with Capital One.

223. Capital One breached its implied contracts with Plaintiffs and class members to protect their PII 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.

224. As a direct and proximate result of Capital One's breach of implied contract, Plaintiffs 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 and were overcharged by Capital One for its services.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 8

CALIFORNIA UNFAIR COMPETITION LAW,

Cal. Bus. & Prof. Code §§ 17200, et seq.

Against All Defendants

225. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat and allege Paragraphs 1–157, as if fully alleged herein.

226. Defendants are "person[s]" as defined by Cal. Bus. & Prof. Code §17201.

227. Defendants violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

228. Defendants' "unfair" acts and practices include:

a. Defendants failed to implement and maintain reasonable security measures to protect Plaintiffs' and California Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Defendants failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security despite knowing the risk of cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiffs and the California Subclass, whose PII has been compromised.

b. Defendants' failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it

use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.

c. Defendants' failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendants' inadequate security, consumers could not have reasonably avoided the harms that Defendants caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82 and Cal. Fin. Code §§ 4050 et seq.

229. Defendants have engaged in "unlawful" business practices by violating multiple laws, including California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Financial Information Privacy Act, Cal. Fin. Code §§ 4050, et seq., California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, the GLBA, and California common law.

230. Defendants' unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and California Subclass members' PII, 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 despite knowing the risk of 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 Plaintiffs' and California Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the GLBA, California's Financial Information Privacy Act, Cal. Fin. Code §§ 4050, et seq., and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and California Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass members' PII, including duties imposed by the FTC Act, the GLBA, 15 U.S.C. § 45, California's Financial Information Privacy Act, Cal. Fin. Code §§ 4050, et seq., and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and California Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass members' PII, including

duties imposed by the FTC Act, 15 U.S.C. § 45, the GLBA, California's Financial Information Privacy Act, Cal. Fin. Code §§ 4050, et seq., and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.

231. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

232. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass members were injured and lost money or property: the money received by the Capital One for its services; the loss of the benefit of their bargain with and overcharges by Capital One as they would not have paid the Capital One for services or would have paid less for such services but for the 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; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

233. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and California Subclass members' rights. Defendants are of such a sophisticated and large nature that other data breaches and public information regarding security vulnerabilities put them on notice that their security and privacy protections were inadequate.

234. Plaintiffs and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable

attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 9

CALIFORNIA CONSUMER LEGAL REMEDIES ACT,

Cal. Civ. Code §§ 1750, et seq.

Against All Defendants

235. The California Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the California Subclass, repeat and allege Paragraphs 1–157, as if fully alleged herein.

236. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, et seq. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

237. Defendants are "person[s]" as defined by Civil Code §§ 1761(c) and 1770, and have provided "services" as defined by Civil Code §§ 1761(b) and 1770.

238. Civil Code section 1770, subdivision (a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

239. Civil Code section 1770, subdivision (a)(7) prohibits one who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another."

240. Plaintiffs and the California Subclass members are "consumer[s]" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

241. Defendants' acts and practices were intended to and did result in the sales of services to Plaintiffs and the California Subclass members in violation of Civil Code § 1770, including, but not limited to, the following:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

242. Defendants' representations and omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

243. Had the Defendants disclosed to Plaintiffs and class members that their computer and data storage systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, the Defendants received, maintained, and compiled Plaintiffs' and class members' PII as part of the services Defendants provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' PII. Accordingly, Plaintiffs and the California Subclass members acted reasonably in relying on the Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

244. As a direct and proximate result of the Defendants' violations of California Civil Code § 1770, Plaintiffs and California 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 and overcharges by Capital One, as they would not have paid Capital One for services or would have paid less for such services but for the 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; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

245. Plaintiffs and the California Subclass have provided notice of their claims for damages to Defendants, in compliance with California Civil Code § 1782(a).

246. Plaintiffs and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS

COUNT 10

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT,

Fla. Stat. §§ 501.201, et seq.

Against All Defendants

247. The Florida Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Florida Subclass, repeat and allege Paragraphs 1–157, as if fully alleged herein.

248. Plaintiffs and Florida Subclass members are "consumer[s]" as defined by Fla. Stat. § 501.203.

249. The Defendants advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

250. The Defendants engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Florida Subclass members' PII, 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 despite knowing the risk of 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 Plaintiffs' and Florida Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Florida Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Florida Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

251. The Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendants' data security and ability to protect the confidentiality of consumers' PII.

252. Had Defendants disclosed to Plaintiffs and class members that their data systems were not secure and, thus, vulnerable to attack, the Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, the Defendants received, maintained, and compiled Plaintiffs' and class members' PII as part of the services the Defendants provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that the Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' PII. Accordingly, Plaintiffs and the Florida Subclass members acted reasonably in relying on the Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

253. As a direct and proximate result of the Defendants' unconscionable, unfair, and deceptive acts and practices, Plaintiffs and Florida 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 and overcharges by Capital One, as they would not have paid Capital One for services or would have paid less for such services but for the 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; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

254. Plaintiffs and Florida Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE TEXAS SUBCLASS

COUNT 11

DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT,

Texas Bus. & Com. Code §§ 17.41, et seq.

Against All Defendants

255. The Texas Plaintiff identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the Texas Subclass, repeats and alleges Paragraphs 1–157, as if fully alleged herein.

256. Defendants are "person[s]" as defined by Tex. Bus. & Com. Code § 17.45(3).

257. Plaintiffs and the Texas Subclass members are "consumer[s]" as defined by Tex. Bus. & Com. Code § 17.45(4).

258. Defendants advertised, offered, or sold services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

259. Defendants engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another;

c. Advertising goods or services with intent not to sell them as advertised.

260. The Defendants' false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Texas Subclass members' PII, 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 despite knowing the risk of 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 Plaintiffs' and Texas Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Texas Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Texas Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

261. Defendants intended to mislead Plaintiffs and Texas Subclass members and induce them to rely on their misrepresentations and omissions.

262. The Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendants' data security and ability to protect the confidentiality of consumers' PII.

263. Had Defendants disclosed to Plaintiffs and class members that their data systems were not secure and, thus, vulnerable to attack, the Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, the Defendants received, maintained, and compiled Plaintiffs' and class

members' PII as part of the services the Defendants provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that the Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' PII. Accordingly, Plaintiffs and the Texas Subclass members acted reasonably in relying on the Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

264. The Defendants had a duty to disclose the above facts due to the circumstances of this case and the sensitivity and extensivity of the PII in their possession. This duty arose because Plaintiffs and the Texas Subclass members reposed a trust and confidence in the Defendants when they provided their PII to the Defendants in exchange for the Defendants' services. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and the Texas Subclass, and the Defendants because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in the Defendants. The Defendants' duty to disclose also arose from their:

a. Possession of exclusive knowledge regarding the security of the PII;

b. Active concealment of the state of their security; and/or

c. Incomplete representations about the security and integrity of their computer and data storage systems, while purposefully withholding material facts from Plaintiffs and the Texas Subclass that contradicted these representations and omissions.

265. The Defendants engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). The Defendants engaged in acts or

practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

266. Consumers, including Plaintiffs and Texas Subclass members, lacked knowledge about deficiencies in the Defendants' data security because this information was known exclusively by the Defendants. Consumers also lacked the ability, experience, or capacity to secure the PII in the Defendants' possession or to fully protect their interests with regard to their data. Plaintiffs and Texas Subclass members lack expertise in information security matters and do not have access to the Defendants' systems in order to evaluate their security controls. The Defendants took advantage of their special skill and access to the PII to hide their inability to protect the security and confidentiality of Plaintiffs and Texas Subclass members' PII.

267. The Defendants intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from the Defendants' conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from the Defendants' unconscionable business acts and practices, exposed Plaintiffs and Texas Subclass members to a wholly unwarranted risk to the safety of their PII and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Subclass members cannot mitigate this unfairness because they cannot undo the Data Breach.

268. The Defendants acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiffs' and the Texas Subclass members' rights. Defendants are of such a sophisticated and large nature that other

data breaches and public information regarding security vulnerabilities put them on notice that their security and privacy protections were inadequate.

269. As a direct and proximate result of the Defendants' unconscionable and deceptive acts or practices, Plaintiffs and the Texas 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 and overcharges by Capital One, as they would not have paid Capital One for services or would have paid less for such services but for the 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; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

270. The Defendants' unconscionable and deceptive acts or practices were a producing cause of Plaintiffs' and Texas Subclass members' injuries, ascertainable losses and economic and non-economic damages.

271. The Defendants' violations present a continuing risk to Plaintiffs and Texas Subclass members as well as to the general public.

272. Plaintiffs and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; treble damages for each act committed intentionally or knowingly; restitution; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS

COUNT 12

WASHINGTON DATA BREACH NOTICE ACT,

Wash. Rev. Code §§ 19.255.010, et seq.

Against All Defendants

273. The Washington Plaintiff identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and alleges Paragraphs 1–157, as if fully alleged herein.

274. Defendants are businesses that own, license, or maintain computerized data that includes Personal Information as defined by Wash. 10 Rev. Code §§ 19.255.010(1), (2).

275. Plaintiffs' and Washington Subclass members' PII includes Personal Information as covered under Wash. Rev. Code § 19.255.010(5).

276. Defendants are required to accurately notify Plaintiffs and Washington Subclass members following discovery or notification of the breach of their data security system if Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code §§ 19.255.010(2), (11).

277. Because Defendants discovered a breach of their security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code §§ 19.255.010(2), (11).

278. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Wash. Rev. Code §§ 19.255.010(2), (11).

279. As a direct and proximate result of Defendants' violations of Wash. Rev. Code §§ 19.255.010(2), (11), Plaintiffs and Washington Subclass members suffered damages, as described above.

280. Plaintiffs and Washington Subclass members seek relief under Wash. Rev. Code §§ 19.255.010(13)(a) and 19.255.010(13)(b), including actual damages and injunctive relief.

COUNT 13

WASHINGTON CONSUMER PROTECTION ACT,

Wash. Rev. Code Ann. §§ 19.86.020, et seq.

281. The Washington Plaintiff identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and alleges Paragraphs 1–157, as if fully alleged herein.

282. Defendants are "person[s]" as defined by Wash. Rev. Code Ann. § 19.86.010(1).

283. Defendants advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

284. Defendants engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Washington Subclass members' PII, 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 despite knowing the risk of 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 Plaintiffs' and Washington Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Washington Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Washington Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Washington Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Washington Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

285. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

286. Defendants acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Washington Subclass

members' rights. Defendants are of such a sophisticated and large nature that other data breaches and public information regarding security vulnerabilities put them on notice that their security and privacy protections were inadequate.

287. Defendants' conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, their conduct affected the public interest, including the many Washingtonians affected by the Data Breach.

288. As a direct and proximate result of Defendants' unfair methods of competition and unfair or deceptive acts or practices, Plaintiffs and Washington 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 and overcharges by Capital One, as they would not have paid Capital One for services or would have paid less for such services but for the 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; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

289. Plaintiffs and Washington Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiffs and Plaintiffs' Lead Counsel to represent the Classes as alleged herein;

b. For injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and class members, including but not limited to an order:

i. Prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. Requiring Defendants to delete, destroy and purge the PII of Plaintiffs and class members unless Capital One can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and class members;

iv. Requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and class members' PII;

v. Prohibiting Defendants from maintaining Plaintiffs' and class members' PII on the AWS cloud;

vi. Requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. Requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. Requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. Requiring Defendants to conduct regular database scanning and securing checks;

xi. Requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII , as well as protecting the PII of Plaintiffs and class members;

xii. Requiring Defendants to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. Requiring Defendants to implement a system of testing to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing

employees' compliance with Defendants' policies, programs and systems for protecting PII;

xiv. Requiring Defendants to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor the Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendants to meaningfully educate all class members about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. Requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvii. Appointing a qualified and independent third party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment.

c. For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;

d. For an award of statutory damages, trebled, and punitive or exemplary damages, as allowed by law in an amount to be determined;

e. For an award of restitution or disgorgement, in an amount to be determined;

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

g. For prejudgment interest on all amounts awarded; and

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

JURY DEMAND

Plaintiffs, on behalf of themselves and the Class of all others similarly situated, hereby demand a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: March 18, 2021

Respectfully Submitted,

/s/ *Steven T. Webster*

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

Plaintiffs' Local Counsel

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Tel: (816) 714-7100
siegel@stuevesiegel.com

Karen Hanson Riebel
LOCKRIDGE GRINDAL NAUEN, P.L.L.P
100 Washington Avenue South, Suite 200
Minneapolis, MN 55401
Tel: (612) 339-6900
khriebel@locklaw.com

John A. Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 223-5505
jyanchunis@ForThePeople.com

Plaintiffs' Co-Lead Counsel