CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

NO: 500-06-001010-194

(Class Action)
SUPERIOR COURT

M. ROYER
and
A. ABOU-KHADRA

Petitioners

-vs.-

CAPITAL ONE BANK (CANADA BRANCH)
and
CAPITAL ONE FINANCIAL CORPORATION
and
CAPITAL ONE BANK (USA), NATIONAL ASSOCIATION
and
AMAZON.COM.CA, INC.
and
AMAZON.COM, INC.
and
AMAZON WEB SERVICES CANADA, INC.
and
AMAZON WEB SERVICES, INC.
and
AMAZON TECHNOLOGIES, INC.

Respondents

RE-AMENDED APPLICATION TO AUTHORIZE THE BRINGING OF A CLASS ACTION & TO APPOINT THE PETITIONERS AS REPRESENTATIVES
(Art. 574 C.C.P. and following)

TABLE OF CONTENTS

TO ONE THE HONOURABLE MR. JUSTICE TREMBLAY OF THE SUPERIOR COURT, SITTING IN AND FOR THE DISTRICT OF MONTREAL, YOUR PETITIONERS STATE AS FOLLOWS:

I. GENERAL PRESENTATION

A) The Action

1. Petitioners wish to institute a class action on behalf of the following group, of which they are members, namely:

    - all persons, entities, or organizations resident in Quebec who were either Capital One Credit Card holders or who had applied for a Capital One Credit Card and whose personal and private information was compromised by the incident that occurred on or about March 22 and 23, 2019 (though such breach was only disclosed to the public on July 29, 2019), or any other group to be determined by the Court;

2. This is a case of negligence, whereby the Respondents, through their failure to adequately protect and safeguard Class Members' personal and private information (including by properly encrypting sensitive data), have compromised their clients' personal and private information by allowing for unauthorized access by an outside individual;

3. Further, this is a case of a delayed notice to Class Members, as the theft occurred on March 22 and 23, 2019, was apparently discovered on July 17, 2019, was confirmed on July 19, 2019, and was only disclosed to the public on July 29, 2019;

3.1 This case involves one of the biggest data security breaches in history. As will be more fully described herein, the data theft occurred when a former employee of Respondent Amazon Web Services, Inc. (Paige Thompson) obtained unauthorized access to the personal and private information of Class Members. She was thereafter captured by the FBI and indicted;

3.2 As information came to light regarding the nature of the attack, a striking set of facts began to emerge – not about the attacker herself – but about Capital One and Amazon who had together, over several years, orchestrated a massive migration of highly-sensitive data from Capital One's private cloud to a public cloud[1] (AWS cloud) under the cover of misleading statements and security software that Capital One and Amazon jointly created and jointly marketed to customers, regulators, and to the public as a means of keeping the data safe;

[1] A private cloud consists of computing resources dedicated exclusively to the customer. Capital One had historically placed its data on company-owned servers. Public clouds are computing resources maintained by a third party, not dedicated to any particular customer, in which any given customer simply leases space. The most prominent public cloud, which Capital One and millions of other customers employed, is Amazon Web Services (AWS).

3.3 Class Members entrusted their most sensitive data – data that could be used by a miscreant to assume those customers' identities – to a bank and a cloud computing company based on their reasonable belief that it would be safe and secure. Capital One and Amazon thoroughly monetized (and continue to monetize) sensitive Capital One customer data, mining it for every edge and insight about their behaviours;

3.4 This case is about Capital One and Amazon's conduct—not the data theft that revealed it. In order to obtain customer data and the lucrative interest and fees those customers generated, both Capital One and Amazon promised customers that their data was safe and protected in Amazon's AWS public cloud for storage and processing of sensitive financial data ("AWS"). These assurances have now been shown to be indisputably false and/or misleading—and they continue to be so;

3.5 As a result of the Respondents' false and/or misleading representations regarding the safety of the data under its control and/or in its possession, Class Members have paid billions of dollars in interest and fees to Capital One that they never would have paid had they known the truth: that their sensitive personal and private data was being pooled in a giant "data lake" on the world's most notoriously insecure public cloud, examined by machine learning tools while at risk of theft via a well-known, unfixed Server Side Request Forgery ("SSRF")[2] attack vector;

4. It is estimated that approximately 100 million persons were affected in the U.S. and approximately 6 million persons in Canada. With respect to Canadians, approximately 1 million social insurance numbers ("SIN") were compromised in the incident;

5. In addition to SIN numbers, it is believed at this time that the data breach affects the following sensitive information that was collected at the time that the individuals and small businesses applied for a Capital One Credit Card between 2005 and 2019 including, but not limited to: names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, self-reported income, credit card application data, bank account numbers, portions of credit card customer data, including, customer status data, e.g., credit scores, credit limits, balances, payment history, contact information, fragments of transaction data from a total of 23 days during 2016, 2017 and 2018, the whole as appears more fully from a press release issued by the Capital One Respondents on July 29, 2019 entitled "Capital One Announces Data Security Incident" and from a copy of extracts from the Capital One Respondents' website at www.capitalone.com, produced herein *en liasse* as **Exhibit R-1**;

[2] In a Server-Side Request Forgery (SSRF) attack, the attacker can abuse functionality on the server to read or update internal resources. The attacker can supply or a modify a URL which the code running on the server will read or submit data to, and by carefully selecting the URLs, the attacker may be able to read server configuration such as AWS metadata, connect to internal services like http enabled databases or perform post requests towards internal services which are not intended to be exposed.

5.1 Unbelievably, the precise conditions created by the Respondents that gave rise to the March data theft persist to this day. The Respondents continue to aggregate and mine customer data under the same unsafe conditions that existed in March of 2019. Years of customer data is even today being aggregated and shared across hundreds of data mining systems, a simple SSRF attack away from another massive theft. This unsafe aggregation of data is not a virus, it is a feature. It is one way that Capital One makes money, and it is how Amazon sells its cloud computing services. Without years' worth of aggregated customer data, both companies would lose a competitive advantage;

5.2 (…)

6. By reason of the Respondents' failure to safeguard their customers' personal and private information, Petitioners and Members of the Class have suffered damages and are entitled to claim *inter alia*:

(a) Trouble and inconvenience by having to carefully review their transactions and be on the lookout for fraud,

(b) The lost inherent value of their personal and private information, which they had been unaware was subject to unlawful access and use,

(c) Inflated prices for Capital One' services, which were represented to be of at least adequate security, but yet employed substandard data security practices,

(d) Any additional credit monitoring services/identity theft protection services not already covered by the Respondents,

(e) Identity theft and fraud resulting from the theft of their personal and private information,

(f) Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts,

(g) 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,

(h) Possible future fraud and identity theft and injury flowing therefrom,

(i) Lower credit scores resulting from credit inquiries following fraudulent activities,

(j) 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 theft, 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, anxiety and annoyance of dealing with the repercussions of the data theft,

(k) (…)

(l) Punitive damages;

B) The Respondents

(i) The Capital One Respondents

7. Respondent Capital One Financial Corporation ("Capital One U.S.") is a publicly-traded financial services company under the laws of the State of Delaware, U.S.A. Capital One U.S. issues MasterCard-branded credit cards throughout Canada, including within the province of Quebec. It is the registrant of the trade-marks "CAPITAL ONE" (TMA469123) and "CAPITAL ONE" (TMA469182), which were both filed on September 25, 1995, the whole as appears more fully from a copy of the trade-marks from the Canadian Intellectual Property Office (CIPO), produced herein *en liasse* as **Exhibit R-2**;

8. Credit is extended through Respondent Capital One Bank (Canada Branch) ("Capital One Canada"), which is a wholly-owned subsidiary of Capital One U.S. and which operates throughout Canada, including within the province of Quebec, as the Canadian branch of Respondent Capital One Bank (USA), National Association the whole as appears more fully from a copy of an extract from the *Registre des entreprises*, produced herein as **Exhibit R-3**;

8.1 Respondent Capital One Bank (USA), National Association ("COBNA") is a financial services company, which offers credit and debit card products, other lending products and deposit products. It is a wholly-owned subsidiary of Respondent Capital One U.S. that has the authority to operate as an authorized foreign bank pursuant to the Bank Act and to conduct its credit card business of providing credit card loans in Canada through its Canadian branch, Respondent Capital One Canada (Exhibit R-10);

9. The most popular of the Capital One Respondents' products are those credit cards used to cardholders for use by customers of Costco, Hudson's Bay, and Saks;

(ii) The Amazon Respondents

9.1 Respondent Amazon.com.ca, Inc. ("Amazon.com.ca") is an American electronic commerce corporation and cloud computing provider, with its head office in Seattle, Washington. It is a wholly-owned subsidiary of Respondent Amazon.com, Inc.;

9.2 Respondent Amazon.com, Inc. (“Amazon.com”) is an American electronic commerce corporation and cloud computing provider, with its head office in Seattle, Washington. It is the parent company under which all of the other Amazon Respondents operate;

9.3 Respondent Amazon Web Services Canada, Inc. (“AWS Canada”) is a Canadian electronic commerce corporation and cloud computing provider that maintains large data centres throughout the country, with its head office in Vancouver, British Columbia. It is a wholly-owned subsidiary of AWSHC, Inc. which operates throughout Canada, including within the province of Quebec. It was incorporated on July 24, 2014, the whole as appears more fully from a copy of an extract from the *Registre des entreprises* and from a copy of an extract from Corporation Canada, produced herein *en liasse* as **Exhibit R-4**;

9.4 Respondent Amazon Web Services, Inc. is an American corporation that maintains data centres in North America;

9.5 Respondent Amazon Technologies, Inc. (“Amazon Technologies”) is an American electronic commerce corporation and cloud computing provider, with its head office in Seattle, Washington. It is the applicant of the trade-marks “AWS” (Application Number 1856434), which was filed on September 7, 2017, “AMAZON WEB SERVICES” (Application Number 1856435), which was filed on September 7, 2017, “AWS” (Application Number 1918922), which was filed on September 7, 2018, and “AWS IS HOW” (Application Number 1953783), which was filed on March 26, 2019, the whole as appears more fully from a copy of the trade-marks from the Canadian Intellectual Property Office (CIPO), produced herein *en liasse* as **Exhibit R-5**;

9.6 Amazon Web Services (AWS) has been available within Canada for years before launching its two “Availability Zones” in December 2016, made up of one or more data centres in Montreal, Quebec and in Toronto, Ontario. This meant that the tens of thousands of Canadians who were using other AWS regions could not use the AWS Cloud to store their data on infrastructure in Canada, the whole as appears more fully from a copies of extracts from the Amazon Respondents’ website at http://aws.amazon.com, from a copy of the IT World article entitled “Amazon Web Services now offers local Canadian region availability” dated December 8, 2016, from a copy of the Data Center Knowledge article entitled “AWS Heads North, Launches Central Canada Cloud Region” dated December 9, 2016, and from a copy of the Amazon Web Services, Inc. press release entitled “Amazon Web Services Cloud Now Available to Customers from Data Centers in Canada” dated December 8, 2016, produced herein *en liasse* as **Exhibit R-6**;

10. Given the close ties between the Capital One Respondents and the Amazon Respondents and considering the preceding, they are all solidarily liable for the acts and omissions of the other;

C) The Situation

(i) Capital One Credit Cards and Capital One's Data Collection Practices

10.1 Capital One is one of the largest credit card issuers in North America; its Canadian offices are located in Toronto, Kitchener-Waterloo, Ontario, and in Montreal, Quebec;

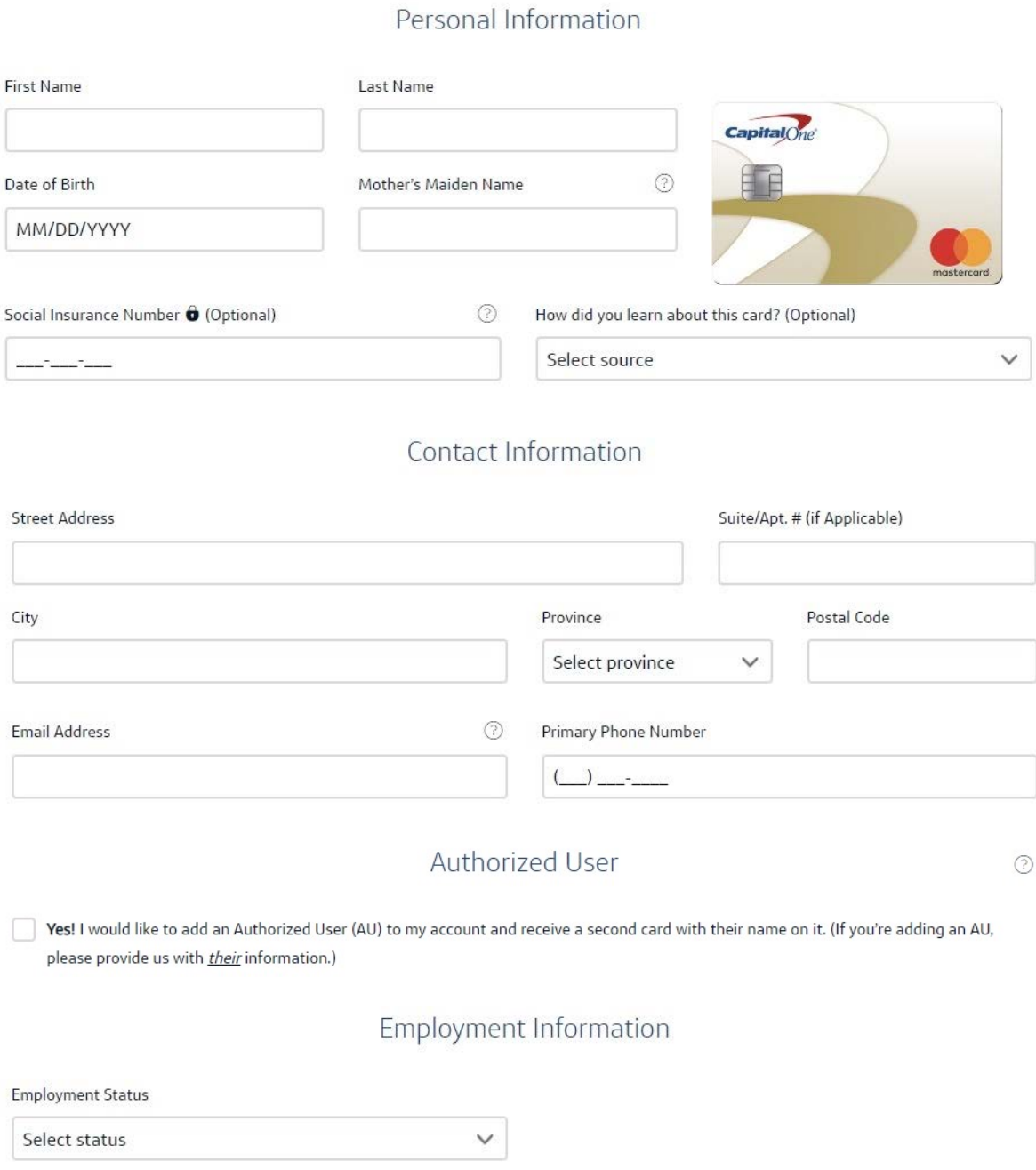
10.2 Capital One has offered Canadians a range of Mastercard credit cards since 1996. Capital One offers Canadian customers various Capital One Mastercard credit card products including a cash-back card for Costco Wholesale members (since 2015), the whole as appears more fully from a copy of the BNN Bloomberg article entitled "6M hacked, 1M SINs exposed: How big is Capital One in Canada?" dated July 30, 2019 and from a copy of an extract from the Capital One Respondents' website at www.capitalone.ca, produced herein *en liasse* as **Exhibit R-7**;

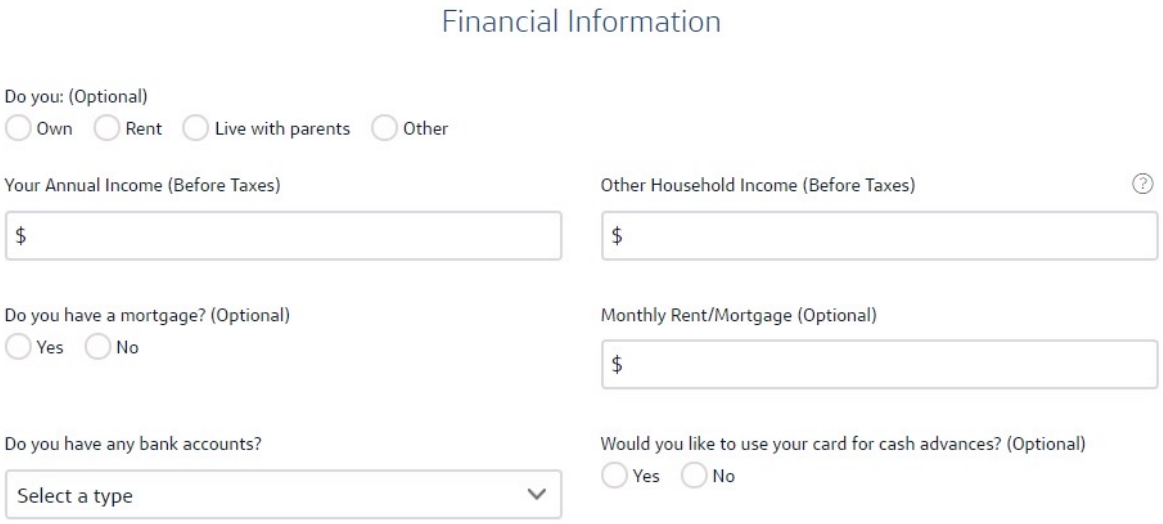
10.3 There are six different types of Capital One credit cards (Exhibit R-7):

1. The Guaranteed Mastercard®
2. The Low Rate Guaranteed Mastercard®
3. The Guaranteed Secured Mastercard®
4. The Aspire Travel™ Platinum Mastercard®
5. The Aspire Cash™ Platinum Mastercard®
6. The Capital One Mastercard®, Exclusively for Costco Members;

10.4 When consumers apply for a credit card and other financial products and services, Capital One requires them to provide personal and private information, including their full name, date of birth, social security number (optional today), address, email address, phone number, employment status, financial information such as annual income, and other valuable, confidential, personal, and private information. Capital One collects and stores this information alongside with additional personal and

private information relating to consumers, including payment and transaction history, account balances, credit limits, and credit scores, the whole as appears more fully from copies of extracts from the Capital One Respondents' website at https://creditapp.capitalone.ca, produced herein *en liasse* as **Exhibit R-8**;





10.5 This personal and private information isn't just received and stored, its used to gather even more sensitive information on credit card applicants, including data from credit bureaus. Before issuing a credit card to an applicant, issuers (like Capital One) run what is called a "credit check" through one or more credit bureaus who then issues them a credit report, which is used by Capital One to form a credit history, which is used to determine how much to lend (i.e. credit limit) to an applicant, at what interest rate, what fees to charge, and other terms of credit for the use of the credit card;

10.6 In short, credit card issuers like Capital One use applicants' sensitive personal and private information to make money. The more personal information a credit card issuer has about its applicants, the more precisely it can target credit risk (and shore up its bottom line) through higher interest rates, low credit limits, and miscellaneous fees;

10.7 Capital One is the best in the business at making money from granularly-targeted fees and interest. Indeed, it is this ability to target people by risk level that has allowed Capital One to profit from the riskiest borrowers. In the past decade, Capital One's credit card business has repeatedly been fined by federal and state regulators for unlawfully aggressive sales and monetization tactics. Between July 2011 and March 1, 2017, the United States Consumer Finance Protection Bureau ("CFPB") received more than 12,000 complaints directed toward Capital One's credit cards:

TABLE 6: MOST-COMPLAINED-ABOUT COMPANIES FOR CREDIT CARD[10]

Company	3 month average: Oct - Dec 2016	% change vs. 3 month period last year	3 month average % untimely: Oct - Dec 2016	Total Credit card complaints
Citibank	372.0	32%	0.1%	15,542
Capital One	218.7	18%	0%	12,074
JPMorgan Chase	210.0	30%	0%	9,614
Synchrony Financial	187.3	18%	0%	8,044
Bank of America	148.3	9%	0%	8,518
Amex	146.7	41%	0%	6,120
Wells Fargo	113.3	99%	41%	3,738
Barclays PLC	91.0	28%	0%	3,163
Discover	88.3	6%	0%	3,902
U.S. Bancorp	55.3	35%	0%	2,238
TD Bank US Holding Company	32.3	24%	0%	1,182

The whole as appears more fully from a copy of the Monthly Complaint Report of the Consumer Financial Protection Bureau dated March 2017, produced herein as **Exhibit R-9**;

10.8 User-targeted fees and interest are only part of the story. In recent years, credit card issuers such as Capital One have developed an even more broadly sweeping way to make money from users' personal and private information: rewards programs. Specifically, card issuers like Capital One use rewards programs to maximize revenue from interchange fees (described below), and they use the personal information of applicants and cardholders to optimally target and shape these rewards programs;

10.9 Credit card companies make money not only from fees and interest paid by their cardholders, but also from processing fees paid by merchants. These fees are typically a flat rate plus a percentage of the total sale. This money is referred to as interchange income, and it is directly tied to the number and size of transactions a cardholder makes on their credit card. Interchange income represents 70% to 90% of the total fees paid to issuers by merchants;

10.10 In order to maximize credit card transaction volume (and thus interchange income), credit card companies like Capital One offer reward programs. These reward programs may create direct financial incentives (for example, "cash back"), restaurant gift cards, or airline miles to incentivize cardholders to make purchases using the issuer's credit card, thereby increasing interchange income;

10.11 At the same time, however, rewards programs create significant risks for issuers, from the out-of-pocket costs to cover the rewards to the risks associated with increased borrowing by cardholders. As a result, credit card issuers like Capital One aggressively compete to identify and attract high-purchase-volume, low-default-risk applicants. The secret sauce in this battle for rewards-program profits is granular, detailed personal information about applicants, which enables precise risk and reward targeting by card issuers. For example, knowledge of a cardholder's proclivity for fine dining can be used to target a rewards program that incentivizes and rewards dining out;

10.12 In 2018, Capital One's net income from interchange fees was approximately USD$2.8 billion[3]. Capital One's 2018 annual filing with the SEC reported that the interchange fees it collected had increased for the year because of "higher purchase volume." Capital One's rewards program – the subject of its well-known, and extremely expensive, "What's In Your Wallet?" national advertising campaign – exists to increase that volume. Indeed, Capital One nets its interchange fees against the cost of its rewards program, which in 2018 was $4.4 billion[4], the whole as appears more fully from a copy of the Capital One Financial Corporation Annual Report dated 2018, produced herein as **Exhibit R-10**;

10.13 In short, the personal information collected from card applicants is vital to every aspect of a credit card issuer's lending business. Personal information is used to: (1) gauge risk; (2) set limits, fees, and interest; and (3) determine the type and overall level of rewards to both attract cardholders and incentivize maximum card use. And the role of personal information is non-binary: because personal information is integral to both revenue maximization and risk minimization, there is a direct, positive correlation between the amount and granularity of personal information a credit company collects and its expected profits from cardholders;

10.14 The more granular and accurate the information a credit card issuer is able to obtain about a borrower, the more predictable and stable its profits become. That is why credit card issuers demand highly sensitive information from applicants; it is integral to their bottom line;

10.15 Even after the credit card application process, the stream of cardholder data continues to pour in. Credit card charges allow credit card companies to predict the expected amount of rewards that they will have to pay out, the amount of interchange income they can expect, the risk of cardholder default, and even complementary products and services that can be marketed to cardholders;

10.16 Put simply, there is an important bargain at the heart of the credit card lender-borrower relationship: the card holder agrees to provide information that the card issuer needs to ensure that its business is profitable and predictable, and in return, the card issuer agrees to safeguard that sensitive customer information;

[3] See page 46 of Capital One's 2018 Annual Report (Exhibit R-10).
[4] See page 67 of Capital One's 2018 Annual Report (Exhibit R-10).

10.17 Capital One is no exception; it needs granular borrower data. In fact, one of the risk factors Capital One routinely discloses to its investors is a failure to accurately estimate its losses (Exhibit R-10):

> Estimates of Inherent Losses: The credit quality of our portfolio can have a significant impact on our earnings. We allow for and reserve against credit risks based on our assessment of credit losses inherent in our loan portfolios. This process, which is critical to our financial condition and results of operations, requires complex judgments, including forecasts of economic conditions. We may underestimate our inherent losses and fail to hold an allowance for loan and lease losses sufficient to account for these losses. Incorrect assumptions could lead to material underestimations of inherent losses and inadequate allowances for loan and lease losses.[5]

10.18 As Capital One's Annual Report (Exhibit R-10) explains, its business depends on the ability to make judgments and forecasts about likely losses. For that, Capital One relies heavily on accurate and timely data about its customers;

10.18.1 In addition to this customary use of Class Member's personal and private information to make credit decisions, Capital One maintains and mines the data for its own purposes of product development, targeted solicitation for new products, and target marketing of new partners – all in an effort to boost its profits;

10.18.2 In other words, Capital One did not need to retain all of this information in the way that it did, for as long as it did, and did not need to store all of this information in the way it did, in order to service its customers, but did so it order for its commercial gain;

10.18.3 From its beginning, Capital One adopted this "Information Based Strategy," or IBS, to obtain a competitive advantage, the whole as appears more fully from a copy of Capital One's Form 10-K for the fiscal year ended December 31, 1996, produced herein as **Exhibit R-31**;

10.18.4 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 diversified products", the whole as appears more fully from a copy of extracts from Capital One's Form 10-K for the fiscal year ended December 31, 2011, produced herein as **Exhibit R-32**;

[5] See page 21 of Capital One's 2018 Annual Report (Exhibit R-10).

10.19 Capital One had been collecting an unprecedented amount of data about its customers (…); this data informed Capital One of the risks of lending its credit card users, of how often its customers spent, what they spent on, and even where they went and what they cared about. Significant amounts of hardware and software infrastructure were necessary to mine this data and to succeed in "machine learning" (a process through which computer algorithms are given raw data and "learn" on their own to discern patterns and accomplish tasks). Capital One needed data centres, storage, and computation power – all with the airtight security befitting a major financial institution;

10.20 (…) 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 scenarios, the costs to maintain the needed infrastructure rises with the increase in the amount of data collected;

10.21 Amazon's AWS public cloud for storage and processing of sensitive financial data presented a potential solution. AWS would allow Capital One to buy only as much computing power and storage as it needed and it allowed Capital One to leverage Amazon's data scientists and machine learning tools, as well as arrays of the graphics processing units capable of the massive simultaneous calculations needed for machine learning;

10.22 Unfortunately, there were serious problems with using AWS to mine customer data. Most importantly, the machine learning models required massive amounts of historical data and if the data was insufficient, the models would not be accurate. In other words, Capital One would need to place years (and potentially over a decade) of sensitive customer information on the AWS cloud. The potential damage from a security breach compromising a large stockpile of historical data would be incalculable;

10.23 To optimize machine learning, Capital One created massive data lakes (i.e., repositories of customer data) containing data retained far in excess of customer expectations. Capital One announced that the hacker had stolen data from credit card applications submitted as early as 2005. Capital One had held on to this data for fourteen years. To ensure that the information the algorithms gleaned was as useful as possible, Capital One also included outcomes (the customer's subsequent performance). Capital One made so much data accessible that any breach would be catastrophic;

10.24 Other large financial institutions knew this risk was too great and exercised extreme caution around customer data and elected not to place their customers' personal and private data in the hands of a public cloud provider;

10.25 While Capital One was looking for a cover for its migration, Amazon was searching for a large financial institution to adopt its AWS ecosystem. AWS's business was being adopted by technology companies, start-ups, and other unregulated or less-regulated enterprises. The prize, however, was a large financial institution—one whose adoption of AWS would signal to other apprehensive financial institutions that it was okay to make the transition to the public cloud;

(ii) AWS: The What, How, and Why of it and the Respondents' Express Promises to Safeguard Sensitive Customer Data

10.25.1 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;

10.25.2 The primary downsides of public cloud computing are the increased data security risk inherent in their use and the related difficulty of meeting regulatory hurdles regarding the security of sensitive information. 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, the whole as appears more fully from a copy of the Carnegie Melon University article entitled "12 Risks, Threats, & Vulnerabilities in Moving to the Cloud" dated March 5, 2018, from a copy of the Federal Reserve Bank of Atlanta article entitled "Supervisory Considerations in Cloud Computing in the Financial Services Industry" dated May 8, 2018, produced herein *en liasse* as **Exhibit R-33**;

10.26 Despite these inherent security risks, in October 2015, when no other bank would[6], Capital One announced that it would migrate its user data and applications from its own private cloud to the AWS cloud at its yearly re-Invent conference. It would move entire swaths of customer data to AWS's S3 servers to form a data lake, a single source of data that Capital One's applications and machine learning models could all draw from. That data lake included years of customer application data in order to better allow artificial intelligence and machine learning algorithms to monetize that data for Capital One and Amazon. This left Capital One only as secure as its least secure division, the whole as appears more fully from copies of extracts from Respondent Amazon Web Services, Inc.'s website at https://aws.amazon.com, from a copy of the Forbes article entitled "How Capital One Became A Leading Digital Bank" dated December 12, 2016, from a copy of the Medium article entitled "Capital One's Cloud Journey Through the Stages of Adoption" dated April 5, 2017, and from a copy of the CIO article entitled "Real world lessons from AWS re:Invent 2015" dated October 20, 2015, produced herein *en liasse* as **Exhibit R-11**;

[6] National Bank of Canada used AWS Cloud to help it collect and process a fast-growing volume of stock-market financial data to optimize its trading operations and generate more revenue (Exhibit R-6).

10.26.1 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;

10.27 For this move to work, this aggregation of sensitive consumer data had to be represented to be safe to Capital One's current and prospective customers. If customers do not believe that their information will be safe, they would never agree to apply for, or use, a Capital One credit card. Capital One, with Amazon's assistance, set out to assuage those fears by making false and/or misleading representations and omissions to current and potential customers, even developing its own software to manage the permissions of its internal computers and customer-facing applications to access the shared data lake. In other words, Capital One and Amazon represented that they were able to guard against the inherent risk of pooling massive amounts of sensitive customer data for mining on the public cloud;

10.28 By way of example, the Capital One Respondents represented the following about AWS cloud computing (Exhibit R-11):

> We didn't want to be in the position of trying to convince stakeholders of the value of the cloud without being able to first assure them that we could responsibly deploy and run any of our applications there;
>
> That meant tackling questions about security early and head on. "As a financial institution, we take the safety of our customer data incredibly seriously," says Brady. "Before we moved a single workload, we engaged groups from across the company to build a risk framework for the cloud that met the same high bar for security and compliance that we meet in our on-premises environments. AWS worked with us every step of the way."

10.28.1 Both Respondents 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 to analyze the trove of customer data it collected from credit applicants, the whole as appears more fully from a copy of an extract from AWS' website at https://aws.amazon.com and from a copy of the Conference Tracker article entitled "Capital One: Banking Is Inherently A Digital Business" dated July 24, 2015, produced herein *en liasse* as **Exhibit R-34**;

10.28.2 Despite 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;

(iii) AWS Cloud Computing's Default Settings Have Known Vulnerabilities

10.29 For years, (…) the AWS cloud environment has suffered from a widely known flaw. AWS servers, unlike those run by its competitors (e.g., Google), were not secured against (…) Server-Side Request Forgery (SSRF) attacks, which would allow an attacker to (…) penetrate a firewall and make requests to the data lake, including requests to pipe the data outside of the firewall 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, the whole as appears more fully from a copy of the Search Security article entitled "Capital One hack highlights SSRF concerns for AWS" dated August 5, 2019, produced herein as **Exhibit R-35**;

10.30 As described more fully below, to provide additional cover for its migration to the public cloud, Capital One created software, called Cloud Custodian, which it jointly showcased and marketed with Amazon. It was described as a "rules engine" that allowed Capital One to set specific access "policies" within AWS that would apply in real time to the various servers that accessed its data lake. The software would, among other things, purportedly automatically scan Capital One's internal systems to ensure that all of the servers and permissions were set according to defined policies. Thus, when a computer wanted to access data from the data lake, it would assume a defined "role" that would then give it access to some portion or all of the data in the data lake (Exhibit R-11). One way to do this is through Identity and Access Management ("IAM") roles, the whole as appears more fully from a copy of an extract from the Amazon Respondents' website at https://aws.amazon.com entitled "Announcing Cloud Custodian Integration with AWS Security Hub" dated November 29, 2018 and from a copy of the TechCrunch article entitled "Capital One open sources Cloud Custodian AWS resource management tool" dated April 19, 2016, produced herein *en liasse* as **Exhibit R-12**;

10.31 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. These (…) IAM roles are used on AWS to allow various computers to access 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 train and deploy machine learning algorithms, could potentially allow that computer to access the entire data lake, while another computer with a more restrictive IAM role may restrict access only to a small subset of consumer data, the whole as appears more fully from copies of extracts from the Amazon Respondents' website at https://aws.amazon.com, produced herein *en liasse* as **Exhibit R-13**;

10.31.1 While the IAM roles work to regulate access to data within the AWS server, the only defence 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;

10.31.2 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 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;

10.31.3 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;

10.31.4 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;

10.31.5 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;

10.31.6 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, the whole as appears more fully from a copy of the Threat Post article entitled "Is AWS Liable in Capital One Breach" dated October 25, 2019 and from a copy of the United States Senate letter to the Federal Trade Commission dated October 24, 2019, produced herein *en liasse* as **Exhibit R-36**;

10.31.7 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", the whole as appears more fully from

copies of extracts from the website https://krebsonsecurity.com, produced herein *en liasse* as **Exhibit R-37**;

10.31.8 In 2016, Capital One and AWS jointly announced that together they had developed a new product it called Cloud Custodian. Respondents announced that with Cloud Custodian they had solved the security problems inherent in using the AWS cloud for machine learning at scale and have billed Cloud Custodian as a comprehensive cloud security tool which would automatically detect and fix security flaws (Exhibits R-12 and R-14);

10.32 The Respondents represented that Cloud Custodian would (…) ensure that IAM roles were given the proper permissions to minimize the risk of a data security breach; in other words, Cloud Custodian would grant the minimum amount of access necessary to complete a given task (Exhibit R-13). For example, a customer-facing application such as a credit card application program would need to access systems to input the customer's data into the appropriate tables and then receive information about whether that applicant was approved and the terms of the approval, but it would not need to access information about Capital One applicants from 2005;

10.33 In more lay terms, (…) the Respondents claimed that Cloud Custodian automatically encrypted all of the data that Capital One made accessible to its employees. Thus, supposedly, even if a hacker penetrated Capital One's firewall, the hacker would still not obtain meaningful data. Unfortunately, the data was not meaningfully encrypted; rather than limiting decryption to relevant persons, Capital One automatically decrypted data for any person with Capital One credentials. 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. As an expert explained, Capital One's encryption was "academic at best";

10.34 The reality was that Cloud Custodian was not a solution to the serious problems posed by the mass aggregation of sensitive data and the open and dynamic access of countless servers to that data. Cloud Custodian's supposed benefit; i.e. ensuring the minimum amount of access necessary to complete a task, is at cross purposes with the goal of aggregating and mining large amounts of customer data for profit. This is because in order to train and apply machine learning and AI systems, those systems need broad and dynamic access to user data, and that data must span years to ensure the accuracy and power of the AI and machine learning models;

10.35 A version of Cloud Custodian designed to minimize risk, then, would not serve Capital One's purpose for migrating to AWS's servers in the first place, which was the monetization of its customers' data. Accordingly, Cloud Custodian could not, and did not, solve the risk presented by the massive aggregation of data for exploitation on a public cloud server;

10.36 All that stood between an attacker and Capital One's data lake was a firewall, a system designed to block unauthorized access while permitting outward communication. The firewalls on Amazon's AWS cloud that guarded web applications were known to be, and continue to be, vulnerable to an SSRF attack. Other cloud providers have implemented additional precautions to ensure that requests from outside the firewall cannot be used to command resources on the inside, but AWS did not implement such precautions and has not done so to this day;

10.37 The net effect is that once an attacker obtains access to a server or system inside an AWS firewall, such as a firewall that protects a customer-facing web application, the attacker has access to all the data available to that server or system. If the attacker obtains access to a single system that can assume a broad IAM role that permits it to access to the data lake, such as those that conduct machine learning tasks, all of that data can be transferred outside of the firewall at will;

10.38 Cloud Custodian could not prevent any of this, notwithstanding the Respondents' statements that it was the solution to risk. This was a peculiar move for Amazon in particular because promotion of Cloud Custodian made no economic sense for Amazon;

10.39 First, Amazon already had a suite of tools that would purportedly ensure the proper configuration of IAM roles and monitor data access. In fact, Amazon made money selling these tools to the users of its cloud. Nonetheless, Amazon agreed to help Capital One promote Cloud Custodian even though it competed with Amazon's own tools;

10.40 Second, Cloud Custodian was both open source and cross-platform, meaning that it could be migrated to competing cloud services, such as Microsoft's Azure or Google's GCP. Accordingly, the relationship between Capital One and Amazon was far from an ordinary business relationship between a cloud provider and one of its customers. A customer that adopted Cloud Custodian could more easily move its operations to a competing provider than one that relied on Amazon's own cloud management and security ecosystem. The only plausible reason that Amazon was willing to make that concession was to coax Capital One, a major financial institution, onto its platform, thus luring other financial institutions to join it;

10.41 Amazon also promoted Capital One's migration to AWS and the Cloud Custodian program. In late 2018, AWS hosted several web pages and videos touting its partnership with Capital One, the migration of Capital One's data to its cloud, Capital One's use of AWS to perform machine learning on its user data at scale, and Cloud Custodian as a tool to keep the data safe. None of that promotion mentioned that Capital One and AWS had not dealt with the longstanding SSRF vulnerability peculiar to AWS (Exhibits R-8, R-9, and R-10);

10.42 Simply put, the only reason for Amazon's business decision to promote a competing product was the immense value of attracting a large bank to its platform

when other financial services companies refused to migrate their sensitive customer data to the public cloud. Capital One's use of AWS would demonstrate the safety of the cloud to financial services companies that sought to mine sensitive customer data. In exchange for this, Capital One would receive cover for its risky migration to the cloud, the pooling of customer data into the data lake, and the vast datamining operations it could conduct on its customers' personal and private information. Together, by developing and promoting Cloud Custodian, Capital One and Amazon gave regulators and customers a false sense of security and created precedent for other large companies to adopt the AWS public cloud, thereby enhancing AWS's cloud ecosystem;

10.43 Capital One and Amazon knew about the inherent flaw in the architecture Capital One would have to deploy in order to exploit AWS's machine learning and AI tools and hardware, including the SSRF vulnerability. Both companies nevertheless falsely and/or misleadingly touted Cloud Custodian as the solution. In 2016, Amazon and Capital One posted the open source software on Amazon's AWS website, along with detailed documentation and marketing. But as both companies marketed Cloud Custodian as the solution to the risks of the data lake approach, they knew that Cloud Custodian was no solution at all;

10.44 For example, in December 2018, Mr. Kapil Thangavelu, Capital One's developer in charge of Cloud Custodian, gave a presentation at Amazon's AWS re:Invent conference. His presentation, entitled "Cloud Custodian—Open Source Security & Governance," touted Cloud Custodian as a solution for the intractable task of maintaining appropriate permissions across several applications sharing aggregations of data. In an alarmingly prescient part of his speech, he discussed IAM roles and the precise vulnerability with poorly secured S3 servers that would later result in a breach of Capital One's own systems. He then touted Cloud Custodian as a cure for that vulnerability, the whole as appears more fully from a copy of the video entitled "AWS re:Invent 2018: Cloud Custodian – OpenSource AWS Security & Governance (DEM78)", produced herein as **Exhibit R-14**;

10.45 Capital one also claimed that it complied with principles requiring it to delete customer data after a reasonable time. Even if a hacker breached Capital One's firewall and even if the hacker somehow decrypted the data, Capital One's deletion practices would purportedly sharply limit the number of persons affected;

10.46 In addition, the Amazon Respondents claimed that "cloud security is our highest priority" and that:

> "As an AWS customer using cloud computing services in the Canada Region, you will benefit from local servers and network architecture built to meet the requirement of the most security-sensitive organizations. AWS allows customers to scale and innovate, and provides the tools to maintain a protected environment. Customers can choose to secure their data locally, to help them meet Canadian PIPEDA regulations (Exhibit R-6);

10.47 Capital One represented that it had implemented a cloud risk framework and cloud governance function that would properly manage its move to the AWS Cloud, referencing its Cloud Custodian, which supposedly automated detection and correction of policy violations. It specifically referenced the following:

> "As a financial institution, we take the safety of our customer data incredibly seriously," says Brady. "Before we moved a single workload, we engaged groups from across the company to build a risk framework for the cloud that met the same high bar for security and compliance that we meet in our on-premises environments. AWS worked with us every step of the way." (Exhibit R-11)

10.48 Data security is important to consumers; so important that credit card companies like Capital One make the promise of electronic safety and security a part of their card offerings. Capital One represented the following:

> How we keep your information safe.
>
> Our strong encryption technology ensures that any data that passes between your computer and our server is secure.
>
> - We use firewall systems and intrusion detection software to prohibit unauthorized access to our systems
> - Our VeriSign Secure Socket Layer Certificate means you can be extra confident that banking online with us is secure
> - We automatically send you an alert informing you of any changes made to your online banking profile
> - The online banking website will automatically log off after a period of inactivity during any session to protect your information.
>
> _____
>
> You're Protected
>
> We're committed to protecting your information.
>
> - Zero Liability protection for unauthorized use of your credit card
> - 24/7 account monitoring for fraudulent activity

The whole as appears more fully from copies of extracts from the Capital One Respondents' website at www.capitalone.ca, produced herein *en liasse* as **Exhibit R-15**;

10.49 Capital One's Terms and Conditions state that "Capital One supports information privacy protection", the whole as appears more fully from a copy of the Capital One Customer Agreement and from a copy of the Capital one Privacy Policy, produced herein *en liasse* as **Exhibit R-16**;

10.50 These statements were false and/or misleading as proven by the data theft that occurred in March 2019;

(iv) <u>The Exploitation of the Known Vulnerability: The Series of (attempted and successful) Data Thefts</u>

10.51 On March 22 and 23, 2019, Paige Thompson, 33, a former employee of Respondent Amazon Web Services, Inc., scanned servers belonging to dozens of companies that had hosted their web applications on AWS and found a vulnerable entrypoint in Capital One's credit card application processing system. Using a server-side request forgery (SSRF) attack, Thompson tricked one of Capital One's servers into sending information from Capital One's data lake to TOR nodes outside of Capital One's firewall and then to a server that she controlled;

(a) SSRF is a web security vulnerability that allows an attacker to induce the server-side application to make HTTP requests to an arbitrary domain of the attacker's choosing. In typical SSRF examples, the attacker might cause the server to make a connection back to itself, or to other web-based services within the organization's infrastructure, or to external third-party systems. A successful SSRF attack can often result in unauthorized actions or access to data within the organization, either in the vulnerable application itself or on other back-end systems that the application can communicate with, the whole as appears more fully from a copy of an extract from the Portswigger website at https://portswigger.net entitled "Server-side request forgery" and from a copy of the Acunetix article entitled "What is Server Side Request Forgery (SSRF)?" dated February 20, 2019, produced herein *en liasse* as **Exhibit R-17**;

(b) TOR is an open-sourced software that enables for anonymous communication; the name "TOR" is derived from an acronym for the original software project name "The Onion Router". The goal of onion routing was to have a way to use the internet with as much privacy as possible, and the idea was to route traffic through multiple servers and encrypt it each step of the way, the whole as appears more fully from copies of extracts from the TOR Project website at www.torproject.org and from a copy of the Hackernoon article entitled "How does Tor actually work?" dated March 1, 2019, produced herein *en liasse* as **Exhibit R-18**;

10.52 The scope of the breach was astounding, with compromised data going back 14 years to 2005. Capital One had aggregated customer data on an unprecedented scale and the compromise of just one of the systems inside its firewall meant the complete compromise of over a decade of sensitive customer data. In other words,

because Capital One had pooled all of its customer data together, unauthorized access to one necessarily implied access to all;

10.53 Not only did Cloud Custodian fail to prevent this data theft, it failed to even detect that it had happened at all; it wasn't until a July 17, 2019 email from a third-party that Capital One even recognized that its systems had suffered from the devastating attack. A picture of the redacted email appears below:

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]

10.54 The email stated that there appeared to be leaked data belonging to Capital One on GitHub, and provided the address of the GitHub file containing this leaked data. After receiving this information, Capital One examined the GitHub file, which was timestamped April 21, 2019. Capital One determined that it contained the IP address for a specific server. According to Capital One, a Web Application Firewall (WAF) misconfiguration permitted commands to reach and be executed by that server, which enabled access to folders or buckets of data in Capital One's storage space on the AWS Cloud;

10.55 Capital One determined that the file contained code for three commands, as well as a list of more than 700 folders or buckets of data. The commands executed by the hacker accomplished the following:

(a) (…) Obtained security credentials for an account known as *****-WAF-Role that (…) enabled access to certain of Capital One's folders on the AWS cloud;

(b) (…) Used the * * * * *-WAF-Role account to list the names of folders or buckets of data in Capital One's storage space on the AWS cloud;

(c) (…) Used the *****-WAF-Role to extract or copy data from those folders or buckets in Capital One's storage space for which the *****-WAF-Role account had the requisite permissions;

The whole as appears more fully from a copy of the Medium article entitled “Capital One’s Cloud Journey Through the Stages of Adoption” dated April 5, 2017, produced herein as **Exhibit R-38**;

10.56 According to Capital One’s logs, a number of connections or attempted connections to Capital One's server from TOR exit nodes, and a number of connections from IP addresses beginning with 46.246, all of which Capital One believes relate to activity conducted by the same person involved in the April 21, 2019, intrusion because they involve similar unusual communications through the misconfigured firewall to the server discussed above. Specifically, according to Capital One, the logs show:

(a) On or about March 12, 2019, IP address 46.246.35.99 attempted to access Capital One’s data. This IP address is controlled by Ipredator, a company that provides Virtual Private Network (VPN) services;

(b) On March 22, 2019, the *****-WAF-Role account was used to execute the List Buckets Command several times. These commands were executed from IP addresses believed to be TOR exit nodes. According to Capital One, the *****-WAF-Role account does not, in the ordinary course of business, invoke the List Buckets Command;

(c) Also on or about March 22, 2019, the *****-WAF-Role account was used to execute the Sync Command a number of times to obtain data from certain of Capital One's data folders or buckets, including files that contain credit card application data. A number of those commands were executed from IP address 46.246.38.224. I know, from checking publicly-available records, that that IP address also is controlled by Ipredator;

(d) One of the files copied from Capital One’s folders or buckets on March 22, 2019, was a file with the name *****c000.snappy.parquet and this was the only time the *****-WAF-Role account accessed the Snappy Parquet File between January 1, 2019 and July 20, 2019;

(e) A List Buckets Command was executed on April 21, 2019, from IP address 46.246.35.103. The IP address from which this command was executed also is controlled by Ipredator. Based on the timestamp on the April 21, 2019 file, and the time that Capital One reports that the command appears in Capital One's logs, that this was the command that was the source of the April 21 file;

10.57 It was clear that Cloud Custodian was either a facade, designed to lull customers and regulators into a false sense of security or it was never properly configured to limit access to years of historical data and it was not programmed to detect anomalies. Either way, all of Capital One and Amazon’s statements about Cloud Custodian were revealed to have been false and/or misleading;

10.57.1 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 at tacker could have potentially gotten access to data once they got in through the misconfigured firewall).

The whole as appears more fully from a copy of the letter from the U.S. Senate to AWS dated August 5, 2019, from a copy of the letter from AWS to the U.S. Senator dated August 13, 2019, and from a copy of the U.S. Senator Press Release entitled "Wyden and Warren to FTC: Investigate Amazon's Negligence in Capital One Hack" dated October 24, 2019, produced herein *en liasse* as **Exhibit R-39**;

10.58 Because the fact of the data theft itself and any investigations related thereto threatened to expose a more existential problem with Capital One's cloud operations, the Respondents continued to downplay the root cause to the public. Both Capital One and Amazon blamed a misconfigured firewall for the data theft, but that assertion is inaccurate. The problem is inherent in the architecture that Capital One chose and AWS enabled. (…) Neither company address that, by design, Cloud Custodian, their touted solution to data vulnerability, was unable to detect or stop the attack;

10.59 Instead, Capital One and Amazon appear content to take no action to correct the issues. Amazon has not fixed its systemic vulnerability to the particular form of attack used in the data theft. Capital One has not fixed its aggregation-based, data-lake architecture that allows a simple hack to have devastating consequences. Both companies continue to profit on risking customers' valuable personal information;

10.60 Further, it was only on July 29, 2019 that Capital one announced that Class Members' personal and private information had been hacked – approximately four months after the incident;

10.60.1 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 theft four months later from an anonymous tip, suggests that Capital One did not have adequate 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;

10.60.2 Indeed, the length of time the data theft went unnoticed and undetected by the Respondents is astonishing, in light of both the public postings made by the alleged hacker Thompson and the activity on the AWS server (Exhibit R-19):

(a) 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.” The Sync Command placed extracted files in a directory containing the name WAF-Role;

(b) 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;

(c) 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 on the AWS server and was determined to be one of the files exfiltrated from Capital One on March 22, 2019;

10.60.3 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 (Exhibit R-37):

10.60.4 The length of time the Github file remained publicly posted without Respondents’ 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;

10.60.5 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 Capital One’s customer data via the AWS WAF vulnerability;

10.61 The admissions in Capital One's announcement (Exhibit R-1), subsequent reporting, and reports from former employees show that Capital One had sacrificed cybersecurity to a dangerous extent, contrary to their repeated claims. Given Capital One's deficient cybersecurity measures, the data theft was inevitable;

10.62 On July 29, 2019, Paige Thompson, also known by the alias "erratic", was arrested and on August 28, 2019, she was indicted by a grand jury in the United States District Court for the Western District of Washington at Seattle for wire fraud and computer fraud and abuse, the whole as appears more fully from a copy of the Complaint for Violation of 18 U.S.C. s 1030 (a)(2) dated July 29, 2019, from a copy of the Indictment dated August 28, 2019, from a copy of the Wired article entitled "The Alleged Capital one hacker Didn't Cover Her Tracks" dated July 29, 2019, and from a copy of the Wired article entitled "Everything We Know About the Capital One Hacking Case So Far" dated August 28, 2019, produced herein *en liasse* as **Exhibit R-19**;

10.63 On July 31, 2019, the Office of the Privacy Commissioner of Canada (OPC) opened an investigation into the data breach at Capital One after receiving complaints from Canadian customers, the whole as appears more fully from a copy of the OPC announcement entitled "OPC launches investigation into Capital One breach" dated July 31, 2019, produced herein as **Exhibit R-20**;

10.64 Capital One, with AWS's knowing assistance, falsely and/or misleadingly represented that it would use industry-standard practices to protect its customers' personal information. They falsely and/or misleadingly represented the capability of Cloud Custodian. They downplayed the data theft. And they are continuing to falsely and or misleadingly represented the security (or lack thereof) of the personal information in the data lake;

10.65 If Class Members knew the truth about the Respondents' data security practices – that the Respondents would not adequately protect and store their data, they would not have entrusted their personal and private information to Capital one, (…) they would not have 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;

(v) Regulatory and Industry Practices for the Protection of Personal and Private Information

10.65.1 The Canadian Competition Bureau has not sought to regulate cybersecurity; however, the U.S. Federal Trade Commission (FTC), to which there is no equivalent in Canada, has had success in policing cyberspace in the United States. The FTC has issued guidance and published regulatory decisions interpreting the measures financial institutions must take to comply with the "Safeguards Rule", which requires financial institutions to have measures in place to keep customer information secure, the whole as appears more fully from a copy of the U.S.-Canada Cooperation Agreement dated August 1995 and from a copy of the U.S.

Electronic Code of Federal Regulations, Title 16, Chapter I, Subchapter C, Part 314, produced herein *en liasse* as **Exhibit R-40**;

10.65.2 The FTC recommends the following in order to keep customer information secure:

- 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;

The whole as appears more fully from a copy of an extract from the FTC website at www.ftc.gov, produced herein as **Exhibit R-41**;

10.65.3 The FTC 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, the whole as appears more fully from a copy of the FTC document entitled "Start with Security: A Guide for Business" dated June 2015, produced herein as **Exhibit R-42**;

10.65.4 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 businesses. The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal and private information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach, the whole as appears more fully from a copy of the FTC document entitled "Protecting Personal

Information: A Guide or Business" dated October 2016, produced herein as **Exhibit R-43**;

10.65.5 The FTC recommends that companies not maintain personal and private information 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 (Exhibit R-42);

10.65.6 The Payment Card Industry (PCI) Security Standards Council, of which Capital One is a participant, 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. In addition, the PCI Security Standards published PCI SSC Cloud Computing Guidelines, last updated in April 2018, the whole as appears more fully from a copy of the PCI Security Standards Council Data Security Standard dated May 2018 and from a copy of the PCI SSC Cloud Computing Guidelines dated April 2018, produced herein *en liasse* as **Exhibit R-44**;

10.65.7 Most recently, the PCI Security Standards Council published a PCI DSS for Large Organizations, such as Capital One, in February 2020, the whole as appears more fully from a copy of the PCI DSS for Large Organizations dated February 2020, produced herein as **Exhibit R-45**;

10.65.8 Capital One violated the standards of PCI-DSS concerning data retention, encryption, and access;

10.65.9 The security industry identified the most common challenges when it comes to AWS security, as well as some of the ways they are rising to meet them as follows:

(a) Prioritizing a security strategy ahead of controls and tools – considering your security strategy before the tools and controls that will implement it allows you to integrate security and security monitoring into all business functions from day one;

(b) Overcoming the lack of security visibility in the cloud – because of the large number of applications that companies use as well as the logins and controls that vary across them, it is difficult to know at all times who is accessing what. To increase visibility, a company would need (i) specifics on what is happening on a host or workload, rather than only that something happened, (ii) host-based intrusion detection identifies behaviour whereas network-based intrusion detection does not, and (iii) protection against an insider threat: it is important to monitoring unusual network activity, unauthorized installs, abnormal login attempts or failures, and key file changes;

(c) Improving confidence in cloud provider security – it is important to communicate with cloud service providers, such as AWS and cloud security providers, before migrating to understand who is responsible for protecting data;

(d) Defining who is liable – liability is oftentimes not so clear-cut so companies need to take a proactive approach to defining access levels and monitoring activity across the network in order to pinpoint liability;

(e) Understanding why attackers are attracted to the cloud – attackers target cloud service providers because they contain sensitive data and they use credential theft. In order to protect data, a company can (i) turn on multi factor authentication for everything, (ii) monitor for anomalous logins using continuous security monitoring, (iii) implement a logging service at the host level, (iv) use a secrets management system to rotate credentials;

(f) Defending against curious onlookers in multi-tenant infrastructures;

(g) Addressing compliance regulations from the start;

The whole as appears more fully from a copy of the Threat Stack article entitled "The Top 7 AWS Security Issues: What You Need to Know" dated June 15, 2016, from a copy of the Threat Stack article entitled "5 Reasons Why Host-Based Intrusion Detection Systems Thrive in the Cloud" dated September 29, 2015, from a copy of the Threat Stack article entitled "How to Manage the Ex-Employee Insider Threat" dated August 6, 2015, produced herein *en liasse* as **Exhibit R-46**;

10.65.10 Capital One was at all times fully aware of its obligation to protect the financial data and personal and private information of its customers and applicants because of its status as a one of the 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;

(vi) *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (PIPEDA)

10.66 The Respondents' data security practices run contrary to PIPEDA and even more inexcusably given the real risk of significant harm that a security breach entails where the personal and private information is highly sensitive and has been or will be misused;

10.67 PIPEDA does not define sensitivity; however, the concept of sensitivity of personal information is discussed in Principle 4.3.4 of PIPEDA which states:

> Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not

be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

10.68 Suffice it to say that Class Members' social insurance numbers, bank account numbers, names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, self-reported income, credit card application data, credit card customer data, including, customer status data, e.g., credit scores, credit limits, balances, payment history, contact information, and transaction data, which could be used by a criminal to assume their identities would be considered highly-sensitive data. The more sensitive the data is, the higher level of protection an organization must employ (PIPEDA, Principle 4.7.2);

10.69 In addition, there was a high probability of misuse of Class Members' personal and private information and that Class Members would be harmed;

10.70 The Respondents should have established adequate security safeguards to prevent and detect unauthorized access to personal and private information;

10.71 Capital One's loose access policies, huge numbers of vast data lakes, and automatic decryption made a hack like the data theft inevitable. With too many authorized requests by Capital One employees and algorithms to access data to monitor, an illegitimate request would be difficult to catch. Indeed, the hacker involved in the data theft accessed Capital One's data three times in March and April 2019 and used Capital One's computer resources to mine bitcoin, without ever being detected;

10.72 The final weakness in Capital One's cybersecurity defences was the Respondents themselves. In 2017, Capital One hired Michael Johnson to be its Chief Information Security Officer ("CISO"), the head of the cybersecurity division. The Respondents considered turnover in that division material and closely monitored it, including in reports to Capital One's board of directors. Johnson immediately alienated the cybersecurity division's employees. The division's turnover in 2018 was about one third. Under Johnson, Capital One's cybersecurity division even omitted to take elementary precautions like installing security software Capital One had purchased;

10.73 The July 29, 2019 announcement of the data theft thus was the inevitable result of Capital One's abandoning cybersecurity practices to carry further its business plan;

(vii) The Respondents' Fault

10.73.1 Both Capital One and Amazon failed to maintain a secure environment and adequate security protocols whereby Class Members' personal and private information would be kept safe and confidential in *inter alia* the following ways:

(a) Failing to maintain an adequate data security system to reduce the risk of data thefts and cyber attacks;

(b) Storing Class Member's personal and private information on an insecure infrastructure that was susceptible to easy access;

(c) Failing to adequately protect the Petitioners' and Class Members' personal and private information;

(d) Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

(e) Failing to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;

(f) Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of personal and private information; and

(g) Failing to effectively train all members of its workforce on the policies and procedures with respect to personal and private information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of personal and private information;

(viii) The Damages

10.73.2 The Respondents' failure to keep Class Members' personal and private information safe and secure has severe ramifications. Given the particularly sensitive nature of the information at present, i.e. names, addresses, postal codes, phone numbers, email address, dates of birth, self-reported income, social insurance 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 Class Members now and into the indefinite future;

10.73.3 The personal and private information exposed in the data theft 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", thereby exposing consumers to identity theft and fraud for years to come. Identity thieves can use the personal and private information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards;

(b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits or medical treatment; (f) file a fraudulent tax return using the victim's information; (g) commit espionage; or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest;

10.73.4 This is especially true for data held by banks, given that the personal and private information compromised in this data theft was precisely the personal and private information 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;

10.73.5 Personal and private information has significant monetary value in part because criminals continue their efforts to obtain this data. 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, between November 1, 2018 and October 31, 2019, 680 data breach reports were reported to the Privacy Commissioner of Canada, which was 6 times the amount of the previous year, the whole as appears more fully from a copy of the CIO article entitled "Data Breaches Rise as Cybercriminals Continue to Outwit IT" dated September 28, 2014 and from a copy of an extract from the Office of the Privacy Commissioner of Canada website at www.priv.gc.ca, produced herein *en liasse* as **Exhibit R-47**;

10.73.6 There are various ways that a fraudster can monetize information obtained from a data breach either by using it to obtain further personal and private information or by combining it with other information obtained from the dark web or else as simply as by doing deep searches on the internet. For example, a software developer from Columbia was able to steal the identities of several acquaintances and even gain access to a bank account in seven shockingly simple steps. All you need is a name, an address, employment status, date of birth, and email address with a google search, the whole as appears more fully from a copy of the ZD Net article entitled "How to Steal an identity in seven easy steps" dated December 15, 2011 and from a copy of the Scientific American article entitled "How I Stole Someone's Identity" dated August 18, 2008, produced herein *en liasse* as **Exhibit R-48**;

10.73.7 Cyber threat actors have both the intent and capability to acquire sensitive information as demonstrated by numerous high-profile data breaches targeting the data of millions of customers around the world. Large databases containing personal information such as names, addresses, phone numbers, financial details, and employment information are valuable to cyber threat actors. The aggregation of data collected from multiple breaches can provide cyber threat actors the ability to build comprehensive profiles to conduct cyber threat activity against specific groups or individuals, the whole as appears more fully from a copy of an extract

from the Canadian Centre for Cyber Security at https://cyber.gc.ca, produced herein as **Exhibit R-49**;

10.73.8 The personal and private information 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, the whole as appears more fully from a copy of the Business Insider article entitled "Here's how much thieves make by selling your personal data online" dated May 27, 2015, produced herein as **Exhibit R-50**;

10.73.9 Just as companies like Capital One and Amazon trade on the value of consumers' personal and private information, consumers recognize the value of their personal and private information and offer it in exchange for goods and services. Petitioners gave Capital One their personal and private information in exchange for Capital One's services, such as providing or potentially providing credit. Further, the value of personal and private information is key to unlocking many parts of the financial sector for consumers. Whether someone can obtain a mortgage, credit card, business loan, tax return, or even apply for a job depends on the integrity of their personal and private information. Similarly, the businesses that request (or require) consumers to share their personal and private information as part of a commercial transaction do so with the expectation that its integrity has not been compromised;

10.73.10 For class members who had their Social Insurance Numbers (SIN) exposed, the unauthorized disclosure can be particularly damaging because, unlike a credit card, Social Insurance Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, that the SIN was used fraudulently. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Canadian Government warns:

> A new Social Insurance Number is not a fresh start or protection from fraud or identity theft.
>
> If someone else uses your old Social Insurance Number and the business does not check the person's identity, you may have to prove you were not involved in the fraud or pay the impostor's debts.

The whole as appears more fully from copies of extracts from the Government of Canada website and from a copy of the Service Canada booklet entitled "Protecting your Social Insurance Number" dated 2020, produced herein *en liasse* as **Exhibit R-51**;

10.73.11 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 SIN, identity theft victims must spend numerous hours

and their own money repairing the impact to their credit. For example, identity theft victims must spend many hours doing the following:

- Go through their bank and credit card statements to look for charges that they do not recognize or remember making and potentially contact their financial institution;
- Move quickly: identity thieves move as fast as they can;
- Contact their bank(s) and credit card companies to put a stop payment on stolen cheques or freeze/cancel their accounts;
- Change passwords and PINs on everything;
- Get a credit report to check for suspicious activity and place a fraud warning on their credit files;
- Contact the police;
- Contact government agencies such as Passport Canada, Citizenship and Immigration Canada, the provincial government to put an alert on their account;
- Contact Canada Post to check if their addresses have been changed;
- Create a paper trail – they must keep all statements, emails and keep track of any communication with potentially-compromised companies;
- Report the fraud to the Canadian Anti-Fraud Centre (CAFC)

The whole as appears more fully from a copy of an extract from the SGI Canada website at www.sgicanada.ca and from a copy of an extract from the Canadian Anti-Fraud Centre's website at www.antifraudcentre-centreantifraude.ca, produced herein *en liasse* as **Exhibit R-52**;

10.73.12 In addition, 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. 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, the whole as appears more fully from a copy of the U.S. Department of Justice bulletin entitled "Victims of Identity Theft, 2014" revised November 13, 2017, produced herein as **Exhibit R-53**;

10.73.13 Identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey (Exhibit R-53) 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;

10.73.14 Identity theft can also exact a physical toll on its victims. The same survey (Exhibit R-53) 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 behaviours;

10.73.15 There may also be a significant time lag between when personal and private information is stolen and when it is actually misused. According to the U.S. Government Accountability Office, 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.

The whole as appears more fully from a copy of the United States Government Accountability Office report entitled “Personal Information” dated June 2007, produced herein as **Exhibit R-54**;

(ix) The U.S. Litigation and the U.S. Penalties

10.74 On or about July 31, 2019, the first U.S. class action was filed in the United States District Court for the District of Columbia, the whole as appears more fully from a copy of the Complaint and Demand for Jury Trial in Civil Action No. 19-2292 dated July 31, 2019, produced herein as **Exhibit R-21**;

10.75 By October 2, 2019, there were 21 actions pending in 12 districts and 40 potentially-related actions filed in 13 districts. On October 2, 2019, 17 civil actions

were centralized in a multi-district litigation in the Eastern District of Virginia by the Panel on Multidistrict Litigation, the whole as appears more fully from a copy of the Transfer Order in MDL No. 2915 dated October 2, 2019, produced herein as **Exhibit R-22**;

10.76 Also on October 2, 2019, a securities class action was filed and on November 20, 2019, a Conditional Transfer Order was issued by the United States Judicial Panel on Multidistrict Litigation upon finding that the securities class action involved questions of fact that are common to actions previously transferred, the whole as appears more fully from a copy of the Class Action Complaint for Violations of the Federal Securities Laws in *Minsky* v. *Capital One Financial Corporation, et al.*, Case No. 1:19-cv-1472 and from a copy of the Conditional Transfer Order (CTO-2) for MDL No. 2915 dated November 20, 2019, produced herein *en liasse* as **Exhibit R-23**;

10.77 A copy of the list of all associated cases in MDL 2915 as well as a copy of the most recently filed class action *In Re: Capital One Customer Data Security Breach Litigation* dated November 15, 2019, are produced herein *en liasse* as **Exhibit R-24**;

10.78 On December 2, 2019, Plaintiffs' Co-Lead Counsel was appointed, the whole as appears more fully from a copy of Pretrial Order #3 dated December 2, 2019, produced herein as **Exhibit R-25**;

10.79 On December 10, 2019, an initial status conference was reset for January 29, 2020, the whole as appears more fully from a copy of the Amended Pretrial Order #4, dated December 10, 2019, produced herein as **Exhibit R-26**;

10.80 On January 17, 2020, an Amended Class Action Complaint for Violations of the Federal Securities Laws was filed in the record, the whole as appears more fully from a copy of the Amended Class Action Complaint for Violations of the Federal Securities Laws dated January 17, 2020, produced herein as **Exhibit R-27**;

10.80.1 On September 7, 2020, an Amended Representative Consumer Class Action Complaint was filed in the record, the whole as appears more fully from a copy of the Amended Representative Consumer Class Action Complaint dated September 7, 2020, produced herein as **Exhibit R-55**;

10.80.2 On August 6, 2020, The U.S. Office of the Comptroller of the Currency assessed an $80 million civil money penalty against Capital One based on the bank's failure to establish effective risk assessment processes prior to migrating significant information technology operations to the public cloud environment and the bank's failure to correct the deficiencies in a timely manner, the whole as appears more fully from a copy of the U.S. Office of the Comptroller of the Currency news release entitled "OCC Assesses $80 Million Civil Money Penalty Against Capital One" dated August 6, 2020, from a copy of the Consent Order #2020-036,

and from a copy of the Consent Order #2020-037 (Cease and Desist), produced herein *en liasse* as **Exhibit R-56**;

10.80.3 In reaching this penalty, the U.S. Office of the Comptroller of the Currency found *inter alia* the following (Exhibit R-56):

(1) In or around 2015, Capital One failed to establish effective risk assessment processes prior to migrating its information technology operations to AWS. Capital One also failed to establish appropriate risk management for the cloud operating environment, including appropriate design and implementation of certain network security controls, adequate data loss prevention controls, and effective dispositioning of alerts;

(2) Capital One's internal audit failed to identify numerous control weaknesses and gaps in the cloud operating environment and did not effectively report on and highlight identified weaknesses and gaps to the Audit Committee;

(3) The Board failed to take effective actions to hold management accountable, particularly in addressing concerns regarding certain internal control gaps and weaknesses by the internal audit;

(4) Capital One engaged in unsafe or unsound practices that were part of a pattern of conduct;

(5) Capital One has begun addressing these issues;

10.80.4 The U.S. Office of the Comptroller of the Currency ordered Capital One to do *inter alia* the following (Exhibit R-56):

(1) To appoint a Compliance Committee of at least three members by August 31, 2020 to monitor and oversee Capital One's compliance with the provisions of the Order;

(2) To have the Compliance Committee submit regular written progress reports to the Board consisting of: (i) a description of the corrective actions needed to achieve compliance with the Order, (ii) the corrective actions undertaken, and (iii) the results of the corrective actions;

(3) To forward the written progress report tot eh Examiner in Charge;

(4) To develop a written action plan detailing the remedial actions necessary, including reasonable timelines for completion and the person(s) responsible;

(5) To submit a plan to improve oversight of Capital One's cloud operating environment information security program;

(6) To submit a plan to improve risk assessment for the Capital One's cloud and legacy technology operating environments;

(7) To submit a plan to improve the Capital One's Cloud Operations Risk Management;

(8) To submit a plan to improve independent risk management of the cloud operating environment;

(9) To submit a plan designed to enhance the Bank's internal controls testing in the cloud environment;

(10) To submit a plan to enhance the Bank's internal audit program;

(x) Summative Remarks

10.80.5 Through their failure to adequately protect Petitioners' and Class Members' personal and private information, Capital One and Amazon allowed a former Amazon employee to obtain access to and to surreptitiously view, remove, and make public Petitioners' and Class Members' personal and private information, which had been entrusted to the Respondents;

10.80.6 The massive breach went undiscovered by the Respondents 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 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, 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" (Exhibit R-1). And all Respondents knew of the particular security vulnerabilities that permitted the Data Breach, but still failed to protect Petitioners' and Class Members' personal and private information (Exhibit R-37);

10.80.7 Capital One claimed that it was able to "immediately address[] the configuration vulnerability" after the data theft, but it was too little too late for the millions of Canadians 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 personal and private information belonging to Petitioners 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, the whole as appears more fully from a copy of Capital One U.S.' Form 8-K dated July 29, 2019, produced herein as **Exhibit R-57**;

10.80.8 Capital One promised 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, the whole as appears more fully from a copy of an extract

from Capital One's website at www.capitalone.com, produced herein as **Exhibit R-58**;

10.81 Without the assurance that Capital One would safeguard their sensitive personal and private information, Class Members would not have agreed to provide this information to Capital One. Potential customers would not apply for, let alone use and pay for (through interest, fees, and foregone rewards from other issuers), a card from an issuer that did not protect the sensitive information provided by the customer. This in turn would significantly harm, even decimate, Capital One's credit card profits. Indeed, Capital One warned of precisely this risk in its 2018 annual report (see Exhibit R-10 – page 30);

(…)

10.82 In a saturated market for credit cards, credit card companies fiercely compete for borrowers with good credit history. A *sine qua non* of this competitive process is the promise to electronically protect an applicant's most sensitive personal and private information using (at a minimum) industry-standard data security practices. As detailed in this application, this is a promise that Capital One made repeatedly – and continues to make – to credit card applicants and cardholders, in numerous places and contexts, to obtain the valuable personal data that drives its bottom line. It is a promise bolstered by Amazon. And it is a promise that was and is knowingly false and/or misleading;

II. FACTS GIVING RISE TO INDIVIDUAL ACTIONS BY THE PETITIONERS

(i) Petitioner Royer

11. Petitioner Royer is a Costco Capital One Credit Card holder, which he applied for (and was accepted) approximately 4-5 years ago (i.e. in 2015). In order to fill out the application form, he was required to furnish his personal, private, and sensitive information, including his SIN number;

12. It is safe to say that his personal and private information has been compromised;

13. Petitioner Royer had every reason to believe, and did indeed believe, that the Respondents would safeguard his personal and private information from any unauthorized access – they failed in this duty;

13.1 On August 14, 2019, Petitioner Royer received an email from Capital One informing him of the data theft and specifying the following:

> "Based on our investigation, we believe your personal information may have been obtained as part of this incident. We're deeply sorry for the understandable worry this has caused and are committed to making this right.
> …
> Personal information impacted.

Our investigation has determined that the person responsible may have gained access to the following information:

- Personal information routinely collected at the time we receive credit applications, including name, address, postal code, phone number, email address, date of birth and self-reported income.
- Customer status data, including credit score, credit limit, account balance, payment history and contact information.
- Fragments of customer transaction data from a total of 23 days during 2016, 2017 and 2018."

The whole as appears more fully from a copy of the email from Capital One to Petitioner Royer with the subject "Michael, important information about a recent cybersecurity incident" dated August 14, 2019, produced herein as **Exhibit R-27**;

14. Petitioner Royer's damages are a direct and proximate result of the Respondents' conduct;

15. In consequence of the foregoing, Petitioner Royer is justified in claiming damages;

(ii) Petitioner Abou-Khadra

15.1 Petitioner Abou-Khadra is a Costco Capital One Credit Card holder, which he applied for (and was accepted) in 2015. In order to fill out the application form, he was required to furnish his personal, private, and sensitive information, including his SIN number;

15.2 On July 30, 2019, in watching the news, Petitioner Abou-Khadra learned that Capital One credit card holders' personal and private information had been compromised by a data theft;

15.3 As a result and, also on July 30, 2019, Petitioner Abou-Khadra checked his online credit card statement and he found two suspicious transactions on his Capital One credit card; one for $267.00 to PowerKeto and the other for $2.55 also to PowerKeto[7], the whole as appears more fully from copies of three screenshots of Petitioner Abou-Khadra's listed credit card transactions, produced herein *en liasse* as **Exhibit R-28**;

15.4 Petitioner Abou-Khadra called Capital One to report the suspicious transactions. After a long wait, he was able to get transferred to the fraud department, who told him that they would investigate the matter;

[7] According to PowerKeto's website at https://powerketodiet.net, PowerKeto Diet Pills are a dietary supplement you can take for helping aid in weight loss.

15.5 Petitioner Abou-Khadra had to follow up with Capital One as the charges were not reversed for two credit card cycles and at that point, the charges were reversed after it was confirmed that his account had in fact been compromised;

15.6 As a result of this, Petitioner Abou-Khadra had to cancel his Capital One credit card and request a replacement;

15.7 Petitioner Abou-Khadra had every reason to believe, and did indeed believe, that the Respondents would safeguard his personal and private information from any unauthorized access – they failed in this duty;

15.8 Petitioner Abou-Khadra's damages are a direct and proximate result of the Respondents' conduct;

15.9 In consequence of the foregoing, Petitioner Abou-Khadra is justified in claiming damages;

III. FACTS GIVING RISE TO INDIVIDUAL ACTIONS BY EACH MEMBER OF THE CLASS

16. Every member of the Class is a holder of a Capital One Credit Card and has or will suffer the damages as alleged in paragraph 6 above;

17. All of these damages to the Class Members are a direct and proximate result of the Respondents' conduct;

IV. CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

A) The composition of the Class makes it difficult or impractical to apply the rules for mandates to sue on behalf of others or for consolidation of proceedings

18. Petitioners are unaware of the specific number of persons who have a Capital One Credit Card, but the Respondents have admitted that approximately 6 million Canadian customers were affected by the data reach and 1 million Canadian SIN numbers were compromised;

19. Class Members are numerous and are scattered across the entire province;

20. In addition, given the costs and risks inherent in an action before the courts, many people will hesitate to institute an individual action against the Respondents. Even if Class Members themselves could afford such individual litigation, it would place an unjustifiable and enormous burden on the courts and, at the very least, is not in the interests of judicial economy. Further, individual litigation of the factual and legal issues raised by the conduct of the Respondents would increase delay and expense to all parties and to the court system;

20.1 This class action overcomes the dilemma inherent in an individual action whereby the legal fees alone would deter recovery and thereby in empowering the

consumer, it realizes both individual and social justice as well as rectifies the imbalance and restore the parties to parity;

21. Also, a multitude of actions instituted in different territorial and judicial districts, risks having contradictory judgments on issues of fact and law that are similar or related to all members of the Class;

22. These facts demonstrate that it would be impractical, if not impossible, to contact each and every member of the Class to obtain mandates and to join them in one action;

23. In these circumstances, a class action is the only appropriate procedure and the only viable means for all of the members of the Class to effectively pursue their respective rights and have access to justice;

B) The claims of the members of the Class raise identical, similar or related issues of law or fact

24. Individual issues, if any, pale by comparison to the numerous common issues that will advance the litigation significantly;

25. The damages sustained by the Class Members flow, in each instance, from a common nucleus of operative facts, namely, the Respondents' misconduct;

26. The claims of the Class Members raise identical, similar or related issues of fact or law, namely:

a) Did the Defendants provide false and/or misleading information regarding their data security practices and their inability to protect the vast amounts of consumer data, including Class Members' personal and private information to Class Members (…)?

b) Did the Defendants falsely and/or misleadingly claim that Cloud Custodian would detect and prevent misconfigured Identity and Access Management (IAM) roles and policy-based permissions?

c) Did the Defendants know or should they have known (…) that their data storage systems were vulnerable to attack, including but not limited to, that their web application firewall was vulnerable to an attack by a Server-Side Request Forgery (SSRF) (…)?

d) (…)

e) (…)

f) Did the Defendants knowingly or recklessly make false and/or misleading statements about the use of customer data on the AWS cloud and the breadth of data that would be stored there?

g) Were the Defendants negligent in the safekeeping of Class Members' personal and private information, which were compromised on or about March 22 and 23, 2019?

h) Did the Defendants employ adequate data protection policies and security safeguards for Class Members' personal and private information?

i) Did the Defendants fail to comply with internal company policies and applicable laws, regulations, and industry standards relating to data security?

j) Should the Defendants have discovered the data theft prior to the external security researcher's report email to the company on July 17, 2019?

k) Did the Defendants timely disclose the data breach to Class Members on July 29, 2019?

l) Are the Defendants responsible for all related damages, including, but not limited to monetary losses, trouble and inconvenience, moral damages, additional credit monitoring, lost time, lost value of their personal and private information, and in what amount?

m) Should an injunctive remedy be ordered to force the Defendants to establish adequate data protections and security safeguards to prevent and detect unauthorized access to personal and private information?

n) Are the Defendants responsible to pay punitive damages to Class Members and in what amount?

27. The interests of justice favour that this application be granted in accordance with its conclusions;

V. NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

28. The action that the Petitioners wish to institute on behalf of the members of the Class is an action in damages and injunctive relief;

29. The conclusions that the Petitioners wish to introduce by way of an application to institute proceedings are:

GRANT the class action of the Plaintiffs and each of the members of the Class;

ORDER the Defendants to establish adequate data protections and security safeguards to prevent and detect unauthorized access to personal and private information;

DECLARE the Defendants solidarily liable for the damages suffered by the Plaintiffs and each of the members of the Class;

CONDEMN the Defendants to pay to each member of the Class a sum to be determined in compensation of the damages suffered, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay to each of the members of the Class, punitive damages, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay interest and additional indemnity on the above sums according to law from the date of service of the application to authorize a class action;

ORDER the Defendants to deposit in the office of this court the totality of the sums which forms part of the collective recovery, with interest and costs;

ORDER that the claims of individual Class Members be the object of collective liquidation if the proof permits and alternately, by individual liquidation;

CONDEMN the Defendants to bear the costs of the present action including expert and notice fees;

RENDER any other order that this Honourable Court shall determine and that is in the interest of the members of the Class;

A) Petitioners request that they be attributed the status of representatives of the Class

30. The Petitioners are members of the Class;

31. The Petitioners are ready and available to manage and direct the present action in the interest of the members of the Class that they wish to represent and are determined to lead the present file to a final resolution of the matter, the whole for the benefit of the Class, as well as, to dedicate the time necessary for the present action before the Courts and the *Fonds d'aide aux actions collectives*, as the case may be, and to collaborate with their attorneys;

32. The Petitioners have the capacity and interest to fairly and properly protect and represent the interest of the members of the Class;

33. The Petitioners have given the mandate to their attorneys to obtain all relevant information with respect to the present action and intend to keep informed of all developments;

34. The Petitioners, with the assistance of their attorneys, are ready and available to dedicate the time necessary for this action and to collaborate with other members of the Class and to keep them informed;

35. The Petitioners have given instructions to their attorneys to put information about this class action on its website and to collect the coordinates of those Class Members that wish to be kept informed and participate in any resolution of the

present matter, the whole as will be shown at the hearing. To date, 8,714 potential Class Members who have inputted their information through the CLG webpage, the whole as appears more fully from a copy of a redacted chart, produced herein as **Exhibit R-30**;

36. The Petitioners are in good faith and have instituted this action for the sole goal of having their rights, as well as the rights of other Class Members, recognized and protected so that they may be compensated for the damages that they have suffered as a consequence of the Respondents' conduct;

37. The Petitioners understand the nature of the action;

38. The Petitioners' interests are not antagonistic to those of other members of the Class;

39. The Petitioners are prepared to be examined out-of-court on their allegations (as may be authorized by the Court) and to be present for Court hearings, as may be required and necessary;

40. The Petitioners have spent time researching this issue on the internet and meeting with their attorneys to prepare this file. In so doing, they are convinced that the problem is widespread;

41. (…)

B) Petitioners suggest that this class action be exercised before the Superior Court of justice in the district of Montreal

42. A great number of the members of the Class reside in the judicial district of Montreal and in the appeal district of Montreal;

43. The Petitioners' attorneys practice their profession in the judicial district of Montreal;

44. The present application is well founded in fact and in law.

FOR THESE REASONS, MAY IT PLEASE THE COURT:

GRANT the present application;

AUTHORIZE the bringing of a class action in the form of an application to institute proceedings in damages and injunctive relief;

APPOINT the Petitioners as representatives of the persons included in the class herein described as:

- all persons, entities, or organizations resident in Quebec who were either Capital One Credit Card holders or who had applied for a Capital One Credit Card and whose personal and private information was

compromised by the incident that occurred on or about March 22 and 23, 2019 (though such breach was only disclosed to the public on July 29, 2019), or any other group to be determined by the Court;

IDENTIFY the principle issues of fact and law to be treated collectively as the following:

a) Did the Defendants provide false and/or misleading information regarding their data security practices and their inability to protect the vast amounts of consumer data, including Class Members' personal and private information to Class Members (…)?

b) Did the Defendants falsely and/or misleadingly claim that Cloud Custodian would detect and prevent misconfigured Identity and Access Management (IAM) roles and policy-based permissions?

c) Did the Defendants know or should they have known (…) that their data storage systems were vulnerable to attack, including but not limited to, that their web application firewall was vulnerable to an attack by a Server-Side Request Forgery (SSRF) (…)?

d) (…)

e) (…)

f) Did the Defendants knowingly or recklessly make false and/or misleading statements about the use of customer data on the AWS cloud and the breadth of data that would be stored there?

g) Were the Defendants negligent in the safekeeping of Class Members' personal and private information, which were compromised on or about March 22 and 23, 2019?

h) Did the Defendants employ adequate data protection policies and security safeguards for Class Members' personal and private information?

i) Did the Defendants fail to comply with internal company policies and applicable laws, regulations, and industry standards relating to data security?

j) Should the Defendants have discovered the data theft prior to the external security researcher's report email to the company on July 17, 2019?

k) Did the Defendants timely disclose the data breach to Class Members on July 29, 2019?

l) Are the Defendants responsible for all related damages, including, but not limited to monetary losses, trouble and inconvenience, moral damages, additional credit monitoring, lost time, lost value of their personal and private information, and in what amount?

m) Should an injunctive remedy be ordered to force the Defendants to establish adequate data protections and security safeguards to prevent and detect unauthorized access to personal and private information?

n) Are the Defendants responsible to pay punitive damages to Class Members and in what amount?

IDENTIFY the conclusions sought by the class action to be instituted as being the following:

GRANT the class action of the Plaintiffs and each of the members of the Class;

ORDER the Defendants to establish adequate security safeguards to prevent and detect unauthorized access to personal and private information;

DECLARE the Defendants solidarily liable for the damages suffered by the Plaintiffs and each of the members of the class;

CONDEMN the Defendants to pay to each member of the Class a sum to be determined in compensation of the damages suffered, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay to each of the members of the Class, punitive damages, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay interest and additional indemnity on the above sums according to law from the date of service of the motion to authorize a class action;

ORDER the Defendants to deposit in the office of this court the totality of the sums which forms part of the collective recovery, with interest and costs;

ORDER that the claims of individual Class Members be the object of collective liquidation if the proof permits and alternately, by individual liquidation;

CONDEMN the Defendants to bear the costs of the present action including expert and notice fees;

RENDER any other order that this Honourable Court shall determine and that is in the interest of the members of the Class;

DECLARE that all members of the Class that have not requested their exclusion, be bound by any judgment to be rendered on the class action to be instituted in the manner provided for by the law;

FIX the delay of exclusion at thirty (30) days from the date of the publication of the notice to the members, date upon which the members of the Class that have not

exercised their means of exclusion will be bound by any judgment to be rendered herein;

ORDER the publication of a notice to the members of the group in accordance with article 579 C.C.P. within sixty (60) days from the judgment to be rendered herein in The Montreal Gazette and *La Presse*;

ORDER that said notice be available on the Respondents' websites, Facebook pages, and Twitter accounts with a link stating "Notice to Capital One Credit Card Holders";

ORDER that said notice be sent by individual letters emailed and/or mailed to Class Members by using the Respondents' customer list;

RENDER any other order that this Honourable Court shall determine and that is in the interest of the members of the Class;

THE WHOLE with costs, including all publication and dissemination fees.

Montreal, October 16, 2020

_____
CONSUMER LAW GROUP INC.
Per: Me Jeff Orenstein
Attorneys for the Petitioners

CONSUMER LAW GROUP INC.
1030 rue Berri, Suite 102
Montréal, Québec, H2L 4C3
Telephone: (514) 266-7863
Telecopier: (514) 868-9690
Email: agrass@clg.org