CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

N°: 500-06-000675-138

SUPERIOR COURT
(Class Action)

E[redacted] ZUCKERMAN

Petitioner

-vs-

TARGET CORPORATION

Respondent

AMENDED MOTION TO AUTHORIZE THE BRINGING OF A CLASS ACTION AND TO ASCRIBE THE STATUS OF REPRESENTATIVE
(Art. 1002 C.C.P. and following)

TO THE HONORABLE JUSTICE MICHEL A. PINSONNAULT (...) OF THE SUPERIOR COURT OF QUEBEC, SITTING IN AND FOR THE DISTRICT OF MONTREAL, THE PETITIONER STATES THE FOLLOWING:

Introduction and General Presentation

1. Petitioner wishes to institute a class action on behalf of the following group, of which Petitioner is a member, namely:

> All persons in Canada (subsidiarily in Quebec and subject to Article 999 C.C.P.), whose personal and/or financial information was lost by and/or stolen from Respondent as a result of the data breach that occurred between at least November 27, 2013 and December 15, 2013 (hereinafter the "**Data Breach**"), and as a Sub-Group, all other persons, businesses, entities, corporations, financial institutions or banks who suffered damages or incurred expenses as a result of said Data Breach, or any other Group(s) or Sub-Group(s) to be determined by the Court;

(hereinafter, both Quebec resident and non-Quebec resident Class Members are collectively referred to as "Class Member(s)", "Group Member(s)", the "Group", the "Class", the "Client(s)" or the "Customer(s)");

2. Respondent TARGET CORPORATION (hereinafter "**Target**") is a U.S. company with its head office located in Minneapolis, Minnesota, U.S.A.;

3. Target is one of the largest discount retailers in the United States with approximately 1,800 retail stores in the U.S.A and estimated annual sales exceeding $73.8 billion, and over 120 retail stores in Canada, either directly or through its related entity Target Canada Co. (hereinafter "**Target Canada**"). According to Respondent's own allegations in the present proceedings, Target Canada is an "indirect, wholly owned subsidiary of Respondent", although Respondent has not provided the details in this regard;

4. As a national retail chain with Point-of-Sale ("POS") computer systems that store credit card and bank card ("ATM") information, Target must ensure that its customers' personal and financial information is safeguarded from theft. When a data breach affecting customers occurs, a national retail chain must immediately and accurately notify its customers to prevent such customers from incurring financial losses, loss of time, expenses, and/or inconvenience as a result of the actual or threatened fraudulent use of stolen personal and financial information. These proceedings stem from Target's faults and/or negligence in this regard;

5. Beginning on or about November 17, 2013 and continuing until on or about December 15, 2013, the POS computer network that processes transactions for all Target retail stores in the U.S.A. was breached by unknown attackers. The breach resulted in one of the (if not the) largest theft of personal and financial information in history and affected at least 40 million credit card and ATM accounts and the personal and financial information of at least 70 million individuals, including approximately 700,000 Canadians. The lost information included, without limitation, the names, phone numbers, home addresses, credit and debit card n6umbers, PIN numbers, expiration dates, magnetic strip information, and passwords;

6. On or about January 14, 2014, a "Class Action Complaint and Demand for Jury Trial" was filed against Target before the United States District Court, Northern District of California, and stemming from the Target Data Breach (hereinafter the "**California Consumer Class Action**"), a copy of which is filed herewith, as though recited at length herein, as **Exhibit R-1**;

7. There have been over 80 similar consumer class action proceedings filed all across the U.S.A., against Target and stemming from the Target Data Breach, as reported by the Wausau Daily Herald in its February 15, 2014 article, a copy of which is communicated herewith as **Exhibit R-2**. Ultimately, the various U.S.A. class actions, including the California Consumer Class Action (R-1), were consolidated, the whole as more fully appears from the Consumer Plaintiff's Consolidated Class Action Complaint, dated August 25, 2014 (hereinafter the "**Consumer Plaintiff's Consolidated Class Action Complaint**"), a copy of which is filed herewith, as though recited at length herein, as **Exhibit R-1A**;

8. Indeed, on or about February 13, 2014, another Class Action Complaint was filed in the United States District Court, Western District of Wisconsin, in which similar claims for the customers/victims of the Target Data Breach are being made but in which a financial institution is also claiming that similar financial institutions or banks have been harmed by the Target Data Breach as well and have incurred costs, namely costs of cancelling and re-issuing credit and debit cards, monitoring accounts, reimbursing customers for fraudulent charges, incurring administrative expenses and overhead charges, compliance costs associated with credit and debit card disposal, and that financial institutions may incur other related damages in the future (hereinafter the "**Bank Class Action**"), a copy of which is filed herewith, as though recited at length herein, as **Exhibit R-3**. Ultimately, various U.S.A. bank class actions, including the Bank Class Action (R-3), were consolidated as well, the whole as more fully appears from the Financial Institutions Consolidated Class Action Complaint, dated August 1, 2014 (hereinafter the "**Financial Institution Consolidated Class Action Complaint**"), a copy of which is filed herewith, as though recited at length herein,

as **Exhibit R-3A**;

9. The California Class Action (R-1), the Consumer Plaintiff's Consolidated Class Action Complaint (R-1A), (...) the Bank Class Action (R-3), and the Financial Institutions Consolidated Class Action Complaint (R-3A) describe(...) in great detail the nature and extent of the Data Breach, representations and claims made by Target in regards to the breach and also refer to other relevant information, sources and/or documents on these issues, all of which Petitioner relies upon, as though recited at length herein, in order to further satisfy his "arguable case" burden herein (aside from what is more fully detailed hereinbelow);

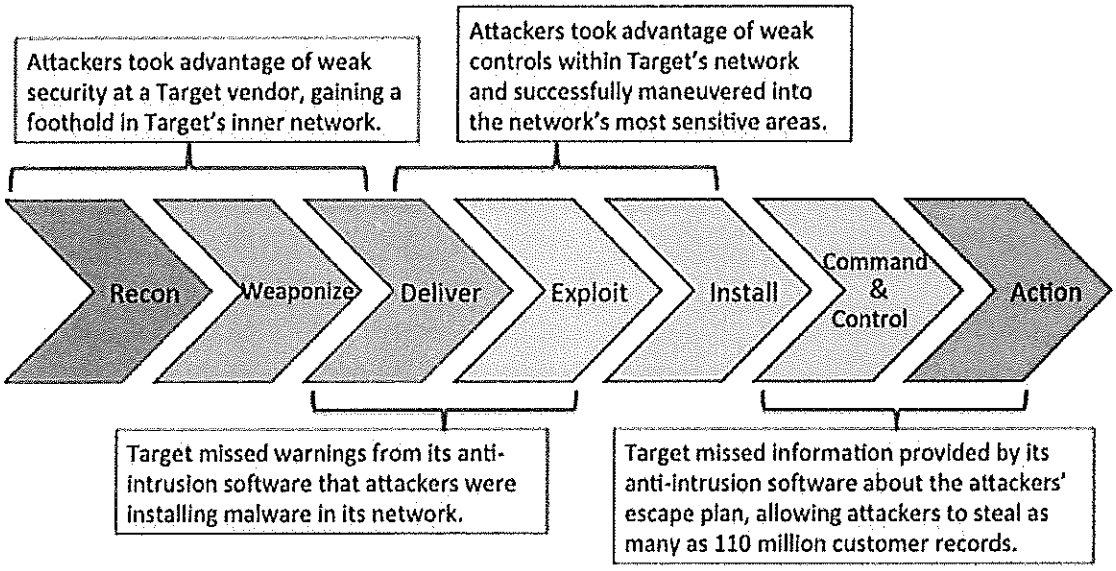
9.1. Furthermore, following the initial institution of the present proceedings, namely on or about March 26, 2014, the U.S. Senate Committee on Commerce, Science & Transportation Chairman Senator John D. (Jay) Rockefeller IV released a staff report titled "A 'Kill Chain' Analysis of the 2013 Target Data Breach", which details how Target was repeatedly warned and alerted of malicious activity prior to the extraction of the financial and personal information from Target's systems. Moreover, said report details how Target negligently missed several opportunities to prevent the Data Breach from occurring (which as mentioned above included the private information of approximately 700,000 Canadians), the whole as more fully appears from a copy of the U.S. Senate press release dated March 25, 2014 and the U.S. Senate Report dated March 26, 2014, filed herewith, as though recited at length herein, *en liasse*, as **Exhibit R-22** (hereinafter the "**March 26, 2014 U.S. Senate Report**");

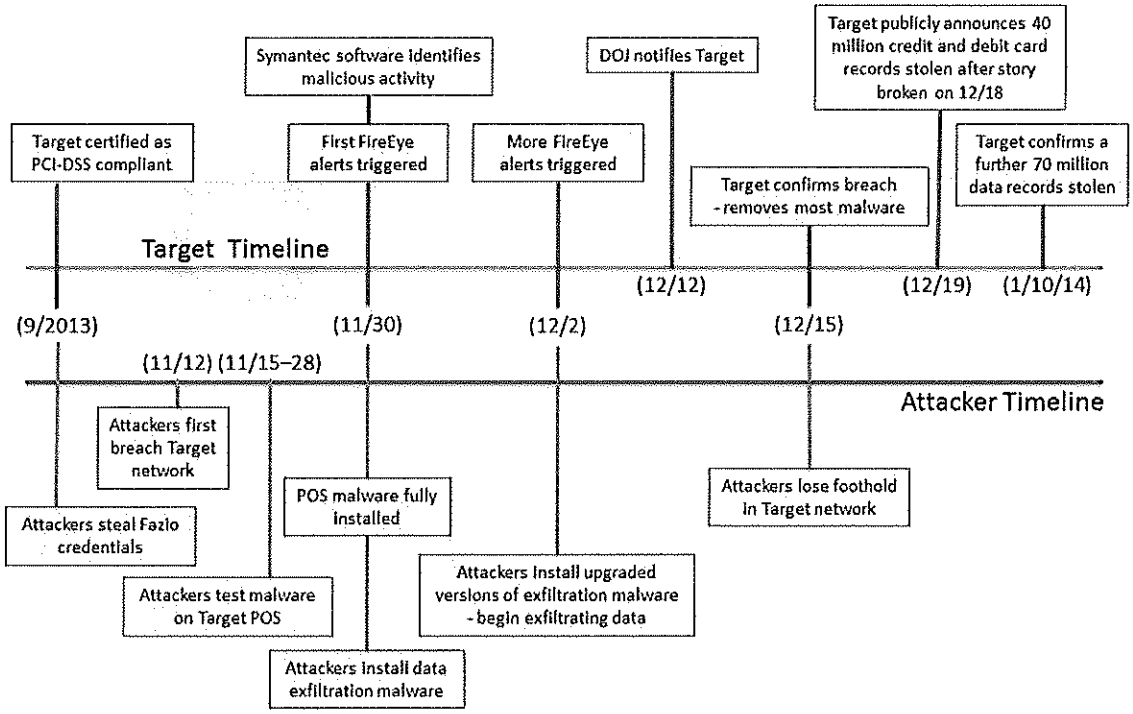
9.2. The March 26, 2014 U.S. Senate Report (Exhibit R-22) concludes the following:

> "This report analyzes what has been reported to date about the Target data breach, using the "intrusion kill chain" framework, an analytical tool introduced by Lockheed Martin security researchers in 2011, and today widely used by information security professionals in both the public and the private sectors. This analysis suggests that Target missed a number of opportunities along the kill chain to stop the attackers and prevent the massive data breach. Key points at which Target apparently failed to detect and stop the attack include, but are not limited to, the following:

- Target gave network access to a third-party vendor, a small Pennsylvania HVAC company, which did not appear to follow broadly accepted information security practices. The vendor's weak security allowed the attackers to gain a foothold in Target's network.
- Target appears to have failed to respond to multiple automated warnings from the company's anti-intrusion software that the attackers were installing malware on Target's system.
- Attackers who infiltrated Target's network with a vendor credential appear to have successfully moved from less sensitive areas of Target's network to areas storing consumer data, suggesting that Target failed to properly isolate its most sensitive network assets.
- Target appears to have failed to respond to multiple warnings from the company's anti-intrusion software regarding the escape routes the attackers planned to use to exfiltrate data from Target's network."

9.3. Moreover, the March 26, 2014 U.S. Senate Report also provides *inter alia* the following tables summarizing the Target Data Breach:

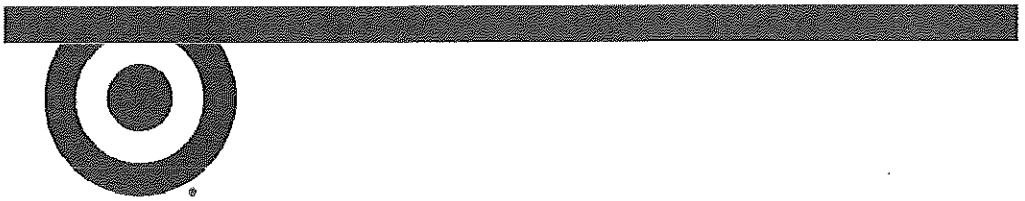




10. Petitioner is reserving his right to amend these proceedings in order to more fully refer to the U.S. proceedings and/or the U.S. Senate investigation and/or to file documents related thereto;

11. As appears from Target Canada's email sent to the Petitioner (and presumably to certain but not all Canadian Class Members) on or about January 20, 2014, a copy of said email being filed herewith, as **Exhibit R-4** (hereinafter the "**Notification Email(s)**"), Target through and/or in conjunction with Target Canada stated and admitted the following:

From: Target Canada <from@email.target.ca>
Subject: Important message from Target to our guests | Message important de Target à l'intention de ses clients
Date: 20 January, 2014 2:34:52 PM EST
To: [redacted]
Reply-To: "reply" <1a90dd8dblayfovcia3lqj5qaaaaab3hcirgc7j2pp4yaaaaa@email.target.ca>



Pour voir la version française, veuillez faire défiler la page vers le bas.

Dear Target Guest,

As you may have heard or read, Target learned in mid-December that criminals forced their way into our systems and took guest information, including debit and credit card data from our U.S. stores; Target Canada stores were not impacted by the payment card breach. In early January, as part of our ongoing investigation, we learned that guest contact information — separate from the payment card data — was also taken, including name, mailing address, phone number or email address. I am writing to make you aware that your name, mailing address, phone number or email address may have been taken during the intrusion.

We have retained a leading third party forensics firm who is conducting a thorough investigation of this incident. Additionally, Target alerted authorities immediately after we discovered and confirmed the initial unauthorized access. We are investing in the internal processes and systems needed to reduce the likelihood that this ever happens again.

I am truly sorry this incident occurred and sincerely regret any inconvenience it may cause you. Because we value you as a guest and your trust is important to us, Target is working on a credit monitoring offer for impacted Canadian guests. We will send you information about that offer when it becomes available in the coming days, so there is no need for you to contact us at this time.

To guard against possible scams, always be cautious about sharing personal information, such as social insurance number, passwords, user IDs and financial account information. Here are some tips that will help protect you:

- Never share information with anyone over the phone, email or text, even if they claim to be someone you know or do business with. Instead, ask for a call-back number.
- Delete texts immediately from numbers or names you don't recognize.
- Be wary of emails that ask for money or send you to suspicious websites. Don't click links within emails you don't recognize.

Target's email communication regarding this incident will never ask you to provide personal or sensitive information.

Thank you for your patience and loyalty to Target. If you have further questions, you may call us at 800-776-4444 or visit Target.ca/support.

Gregg Steinhafel

Gregg Steinhafel

Chairman, President and CEO

12. Through its above-cited Notification Email (Exhibit R-4), Target, through its mandatary and/or together with its wholly owned subsidiary Target Canada, has clearly admitted the following, *inter alia*:

a) That Target had lost debit and credit card data of the Class Members from its U.S. stores;

b) That separate from this payment card data lost, it had also lost Class Members' contact information including name, mailing address, phone number and email address (it seems in this regard that this lost information is not linked to any specific time frame for purchases at Target Stores in the U.S. and that, therefore, it involves all people who have ever shopped at a Target store in the U.S.A. (providing their personal information);

c) That this loss of information may cause Class Members "inconvenience", which Target "sincerely regret[s]";

d) That the affected Class Members will require credit monitoring;

e) That the Class Members should "always be cautious about sharing personal information", in order to "guard against possible scams" (referred to as "*manoeuvres frauduleuses*" in the French version of the R-4 Notification Email), therefore admitting that it is reasonably possible that unauthorized persons could have received, accessed or misused the personal information of the Class Members;

f) That Target is "investing in the internal processes and systems needed to reduce the likelihood that this ever happens again", therefore admitting

that the required measures were not originally in place which would have prevented this loss of information in the first place;

13. As appears from Target Canada's follow-up email sent to the Petitioner (and presumably certain but not all Canadian Class Members) on or about January 24, 2014, a copy of said email being filed herewith, as **Exhibit R-5** (hereinafter the "**Follow-up Email(s)**"), Target through and/or in conjunction with Target Canada stated and admitted the following:

From: Target Canada <from@email.target.ca>
Date: January 24, 2014 at 9:25:02 AM EST
To: [redacted]
Subject: Important message from Target about free credit monitoring offer | Message important de Target à propos de l'offre gratuite de surveillance du crédit
Reply-To: "reply" <17f4c61a1layfovcia3lqw3aaaaaab3hcirgc7lyhqeyaaaaa@email.target.ca>

Pour voir la version française, veuillez faire défiler la page vers le bas.

Dear Target Guest,

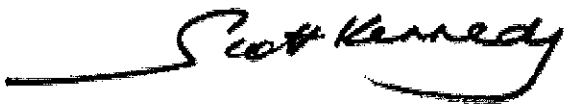
As we shared with you earlier this week, your contact information, such as your name, mailing address, phone number or email address may have been taken during the recent data intrusion at Target. This is generally publicly available information, so the primary risk is increased exposure to consumer scams, such as phishing, web scams and social engineering. (As a reminder, the payment card data that was also stolen during the incident only impacted our U.S. stores; Target Canada stores were not impacted by the payment card breach.)

Because we value you as a guest and your trust is important to us, Target is offering you one year of free credit monitoring through the Equifax Complete™ Advantage Plan, which includes identity theft insurance where available. If you wish to sign up for this free credit monitoring service, please go to myservices.equifax.ca/enroll. During enrollment, you will be asked to provide payment type. **Do not enter your payment information unless you would like to purchase other services or coverage beyond this first year of free credit monitoring.** Instead, use the promotional code **850461588954** in the promotion code field to receive the first year for free. Any product pricing information for the Equifax

Complete™ Advantage Plan will not apply to you for the first year if you use the promotional code. **Please note that submitting your Social Insurance Number in the enrollment process is also optional.** You must register by April 30, 2014, as the offer expires after this date. By enrolling in this service, you will receive:

- Comprehensive view of your Equifax Credit Report
- Equifax Credit Score™ to see how lenders may perceive you
- 24/7 credit monitoring with email notification of key changes to your file
- Quarterly credit updates of your Equifax Credit Report and Score
- Dedicated fraud specialists
- Up to $25,000 identity theft insurance†

We are truly sorry this incident occurred and sincerely regret any inconvenience it may cause you. If you have further questions, please visit Target.ca/support.



Scott Kennedy, President, Target Financial and Retail Services

†Identity theft insurance underwritten by subsidiaries or affiliates of Chartis Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Coverage may not be available in all jurisdictions.

14. Through its above-cited Follow-up Email (Exhibit R-5), Target, through its mandatary and/or together with its wholly owned subsidiary Target Canada, has clearly admitted the following, *inter alia*:

a) That "primary risk" of Target's loss of the Class Members' personal information "is increased exposure to consumer scams, such as phishing, web scams, and social engineering"[1] (or in French: "*une vulnérabilité accrue aux escroqueries telles que l'hameçonnage, les fraudes sur le Web et le piratage psychologique*");

b) That Target was responsible toward Class Members to pay for (and was offering to pay for) one year of credit monitoring (which includes, only in

[1] Phishing is the act of attempting to acquire information such as usernames, passwords, credit card details, etc. (and sometimes, indirectly, money) by masquerading as a trustworthy entity or company in an electronic communication. Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information, including without limitation by means of confirming certain confidential information already possessed about the person in order to convince that person to provide his or her other confidential information.

some jurisdictions it seems, identity theft insurance);

c) That Target is once again "truly sorry this incident occurred and sincerely regrets any inconvenience" caused to Class Members;

15. Petitioner will now detail certain facts which led up to the Target Data Breach in question and the Notification Emails sent to certain but not all Class members approximately two (2) months after the Data Breach had begun;

Target Collects and Stores its Customers' Personal Information

16. Target is the second-largest discount retailer in the United States and is currently ranked 36th on the "Fortune 500" list of top US companies. Target advertises and sells discounted merchandise directly to millions of consumers through its approximate 1,800 retail stores in the United States, through its www.target.com website, and at over 120 retail stores in Canada either directly or through its (...) wholly owned subsidiary Target Canada;

17. When a customer makes a purchase at Target retail stores using a credit or debit card, including Target's branded REDcard, Target collects information related to that card including the card holder name, the account number, expiration date, card verification value (CVV), and PIN for ATM/debit cards. It stores this information in its Point-of-Sale ("POS") system and transmits this information to a third party for completion of the payment. Target also collects and stores customer names, mailing addresses, phone numbers, and email addresses;

18. Target recognizes that its customers' personal and financial information is highly sensitive and must be protected. According to Target's November 14, 2013, Privacy Policy, "[b]y interacting with Target, you consent to use of information that is collected or submitted as described in this privacy policy." Target states:

> "We maintain administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information."

the whole as more fully appears from Target's Privacy Policy as it was posted on its website in November 2013, communicated herewith as **Exhibit R-6**;

19. The PCI Security Standards Council[2] "Payment Card Industry (PCI) Data Security Standard" (hereinafter the "**PCI DSS**") is an industry standard for large retail institutions that accept credit card and debit card transactions. The standard consists of 12 general requirements:

a. Install and maintain a firewall configuration to protect data;

b. Do not use vendor-supplied defaults for system passwords and other security parameters;

c. Protect stored data;

d. Encrypt transmission of cardholder data and sensitive information across public networks;

e. Use and regularly update anti-virus software;

f. Develop and maintain secure systems and applications;

g. Restrict access to data by business need-to-know;

h. Assign a unique ID to each person with computer access;

i. Restrict physical access to cardholder data;

j. Track and monitor all access to network resources and cardholder data;

k. Regularly test security systems and processes;

l. Maintain a policy that addresses information security

the whole as more fully appears from a copy of the PCI Security Standards Council's "About Us" page and the PCI DSS "Requirements and Security Assessment Procedures", communicated herewith, *en liasse*, as **Exhibit R-7**;

---

[2] Founded by global payment brands American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.

20. The PCI DSS (R-7) is intended to build and maintain a secure network, protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies;

21. Through its fault and/or negligence, Target did not follow or properly implement the PCI DSS or any other equally effective industry standard to protect customers' personal and financial information and is therefore responsible for the Data Breach;

Vulnerability of Corporate POS Systems Was Made Known to Target Years Before this Data Breach

22. The massive Target POS data breach could have been prevented;

23. As early as 2007[3] Target was specifically warned by a data security expert about the possibility of a POS data breach, it was told how to prevent such a breach, and it was even told that failure to act could possibly result in the compromise of as many as 58 million charge accounts. Target described the security expert's suggestions as "good ideas" but did not (or did not fully) implement the required actions to prevent such a breach and it did not have the proper systems in place to at least discover the POS data breach sooner than it did;

24. More specifically, on August 27, 2007, Dr. Neal Krawetz of Hacker Factor Solutions publicly disclosed a white paper titled "Point-of-Sale Vulnerabilities" (hereinafter the "**White Paper**"). The White Paper Abstract describes its content as follows:

> Point-of-Sale (POS) systems provide the initial interface for credit card transactions. While the communications between POS systems have been hardened through the use of cryptography and a variety of authentication

[3] In this regard, Petitioner refers to the relevant portions of the Exhibit R-1 California Class Action (paragraphs 22 and following).

> techniques, the devices themselves provide virtually no security. Few POS systems implement best practices for handling sensitive information, such as the Visa standards for credit card management. This document describes common risks to credit card users due to POS systems.

the whole as more fully appears for a copy of the White Paper, communicated herewith as **Exhibit R-8**;

25. The White Paper describes as background how between January and March 2006, thousands of credit card customers received letters containing replacement cards and stating that their card information may have been compromised. "[T]he potentially compromised information was everything on the card: name, card number, expiration date, possibly the CVV2 (number on the back of the card), and possibly the PIN code." The background section concludes:

> Although the person responsible for the compromise is unknown, the retailer is inconclusive, and the details of the compromise continually change, the method for conducting the compromise is likely due to a lack of POS security. Furthermore, the unsafe storage of credit card information in POS systems is not limited to FTS or OfficeMax; it impacts nearly **every** POS vendor and retailer. This vulnerability was discussed with Verifone between 1992 and 1993 – this is a fourteen-year-old attack method.

26. Presciently, the 2007 White Paper uses Target as an example of the potential ramifications of a POS data breach at a major retailer. It estimates that as many as 58 million card accounts could be compromised if Target's POS system was compromised;

27. In his conclusion for the White Paper (R-8) Dr. Krawetz specifically notes:

> Point-of-sale terminals and branch servers store credit card information in ways that are no longer secure enough. These vulnerabilities are not limited to any single POS vendor; they pose a fundamental hole in the entire POS market. It seems that nearly every POS provider is vulnerable, including Verifone, FujitsuTransaction Solutions, Retalix, Hypercom, Autostar, Innovax, JDA, JPMA, NCR, StoreNext, IBM, and Systech. Similarly, these vulnerabilities impact all retailers that use these systems, including (but not limited to) OfficeMax, BestBuy, Circuit City, **Target**, Wal- Mart, REI, Staples, Nordstrom, and Petco. The amount of vulnerability varies between retailers and their implementations. But in general, if a credit card is not required to return a product, or the product can be returned at any store, then the retailer likely has a serious vulnerability.

(Emphasis added)

28. Dr. Krawetz, continues by summarizing the vulnerable aspects of the POS architecture, including Branch Servers and closes with:

> Even though other sightings have occasionally surfaced, the February 9th [2006] announcement showed the first big vendor being publicly hit with this problem. This compromise was not the first, it is unlikely to be the last, and it certainly will not be the biggest. It is only a matter of time before a national branch server at a large retailer is compromised.

29. On or about August 7, 2007, a Target employee responsible for Target's POS system acknowledged receipt of the White Paper and requested permission to provide it to other Target employees. The Target employee described Dr. Krawetz suggestions as "good ideas"[4];

30. Dr. Krawetz' website logs the web domains that download copies of his documents. A domain registered to Target Corporation downloaded 17 copies of the White Paper between August 2007 and May 2013. Search terms that led to downloads of the White Paper to the Target domain as late as May 2013, included "POS vulnerability."[5];

30.1. Furthermore, shortly before the Data Breach, Target experienced other intrusive attacks to its POS system. Despite said attacks, Target still did not protect its systems adequately, the whole as more fully appears from the Consumer Plaintiff's Consolidated Class Action Complaint (R-1A – paragraphs 200 and following);

30.2. Indeed, and most alarmingly, the March 26, 2014 U.S. Senate Report (Exhibit R-22) confirms that Target had been repeatedly alerted to the November and December 2013 intrusions **before** the personal and financial information of the Class Members had been extracted from Target's systems, but that Target

[4] Id.
[5] Id.

simply chose to ignore said alerts:

> "A Dell SecureWorks report shows that the attackers also installed malware, designed to move stolen data through Target's network and the company's firewall, on a Target server. The Dell SecureWorks team was able to analyze a sample of the actual malware used in the Target attack. The attackers reportedly first installed three variants of this malware on November 30 and updated it twice more, just before midnight on December 2 and just after midnight on December 3. According to a *Bloomberg Businessweek* report, Target's FireEye malware intrusion detection system triggered urgent alerts with each installation of the data exfiltration malware. However, Target's security team neither reacted to the alarms nor allowed the FireEye software to automatically delete the malware in question. Target's Symantec antivirus software also detected malicious behavior around November 28, implicating the same server flagged by FireEye's software."

30.3. Petitioner files herewith as **Exhibit R-23**, as though recited at length, a copy of the above-mentioned Bloomberg Businessweek article (dated March 13, 2014) (hereinafter the "**Bloomberg Report**") that initially broke the story regarding the alerts by FireEye to Target prior to the Data Breach, which were ultimately ignored by Target;

30.4. In this regard, Petitioner also files herewith as **Exhibit R-24**, as though recited at length, various news articles published following the release of the Bloomberg Report (Exhibit R-23), in which Target admits that its own security software had detected the malicious activity involved in the Data Breach, but that its staff decided not to take immediate action;

30.5. Indeed, on March 26, 2014, Target's Executive Vice President and Chief Financial Officer John Mulligan provided a written statement to the U.S. Senate Committee on Commerce, Science, & Transportation in which he admitted *inter alia* that:

> "It appears that intruders entered our system on November 12. We now believe that some intruder activity was detected by our computer security systems, logged and surfaced to the SOC [Target's Security Operations Center] and evaluated by our security professionals. With the benefit of hindsight and new information, we are now asking hard questions regarding the

judgments that were made at that time and assessing whether different judgments may have led to different outcomes.";

the whole as more as more fully appears from a copy of the March 26, 2014 written statement by Target's Executive Vice President and Chief Financial Officer John Mulligan, filed herewith as **Exhibit R-25**;

30.6. Moreover, both the March 26, 2014 Senate Report (R-22) and the Bloomberg Report (R-23) confirm the following *inter alia*:

a) That the malicious POS software used to steal the financial and personal information of Target Customers was uploaded from Russia (Exhibit R-23, page 6);

b) That the financial and personal information of as many as 110 million Target Customers was stolen and then removed from Respondent's network to a server in Eastern Europe (Exhibit R-22, page i);

c) That once the malware was successfully in place, the data was sent to different U.S. staging points before being sent to a Russian-based server (Exhibit R-23, page 4 and 5 and Exhibit R-22, page 4);

d) That some of the compromised servers used as external data drop locations were located in Miami and Brazil (Exhibit R-22, page 4);

e) That Andrey Khodyrevski, a 22 year-old hacker from Odessa, Ukraine, who goes by the moniker "Rescator", was believed to be behind the cyber-attack (Exhibit R-23, page 7);

The Data Breach:

31. As previously mentioned, sometime between at least November 27, 2013 and on or about December 15, 2013, hackers gained access to Target's data network and stole the credit and debit card information of about 40 million Target shoppers and the personal information of 70 million people, including approximately 700,000 Canadian Class Members. The lost information included, without limitation, the names, phone numbers, home addresses, credit and debit card numbers, PIN numbers, expiration dates, magnetic strip information, and passwords;

32. The hackers were in fact able to harvest data from Target's systems daily, over the course of several weeks[6]. Accordingly, Target negligently did not have the proper security measures and protocols in place to prevent the intrusions in the first place, nor did it monitor its systems in order to be alerted once the intrusions had first occurred;

33. Target has said that it had been (...) made aware of the Data Breach sometime during the week of December 9, 2013[7] (although Target had received security alerts about the intrusion prior to this date, which alerts Target chose to ignore, the whole as mentioned above and as detailed at length in the Consumer Plaintiff's Consolidated Class Action Complaint (R-1A – paragraphs 152 and following);

34. However, news of the Data Breach was first reported on December 18, 2013 by computer security blogger Brian Krebs on his blog, krebsonsecurity.com. In breaking the story, Krebs confirmed with independent fraud analysts that Target had been breached after they were able to buy a number of stolen card accounts

[6] The whole as mentioned in the Exhibit R-3 Bank Class Action and reported in the January 17, 2014 article on the forbes.com website, a copy of which is communicated herewith as **Exhibit R-9**.

[7] As mentioned in the Exhibit R-3 Bank Class Action.

from a well-known "card shop" – an online store advertised in cybercrime forums as a place where thieves can reliably buy stolen credit and debit cards, the whole as more fully appears from Brian Kreb's blog post dated December 18, 2013, communicated herewith as **Exhibit R-10;**

35. Accordingly, the next day (on December 19, 2013), Target issued its first press release confirming that unknown attackers were able to gain unauthorized access to Target's payment card data. According to Target, the unknown data thieves stole data including customer names, credit or debit card numbers, card expiration dates, and the card verification value (CVV), the whole as more fully appears from Target's December 19, 2013 "Important Notice: Unauthorized access to payment card data in U.S. stores", communicated herewith as **Exhibit R-11**;

36. Target's December 19, 2013 press release (R-11) only refers to the loss of Class Members' payment information for those Class Members who had shopped in a U.S. store between November 27, 2013 and December 15, 2013. The press release does not mention the 40 million people whose personal information had also been lost (which lost information is not linked to the same November 27 to December 15, 2013 shopping time frame, as mentioned above);

37. Target posted its said release to customers on its corporate website www.corporate.target.com, as opposed to its general consumer website (www.target.com). This decreased the likelihood that Target shoppers would read the notification and was perhaps intended to minimize the adverse effects of the Data Breach on Target sales during the busy holiday shopping period. Furthermore, this did not help Canadian Class Members who obviously would be more likely to consult the www.target.ca website, instead of a US corporate website;

38. The said December 19, 2013 release also mentioned steps that Class Members could take to protect themselves from fraud or identity theft, such as obtaining credit reports, reviewing account statements, initiating fraud alerts and security

freezes, etc. However, the release does not offer to assist Class Members in this regard nor does it undertake to indemnify the Class Members for damages suffered or expenses incurred. In this regard, the notice told customers:

> You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect fraud, be sure to report it immediately to your financial institutions. In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft.

the whole as more fully appears from Exhibit R-11;

39. On December 20, 2013, Target's CEO Gregg Steinhafel released a statement on the Target corporate website, the whole as more fully appears from the "Message from CEO Gregg Steinhafel about Target's payment card issues", communicated herewith as **Exhibit R-12**;

40. The message from Target's CEO (R-12) states and/or admits *inter alia* that:

a) the Data Breach "creates stress and anxiety about the safety of your payment card data at Target";

b) there is no indication that Class Members' PINs had also been compromised (although this statement later turned out to be false, as mentioned below);

c) that Banks or Target would ultimately be responsible for fraudulent charges;

41. Additionally, on December 20, 2013, Target sent a short email to certain U.S. customers and posted a copy of said email together with additional information on its corporate website, copies of which are communicated herewith, *en liasse*, as **Exhibit R-13**. In R-13, Target downplayed the threat to consumers by stating

that "[t]here is no indication that PIN numbers have been compromised on affected bank issued PIN debit cards or Target debit cards" and that the CVV codes that were stolen are not the same as the three-digit security code on the back of consumers' cards;

42. The R-13 e-mail was not sent to Class Members in Canada and Target does not have the email address of all of the Canadian Class Members in any case;

43. Once again, Target was representing to the public that the Data Breach affected only customers of Target's brick-and-mortar U.S. store locations, during November 27, 2013 to December 15, 2013, and not those who shopped at Target's online store or Canadian stores. However, as mentioned, the Data Breach also included the personal information of Canadian Class Members who had not shopped in a U.S. store during that specific time frame;

44. Target also undertook in its email to U.S. customers sent on December 20, 2013 (R-13) to offer "free credit monitoring services for everyone impacted" although its subsequent offer was limited to only one year of monitoring, which is not adequate, and initially only offered to those customers having shopped in a U.S. store;

45. Once again, Target downplayed the data theft, by telling customers that they were offering the identity theft protection package because "your trust is important to us" instead to advising customers of the high risk of fraud and identity theft associated with the stolen data, the whole as more fully appears from the Credit Monitoring FAQ page found on the Target website, communicated herewith as **Exhibit R-14;**

46. Target's initial offer of one year of free credit monitoring to all affected shoppers, namely those who had shopped at U.S. stores between November 27 and December 15, 2013, soon changed. As it appears from the Credit Monitoring

FAQ (R-14), Target expanded the group of customers eligible for free credit monitoring to anyone who has ever who shopped in U.S. stores;

47. The above-mentioned action clearly evidences that Target is still uncertain of exactly what was lost during the Data Breach, who is affected by the loss of information, and the extent of the risks the victims of the breach now face;

48. Furthermore, it is interesting to note from the FAQs (R-14) that in order to sign up for the credit monitoring, following the breach of Target's systems, customers were being asked to enter their name and email address on Target's creditmonitoring.target.com website and to await a further email from Target (within 72 hours), instead of directing customers to third party secured means, such as contacting Equifax or other credit agencies directly;

49. This is particularly interesting since Target, who had just lost its customers' personal information, was asking those same customers to provide it, once again, with their personal information. This requirement likely dissuaded many affected customers from signing up to the credit monitoring through Target's offer;

50. In addition, at the last page of the FAQs (R-14), Target admits and recognizes that some of its emails, and we submit such as the Notification Emails ultimately sent to certain Canadian Class Members, may very well end up (or may have ended up) in the "junk or spam email folder", therefore never being read by the Class Members. It also recognizes the possibility of fraudulent emails being sent to Class Members following the Data Breach, putting the burden and risk onto the Class Members to check the Target.com/databreach website to see if the emails being received are authentic;

51. Moreover, we note that the credit monitoring services offered to U.S. customers, although still inadequate, contained additional protections and insurance coverage as compared to what was to ultimately be offered to Canadian Class Members, *inter alia* offering the U.S. victims identity theft insurance of $1 million,

as opposed to the $25,000 identity theft insurance offered to the Canadian Class Members (not available in all jurisdictions as Target mentions in the Follow-Up Email to the Petitioner (R-5));

52. In any case, although Target ultimately offered free credit monitoring to some customers, and later to all customers, the credit monitoring services do not anything to prevent credit card fraud. Credit monitoring only informs a person of instances of fraudulent opening of new accounts, not fraudulent use of existing credit cards. Target recognizes the limited protection credit monitoring offers and recommends that *"Guests who sign up for free credit monitoring should continue to monitor their accounts and report any unusual or suspicious activity to their bank."*, the whole as more fully appears from the January 10, 2013 "Target to Offer Free Credit Monitoring to all Guests" press release, communicated herewith as **Exhibit R-15**;

53. Accordingly, Class Members must take additional steps to protect their credit;

54. Furthermore, stolen data is typically held for up to one year or more before being used to commit identity theft and once stolen data has been sold or posted on the Internet, fraudulent use of that information may continue for years, the whole as confirmed at paragraph 19 of the Exhibit R-3 Bank Class Action, which quotes from the GAO Report to Congressional Requesters of June 2007;

55. Therefore, the one year credit monitoring offered by Target is wholly inadequate and insufficient because it assumes that after the 12 months period the stolen information is no longer at risk of being abused, thus giving millions of Target guests a false sense of security; Target has passed the burden and expense of additional years of coverage or security measures onto the Class Members, which the Class Members are entitled to claim from Target;

56. On December 27, 2013, Target, changed its initial story and finally disclosed that PIN data was stolen during the breach. Nevertheless, even then, Target once

again downplayed the PIN data theft by only telling customers that "strongly encrypted PIN data was removed from our system during the data breach incident," "your debit card account has not been compromised," and "PINs are safe and secure.", the whole as more fully appears from the "Update to Guests About PINs" dated December 27, 2013, a copy of which is communicated herewith as **Exhibit R-16;**

57. Despite Target's statements, experts believe the stolen PIN data may reasonably be decrypted and fraudulently used and Target recognizes that Class Members may have concerns and in turn choose to change said PINs;

58. On January 10, 2014, nearly two months after the breach, Target again changed its story, this time concerning the nature and extent of POS Data Breach in general. Target stated that in addition to the 40 million compromised credit and debit accounts, 70 million customer names, mailing addresses, phone numbers and email addresses were also stolen in the POS data breach, the whole as more fully appears from the Target release entitled "An Update on our Data Breach and Financial Performance", dated January 10, 2014, a copy of which is communicated herewith as **Exhibit R-17**;

59. As appears from said R-17 release, Target states that "in cases where Target has an email address, we will attempt to contact affected guests". This therefore signifies that Target did not notify all of the Class Members of the loss of their personal and/or financial information. Said Class Members are therefore even more at risk of fraud or identity theft;

60. In said R-17 release, Target's CEO admits that this situation is frustrating for Class Members, that he is sorry that Class Members are having to endure this, and that the Class Members' "expect more from [Target] and deserve better";

61. Investigators believe that the data was obtained via software installed on the POS machines at Target stores that customers used to swipe their credit cards when

paying for merchandise. Through this software, the thieves were able to steal the name, account number, expiration date, and CVV for each card that was swiped (They were then able to also gain access to the personal information of the Class Members which was stored by Target);

62. The type of data stolen – also known as "track data" – allows fraudsters to create counterfeit cards by encoding the information onto any card with a magnetic stripe. Thus, the thieves could take the credit card information and create a fake credit card that could be swiped and used to make purchases as if it were the real credit card. Additionally, the thieves could reproduce stolen debit cards and use them to withdraw cash from ATMs. With the additional personal information that Target disclosed was stolen on January 10, 2014, thieves could seek to change credit card billing addresses and create completely fictional credit accounts in unsuspecting victim's names;

63. Security experts said the timing of the breach corresponds with a recent surge of stolen credentials being offered for sale on underground cybercrime forums;

64. Moreover the fact that the three-digit CVV security codes were stolen shows that Target was storing CVV codes, which has long been banned by the card brands and the PCI standards;

65. Thieves could not have accessed Target's network and stolen consumers' credit card, ATM/debit card and personal information but for Target's inadequate security protections. Target failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information that was compromised;

66. Personal and financial information is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen credit card numbers, Social Security numbers or Social Insurance Numbers, and other personal information

on a number of websites;

67. In fact, certain Class members' account information stolen during the Target Data Breach are likely being divided up and sold off regionally in the underground black markets, at a cost of anywhere between $20 to $100 per card, the whole as more fully appears from Brian Krebs' blog post (who initially reported the data breach) dated December 20, 2013, communicated herewith as **Exhibit R-18**;

68. In addition, the online black markets also provided purchasing thieves with the zip code and location of the Target store where the information was stolen. This allowed thieves to make same-state purchases, thus avoiding any blocks from banks who suspect fraud;

Target's Failure to Promptly and Accurately Notify

69. Target did not promptly disclose the Data Breach and did not notify victims in a reasonable or timely manner. Quite the contrary, Target did not disclose the Data Breach at all until the day after Brian Krebs, a computer security and cybercrime blogger, reported it on his blog on December 18, 2013 (R-10), and the Data Breach became widely reported in the press;

70. As mentioned above, Target, for some reason through its (...) wholly owned subsidiary Target Canada[8], only sent the Notification Emails to certain Canadian Class Members as of January 20, 2014 and as already mentioned, Target has not notified many Class Members;

71. Target's claims imparted a false sense of security to affected consumers. Target also downplayed the risk, urging consumers to merely check their account for any

[8] Petitioner presently has no knowledge of Target Canada's possible implication in relation to the Data Breach (if any). Petitioner therefore reserves his right to amend these proceedings in this regard should new information be discovered *inter alia* in order add in Target's wholly owned subsidiary Target Canada as an additional Respondent/Defendant.

suspicious or unusual activity;

72. Target's failure to promptly and effectively inform customers earlier of the data theft left an untold number vulnerable to attack;

73. Despite advising Target customers who used a Target branded REDcard to contact Target if something appears fraudulent, many customers reported that they were unable to ascertain whether their card was impacted because Target's REDcard website repeatedly timed out and the consumer toll-free number was inundated by complaints, making it impossible to check if any fraudulent charges had been made;

74. Petitioner and likely the other Class Members have already and will continue to experience fear, inconvenience, expenses, and/or loss of time due to the loss of their personal and/or financial information, which has made Petitioner and other Class Members potential targets for fraud and/or identity theft;

75. The Petitioner and the Class Members have suffered certain inconveniences including but not limited to the following:

a) Having to set up the proper credit monitoring and security alerts on their credit files;

b) Delays in the processing of any future requests or applications for credit in the future;

c) The obligation to closely monitor their accounts looking for possible fraud for all periods subsequent to the loss of information;

d) The obligation to be even more attentive than normally necessary concerning the communication of their personal information, due to the higher possibility of fraudulent activity caused by Respondent's loss of the

information;

e) The obligation to inform certain financial institutions or credit card companies of the loss of the information by the Respondent and to deal with said financial institution in order to reduce risk of fraud as much as possible;

f) Obtaining their credit report in order to look for unauthorized transaction or fraud;

76. Petitioner and many Class Members have also paid certain fees or costs in order to further protect themselves, such as in order to activate a more comprehensive and/or complete credit monitoring service (for a longer period than the one year offered by Target), in order to purchase insurance, to post a security alert on their credit file, etc. Respondent is solely responsible and liable for these costs or fees paid by Class Members and for the inconvenience caused to Class Members in this regard;

FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY THE PETITIONER

77. As mentioned above and confirmed in the January 20, 2014 Notification Email (R-4) and the January 24, 2014 Follow-up Email (R-5) that Target sent to Petitioner, Petitioner's information was lost together with the information of the Class Members during the Data Breach in question;

78. Petitioner and the Class Members, in good faith, were reasonably justified in assuming that Target would properly safeguard their personal information, which it clearly did not, as Target admits;

79. Petitioner first heard about the data breach in question from various news outlets but was not sure whether or not he was affected at that time;

80. It was only on or about January 20, 2014, namely approximately two (2) months after the Data Breach had begun, that Petitioner received Target Canada's Notification Email (R-4);

81. On January 23, 2014, after not hearing back from Target, Petitioner contacted Equifax Canada and purchased a credit monitoring package, at a price of $19.95 per month. Petitioner indeed paid $19.95 to Equifax, which he claims from Target;

82. The next day, on January 24, 2014, Petitioner received Target Canada's Follow-Up Email (R-5) with Target's offer and promotional code for the one year credit monitoring service provided by Equifax Canada. Petitioner therefore activated this service online and called Equifax Canada in order to discontinue the credit monitoring package that he had purchased, for the future months going forward;

83. Relying upon Target Canada's representations in its Follow-Up Email, Petitioner assumed that Target had initiated the proper measures by offering the one year credit monitoring service, with Equifax Canada, which would presumably protect him from identity theft and/or fraud going forward, considering the particular facts of this case involving a Data Breach and fraud occurring in and/or passing through the U.S.A., Eastern Europe, Russia, and Brazil (...);

84. However, in early March 2014, Petitioner, still concerned about his credit file and identity theft, conducted a google search to seek more information about the Target Data Breach. Through said research, Petitioner discovered the following:

a) Target's credit monitoring offer will not protect Target's customers from identity theft;

b) Target's credit monitoring offer is wholly inadequate and insufficient because it assumes that after the one (1) year period, the stolen information will no longer be at risk of being abused, which is wrong as

confirmed at paragraph 19 of the Exhibit R-3 Bank Class Action (as mentioned above);

c) Target's credit monitoring offer gives Target's customers a false sense of security into believing that they are protected from identity theft or fraud;

d) That the three (3) major US credit bureaus (Equifax, TransUnion and Experian), collect different information and that Target is only offering a one-bureau credit monitoring package instead of the recommended three (3) bureau credit monitoring;

e) That the Experian coverage offered to the US customers do not monitor day-to-day transactions made by debit and credit cards;

the whole as more fully appears from a copy of the March 5, 2014 news article entitled "Target Data breach: Credit monitoring will not protect you from identity theft", and from the February 6, 2014 Consumer Report Article, communicated herewith as **Exhibit R-19** *en liasse*;

85. Accordingly, on March 9, 2014, Petitioner, concerned about the information he had recently discovered, called Target to seek more information about the breach and to receive a follow up about his particular credit file;

86. Petitioner indicated to the Target agent (who identified himself as "JC", employee A549765) that further to his review of the R-19 online sources, he insisted on receiving more than one year of credit monitoring since the threat of fraud or identity theft will surely persist longer than one year. The Target agent replied that no one at Target would offer more coverage that the one year "complementary" credit monitoring already offered;

87. Petitioner also asked if a security or fraud alert would be posted on his credit file for more than one year, alerting him of any new credit requests or applications.

The Target agent said no to this as well;

88. The Target agent actually attempted to reassure the Petitioner by stating that "a lot of the fraud that has been happening has already happened" which was why Target was apparently only offering the one year credit monitoring and that after that one year period, Petitioner would have the burden to contact his credit card company directly to get any suspicious charges reversed. This did not reassure the Petitioner (and this does not release Target from its obligations and liability toward the Class Members stemming from the Data Breach);

89. Since the credit card that Petitioner used when shopping at the U.S. Target stores was an American issued credit card (namely from the Bank of America) and since the Data Breach occurred in the U.S. (and as mentioned above occurring and/or passing through Eastern Europe, Russia and Brazil as well), with fraud apparently already occurring as confirmed by the Target agent, Petitioner asked why he was only offered the Equifax Canada protection. The Target agent explained to Petitioner that as a Canadian, he was only eligible for that coverage;

90. Indeed, Canadian Class Members would not be able to sign up for monitoring by a U.S. credit agency unless they have a U.S. Social Security Number (which most Canadians do not have, since they have Canadian Social Insurance Numbers);

91. The Target agent recommended that "to make it better", Petitioner should call the Bank of America to cancel his existing U.S. credit card and to request that a new credit card number be issued, so that fraudster in the U.S. would not be able to use that old credit card number going forward. Accordingly, Petitioner called the Bank of America to cancel his credit card and have a new number issued;

92. Petitioner notes that Target has not recommended that other Canadian Class Members also cancel their existing credit or debit cards (which had been used at the U.S. Target stores), leaving these Class Members with their existing card

numbers at continued risk of fraud;

93. Finally, and as mentioned above, Petitioner notes that Target's U.S. clients have been offered $1 million of identity theft insurance coverage whereas Canadian Class Members (including the Petitioner) were only offered coverage for up to $25,000 (with limitations). There is absolutely no reason to offer less insurance coverage to Canadian Class Members and Petitioner submits that Target has admitted that at least $1 million of coverage is warranted in this particular case (but Target has refused to offer the same coverage to Canadian Class Members). Target is liable for the cost of such additional coverage;

94. Further to his telephone conversation with the Target agent, Petitioner called Equifax Canada to have a fraud alert posted on his credit file, for a period of six (6) years, as recommended by Equifax Canada;

95. Target's credit monitoring offer to Canadian customers is clearly inadequate since it does not offer monitoring of U.S. accounts or U.S. issued debit or credit cards. Therefore, a fraudster can easily use the lost credit card information and create a false credit card that could be swiped and used to make purchases in the U.S. without any notification to Equifax Canada or the Class Members. This is obviously a serious consideration in this case since the Class Members' information had been stolen in the U.S.A. (passing through Eastern Europe, Russian, and Brazil, if not other locations as well, as mentioned above) and as mentioned above, there are already reports of the stolen information being sold online and the Target agent admitted to Petitioner that fraud has already occurred;

96. Moreover, any fraudulent activity in the U.S. using the stolen information would not be reported to Equifax Canada, and thus the Class Members would not be alerted of said fraudulent activity (since credit products issued to Canadian in the U.S.A. do not necessarily get posted to the Equifax Canada credit file);

97. Petitioner must now be mindful and consult his statements more attentively and

more frequently, since he is clearly at greater risk for fraud or identity theft;

98. Therefore, as a result of the loss of his information by Target, Petitioner has experienced fear, inconvenience, loss of time and expenses dealing with the issues stemming from the loss of information in question and said inconvenience and loss of time will continue in terms of monitoring his accounts and the delays involved with the security measures posted on his credit file (as detailed above);

99. To his knowledge, Petitioner has not been the victim of fraud and will amend these proceedings or otherwise inform the Court and Target should that change before the authorization hearing, or thereafter during these proceedings;

100. Petitioner would not have shopped at Target, would not have provided Target with his personal information, and would not have used his USD Bank of America credit card at Target retail stores, had he known that Respondent was not properly securing Petitioner's personal and banking information, was retaining his payment information unnecessarily, and was in all probability noncompliant with POS industry standards (as detailed above);

Punitive Damages:

101. For all of the reasons more fully detailed above, which are reiterated as though recited at length in the present section, Petitioner respectfully submits that Respondent was grossly and/or intentionally negligent and is liable to pay punitive damages to the Class Members;

102. In fact, without limiting the generality of the forgoing, Respondent was grossly negligent and/or intentionally negligent when it:

a. did not follow or properly implement the PCI Data Security Standard or any other equally effective industry standard to protect customers' personal and financial information (after being warned of such risks);

b. failed to promptly notify the Class Members, if at all;

c. decided, through and/or in conjunction with its wholly owned subsidiary Target Canada, to only notify the Class Members by way of email or press releases on the Target Corporate site, as opposed to the target.com and target.ca websites, therefore decreasing the likelihood that Canadian Class Members would read the notification. Notification by email was sent to a limited number of Class Members as mentioned above since Target does not have all of the Class Members' email addresses. In fact, many Class Members, whose credit or debit information was lost when they shopped at a U.S. store, have never provided their contact information to Target at all and therefore have not been addressed any specific and direct notification (increasing the possibility and likelihood that many Class Members are not aware of the loss of their personal information);

103. Target could have contacted the credit agencies and placed security or fraud alerts on all of the Class Members' credit files and/or otherwise contacted and protected all Class Members. Instead, Target wants the Class Members, who have been informed of the breach, to get a code and sign up, obviously reducing the likelihood that all Class Members will sign up for the credit monitoring service, and therefore reducing the cost for Target. Target by merely issuing press releases and sending some emails as mentioned in more detail above is clearly trying to limit its own costs, at the expense of the Class Members;

104. Considering the above, Respondent is liable to pay punitive damages to all of the Class Members due to the loss of private information itself, aside from any other compensable damages suffered by the Class Members;

105. Respondent's above detailed actions qualify its fault as intentional which is a

result of wild and foolhardy recklessness in disregard for the rights of the Class Members, with full knowledge of the immediate and natural or at least extremely probable consequences that its action would cause to the Class Members;

106. Respondent's negligence has shown a malicious, oppressive and high-handed conduct that represents a marked departure from ordinary standards of decency. In that event, punitive damages should be awarded to Class Members;

FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY EACH OF THE MEMBERS OF THE GROUP

107. Every member of the Group had his or her personal, debit and/or credit information lost by Respondent as described hereinabove, including names, address, email address, phone number, credit or debit card number, card's expiration date, and CVV;

108. Many if not all of the Class Members, that have been notified, has or will experience fear, confusion, inconvenience, or loss of time due to the loss of information, if they are even informed of it;

109. The notified Class Members have to closely monitor their accounts looking for possible fraud from now on and for all periods subsequent to the loss of information;

110. Class Members will be inconvenienced by any safety measures that may become necessary in order to prevent further fraud exposure, such as signing up for credit monitoring service, posting an alert on their accounts or credit files, changing their personal information or account numbers, transferring money from one account to another, etc.;

111. Furthermore, every Group Member may be required to pay costs or fees in order

to sign up for additional credit monitoring services (for instance for a period greater than the one (1) year offered), to post an alert on their accounts or credit files, to change their personal information, to purchase insurance, or in order to otherwise protect themselves from further fraud exposure;

112. Moreover, as mentioned above, Respondent, through and/or in conjunction with its wholly owned subsidiary Target Canada, chose to send out the Notification Emails to certain Class Members and to notify customers on their corporate website, as opposed to their general consumer websites, although Respondent knew or should have known that by doing so it would decrease the likelihood that Canadian Target shoppers would read the notification. It is therefore possible that many Class Members have not actually been notified of the loss of their information, especially considering the fact that Target does not necessarily have the contact information of all of the Class Members whose credit or debit information was compromised;

113. In this regard, it is safe to assume that there are many Canadian Class Members, who shopped at Target in the U.S.A. with a credit or debit card, but who do not consult websites or have email addresses. Target has not notified these Class Members;

114. In fact, according to a Reuters/Ipsos poll, only "40% of people who shopped at Target during the period of the data breach had not been notified about the incident. Thirty-one percent said they had been notified by Target and 28 percent said they had been notified by their bank or credit card company", the whole as more fully appears from the Yahoo finance article dated (...) January 10, 2014, communicated herewith as **Exhibit R-20**. These figures are clearly lower when dealing with the Canadian Class Members, for reasons detailed above;

115. The credit file of the shoppers that were not notified is therefore even more at risk since said Class Members will not even be looking for possible fraudulent use of

their credit file or information, and will not have the opportunity to take further preventative measures in order to protect their credit file. These Class Members therefore do not even know that they may be entitled to claim damages from Respondent;

116. Every member of the Group can still fall victim to fraud or identity theft, in the future, due to Respondent's negligence in the safekeeping of their credit, debit and personal information;

116.1. In fact, according to experts, one out of four Data Breach notification recipients became a victim of identity fraud, the whole as alleged in the Consumer Plaintiff's Consolidated Class Action Complaint (R-1A – paragraph 219);

CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

117. The composition of the group makes the application of article 59 or 67 C.C.P. impractical for the following reasons;

118. Petitioner is unaware of the specific number of Class Members whose personal and/or financial information was lost as part of the Target Data Breach but it is estimated that at least approximately 700,000 Canadians were directly affected, aside from the other entities or companies who have also suffered damages or expenses as a result of the said Data Breach, the whole as more fully appears from the CBC.ca article dated January 20, 2014, a copy of which is communicated herewith, as **Exhibit R-21**;

119. Class Members are numerous and are scattered across the entire province and country since people from all across Canada travel to the U.S.A. each year and shop at Target;

120. In addition, given the costs and risks inherent in an action before the Courts, many people will hesitate to institute an individual action against Target. Even if the Class Members themselves could afford such individual litigation, the Court system could not as it would be overloaded. Further, individual litigation of the factual and legal issues raised by the conduct of Target would increase delay and expense to all parties and to the Court system;

121. Moreover, a multitude of actions instituted risks having contradictory judgments on questions of fact and law that are similar or related to all Class Members;

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

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

124. The damages sustained by the Class Members flow, in each instance, from a common nucleus of operative facts, namely the Target Data Breach and Target's conduct, negligence and/or fault in relation thereto (and Target's actions thereafter);

125. The recourses of the members raise identical, similar or related questions of fact or law, namely:

a) Was Respondent negligent in the storing and safekeeping of the personal and financial information of the Class Members whose information was ultimately lost and/or stolen between at least November 27, 2013 and December 15, 2013 (hereinafter the "**Target Data Breach**")?

b) Is Respondent liable to pay damages to the Class Members as a result of the Target Data Breach, including actual monetary losses or expenses incurred, loss of time, inconvenience, moral damages, and/or punitive damages caused by the loss of said information, and if so in what amounts?

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

NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

127. The action that Petitioner wishes to institute for the benefit of the Class Members is an action in damages;

128. The conclusions that Petitioner wishes to introduce by way of a motion to institute proceedings are:

> **GRANT** Plaintiff's action against Defendant;
>
> **CONDEMN** Defendant to pay to the Group Members compensatory damages for all monetary losses or expenses caused as a result of Defendant's loss of said Group Member's personal information, and **ORDER** collective recovery of these sums;
>
> **CONDEMN** Defendant to pay to the Group Members compensatory and/or moral damages to every Group Member in the amount to be determined by the Court as a result of Defendant's loss of said member's personal information, and **ORDER** collective recovery of these sums;
>
> **CONDEMN** Defendant to pay an amount in punitive / exemplary damages to every Group Member, in the amount to be determined by the Court, and **ORDER** collective recovery of these sums;
>
> **GRANT** the class action of Plaintiff on behalf of all the Group Members;
>
> **THE WHOLE** with interest and additional indemnity provided for in the Civil Code of Quebec and with full costs and expenses including experts' fees and publication fees to advise members;

129. Petitioner suggests that this class action be exercised before the Superior Court in the District of Montreal for the following reasons:

a) A great number of the Class Members, including Petitioner, reside in the Judicial District of Montreal;

b) Respondent, through Target Canada, carries on retail business in the District of Montreal and has offices in Montreal;

c) The undersigned attorneys representing the Petitioner and the proposed Group, and the attorneys representing the Respondent, practice in the District of Montreal;

130. Petitioner who is requesting to obtain the status of representative, will fairly and adequately protect and represent the interest of the Class Members for the following reasons:

a) His personal information was lost by Target as more fully described hereinabove (as though recited at length);

b) He has already and will continue to suffer inconvenience, stress, loss of time, and out-of-pocket expenses as a result of said loss of information (as detailed above);

c) He contacted Target in order to try to resolve the issue but Target refused to offer additional coverage and security measures, as detailed above;

d) He may in the future fall, victim to fraud and/or identity theft because of Target's loss of his personal information;

e) He understands the nature of the action and has the capacity and interest to fairly and adequately protect and represent the interest of the Class Members;

f) He is available to dedicate the time necessary for the present action before the Courts of Quebec and to collaborate with Class attorneys in this regard and Petitioner is ready and available to manage and direct the present action in the interest of the Class Members that Petitioner wishes to represent;

g) Petitioner is determined to lead the present file until a final resolution of the matter, the whole for the benefit of the Class;

h) His interests are not antagonistic to those of other Class Members;

i) He has given the mandate to the undersigned attorneys to obtain all relevant information to the present action and intends to keep informed of all developments;

j) He, with the assistance of the undersigned attorneys, is ready and available to dedicate the time necessary for this action and to collaborate with other Members of the Group and to keep them informed;

k) has given the mandate to the undersigned attorneys to post the present motion, with a case description, on a designated page of their firm website in order to keep the Class Members informed of the progress of these proceedings and in order to more easily be contacted or consulted by said Class Members going forward, which Class Members will be able to sign up on said firm website. In this regard, Petitioner files herewith, as though recited at length, under seal as **Exhibit R-26**, *en liasse*, the various online submissions received to date from Class Members, some of which briefly describe the damages they suffered, including fraud. Petitioner reserves his right to file additional online submissions received before the authorization hearing;

131. The present motion is well founded in fact and in law;

FOR THESE REASONS, MAY IT PLEASE THE COURT:

GRANT the present motion;

AUTHORIZE the bringing of a class action in the form of a motion to institute proceedings in damages;

ASCRIBE the Petitioner the status of representative of the persons included in the group herein described as:

> All persons in Canada (subsidiarily in Quebec and subject to Article 999 C.C.P.), whose personal and/or financial information was lost by and/or stolen from Respondent as a result of the data breach that occurred between at least November 27, 2013 and December 15, 2013 (hereinafter the "**Data Breach**"), and as a Sub-Group, all other persons, businesses, entities, corporations, financial institutions or banks who suffered damages or incurred expenses as a result of said Data Breach, or any other Group(s) or Sub-Group(s) to be determined by the Court;

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

a) Was Respondent negligent in the storing and safekeeping of the personal and financial information of the Class Members whose information was ultimately lost and/or stolen between at least November 27, 2013 and December 15, 2013 (hereinafter the "**Target Data Breach**")?

b) Is Respondent liable to pay damages to the Class Members as a result of the Target Data Breach, including actual monetary losses or expenses incurred, loss of time, inconvenience, moral damages, and/or punitive damages caused by the loss of said information, and if so in what amounts?

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

> **GRANT** Plaintiff's action against Defendant;
>
> **CONDEMN** Defendant to pay to the Group Members compensatory damages for all monetary losses or expenses caused as a result of Defendant's loss of said Group Member's personal information, and **ORDER** collective recovery of these sums;
>
> **CONDEMN** Defendant to pay to the Group Members compensatory and/or moral damages to every Group Member in the amount to be determined by the Court as a result of Defendant's loss of said

member's personal information, and **ORDER** collective recovery of these sums;

CONDEMN Defendant to pay an amount in punitive / exemplary damages to every Group Member, in the amount to be determined by the Court, and **ORDER** collective recovery of these sums;

GRANT the class action of Plaintiff on behalf of all the Group Members;

THE WHOLE with interest and additional indemnity provided for in the Civil Code of Quebec and with full costs and expenses including experts' fees and publication fees to advise members;

DECLARE that all members of the group that have not requested their exclusion from the group in the prescribed delay to be bound by any judgment to be rendered on the class action to be instituted;

FIX the delay of exclusion at 30 days from the date of the publication of the notice to the members;

ORDER the publication of a notice to the Class Members in accordance with Article 1006 C.C.P., pursuant to a further Order of the Court, and **ORDER** Respondents to pay for said publication costs;

THE WHOLE with costs including the costs related to preparation and publication of the notices to class members.

MONTREAL, (...) November 14, 2014

LEX GROUP INC.

(s) David Assor

Per: David Assor
Attorneys for Petitioner

N°.: **500-06-000675-138**

SUPERIOR COURT
(CLASS ACTION)

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

EVAN ZUCKERMAN

Petitioner

-V.-

TARGET CORPORATION

Respondent

AMENDED MOTION TO AUTHORIZE THE BRINGING OF A CLASS ACTION AND TO ASCRIBE THE STATUS OF REPRESENTATIVE

ORIGINAL

Me David Assor

LEX GROUP

BL 5606

Lex Group Inc.
4101 Sherbrooke St. West
Westmount, (Québec), H3Z 1A7

T: 514.451.5500
F: 514.875.8218