Court File No.: CV-16-562278-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N :

RYAN LAWRENCE AND FLORENCE FAZARI

Plaintiffs

- and -

SYMANTEC CORPORATION

Defendant

Proceeding under the *Class Proceedings Act*, *1992*

STATEMENT OF DEFENCE

1 The defendant, Symantec Corporation (**Symantec**), denies each and every allegation set out in the Amended Statement of Claim (the **Claim**), except as admitted below.

2 During the class period, Symantec sold market-leading antivirus software that provided multi-layered protection from cyber security threats. Symantec's representations were consistent with the quality and nature of Symantec's product offering. Symantec made no false, misleading or deceptive representations about its software.

3 The alleged software defect (the **Alleged Defect**) described in the Claim did not undermine the overall protection that Symantec's products provided to class members. In particular, Symantec is not aware of any consumer's system having been compromised as a result of the Alleged Defect. Class members received full value for their money.

Symantec

4 Symantec is a global cyber security company incorporated under the laws of Delaware and headquartered in Mountain View, California.

5 Among other things, Symantec develops and markets a line of cyber security software for consumer use under the “Norton by Symantec” brand.

6 At various points during the class period, Symantec’s Norton software line included some or all of the following products: Norton Antivirus, Norton Internet Security, Norton 360, Norton One, Norton AntiVirus Basic, Norton Security Standard, Norton Security Deluxe and Norton Security Premium (the **Norton Software**).

7 In or around October 2014, Symantec began streamlining its Norton brand software, and ultimately discontinued Norton AntiVirus, Norton Internet Security, Norton 360 and Norton One.

Symantec has made no misrepresentations

8 The statements identified as alleged misrepresentations in the Claim are true and accurate descriptions of the qualities and capabilities of the Norton Software during the class period. At all times during the class period, Symantec accurately and fairly represented the qualities and capabilities of the Norton Software to class members.

9 As detailed below, at all relevant times, the Norton Software provided active and timely protection of computers and data from malware, viruses, spyware and hackers.

Proactive, layered cyber security protection

10 At all relevant times during the Class Period, the Norton Software provided multi-layered cyber security protection. Multi-layered cyber security protection involves multiple technologies or software features working together to identify, prevent and remediate cyber security threats.

11 Among others features and technologies, the multi-layered cyber security protection provided to customers using the Norton Software during the class period included or used the following, without limitation:

(a) signature-based antivirus protection;

(b) heuristic-based antivirus protection;

(c) behavioural, zero-day threat protection;

(d) personal firewall protection;

(e) password management;

(f) parental control services;

(g) identity theft protection;

(h) data backup and storage services;

(i) email spam filtering;

(j) computer maintenance and tuning;

(k) phishing protection;

(l) network mapping and monitoring;

(m) bot detection;

(n) rootkit detection; and

(o) virus removal.

12 Individually and collectively, the technologies and features listed above provided significant value to class members by protecting them from cyber security threats.

13 While the technologies and features available to class members varied by the type and version of Norton Software (some Norton Software products had more features than others), all types and versions of the Norton Software included signature-based and heuristic-based antivirus protection during the class period.

14 Moreover, operating systems often contain their own protection mechanisms that add to a computer's protection. For example, Address Space Layout Randomization (**ASLR**) is a memory-protection process included in Microsoft Windows that specifically guards against buffer-overflow attacks. The Norton Software operates in concert with operating system-based features like ASLR that provide additional protection.

15 To the extent that any defect, including the Alleged Defect described in the Claim, existed in the way in which any of these features or technologies operated during the class period, which is denied, customers using the Norton Software remained protected by the numerous other layers of cyber security protection provided as part of the Norton Software or that were otherwise incorporated into their computer systems.

Norton Software provides substantial cyber security protection

16 The Norton Software successfully protected class members' systems as designed and advertised during the class period.

17 To Symantec's knowledge, no class member was victimized through any exploitation of the Alleged Defect set out in the Claim, during the class period or otherwise.

18 The Norton Software was effective in preventing many different types of malware (including viruses) and other issues from compromising class members' systems during the class period. For instance, the Norton Software isolated and defended against the following

specific malware, each of which had a significant negative impact on infected computers during the class period:

(a) Waledac botnet (2010): The "Waledac" botnet was a computer "worm" capable of causing infected computers to send approximately 1.5 billion spam messages per day. The Norton Software was programmed to protect against the Waledac botnet on the day Waledac was discovered;

(b) Alureon Trojan (2010): The Alureon Trojan was a virus that stole data by intercepting a system's network traffic and searching for banking usernames, passwords and credit card information. Millions of computers were affected. The Norton Software was programmed to protect against the Alureon Trojan on the day it was discovered;

(c) SpyEye (2010): SpyEye infected more than 50 million computers, causing nearly $1 billion in damage to individuals and financial institutions around the world. The Norton Software was programmed to protect against SpyEye within one day of its discovery;

(d) ZeroAccess botnet (2011): ZeroAccess was estimated to have infected between 1 million and 2.2 million computers. The Norton Software was programmed to protect against ZeroAccess on the day it was discovered;

(e) Dorkbot (2011): Dorkbot is malware that is used to steal online payment information, participate in distributed denial-of-service (**DDoS**) attacks,[1] and deliver other types of malware to victims' computers. Dorkbot infected more than

[1] A Distributed Denial-of-Service attack is one in which a perpetrator attempts to render a computer or network resource unavailable by disrupting services of a host that is connected to the internet, which often takes place through "flooding" the system in an attempt to overload it.

one million computers in over 190 countries. The Norton Software was programmed to protect against Dorkbot on the day it was discovered;

(f) Flame (2012): Deemed to be the most complex malware ever detected at the time, Flame initially infected approximately 1,000 computers used by governmental organizations, educational institutions and private individuals. The Norton Software was programmed to protect against Flame on the day it was discovered;

(g) Shamoon (2012): The Shamoon virus has been used as part of cyber attacks on the national oil companies of Saudi Arabia and Qatar. The Norton Software was programmed to protect against Shamoon on the day it was discovered;

(h) CryptoLocker Trojan (2013): CryptoLocker is ransomware that encrypts victims' files and advises victims that they have three days to pay a ransom to a third party payments system. The operators of CryptoLocker are estimated to have extorted approximately $3 million from victims. The Norton Software was programmed to protect against CryptoLocker on the day it was discovered;

(i) Bashlite (2014): Bashlite is malware that infects Linux systems in order to launch DDoS attacks. By 2016, Bashlite is estimated to have infected more than one million devices. The Norton Software was programmed to protect against Bashlite on the day it was discovered;

(j) Dyre (2014): Dyre is a virus capable of hijacking internet browsers in order to intercept online banking sessions and send the victim's banking credentials to attackers. Dyre was used to steal an estimated $5.5 million USD from Ryanair DAC, an airline, and to steal from a number of other businesses using fraudulent

wire transfers in the amount of $1.5 million each. The Norton Software was programmed to protect against Dyre on the day it was discovered;

(k) Locky (2016): Locky is ransomware capable of encrypting a wide range of file types. It is estimated to have been sent to approximately 500,000 computers on February 16, 2016, and millions more thereafter. The Norton Software was programmed to protect against Locky within one day of its discovery; and

(l) Petya (2016): Said to have been the most destructive cyberattack in history, the damage caused by Petya has been estimated at more than $10 billion. Among other things, Petya was responsible for causing the radiation monitoring system at Chernobyl to go offline. The Norton Software was programmed to protect against Petya within one day of its discovery.

19 Between 2010 and 2016, independent testers scored the Norton Software at or above industry average for systems protection.

Symantec not liable for misrepresentations

20 The "Security Protection Representation", as alleged and defined in paragraph 10 of the Claim, was at all material times an accurate representation of the Norton Software and its capabilities.

21 At no point did Symantec ever represent that the Norton Software was capable of preventing every possible cyber security threat, or that the Norton Software would make a class member's system completely invulnerable to cyber-attack.

22 Further, class members would have reasonably understood that the Security Protection Representation amounted to a promise of perfect cyber security protection. Instead, class

members reasonably expected that Symantec would work diligently to program the Norton Software to address cyber security threats promptly following their discovery by Symantec.

23 Certain features of the Norton Software emphasize the fact that the Norton Software cannot and does not offer perfect cyber security protection:

(a) Norton Power Eraser: Symantec offers a free virus removal tool known as the Norton Power Eraser. This software tool is available for download by the public from Symantec's website and can be used to scan for and erase harmful malware. The Norton Power Eraser is a damage minimization feature, and a layer in the Norton Software's multi-layered security protection. Symantec's provision of the Norton Power Eraser to the public for free made it clear to users of Norton Software that there is always a risk that malware can infect a user's system; and

(b) Virus Protection Promise: In connection with certain Norton Software products, Symantec offers the 'Virus Protection Promise' (**VPP**), which states that, if a user's system is running the Norton Software and is fully updated, Symantec will remove any virus from the user's system and, if it cannot, will provide a full refund to the user. The offer of the VPP makes clear to users of Norton Software that there is always a risk that malware can infect a user's system, even while the Norton Software is operational.

24 The conduct that the plaintiffs allege comprises "Best Practices Representation" in paragraph 10A of the Claim, which includes Symantec urging users to comply with best practices, does not amount to any representation about Symantec's own conduct.

25 Symantec denies that it made the Best Practices Representation during the class period.

26 Further, Symantec denies that “best practices” is a term with any discernable meaning, at law or otherwise. Symantec denies that any class member would have understood the content of “best practices” to mean what the plaintiffs allege, or at all.

27 In the alternative, Symantec was substantially compliant with best practices throughout the class period with respect to the development and supply of the Norton Software and puts the plaintiffs to the strict proof of the contrary.

28 In the further alternative, to the extent that Symantec made either the Security Protection Representation or the Best Practices Representation, such representation was mere puffery and understood by the customer not to be a meaningful representation as to the qualities or characteristics of the Norton Software.

29 Symantec specifically denies the allegations made at paragraph 11 of the Claim that, if made, the Security Protection Representation and the Best Practices Representation were false. In particular, the Norton Software was not a threat vector for users. Nor did it heighten the susceptibility of class members’ computers and data to viruses, malware, spyware, hacking or other cyber security threats. To the contrary:

(a) users of the Norton Software were as well or better protected than users of no security product or other comparable security products during the class period; and

(b) not one class member has ever reported being victimized as a result of the allegations set out in paragraph 11 or the Alleged Defect described at paragraphs 12-17 of the Claim.

Plaintiffs' description of Alleged Defect is inaccurate

30 The alleged characteristics of the Norton Software set out in paragraphs 12-17 of the Claim are not accurately described and do not constitute any defect in the Norton Software.

31 In particular:

(a) the decomposer used in the Norton Software does not run in the kernel, as alleged in paragraph 13(a) of the Claim, or alternatively does not run in the kernel at all times or in all circumstances;

(b) the decomposer did not operate with an unnecessarily high degree of privileges, as alleged in paragraph 13(a) of the Claim;

(c) there were not numerous memory corruption bugs in the open source code used in the Norton Software decomposer, as alleged in paragraph 13(b) of the Claim. Memory corruption bugs did not cause or contribute to the Alleged Defect;

(d) there were not numerous publicly-known vulnerabilities in the source code used in the Norton Software decomposer, as alleged in paragraph 13(b) of the Claim. Further, the vulnerabilities alleged in paragraph 13(b) did not cause or contribute to the Alleged Defect; and

(e) Symantec did not have inadequate vulnerability management in respect of the open source code it was using in the Norton Software during the class period or otherwise, and Symantec did not fail to update the Norton Software by importing necessary security patches that had been released by open source libraries to address vulnerabilities and/or exploits in the Norton Software open source code.

32 Even if the alleged characteristics of the Norton Software set out in paragraphs 12-17 of the Claim have been described accurately, which is denied, those characteristics do not amount to any defect that compromised the protective capacity of the Norton Software. Symantec has no information suggesting that any class member's system was ever compromised as a result of or in connection with the alleged characteristics of the Norton Software set out in paragraphs 12-17 of the Claim.

33 Even if the alleged characteristics of the Norton Software set out in paragraphs 12-17 of the Claim have been described accurately, which is denied, those characteristics do not diminish the value proposition of the Norton Software. The Norton Software provided effective cyber security protection during the class period, with class members protected by a level of security that was comparable to or stronger than that provided by Symantec's competitors. In particular, Symantec denies that:

(a) the Norton Software failed to provide a reasonably expected measure of security and protection;

(b) the Norton Software significantly compromised the security and protection of class members' computers and data; and/or

(c) the Norton Software was essentially without any value or utility.

No breach of implied warranty

34 The Norton Software operates on a sales-as-a-service model: users of Norton Software purchase annual subscriptions that provide them with access to recurring updates to address new threats as Symantec learns of those threats and develops ways to defend against them.

35 The Norton Software is offered to customers by way of license and subscription. The Norton Software is not offered via a contract of sale or an agreement to sell, and Symantec never transfers or agrees to transfer property in the Norton Software to the customer. At no point is the Norton Software ever sold to a customer; rather, the customer merely acquires a right of access for a specified service period.

36 Since the Norton Software is offered on a subscription-based, sales-as-a-service model, it does not constitute "goods" as that term is defined in the *Sale of Goods Act*, R.S.O. 1990, C. S.1 (the ***Sale of Goods Act***). Nor did Symantec enter into a contract of sale of goods with its customers at any point.

37 As a result, Symantec denies that the *Sale of Goods Act* applies to the Norton Software.

38 In the alternative, if the Norton Software may be considered "goods" for purposes of the *Sale of Goods Act*, Symantec has not breached any implied condition of merchantability in the sale of the Norton Software. The Norton Software was of merchantable quality at all times during the class period.

39 Symantec denies that s. 9(2) of the *Consumer Protection Act, 2002*, S.O. 2002, c. 30, Sched. A (the ***Consumer Protection Act***) applies to the facts at issue in this action.

40 To the extent that the supply of the Norton Software constitutes the sale of services as defined in the *Consumer Protection Act*, the services provided via the Norton Software were of reasonably acceptable quality during the class period.

Express misrepresentation claims precluded by user License Agreement

41 Before any class member could use the Norton Software, he or she was required to accept terms and conditions set out in a license agreement (the **License Agreement**). Among

other things, those terms and conditions required the class member to acknowledge that the Norton Software would not necessarily meet their requirements or be error-free. For example, terms substantially similar to the following were contained in every License Agreement entered into during the class period:

> Symantec does not warrant that the Software and Services will meet Your requirements or that operation of the Software and Services will be uninterrupted or that the Software and Services will be error-free. For the avoidance of doubt, references to "Software and Services" in the foregoing sentence shall include, but not be limited to, the Online Backup Feature and Technical Support.
>
> TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIAL LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

42 The License Agreement also contained an "entire agreement" clause that limits Symantec's representations to those in the License Agreement. Terms substantially similar to the following were contained in every License Agreement entered into during the class period:

> This License Agreement is the entire agreement between You and Symantec relating to the Software and Services and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgement, or similar communications between the parties. Notwithstanding the foregoing, nothing in this License Agreement will diminish any rights You may have under existing consumer protection legislation or other applicable laws in Your jurisdiction that may not be waived by contract. Symantec may terminate this License Agreement if You breach any term contained in this License Agreement (other than a trivial or inconsequential breach) and, if such termination occurs, You must cease use of and destroy all copies of the Software and Services and Documentation. The disclaimers of warranties and damages and limitations on liability shall survive and continue to apply after termination.

43 The entire agreement clause contained in each class member's License Agreement precludes the plaintiffs from pursuing their claims for misrepresentations outside of the express representations made in the License Agreement, whether at common law or pursuant to the *Consumer Protection Act*.

No actionable misrepresentations were made to customers whose License Agreements were automatically renewed

44 Symantec offers an automatic-renewal program for Norton Software subscriptions, whereby existing License Agreements are automatically renewed and extended.

45 The alleged misrepresentations were not made to Norton Software users who entered into License Agreements with Symantec prior to the class period and continued using the Norton Software during the class period as a result of automatic renewals (the **Auto-Renewal Users**).

46 Symantec expressly denies that any of the Auto-Renewal Users have any actionable claim for rescission or damages against Symantec under the *Consumer Protection Act*.

No unfair practices

47 Symantec has not engaged in any unfair practices. Symantec did not make any false, misleading or deceptive representation to class members during the class period.

48 Symantec repeats and relies on the terms of the License Agreement agreed by every class member in advance of having access to the Norton Software, including the exclusion of extra-contractual warranties and representations in s. 7 and the entire agreement clause contained in s. 12, which preclude class members from relying on any alleged extra-contractual representations made by Symantec. Class members expressly waived all representations

about the Norton Software other than those contained in the License Agreement, which waiver eliminates any claim in regard to unfair practices.

49 In the alternative, Symantec denies that it has engaged in any unfair practices or has engaged in any of the conduct set out in s. 14(2) of the *Consumer Protection Act*. At all times, Symantec's representations regarding the Norton Software contained true and accurate descriptions of the characteristics, benefits and qualities of the Norton Software.

No damages suffered

50 No class member has suffered damage as a result of any of the conduct described in the Claim, which is denied, and Symantec puts the plaintiffs and class members to the strict proof of any damages claim.

51 Customers who purchased licenses for the Norton Software acquired access to quality cyber security protection that did, in fact, protect their computers from a multitude of cyber security threats during the class period. Class members are not entitled to any reduction in the purchase price paid for the Norton Software.

52 Even if the plaintiffs and class members can prove that they are entitled to an award of damages, the requirements of s. 24 of the *Class Proceedings Act*, S.O. 1992, Chapter 6, are not met. The extent to which the Alleged Defect, if proven, affected the value proposition for class members in acquiring the Norton Software is predicated on the specific details of how each class member used his or her computer system (including the frequency of updates, the extent of participation in potentially dangerous online activity, and the number of real cyber security threats actually stopped by the Norton Software).

53 As Symantec has not engaged in any unfair practices, rescission is not an available remedy pursuant to the *Consumer Protection Act*.

54 The conduct described in the Claim, which is denied, does not provide a basis for an award of aggravated, exemplary or punitive damages.

Class members have not given notice under the *Consumer Protection Act*

55 No class member has provided notice in accordance with s. 18 of the *Consumer Protection Act*. It is not in the interests of justice to waive the consumer notice requirement.

Limitations

56 The claims advanced in this action are statute-barred, in whole or in part, because these claims were brought outside the prescribed statutory limitations period set out in the *Limitations Act, 2002*, SO 2002, c. 24, Schedule B.

57 Symantec requests that this Claim be dismissed with costs ordered to be payable to Symantec on a substantial indemnity basis.

March 5, 2019

Norton Rose Fulbright Canada LLP
Royal Bank Plaza, South Tower, Suite 3800
200 Bay Street, P.O. Box 84
Toronto, Ontario M5J 2Z4 CANADA

Linda Fuerst LSO #: 22718U
Tel: 416.216.2951
Email: linda.fuerst@nortonrosefulbright.com

Andrew McCoomb LSO #: 61618B
Tel: 416.216.4039
Email: andrew.mccoomb@nortonrosefulbright.com

Ted Brook LSO #: 68672U
Tel: 416.203.4457
Email: ted.brook@nortonrosefulbright.com

Fax: 416.216.3930

Lawyers for the Defendant

TO: Investigation Counsel P.C.
Barristers & Investigation Consultants
350 Bay Street, Suite 300
Toronto, ON M5H 2S6

John Archibald LSO#: 48221L
Tel: 416.637.3152
Fax: 416.637.3445
Email: jarchibald@investigationcounsel.com

Lawyers for the Plaintiffs

RYAN LAWRENCE et al.
Plaintiffs

and

SYMANTEC CORPORATION
Defendant

Court File No.: CV-16-562278-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

Proceeding commenced at TORONTO

Proceeding under the *Class Proceedings Act*, *1992*

STATEMENT OF DEFENCE

Norton Rose Fulbright Canada LLP
Royal Bank Plaza, South Tower, Suite 3800
200 Bay Street, P.O. Box 84
Toronto, Ontario M5J 2Z4 CANADA

Linda Fuerst LSO #: 22718U
Tel: 416.216.2951
Email: linda.fuerst@nortonrosefulbright.com

Andrew McCoomb LSO #: 61618B
Tel: 416.216.4039
Email: andrew.mccoomb@nortonrosefulbright.com

Ted Brook LSO #: 68672U
Tel: 416.203.4457
Email: ted.brook@nortonrosefulbright.com

Fax: 416.216.3930

Lawyers for the Defendant