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

ONTARIO
SUPERIOR COURT OF JUSTICE

BETWEEN:

RYAN LAWRENCE AND FLORENCE FAZARI

Plaintiffs

—and—

SYMANTEC CORPORATION

Defendant

Proceeding under the *Class Proceedings Act, 1992*

AMENDED STATEMENT OF CLAIM

TO THE DEFENDANT:

A LEGAL PROCEEDING HAS BEEN COMMENCED AGAINST YOU by the plaintiffs. The claim made against you is set out in this statement of claim.

IF YOU WISH TO DEFEND THIS PROCEEDING, you or an Ontario lawyer acting for you must prepare a statement of defence in Form 18A prescribed by the Rules of Civil Procedure, serve it on the plaintiffs' lawyer and file it, with proof of service, in this court office, WITHIN TWENTY DAYS after this statement of claim is served on you, if you are served in Ontario.

If you are served in another province or territory of Canada or in the United States of America, the period for serving and filing your statement of defence is forty days. If you are served outside Canada and the United States of America, the period is sixty days.

Instead of serving and filing a statement of defence, you may serve and file a notice of intent to defend in Form 18B prescribed by the Rules of Civil Procedure. This will entitle you to ten more days within which to serve and file your statement of defence.

IF YOU FAIL TO DEFEND THIS PROCEEDING, JUDGMENT MAY BE GIVEN AGAINST YOU IN YOUR ABSENCE AND WITHOUT FURTHER NOTICE TO YOU. IF YOU WISH TO DEFEND THIS PROCEEDING BUT ARE UNABLE TO PAY LEGAL FEES, LEGAL AID MAY BE AVAILABLE TO YOU BY CONTACTING A LOCAL LEGAL AID OFFICE.

IF YOU PAY THE PLAINTIFFS' CLAIM, and $5,000.00 for costs, within the time for serving and filing your statement of defence, you may move to have this proceeding dismissed by the court. If you believe the amount claimed for costs is excessive, you may pay the plaintiffs' claim and $400.00 for costs and have the costs assessed by the court.

Date:

Issued by _____

Local registrar

Address court office: 393 University Avenue
10th Floor
Toronto ON M5G 1E6

TO: **SYMANTEC CORPORATION**
350 Ellis Street
Mountain View CA 94043
USA

CLAIM

1. The plaintiffs, Ryan Lawrence and Florence Fazari (the "Plaintiffs"), claim on their own behalf and on behalf of all Class Members (as defined below):

(a) an order pursuant to the *Class Proceedings Act 1992*, S.O. 1992, c. 6 (the "*CPA*") certifying this action as a class proceeding and appointing them as the representative plaintiffs;

(b) damages of $10,000,000 or in such amount as the Court may find appropriate for breach of the *Consumer Protection Act 2002*, S.O. 2002, c.30, Sch. A (the "*Consumer Protection Act*");

(c) punitive damages in such amount as the Court may find appropriate;

(d) an order directing a reference or giving such other directions as may be necessary to determine issues not determined at the trial of the common issues;

(e) pre-judgment interest compounded and post-judgment interest pursuant to the *Courts of Justice Act*, R.S.O. 1990, c. C.43 (the "*CJA*"), as amended;

(f) costs of this action and, pursuant to section 26(9) of the *CPA*, the costs of notice and administering the plan of distribution of the recovery in this action plus applicable taxes; and

(g) such further and other relief as to this Honourable Court may seem just.

THE PARTIES

2. The plaintiff Ryan Lawrence resides in Borden, Ontario. In October 2011, he purchased a one-year license for Norton 360™, one of the Norton Products (defined below) manufactured and supplied by the defendant through its website norton.com. He subsequently purchased a license renewal for Norton 360 in each of the years 2012, 2013, 2014, and 2015 through norton.com. Mr. Lawrence was located in Ontario when he made each of these purchases.

3. The plaintiff Florence Fazari resides in Innisfil, Ontario. In August 2015, she purchased a one-year license renewal for Norton 360™ through norton.com. At the time of her purchase, she was located in Ontario.

4. The defendant Symantec Corporation ("Symantec") is a corporation organized pursuant to the laws of the State of Delaware in the United States. Its head office is situated in Mountain View, California. It carries on business in Ontario via its wholly owned, controlled, and operated websites symantec.com and norton.com.

PARTICULARS OF THE CLASS

5. The Plaintiffs bring this action pursuant to the *CPA* on their own behalf and on behalf of all other residents of Ontario who, between July 24, 2010 and June 27, 2016 (the "Class Period"), purchased or licensed one or more of the Norton Products (defined below) via symantec.com or norton.com (the "Class" or "Class Members").

THE DEFECTIVE NORTON PRODUCTS

6. Symantec is among the world's largest security technology companies, having a market capitalization of USD$15 billion. It has described itself in United States securities filings as:

> a global provider of security, storage and systems management solutions that help businesses and consumers secure and manage their information…[and] provid[ing] customers with software and services that protect, manage and control information risks related to security, data protection, storage, compliance, and systems management.

7. Symantec sells and/or licenses its security software products and services to individuals and companies in Ontario and elsewhere through its wholly owned, controlled, and operated websites

symantec.com and norton.com. Throughout the Class Period, these websites were registered in the name of Symantec Corporation.

8. Symantec's Norton™ brand consists of security software products and services that Symantec targets and supplies to consumers. These products and services make up Symantec's Consumer Security segment from which Symantec earned revenue of approximately USD$1.7 billion in 2016. It earned billions of dollars in revenue from the sale or licensing of its Norton software products during the Class Period.

9. During the Class Period, Symantec sold and/or licensed to consumers, including the Plaintiffs and other Class Members, the following Norton software products for Windows and Mac operating systems (hereinafter, the "Norton Products"):

- Norton™ AntiVirus
- Norton™ Internet Security
- Norton™ Security
- Norton™ Security with Backup
- Norton 360™
- Norton™ One

The Norton Products shared certain common design defects which are described further below at paragraphs 12 to 17 of this Statement of Claim.

SYMANTEC'S REPRESENTATIONS TO ONTARIO CONSUMERS

10. **The Security Protection Representation.** Throughout the Class Period, Symantec made representations about the Norton Products on its norton.com and symantec.com websites through which the Plaintiffs and other Class Members purchased and/or licensed the Norton Products. The

object, effect, and common import of those representations was to create the impression, and lead Ontario consumers including the Plaintiffs and other Class Members to reasonably expect, that the Norton Products provided secure access to computers and active, up-to-date and timely protection of computers and data from malware, viruses, spyware, and hackers (collectively, the "Security Protection Representation"). A collection of exemplar webpages from these two websites containing the Security Protection Representation is attached at **Schedule A** to this Statement of Claim. The following are just a few examples of the Security Protection Representation:

- **Key Benefits**

  Stops viruses, spyware, bots and more—Proactive protection automatically removes threats and stops new attacks before they can do damage.

  . . .

  Intelligent Threat Protection

  NEW! Analyzes downloads, files and applications and tells you if they can be trusted before you install and use them.

  IMPROVED! Norton Protection System uses multiple layers of security that work together to proactively block attacks and detect and remove threats traditional virus scanning alone can't stop.

  IMPROVED! Vulnerability Protection guards security holes in your operating system, applications, browsers and browser plug-ins.

  . . .

  Automatically scan emails and IMs for threats. Finds and eliminates bots to prevent hackers from taking over your PC

  . . .

  Additional Features

  Automatically downloads protection updates and new product features as they become available during your service period.

(Norton AntiVirus 2010)

- Advanced protection to surf, bank and shop online without interruption.

Delivers superior protection and performance

Powerful online identity theft protection

Stops viruses, spyware and spam

. . .

Benefits

Stop viruses, spyware, and online identity theft

• Offers advanced protection from online threats.

• Four different layers of smart protection proactively detect and eliminate threats before they reach your computer.

• Identifies and stops new threats fast.

. . .

Features

• Norton Protection System - provides four unique layers of powerful protection to proactively stop online threats before they can infect your computer.

• Insight - checks where files came from and how long they've been around to stop new online threats before they can cause you trouble.

. . .

Vulnerability protection - stops cybercriminals from using security holes (vulnerabilities) in applications to sneak threats onto your PC.

. . .

Norton Pulse Updates - updates your protection every 5 to 15 minutes—without disrupting you—for up-to-the minute protection against the latest threats.

(Norton Internet Security 2012)

- Keeps you safe when you surf, shop and bank online

  . . .

  Stops both today's and tomorrow's threats

  . . .

  Blocks infected and dangerous downloads

  . . .

  Actively protects you from viruses, spam, identity theft and social media dangers

  . . .

  Automatic, silent updates keep you one step ahead of new threats and those not yet invented

  Automatic product downloads and installations when you're not using your computer ensure your protection is always up to date.

  (Norton 360 2014)

- Benefits for you

  Rock-solid Norton protection for all the devices you use

  . . .

  Guaranteed protection

  . . .

  Stay safe with specialized security.

  Our protection helps keep your devices safe. Your PC and Mac are protected from viruses, online threats, identity theft and financial scams, while your smartphone and tablet are safe from loss and privacy concerns like unwanted access to your messages, contacts and photos.

  (Norton Security 2015)

- Benefits for you

  Provides real-time protection against existing and emerging viruses and malware.

Delivers comprehensive protection you can't get from free antivirus software or your computer's operating system.

Protects better and faster than the competition.

(Norton Security 2016)

- We see more, analyze more and stop more online threats.

  How long does it take for malware to infect your brand-new computer? If you use free or other inferior security software, maybe not long at all.

  Cybercriminals are more sophisticated than ever before, and they use a diverse arsenal of tools to gain access to your information. Other security products just don't have the resources to keep up with new threats as they emerge.

  But Norton products do. As the threats get worse, our products just keep getting better. Our teams of security experts are constantly analyzing new threats and devising new ways to protect your devices from them.

10A. **The Best Practices Representation.** During the Class Period, Symantec also published on its websites hundreds of Security Responses and numerous Security Advisories, Intelligence Reports, Internet Security Threat Reports, and other content, all of which remains publicly available on its websites, in which Symantec encourages users of its products to follow and "strongly recommend[s]" certain "basic security best practices" including, among others, running applications under the principle of least privilege to limit the impact of a potential exploit, having a multi-layered approach to security, and promptly updating applications with the current vendor patches (collectively the "Best Practices"). Symantec's strong recommendation to follow the Best Practices, in conjunction with its representations of being a leading cyber security company, amounted by necessary implication to a representation that Symantec itself was Best Practices-complaint and

followed Best Practices when developing and supplying the Norton Products to consumers (the "Best Practices Representation").

11. Throughout the Class Period, the Security Protection Representation and the Best Practices Representation ~~was~~ were false and misleading at the time Symantec made ~~it~~ them. The Norton Products had long-standing, serious design defects in a key component of those products known as the "decomposer engine" or "decomposer". As a result of those serious defects, the Norton Products did not offer the effective, timely and up-to-date virus, security, and malware protections represented by Symantec. To the contrary, throughout the Class Period, the defects in fact made the Norton Products a threat vector[1] for a wide variety of attack types and, as a result, Class Members' computers and data were significantly more susceptible to viruses, malware, spyware, hacking, and other cybersecurity threats than they would have otherwise been had Class Members not purchased the Norton Products. Symantec ought to have known about these serious defects in the Norton Products. The defects resulted from Symantec's failure to follow the Best Practices.

THE COMMON DEFECTS IN THE NORTON PRODUCTS

12. Each of the Norton Products contained design defects in a critical component of the antivirus software, the decomposer. The decomposer carries out the unpacking and parsing of compressed executable files in formats including RAR, ZIP, and CAB, among others. Malware[2] ~~in the form of executables~~ is commonly compressed or "packed" using freely available compressors or

[1] A threat vector, also known as an attack vector, is a path or means by which a hacker can gain access to a computer or network server in order to deliver malicious code. Attack vectors enable hackers to exploit system vulnerabilities.
[2] Malware refers to malicious software that is intended to perform actions the computer's owner considers harmful. This may include stealing sensitive information, deleting files, ~~damage~~ or disableing the computer's ~~and computer~~ systems.

packers.[3] The decomposer is needed to decompress or unpack these compressed executable files so that they can then be scanned for malicious code by the Norton Products' antivirus engine.

13. The Norton Products' decomposer was defective in two key respects:

(a) First, it unpacked and parsed the (untrusted) compressed executable files using an unnecessarily high degree of privileges, in violation of the Best Practices. This includes "NT AUTHORITY\SYSTEM" in Windows and "root" in (Mac OS X and Linux), privileged administrator accounts which have the permissions to perform effectively any action on a computer. Furthermore, on Windows, the decomposer would even run in ~~in the privileged central core of a computer's operating system ("OS"), known as~~ the "kernel" (in Windows OS) where there is no protection from malicious code. ~~and "root" (in Mac OS and Linux OS)~~. Symantec failed to ensure that the Norton Products had a "sandbox", which is a ~~secure~~ less privileged, isolated environment where the decomposer could unpack the (untrusted) compressed file without ~~interfering with~~ a bug in the decomposer granting an attacker access to the most privileged and sensitive part of the host computing system. Unpacking untrusted files in the most privileged part of the OS was a serious defect because it made the Norton Products a threat vector for a wide variety of attack types. It was unnecessary for the decomposer to run at the highest privilege levels. To the contrary, the act of decomposing a file does not require any operating system privileges at all and can and should take place in an insulated environment to limit the impact of a potential threat. After news of the defects was widely reported, Symantec re-designed its Norton Products to include a sandbox.

(b) Rather than developing its own dedicated decomposer with its own unique source code[4], Symantec relied on third-party "open source" code, including open source libraries libmspack and unrarsrc, in designing the decomposer

---

[3] Compression is a reduction in the number of bits needed to represent data. Compressing data can save storage capacity, speed file transfer, and decrease costs for storage hardware and network bandwidth. The main disadvantage of compression is the performance impact resulting from the use of the computer's central processing unit and memory resources to compress and decompress the data.

[4] Source code is software code written by programmers in a high-level language – such as Java, C/C++ or Perl – readable by people, but not by computers. Source code, often referred to as the "source" of a software program, contains variable declarations, instructions, functions, loops and other statements that tell the software program how to function. Source code must be converted to object code or machine language by a compiler before a computer can read or execute a software program.

which was common to the Norton Products.[5] There were numerous memory corruption bugs[6] and publicly known vulnerabilities[7] in the open source code that Symantec ~~used to~~ included in the design the Norton Products' decomposer. There were also publicly available exploits of many of those vulnerabilities. During the Class Period, Symantec had no or inadequate vulnerability management in respect of the open source code it was using in its Norton Products. That is, in violation of Best Practices, Symantec failed to update its Norton Products by importing the security patches[8] that the third-party open source libraries had released in order to address vulnerabilities and exploits in their open source code. Because of the open source code used ~~to design~~ in Symantec's ~~the~~ decomposer engine, the Norton Products were exploitable by hackers until such time as the latest security patches were installed, which did not occur during the Class Period.

13A. These serious defects resulted from Symantec's failure to follow certain basic security best practices, namely:

(a) Applying the principle of least privilege whereby any user, program, or process should have only the bare minimum privileges necessary to perform its function; and

(b) Having a multi-layered approach to security; and

(c) Promptly updating all operating systems and applications with the latest vendor patches.

14. These serious defects in the Norton Products' decomposer provided hackers the ability to corrupt computing memory, decrypt data, and otherwise completely compromise Class Members' computers and data (irrespective of where those computer and data were

[5] Open-source software is computer software with its source code made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose.

[6] A software bug is an error, flaw, failure or fault in a computer program or system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways. Memory corruption occurs when the contents of a memory location are modified due to programming errors which enable attackers to execute an arbitrary code.

[7] In computer security, a vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

[8] A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs.

geographically located in relation to the hackers) simply by sending them malicious and self-replicating code through unopened emails or un-clicked links, a process known as "remote code execution." The defects could be used to create computer worms[9] without any action on the part of the computer's user being required. They could also be used by attackers to install their own "backdoor" on a targeted system, allowing them to remotely come and go as they please in respect of their access to that system. Malware installed on a computing system for this purpose is known as a remote access Trojan, or a RAT, and can be used to install other malware on that system or to exfiltrate[10] that system's data.

15. The defects in the Norton Products were so serious that a cybersecurity expert with Google, who had reported certain severe vulnerabilities relating to those defects to Symantec in or around April 2016, said the following in a widely-reported June 28, 2016 blog post:

> These vulnerabilities are as bad as it gets. They don't require any user interaction, they affect the default configuration, and the software runs at the highest privilege levels possible. In certain cases on Windows, vulnerable code is even loaded into the kernel, resulting in remote kernel memory corruption.
> ...
> Because no interaction is necessary to exploit it, this is a wormable vulnerability with potentially devastating consequences to Norton and Symantec customers.

16. The Plaintiffs and the other Class Members have sustained ascertainable losses and damages in connection with their purchase of the Norton Products in that they did not receive

---

[9] A computer worm is a self-replicating computer program that ~~penetrates an operating system with the intent of spreading malicious code~~ spreads itself without action on behalf of the computer's user. Worms utilize networks to send copies of the original code to other computers, causing harm by consuming bandwidth or possibly deleting files or sending documents via email. Worms can also install backdoors on computers. Worms are often confused with computer viruses; the difference lies in how they spread. Computer worms self-replicate and spread across networks, exploiting vulnerabilities, automatically; that is, they do not need actions by a user or a hacker's guidance, nor do they need to latch onto another computer program.

[10] Data exfiltration, also called data extrusion, is the unauthorized transfer of data from a computer. Such a transfer may be manual and carried out by someone with physical access to a computer or it may ~~be automated and carried out through malicious programming~~ involve transmitting information over a network. Data may be exfiltrated through manual action by an attacker, or may be performed automatically by malicious software.

what they paid for: uncompromised software which provides security and reasonably and adequately protects their computers and data from viruses, malware, spyware, and hacking. The Plaintiffs plead, on their own behalf and on behalf of the other Class Members, that had they known that the Norton Products contained the defects described above, and that using the Norton Products in fact placed their computers and data at significantly increased risk of attack from viruses, malware, spyware, and hacking, they never would have purchased the Norton Products.

17. Because the Norton Products did not provide a reasonably expected measure of security and protection and even significantly compromised the security and protection of Class Members' computers and data, the Norton Products were essentially without any value or utility.

SYMANTEC'S BREACH OF IMPLIED CONDITIONS AND WARRANTIES

18. Symantec breached the implied conditions and warranties which applied to its supply of the Norton Products by virtue of the section 9(2) of the *Consumer Protection Act.*

19. The implied conditions and warranties as to quality and fitness are contained in section 15 of the *Sale of Goods Act*, R.S.O. 1990, c. S.1 (the "*Sale of Goods Act*").

20. As a result of the defects described above, the Norton Products were not reasonably fit for their intended purpose of providing active, up-to-date and timely security and protection to Class Members' computers and data. The Norton Products were also not of merchantable quality because their defects made them a threat vector and placed the Class Members'

computers and data at significantly greater risk of being compromised by cybersecurity threats than had the Class Members not used the Norton Products.

SYMANTEC'S UNFAIR PRACTICES

21. The Plaintiffs and other Class Members entered into contracts in the form of license agreements with Symantec for the supply of the Norton Products. These contracts, and Class Members' purchases and/or licensing of the Norton Products via Symantec's websites norton.com and symantec.com, comprised consumer transactions within the meaning of Section 2(1) of the *Consumer Protection Act*.

22. It is an unfair practice within the meaning of the *Consumer Protection Act* to make a "false, misleading or deceptive representation" or to make an "unconscionable representation".

23. The Security Protection Representation and the Best Practices Representation, and any and all actions or omissions of Symantec which had the effect of confirming the Security Protection Representation and the Best Practices Representation, ~~was a~~ were false, misleading and deceptive representations because:

(a) ~~it~~ they represented to the Plaintiffs and other Class Members that the Norton Products offered by Symantec had sponsorship, approval, performance characteristics, benefits and qualities they did not have;

(b) ~~it~~ they represented to the Plaintiffs and other Class Members that the Norton Products were of a particular standard, quality or grade, when they were not; ~~and~~

(c) ~~it~~ they used exaggeration, innuendo and ambiguity as to a material fact and/or failed to state a material fact in respect of the Norton Products where such use or failure deceived or tended to deceive~~.~~; and

(d) (in respect of the Best Practices Representation only), it represented to the Plaintiffs and other Class Members that that Symantec had a status – namely a Best Practices-compliant cyber security company – that it did not have.

24. The Security Protection Representation and the Best Practices Representation ~~was an~~ were unconscionable representations because Symantec knew or ought to have known that:

(a) the Plaintiffs and other Class Members would repose their trust and confidence in Symantec, as a global leader in cybersecurity, whose objects include protecting customers' computers and data from cybersecurity threats such as viruses, malware, spyware, and hacking;

(b) the Plaintiffs and other Class Members were unable to receive a substantial benefit from the Norton Products (the subject-matter of the Security Protection Representation) and in fact by using the Norton Products they placed their computers and data at significantly increased risk of attack from cybersecurity threats than otherwise would have been the case had they not purchased the Norton Products; and

(c) (in respect of the Security Protection Representation only), it contained a statement of opinion that is misleading and the Plaintiffs and other Class Members were likely to rely on it to their detriment.

25. The Plaintiffs plead and rely on subsections 14(1), 14(2) 1, 2, 3 and 14, 15(1), 15(2)(a), (c), and (g) of the *Consumer Protection Act*.

26. Symantec breached the *Consumer Protection Act* by making the Security Protection Representation and the Best Practices Representation, and by supplying the Norton Products which did not meet the implied conditions and warranties as to quality and fitness. The Plaintiffs seek to recover the amounts by which Class Members' payments to Symantec for the Norton Products exceeded the value, if any, of those products to the Class Members and damages for Symantec having engaged in unfair practices pursuant to subsections 18(1) and (2) of the *Consumer Protection Act*.

NOTICE UNDER THE *CONSUMER PROTECTION ACT*

27. The Plaintiffs plead that it is in the interests of justice not to require that notice be made under the *Consumer Protection Act*, or alternatively that the within statement of claim be regarded as notice to the defendant for the purpose of the *Consumer Protection Act*.

DAMAGES

28. The Plaintiffs and other Class Members have suffered losses and damages arising from the above-described breaches of the *Consumer Protection Act*, including their total cost to purchase or licence the Norton Products, and are entitled to damages in lieu of rescission of their agreements for the purchase or licensing of the Norton Products during the Class Period.

29. The Plaintiffs plead that this Court should order damages to be paid to the Class on an aggregate basis or otherwise in accordance with sections 23, 24, and 25 of the *CPA*.

30. Symantec's conduct as particularized above was reckless, wanton, entirely without care and in complete disregard for the rights of consumers, including the Plaintiffs and other Class Members, thereby justifying an award of punitive damages in such an amount as will serve to deter Symantec from similar conduct in the future.

LEGISLATION

31. The Plaintiffs plead and rely on the *Consumer Protection Act*, the *Sale of Goods Act*, the *CPA*, and the *CJA*.

SERVICE

32. The originating process herein may be served outside Ontario, without court order, pursuant to Rule 17.02 of the *Rules of Civil Procedure*. Specifically, the claim is:

(a) in respect of personal property situated in Ontario (Rule 17.02(a));

(b) in respect of a tort committed in Ontario (Rule 17.02(g));

(c) authorized by statute to be made against a person outside Ontario by a proceeding commenced in Ontario (Rule 17.02(n)); and

(d) against a person carrying on business in Ontario (Rule 17. 02(p)).

PLACE OF TRIAL

33. The Plaintiffs propose that the trial of this action be in the City of Toronto, in the Province of Ontario, as a proceeding under the *CPA*.

October 12, 2016

INVESTIGATION COUNSEL P.C.
Barristers and Investigation Consultants
350 Bay Street, Suite 300
Toronto ON M5H 2S6

John Archibald (LSUC #48221L)
Tel: (416) 637-3144
Fax: (416) 637-3445
jarchibald@investigationcounsel.com

Lawyers for the Plaintiffs