**CANADA**
**PROVINCE OF QUEBEC**
**DISTRICT OF MONTREAL**

S U P E R I O R C O U R T
(Class Action)

No.: 500-06-000894-176

**MICHEL CARRIÈRE**

Plaintiff

v.

**SYMANTEC CORPORATION**

Defendant

# DEFENCE

**IN DEFENCE TO THE PLAINTIFF MICHEL CARRIÈRE'S ORIGINATING APPLICATION (APPLICATION) OF A CLASS ACTION LAWSUIT, THE DEFENDANT, SYMANTEC CORPORATION RESPECTFULLY SUBMITS THE FOLLOWING:**

1. With regard to paragraph 1 of the Application, it admits that it licensed the use of the listed products to users, and denies that it ever sold the products to users.

2. It denies the allegations contained in paragraphs 2, 3 and 4 of the Application.

3. With regard to paragraphs 5 and 6 of the Application, it refers to the Authorization Judgment rendered on April 16, 2019 by the Honourable François P. Duprat, but denies that the present class action is well-founded whether in fact or in law.

4. It denies the allegations contained in paragraph 7 of the Application, specifying that Symantec is known as NortonLifeLock Inc. as of November 4, 2019 and shall be referred to throughout the present Plea as **NLL**, and is headquartered in Tempe, Arizona.

5. With regard to paragraphs 8 and 9 of the Application, it refers to the 2016 Annual Report, Exhibit P-1, denying anything inconsistent therewith.

6. With regard to paragraphs 10 and 11 of the Application, it denies that it sold the products in question and specifies that it licensed the use of the products.

7. With regard to paragraph 12 of the Application, it refers to the Terms and Conditions, Exhibit P-2, denying anything inconsistent therewith.

8. It denies the allegations contained in paragraph 13 of the Application.

9. With regard to paragraph 14 i) to vii) of the Application, it refers to the License History, Exhibit P-3, denying anything inconsistent therewith; it denies that the credit card statements, Exhibits P-4, P-5 and P-6 and the invoice P-7 demonstrate what the Plaintiff alleges they do; and denies the balance of paragraph 14 i) to vii).

10. It denies the allegations contained in paragraphs 15, 16 and 17 of the Application.

11. It denies as drafted the allegations contained in paragraphs 18 and 19 of the Application, and refers to its further pleadings below.

12. It denies the allegations contained in paragraphs 20 to 37 and refers to its further pleadings below.

**AND FOR FURTHER DEFENCE, THE DEFENDANT RESPECTFULLY SUBMITS THE FOLLOWING:**

## I. Introduction

13. During the class period, NLL, sold market-leading antivirus software that provided multi-layered protection from cyber security threats.

14. The alleged defect described in the Application (the **Alleged Defect**) did not undermine the overall protection that NLL's products provided to class members.

15. In particular, NLL 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.

16. As a result, NLL's representations were consistent with the quality and nature of Symantec's product offering. At no time did NLL made any false, misleading or inaccurate representations about its software, within the meaning of the CPA.

## II. The Defendant NLL

17. NLL is a global cyber security company incorporated under the laws of Delaware and headquartered in Tempe, Arizona.

18. Among other things, during the class period, NLL developed and marketed a line of cyber security software for consumer use under the "Norton by Symantec" brand.

19. At various points during the class period, NLL'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**).

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

## III. The Norton Software is fit for the purpose for which security software is ordinarily used

### 1) The Consumer Protection Act ch. P-4.1 does not apply to the Norton Software

21. 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.

22. 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.

23. 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 *Consumer Protection Act*, ch. P-40.1 (**CPA**). Nor did Symantec enter into a contract of sale of goods with its customers at any point.

24. As a result, Symantec denies that the CPA applies to the Norton Software.

**2) Proactive, layered cyber security protection**

25. At all relevant times during the class period, the Norton Software provided multi-layered cyber security protection which rendered it entirely fit as a computer antivirus tool. Multi-layered cyber security protection involves multiple technologies or software features working together to identify, prevent and remediate cyber security threats.

26. 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.

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

28. 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.

29. 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.

30. To the extent that any defect, including the Alleged Defect described in the Application, 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.

**3) The Norton Software provides substantial cyber security protection**

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

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

33. 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, and deliver other types of malware to victims' computers. Dorkbot infected more than 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.

34. Recognizing the significant value it provides users, independent testers scored the Norton Software at or above industry average for systems protection, between 2010 and 2016.

35. In addition, to the extent that the supply of the Norton Software constitutes the supply of services as defined in the CPA, the services provided via the Norton Software were of reasonably acceptable quality during the class period.

**4) Plaintiffs' description of the Alleged Defect is inaccurate**

36. The alleged characteristics of the Norton Software set out particularly in paragraphs 20 to 28 of the Application and in Exhibit P-9 are not accurately described and do not constitute any defect in the Norton Software.

37. In particular:

(a) the decomposer used in the Norton Software does not run in the kernel, 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;

(c) there was no memory corruption in the code used in the Norton Software decomposer. 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. Further, these alleged vulnerabilities did not cause or contribute to the Alleged Defect; and

(e) NLL 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 NLL did not fail to update the Norton Software.

38. Even if the alleged characteristics of the Norton Software set out in paragraphs 20 to 28 of the Application and in Exhibit P-9 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.

39. Even if the alleged characteristics of the Norton Software 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 NLL'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.

**IV. NLL has not made any misrepresentations**

40. The statements identified in the Application as alleged omissions and misrepresentations, particularly in paragraphs 29 and 30, 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, NLL accurately and fairly represented the qualities and capabilities of the Norton Software to class members.

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

42. More particularly, representations to the effect that the Norton Software would provide "improved", "superior", "proactive", "rock solid", "up-to-date" and "layered" protection against viruses, malware and hacking were at all material times an accurate representation of the Norton Software and its capabilities.

43. At no point did NLL 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.

44. Further, class members would not have reasonably understood that NLL's representations about the level of security offered by the Norton Software amounted to a promise of perfect cyber security protection. Instead, class members reasonably expected that NLL would work diligently to program the Norton Software to address cyber security threats promptly following their discovery by NLL.

45. In fact, 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: NLL offers a free virus removal tool known as the Norton Power Eraser. This software tool is available for download by the public from NLL'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. NLL'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, NLL offers the 'Virus Protection Promise' (VPP), which states that, if a user's system is running the Norton Software and is fully updated, NLL 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.

46. In addition, 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.

47. 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.

48. 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.

49. Furthermore, NLL denies that it did not adhere to what the Plaintiff terms "fundamental and basic security best practices" or that it failed to advise customers of this so-called fact.

50. First, NLL denies that "best practices" is a term with any discernable meaning, at law or otherwise. NLL denies that any class member would have understood the content of "best practices" to mean what the Plaintiff alleges, or at all.

51. In the alternative, NLL was substantially compliant with best practices throughout the class period with respect to the development and supply of the Norton Software.

52. In the further alternative, to the extent that Symantec made the representations alleged by the Plaintiff, such representations were mere puffery and understood by the customer not to be a meaningful representation as to the qualities or characteristics of the Norton Software.

53. 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 Alleged Defect.

## V. The specific situation of customers whose License Agreements were automatically renewed

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

55. The alleged misrepresentations were not made to Norton Software users who entered into License Agreements with NLL 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).

56. Symantec expressly denies that any of the auto-renewal users have any actionable claim for rescission or damages against NLL under the CPA.

## VI. No damages suffered

57. No class member has suffered actual damage (in the nature of a virus attack, malware or other cyber breach) as a result of any of the conduct described in the Application, which is denied, and NLL puts the Plaintiff and class members to the strict proof of any damages claim.

58. To the extent that class members claim a reduction of the purchase price paid for the Norton Software, NLL puts the Plaintiff and class members to the strict proof of quantifying the alleged reduction to which they are entitled relating to the conduct described in the Application. NLL denies that the Norton Software had no value whatsoever during the class period, as alleged by the Plaintiff.

59. 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.

60. Even if the plaintiffs and class members can prove that they are entitled to an award of damages, the requirements of article 595 C.C.P. regarding collective recovery 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).

61. Finally, the conduct described in the Application, which is denied, does not provide a basis for an award of punitive damages.

## VII. Prescription

62. The claims advanced in the Application are prescribed, in whole or in part, because these claims were brought three years after the right of action arose. .

**WHEREFORE, MAY IT PLEASE THE COURT TO:**

**GRANT** the present Defence;

**DISMISS** the Plaintiff's Originating Application of a Class Action Lawsuit;

**THE WHOLE** with costs.

Montreal, February 14, 2020

Norton Rose Fulbright Canada LLP

**NORTON ROSE FULBRIGHT CANADA** LLP
(Mtres Éric Dunberry and Maya Angenot)
Attorneys for Defendant
Symantec Corporation

1 Place Ville Marie, Suite 2500
Montréal, Quebec H3B 1R1
Telephone: 514.847.4310
Fax: 514.286.5474
Email: eric.dunberry@nortonrosefulbright.com
maya.angenot@nortonrosefulbright.com
Notification: Notifications-mtl@nortonrosefulbright.com
Our reference: 1001009248

## Cabba, Christiane

**De:** Cabba, Christiane
**Envoyé:** 14 février 2020 16:16
**À:** 'Pierre Boivin'
**Cc:** Angenot, Maya (maya.angenot@nortonrosefulbright.com); Dunberry, Eric
**Objet:** NOTIFICATION / Michel Carrière v. Symantec Corporation | 500-06-000894-176
**Pièces jointes:** Defence (Symantec).pdf

**Suivi:**

| Destinataire | Réception |
|---|---|
| 'Pierre Boivin' | |
| Angenot, Maya (maya.angenot@nortonrosefulbright.com) | Remis: 2020-02-14 16:16 |
| Dunberry, Eric | Remis: 2020-02-14 16:16 |

# NOTIFICATION PAR COURRIEL / NOTIFICATION BY EMAIL
# (Articles 133 et/and 134 C.p.c. / C.C.P.)

| EXPÉDITEUR / SENDER | |
|---|---|
| **NORTON ROSE FULBRIGHT CANADA S.E.N.C.R.L., s.r.l. / LLP**<br>Me / Mtre. Éric Dunberry and Maya Angenot<br>1, Place Ville Marie, # 2500<br>Montréal (Québec) H3B 1R1<br>Tel. : (514) 847-4747 – Fax : (514) 286-5474<br>Notifications-mtl@nortonrosefulbright.com | |
| **Date :** | Montreal, February 14, 2020 |
| **Nature du document / Nature of the document :** | Defence |
| **N° du dossier de Cour / Court File # :** | 500-06-000894-176 |
| **Nom des parties / Name of the parties :** | Michel Carrière v. Symantec Corporation |
| **Nombre de pages / Number of the pages :** | 10 |
| **Heure de transmission / Time of transmission :** | 16H15 |
| **Notre référence / Our reference :** | 1001009248 |
| **DESTINATAIRE(S) / RECIPIENT(S)** | |
| **Nom / Name :** Mtre. Pierre Boivin<br>**Étude / Firm :** **KUGLER KANDESTIN LLP**<br>1, Place Ville Marie – suite 1170<br>Montréal (Québec) H3B 2A7 | |

**Christiane Cabba**
Adjointe juridique
Legal Assistant
Adjointe de / Assistant to Claudia Déry, Pierre A. Michaud, Maya Angenot et/and Dominique Noël

Norton Rose Fulbright Canada S.E.N.C.R.L., s.r.l. / LLP
1, Place Ville Marie, Bureau 2500, Montréal, QC, H3B 1R1, Canada

T: +1 514.847.4990 | F: +1 514.286.5474
christiane.cabba@nortonrosefulbright.com

**NORTON ROSE FULBRIGHT**

## Cabba, Christiane

**De:** Microsoft Outlook <postmaster@nortonrosefulbright.com>
**À:** Pierre Boivin
**Envoyé:** 14 février 2020 16:16
**Objet:** Relayé : NOTIFICATION / Michel Carrière v. Symantec Corporation | 500-06-000894-176

**La remise à ces destinataires ou groupes est terminée, mais aucune notification de remise n'a été envoyée par le serveur de destination :**

Pierre Boivin

Objet : NOTIFICATION / Michel Carrière v. Symantec Corporation | 500-06-000894-176

**NO: 500-06-000894-176**

**S U P E R I O R C O U R T**

**DISTRICT OF MONTREAL**

**MICHEL CARRIÈRE**

Plaintiff

-v-

**SYMANTEC CORPORATION**

Defendant

**DEFENCE**

**O R I G I N A L**

BO-0042 # 1001009248

Mtres. Éric Dunberry & Maya Angenot
**NORTON ROSE FULBRIGHT CANADA** LLP
BARRISTERS & SOLICITORS
1 Place Ville Marie, suite 2500
Montréal (Quebec) H3B 1R1 CANADA
Telephone: +1 514.847.4310
Fax: +1 514.286.5474

Notifications-mtl@nortonrosefulbright.com