ROBERT C. SCHUBERT (S.B.N. 62684)
rschubert@sjk.law
WILLEM F. JONCKHEER (S.B.N. 178748)
wjonckheer@sjk.law
NOAH M. SCHUBERT (S.B.N. 278696)
nschubert@sjk.law
CASSIDY KIM (S.B.N. 315236)
ckim@sjk.law
SCHUBERT JONCKHEER & KOLBE LLP
Three Embarcadero Center, Suite 1650
San Francisco, California 94111
Telephone: (415) 788-4220
Facsimile: (415) 788-0161

Attorneys for Plaintiff Montgomery Beyer

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

MONTGOMERY BEYER, Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

v.

SYMANTEC CORPORATION

Defendant.

Case No.

Complaint for Violation of Cal. Civ. Code §§ 1750 *et seq.*, §§ 1790 *et seq.*, Cal. Bus. & Prof. Code §§ 17500 *et seq.*, §§ 17200 *et seq.*, and Unjust Enrichment

Class Action

Demand for Jury Trial

Upon personal knowledge as to his own acts, and based upon his investigation, his counsel's investigation, and information and belief as to all other matters, plaintiff Montgomery Beyer, on behalf of himself and all others similarly situated, alleges:

SUMMARY OF ACTION

1. This is a class action on behalf of persons and entities who purchased and/or licensed certain network security software products sold by Symantec Corporation ("Symantec") between December 21, 2005 and September 19, 2016 (the "Class Period") containing Symantec's AntiVirus Decomposer Engine. The network security software products at issue were sold or licensed to consumers under the Norton brand ("Norton Products") and to businesses under the Symantec brand ("Enterprise Products," and together with the Norton Products, the "Affected Products").

2. This action arises out of revelations about critical security flaws in the Affected Products, as revealed by Project Zero. Project Zero is a team of expert cybersecurity analysts employed by Google, Inc., dedicated to identifying and resolving "zero-day" vulnerabilities, or flaws in software that can be exploited by hackers. On or about April 28, 2016, Project Zero notified Symantec of critical vulnerabilities in Symantec's AntiVirus Decomposer Engine, a key component of Symantec's antivirus software that decompresses or unpacks compressed executable files so that they can then be scanned for malicious code.

3. In particular, Project Zero revealed that the Affected Products were equipped with old third-party open source code with known corruption bugs that could be exploited by hackers and malicious software. Third-party open source providers had released software updates or "patches" to resolve those bugs in subsequent iterations of their code. Symantec, however, systematically failed to update the Affected Products with these patches. In addition, Project Zero revealed that Symantec failed to design the AntiVirus Decomposer Engine to limit the impact of a vulnerability, in contravention of a fundamental cybersecurity best practice known as the principle of least privilege. Instead, the AntiVirus Decomposer Engine unpacked and examined compressed executable files in the most sensitive part of a computer's operating

system, which exposed millions of computer systems to the risk of "a clean overflow as root" on Linux, Mac, and other UNIX systems or "kernel memory corruption" on Windows systems. These defects caused the Affected Products to be susceptible to serious vulnerabilities that, according to Project Zero, "[were] as bad as it gets."

4. In the months following the notification, Project Zero worked with Symantec to help verify and resolve the reported issues. On June 28, 2016, Symantec issued a broad security advisory describing software patches it was deploying to resolve the critical vulnerabilities identified by Project Zero, including the serious buffer overflow and memory corruption bugs. The patches were also designed to address the outdated third-party open source code that Symantec had failed to update over a period of at least seven years. Given the sheer number of products that required patching, Symantec was unable to release all the necessary updates at the same time. Instead, the company rolled out the security patches in phases over nearly five months. Furthermore, enterprise customers had to proactively patch their products themselves because Symantec was unable to push through automatic updates for the Enterprise Products. Symantec continued to push out critical security updates to its customers until September 19, 2016.

5. It was not until 2017 that Symantec updated its Norton and Enterprise Products to comply with the principle of least privilege by including a "sandbox" such that, rather than opening files in the most sensitive part of the operating system, the Affected Products "[would] run and analyze suspicious and unknown files in an isolated protected virtual environment before they're let go through [sic] and get onto [the user's] device."

6. During the Class Period, millions of consumers and businesses remained unaware that their antivirus software had utterly failed to perform as expected, and instead, had exposed their systems to remote attacks and other easily exploitable security vulnerabilities.

7. Symantec had a statutory obligation to sell functioning antivirus software that conformed to cybersecurity best practices and reasonably protected users' computer systems against hackers, malware, and viruses, in a manner consistent with its express and implicit representations to its users and the public. Despite its statutory obligation, Symantec sold

antivirus software that did not conform to cybersecurity best practices, did not reasonably protect users' computer systems against online threats, and in fact, made users' computer systems *more susceptible* to cyberattacks than they would have otherwise been without that software. As such, Symantec sold goods that were not adequately packaged and labeled, and were not fit for their intended, or any other legitimate, use. Symantec concealed these defects throughout its marketing, advertising, and packaging of the Norton Products and the Enterprise Products.

8. Symantec's misrepresentations and omissions concerning the Affected Products violated the California False Advertising Law ("FAL"), CAL. BUS. & PROF. CODE §§ 17500 *et seq*. Purchasers of the Norton Products are further entitled to recover monetary damages for the full purchase price of their antivirus software under the California Consumer Legal Remedies Act ("CLRA"), CAL. CIV. CODE §§ 1750 *et seq*., and the California Song-Beverly Consumer Warranty Act, CAL. CIV. CODE §§ 1790 *et seq*. Symantec's conduct was also unlawful, fraudulent, and unfair in violation of the California Unfair Competition Law ("UCL"), CAL. BUS. & PROF. CODE §§ 17200 *et seq*.

9. As a direct result of Symantec's misrepresentations and omissions, set out below, plaintiff Montgomery Beyer and the Class suffered damages, including costs associated with purchasing, licensing, and renewing the Affected Products.

PARTIES

10. Plaintiff Montgomery Beyer ("Mr. Beyer") is a citizen of Michigan and a resident of Walker, Michigan. During the Class Period, Mr. Beyer purchased and renewed several Norton Products, including the Norton 360 and Norton 360 Premier software products.

11. Defendant Symantec is a citizen of California and a Delaware corporation with its principal place of business in Mountain View, California. In its public statements, Symantec describes itself as "the global leader in cybersecurity" and that it "protect[s] more customers from the next generation of attacks [by helping] companies, governments and individuals secure their most important data wherever it lives." Symantec operates a business segment for

consumer and home business security through its Norton-branded services, as well as a separate enterprise security segment for mid-size and large organizations. Symantec's end user license agreements for the Affected Products identify California law as the choice of law for U.S. purchasers.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because (a) this is a class action in which the matter in controversy exceeds $5 million, exclusive of interests and costs; (b) there are more than one hundred class members; and (c) Plaintiff and the class are citizens of different states than at least one defendant, satisfying the minimal diversity requirement.

13. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is located in California. Defendant also has sufficient minimum contacts with California such that the exercise of jurisdiction by this Court is permissible under traditional notions of fair play and substantial justice. A substantial portion of the wrongdoing alleged in this complaint took place in California; Defendant conducts business in California and otherwise avails itself of the protections and benefits of California law through the promotion, marketing, and sale of its antivirus software in this State, as evidenced by the selection of California law as the choice of law in Defendants' end user license agreements; and this action arises out of or relates to those contacts.

14. Venue is proper under 28 U.S.C. § 1391 because (1) Defendant is subject to personal jurisdiction in the Northern District of California, and (2) a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District. Defendant promotes, markets, and sells antivirus products and services in this District, maintains its headquarters in this District, employs workers in this District, and advertises in this District.

15. Intradistrict Assignment: Pursuant to Civil L.R. 3-2(c) and 3-5(b), assignment to the San Jose Division of the Northern District of California (the "Division") is proper, because a substantial part of the events or omissions which give rise to the claims occurred in this

Division. Defendant promotes, markets, and sells antivirus products and services in this Division, maintains its headquarters in this Division, employs workers in this Division, and advertises in this Division.

FACTUAL ALLEGATIONS

Symantec Represents Itself as a Leading Provider of Security Products

16. Symantec is a provider of network security solutions and has boldly promoted itself as a global leader in the field.[1] The company recently reported "its #1 market share leadership position in the overall security software for 2015" including "the largest market share in . . . Endpoint Protection Platform, Data Loss Prevention software . . . Secure Email Gateway, and Consumer Security Software."[2] Symantec further reported that it "protect[s] 175 millions of endpoints worldwide [and] continues to be the largest endpoint security vendor."[3]

17. Symantec's products are supported by the "same core engine across their entire product line,"[4] known as the AntiVirus Decomposer Engine.[5] This core engine decompresses or

---

[1] *See Investor Fact Sheet, 4th Quarter Fiscal 07,* SYMANTEC (May 2007), http://s1.q4cdn.com/585930769/files/doc_financials/2007/Q4/SYMCIRFSQ407.pdf (describing that "Symantec is a global leader in infrastructure software"); *Investor Presentation*, SYMANTEC (Nov. 2015), http://s1.q4cdn.com/585930769/files/doc_presentations/2015/Symantec-Investor-Presentation_November-2015_FINAL-(1).pdf (representing that Symantec is a global leader in cybersecurity); Symantec Corporation, *Annual Report (Form 10-K)* (May 20, 2016), http://s1.q4cdn.com/585930769/files/doc_financials/2016/Q4/Symantec2016-10K.pdf (describing Symantec as a global leader in security).

[2] Sara Pan, *Symantec Achieves More Than 15 Years of Market Share Leadership in Overall Security Software,* SYMANTEC BLOG (Apr. 7, 2016), https://www.symantec.com/connect/blogs/Symantec-achieves.

[3] *Id. See also* Sri Sundaralingam, *It's a Sweep: Symantec Endpoint Protection 14 Leads in Latest Analyst Ratings,* SYMANTEC BLOG (Mar. 3, 2017), https://www.symantec.com/blogs/product-insights/symantec-endpoint-protection-14-leads-latest-analyst-ratings.

[4] Tavis Ormandy, *How to Compromise the Enterprise Endpoint,* PROJECT ZERO BLOG (Jun. 28, 2016), https://googleprojectzero.blogspot.com/2016/06/how-to-compromise-enterprise-endpoint.html ("Project Zero Disclosures").

[5] *Security Advisories Relating to Symantec Products - Symantec Decomposer Engine Multiple Parsing Vulnerabilities,* SYMANTEC (Jun. 28, 2016),

unpacks compressed executable files so that they can then be scanned for malicious code. In many ways, the AntiVirus Decomposer Engine operates as "the backbone of both [Symantec's] consumer and enterprise security products."[6]

18. As a prominent provider of security solutions, Symantec markets its products as the best security solutions available on the market. For instance, for the Norton Products, Symantec has represented the following:

> ***Norton 360 v. 4.0 Premier Edition (2010)***
>
> Features
>
> . . .
>
> **NEW! Provides unprecedented and unmatched threat detection** — Adds an additional layer of protection to detect viruses, Trojans, spyware, and other threats. Norton™ reputation service technology scrutinizes different attributes of files and applications in real-time to determine if they are safe.
>
> **NEW! Warns you of dangerous downloads** — Proactively protects you by analyzing newly downloaded files and applications for threats before you install or run them on your PC.
>
> . . .
>
> **Protects your PC, online activities and your identity** – Delivers industry-leading, all-in-one protection against identity theft, online fraud, phishing, viruses, Trojans, bots, rootkits, spyware, and the latest cyber-threats.[7]
>
> ***Norton AntiVirus (2011)***
>
> . . .
>
> Protects your PC against the latest viruses, spyware, and other threats.
>
> Delivers fast, powerful online protection to keep you a step ahead of cyber attacks.

---

https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160628_00 ("Symantec Security Advisory").

[6] Charlie Osborn, *Symantec Security Flaws Are "As Bad As They Get," Says Researcher*, ZDNET (Jun. 29, 2016), http://www.zdnet.com/article/symantec-antivirus-product-bugs-as-bad-as-they-get.

[7] Product Page, *Norton 360™ Version 4.0 Premier Edition* (archived Sep. 28, 2010), https://web.archive.org/web/20100928175101/http://us.norton.com/360-premier-edition/ (last visited Mar. 29, 2018).

. . .

Features

Protects your PC against the latest known viruses, spyware, and other threats

Norton Reputation Service instantly checks where files came from and how long they've been around to identify and stop new crimeware faster than other, less sophisticated security software.

Norton Protection System uses several overlapping layers of protection that work together to stop viruses, spyware and other online attacks.

Norton Pulse Updates provides up-to-the-minute updates that protect against the latest threats without slowing down your computer.

SONAR 3 Behavioral Protection monitors your PC for suspicious behavior to quickly detect new online threats.

Norton Bootable Recovery Tool creates an emergency CD/DVD/USB that gets you back up and running even if your PC has become so infected that it won't start up.

Bot detection blocks the automated programs cybercriminals use to take control of your PC, access your private information, and use your computer to send out spam and launch attacks on other PCs.

Worm protection safeguards your PC against fast-spreading Internet worms and prevents you from accidentally passing them on to others.

Rootkit detection finds and removes deeply buried crimeware that can hide other types of threats and allow cybercriminals to take control of your PC.[8]

Norton 360 v. 5.0 Premier Edition (2012)

Key Features

. . .

Email, chat, and download files without worry

Detects and eliminates viruses, spyware, and other threats before they can do damage.

Warns you if a downloaded file is dangerous before you install it on your PC.

Prevents crimeware from being secretly downloaded to your computer.

[8] Product Page, *Norton™ AntiVirus 2011* (archived Sep. 28, 2010), https://web.archive.org/web/20100928150519/http://us.norton.com/antivirus/ (last visited Mar. 29, 2018).

Blocks annoying and potentially dangerous spam.[9]

19. Similarly, Symantec has represented superior security and data protection features for its Enterprise Products, as follows:

> ***Symantec Endpoint Protection (2014)***
>
> Unrivaled Security
>
> Today's complicated threat landscape requires sophisticated protection from large-scale malware to the most targeted attacks. Only Symantec uses Insight, with the collective wisdom of 200+ million systems in over 200 countries to identify and create a security rating for every file accessed through the internet. This superior reputation technology is combined with network, behavior, file and repair layers of defense to provide unrivaled security against known, and unknown, threats.[10]
>
> ***Symantec Protection Suite Enterprise Edition (2014)***
>
> New Features
>
> . . .
>
> Fastest, Most-effective Endpoint Security:
>
> Symantec Insight - Separates files at risk from those that are safe, for faster and more accurate malware detection.
>
> Real Time SONAR 3 - Examines programs as they run, identifying and stopping malicious behavior even of new and previously unknown threats.
>
> . . .
>
> Key Features
>
> Fastest, most-effective protection, powered by Symantec Insight, for laptops, desktops, servers, messaging and web gateways--protection beyond antivirus.
>
> Catch more than 99% of spam and prevent data loss with advanced content filtering to identify and control the flow of sensitive data in email and IM.

---

[9] Product Page, *Norton 360™ Premier Edition* (archived Feb. 3, 2012), https://web.archive.org/web/20120203035935/http://us.norton.com:80/360-premier-edition (last visited Mar. 29, 2018).

[10] Product Page, *Symantec Endpoint Protection* (archived May 16, 2014), https://web.archive.org/web/20140516155754/http://www.symantec.com:80/endpoint-protection (last visited Mar. 29, 2018).

> Web gateway security that protects against web threats, including malicious software, spyware, botnets, viruses, and malware.
>
> Rapid data and system recovery recovers individual files and folders in seconds or complete Windows systems in minutes to dissimilar hardware or virtual environments.[11]

Plaintiff Montgomery Beyer Purchased Several Norton Products In Reliance on Symantec's Representations

20. In March 2007, Mr. Beyer purchased a Dell desktop computer that came equipped with the Norton 360 software ("First Software"), an Affected Product. Prior to purchase, Mr. Beyer reviewed Symantec's website and information materials regarding the First Software, available at http://www.symantec.com:80/norton360/about (archived via the Wayback Machine). This webpage provided an overview and explanation of key security features included in the First Software. There, Symantec represented that the First Software "[d]efends your PC against a broad range of threats" and "[p]rotects against the latest online threats." Under the "Norton 360 FAQ" section, Symantec further represented:

> **Q: What PC Security features does Norton 360 provide?**
>
> **A.** Backed by the largest Security Response network in the world, Norton 360 provides the following PC Security features with an unmatched depth of security technologies:
>
> Virus detection and remediation
> Spyware detection and remediation
> Two-way silent firewall
> Intrusion prevention
> Vulnerability assessment

21. When the First Software expired in March 2009, Mr. Beyer purchased an upgrade to Norton 360 Premier, v. 2.0 ("Second Software"), also an Affected Product. Prior to this purchase, Mr. Beyer again reviewed the product page on Symantec's website. There, Symantec represented that Norton 360 Premier, v. 2.0 "defends you against a broad range of online threats" through key technologies, including antivirus, antispyware, rootkit detection, and automatic updates. Symantec also represented that the Second Software provides "enhanced

[11] Product Page, *Symantec Protection Suite Enterprise Edition* (archived Sep. 25, 2014) https://web.archive.org/web/20140925100516/http://www.symantec.com:80/protection-suite-enterprise-edition?fid=endpoint-protection (last visited Mar. 29, 2018).

protection" through "industry leading virus, spyware and firewall protection." Mr. Beyer subsequently installed a second license for the Second Software on April 24, 2009, and a third and final license on August 16, 2009.

22. That same year, Mr. Beyer purchased another Norton 360 Premier, v. 2.0 subscription ("Third Software") at a Best Buy store, which he installed on a separate Dell desktop computer. Mr. Beyer reviewed the relevant product page on Best Buy's website, http://www.bestbuy.com/:80/site/olspage.jsp?skuId=8734051&type=product&id=1201307759964 (archived via the Wayback Machine). There, Mr. Beyer relied on similar representations that the Third Software "[p]rotects against viruses, spyware, hackers, rootkits, identity theft, phishing scams, and fraudulent Web sites." To the best of his knowledge, Mr. Beyer also reviewed and relied upon the various comparable representations and statements on the software's packaging and box in connection with the purchase.

23. On March 5, 2010, Mr. Beyer purchased a renewal for the Second Software ("Fourth Software"), along with a PC Jump Start Service program ("Fifth Software") designed to clean up Mr. Beyer's computer system. Upon installation of the Fifth Software, however, Mr. Beyer's computer failed to restart. After fruitless attempts to resolve the issue with Symantec's support service, during which Mr. Beyer was repeatedly told there was no software problem, Mr. Beyer ultimately replaced his hard drive. Subsequently, Mr. Beyer noticed a considerable slowdown of his operating system, and suspecting a virus, Mr. Beyer requested and received a full refund for the Fourth Software and the Fifth Software purchases. This was the first and only time Mr. Beyer requested a refund for his purchase of any of the Norton Products. The Third Software eventually expired in 2011. Mr. Beyer did not purchase a renewal or any other Symantec product thereafter.

24. The representations and statements described above in ¶¶ 20-23 were material to Mr. Beyer when he purchased the software to protect his computers. At all points of sale, however, Symantec did not disclose that its products suffered from a core decomposer engine defect that exposed entire computer operating systems to various security vulnerabilities. Symantec also failed to disclose that it did not implement patches for third-party source code

that it used throughout its product line. Based on the foregoing representations and omissions, Mr. Beyer believed he was purchasing industry-leading security products that would protect his computers from viruses, spam, and other online vulnerabilities. Had he known that Symantec designed its products with a fundamental core engine defect and did not patch vulnerable third-party source code, Mr. Beyer would not have purchased a single security product from Symantec.

Symantec's Products Suffered from a Defective AntiVirus Decomposer Engine

25. On June 28, 2016, Google's Project Zero team published its findings on Symantec's product vulnerabilities,[12] followed by Symantec's security advisory release the same day.[13] In its disclosures, Project Zero discussed at length Symantec's dangerous software design of unpacking compressed executable files in the privileged core of a computer's operating system ("OS"). [14] Specifically, Project Zero discovered that the AntiVirus Decomposer Engine in the Affected Products scanned for malicious files by unpacking and examining compressed executable files within the kernel (in Windows OS) or the root (in Mac or Linux OS). This was the result of Symantec unnecessarily assigning the highest privilege levels to the file scanning and analysis function of the Antivirus Decomposer Engine, which was a serious design defect (the "High Privilege Defect").

26. Security experts routinely emphasize that the file scanning and analysis function of a decomposer engine should not be executed at high privilege or trust levels of the computer's OS.[15] However, by doing so, Symantec violated a key cybersecurity best practice, the principle of least privilege, which states that software should operate using the least amount of privilege necessary to complete the task.

---

[12] Project Zero Disclosures, *supra* at 4.
[13] Symantec Security Advisory, *supra* at 5.
[14] Project Zero Disclosures, *supra* at 4.
[15] Robert Hackett, *Google Found Disastrous Symantec and Norton Vulnerabilities that are 'As Bad As It Gets,"* FORTUNE (Jun. 29, 2016), http://fortune.com/2016/06/29/symantec-norton-vulnerability/.

27. Symantec further failed to implement industry-standard security measures, such as "sandboxing," which is a "software management strategy that isolates applications from critical system resources and other programs," thereby "provid[ing] an extra layer of security that prevents malware or harmful applications from negatively affecting your system."[16] Sandboxing would have ensured that potential malware and other untrusted files were processed in a secure environment, isolated from the most privileged and sensitive part of the OS.[17] But by failing to implement sandboxing and other industry-standard security measures in the Affected Products, Symantec exposed users' entire computer systems to a critical vulnerability that "would let attackers subvert the unpacker to take control of a victim's machine."[18]

28. Symantec's failure to implement the principle of least privilege in the design of the AntiVirus Decomposer Engine made the Affected Products a threat vector for a wide variety of cyberattacks in millions of computer systems.[19] Certain vulnerabilities resulting from the High Privilege Defect received "critical" security scores, ranging from 9.0 to 10.0, on the Common Vulnerability Scoring System ("CVSS"), a standardized system for measuring the severity of a vulnerability.[20] In pertinent part, the CVSS reported that these vulnerabilities had low access complexity, meaning "[v]ery little knowledge or skill is required to exploit" them,[21]

---

[16] Per Christensson, *Software Terms: Sandboxing Definition*, TECHTERMS (Jul. 8, 2016), https://techterms.com/definition/sandboxing.

[17] Project Zero Disclosures, *supra* at 4.

[18] Kim Zetter, *Symantec's Woes Expose the Antivirus Industry's Security Gaps,* WIRED (Jun. 30, 2016), https://www.wired.com/2016/06/symantecs-woes-expose-antivirus-software-security-gaps/.

[19] Project Zero Disclosures, *supra* at 4.

[20] The CVSS, now in its third iteration, is a quantitative model "for communicating the characteristics and impacts of IT vulnerabilities." *Vulnerability Metrics,* NAT'L INST. OF STDS. AND TECH., https://nvd.nist.gov/vuln-metrics/cvss (last visited Jan. 23, 2018). It serves as a standard measurement system that "ensures repeatable accurate measurement" across industries and governments "while enabling users to see the underlying vulnerability characteristics that were used to generate the scores." *Id.* The CVSS severity ratings are divided into five categories: (1) None - score of 0.0.; (2) Low - score of 0.1-3.9; (3) Medium - score of 4.0-6.9; (4) High - score of 7.0-8.9; and (5) Critical - score of 9.0-10.0. *Id.*

[21] *CVE Vulnerability Details,* CVE-2016-2210 (Jun. 30, 2016), https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2016-2210. *See also CVE Vulnerability Details* for CVE-2016-3644 (Jun. 30, 2016), https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2016-

and that a potential attacker could cause "a total shutdown of the affected resource . . . render[ing] the resource completely unavailable."[22]

Symantec Failed to Patch Known Vulnerabilities in Third-Party Open Source Code

29. Symantec relied on third-party open source code[23] to design the AntiVirus Decomposer Engine. In its analysis, Project Zero reviewed "the decomposer library shipped by Symantec [which] showed that they were using code derived from open source libraries like libmspack and unrarsrc."[24] Upon further review, Project Zero discovered that Symantec had failed to update the open source code for at least seven years ("Outdated Source Code Defect"), which Symantec subsequently confirmed.[25] Project Zero's Tavis Ormandy further explained that "[b]etween the version of unrar that Symantec runs . . . and the . . . current version, **literally hundreds of critical memory corruption bugs have been resolved**."[26] This considerable lag in source code updates meant that, for years, all systems running Symantec's products were exposed to "[d]ozens of public vulnerabilities . . . some with public exploits," even though the patches were readily available.[27]

3644; CVE-2016-3645 (Jun. 30, 2016), https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2016-3645; CVE-2016-2208 (May 19, 2016), https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2016-2208; CVE-2016-2209 (Jun. 30, 2016), https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2016-2209.

[22] *Id.*

[23] Source code is the underlying software code that programmers write and manipulate to effect specific program or application functions. Open source code is source code that is made available for others to view, copy, modify, and otherwise analyze. *See What is open source?*, OPENSOURCE.COM, https://opensource.com/resources/what-open-source (last visited Jan. 23, 2018).

[24] Project Zero Disclosures, *supra* at 4.

[25] *See* Project Zero Disclosures, *supra* at 4; *Security Advisories Relating to Symantec Products - Symantec Decomposer Engine Security Update,* SYMANTEC (Sep. 19, 2016), https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160919_00.

[26] *Issue 810, Symantec Antivirus multiple remote memory corruption unpacking RAR CVE-2016-2207*, MONORAIL PROJECT-ZERO (Apr. 28, 2016), https://bugs.chromium.org/p/project-zero/issues/detail?id=810&can=1&q=symantec (emphasis added) ("Monorail Issue 810").

[27] Project Zero Disclosures, *supra* at 4.

30. Symantec's "astonishing [failure to] track new releases of third party code"[28] was yet another violation of a fundamental cybersecurity principle. Experts routinely point to patching as one of the most important and highly recommended security practice to stay safe online.[29] Symantec's failure to update its software resulted in critical vulnerabilities that caused the products to suffer from low access complexity levels and the risk of a total system shutdown.[30] In addition, "[t]here [wa]s total information disclosure, resulting in all system files being revealed," and "total compromise of system integrity."[31] These vulnerabilities received a "critical" CVSS score of 10.0, indicating the most severe vulnerability.[32]

31. Project Zero concluded that "[t]hese vulnerabilities [we]re as bad as it gets"[33] because the AntiVirus Decomposer Engine ran at the highest privilege levels and its code was severely outdated. Attackers did not require any user interaction or specialized access conditions to exploit the vulnerabilities. As such, Symantec's use of the AntiVirus Decomposer Engine across its entire product line exposed users to significant harm.

Symantec Was Put on Notice of the Threat of Bad Security Practices

32. As a key player in the antivirus software marketplace, Symantec had every reason to review its product designs and security practices prior to product release. For instance, Project Zero had previously disclosed similar vulnerabilities associated with improper privilege escalation in other security products.

33. Notably, in 2015, Project Zero reported Kaspersky Lab, a multinational cybersecurity and antivirus provider, for running its antivirus software unpacker with

---

[28] Monorail Issue 810, *supra* at 26.
[29] Iulia Ion, et al., *" . . . no one can hack my mind": Comparing Expert and Non-Expert Security Practices*, USENIX SYMPOSIUM ON USABLE PRIVACY AND SECURITY, Jul. 22-24, 2015, available at https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf.
[30] *CVE Vulnerability Details,* CVE-2016-2207 (Jun. 30, 2016), https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2016-2207.
[31] *Id.*
[32] *Id*.
[33] Project Zero Disclosures, *supra* at 4.

unnecessarily high OS privileges, which exposed entire computer systems to easy exploitation.[34] As Project Zero explained, "[b]ecause antivirus products typically intercept filesystem and network traffic, simply visiting a website or receiving an email [without opening or reading it] is sufficient for exploitation" and therefore, it is critical to "add sandboxing to [the] development roadmap today."[35] This warning rings alarmingly similar to what Project Zero reiterated months later with respect to its Symantec findings.[36] Yet, Symantec was found to have ignored, or remained utterly ignorant of, the same fundamental defect with its AntiVirus Decomposer Engine. It was not until 2017 that Symantec introduced a sandboxing feature to its Norton and Enterprise Products.[37]

34. Project Zero further highlighted the unique importance of holding security vendors to the highest security standards given "strong evidence that an active black market trade in antivirus exploits exists."[38] In particular, Project Zero found that "anti virus exploits and information are actively traded," and therefore, providers of security solutions have a heightened responsibility to minimize potential harms caused by their software.[39]

Symantec Failed to Comply with Its Own Security Best Practices

35. As a prominent player in the cybersecurity marketplace, Symantec regularly publishes advisories, threat reports, support documentation, and other security content to educate users of the latest vulnerabilities, threat factors, and solutions. Notably, in these

---

[34] Tavis Ormandy, *Kaspersky: Mo Unpackers, Mo Problems,* PROJECT ZERO BLOG (Sep. 22, 2015), https://googleprojectzero.blogspot.com/2015/09/kaspersky-mo-unpackers-mo-problems.html ("Project Zero Kaspersky Disclosures").

[35] Project Zero Kaspersky Disclosures, *supra* at 34.

[36] *See* Project Zero Disclosures, *supra* at 4 (recommending the use of "sandboxing and a Security Development Lifecycle" to mitigate vulnerabilities with unpackers in antivirus software).

[37] *See* Norton Beta Software Page, *Norton Security 2017 Beta* (archived Jul. 5, 2017), https://web.archive.org/web/20170705215359/https://www.nortonsecurityonline.com/security-center/norton-beta.html (last visited Mar. 29, 2018) (reporting "[s]andboxing, or isolating potential threats" as a new feature in "Norton Security Version 2017 Beta").

[38] Project Zero Kaspersky Disclosures, *supra* at 34.

[39] Project Zero Kaspersky Disclosures, *supra* at 34.

publications, Symantec often includes a litany of security recommendations and best practices for both individual consumers and enterprise customers. Some examples follow:

> ***Symantec Security Advisory – Symantec Discovery Insecure File Permissions***
>
> . . .
>
> Best Practices
>
> As part of normal best practices, Symantec strongly recommends:
>
> - Restrict access to administration or management systems to privileged users.
> - Restrict remote access, if required, to trusted/authorized systems only.
> - **Run under the principle of least privilege where possible to limit the impact of exploit by threats.**
> - **Keep all operating systems and applications updated with the latest vendor patches.**
> - Follow a multi-layered approach to security. Run both firewall and anti-malware applications, at a minimum, to provide multiple points of detection and protection to both inbound and outbound threats.
> - Deploy network and host-based intrusion detection systems to monitor network traffic for signs of anomalous or suspicious activity. This may aid in detection of attacks or malicious activity related to exploitation of latent vulnerabilities.[40]

> ***Security Advisories Relating to Symantec Products - Symantec Endpoint Protection File Overwrite***
>
> . . .
>
> Best Practices
>
> As part of normal best practices, Symantec strongly recommends:
>
> - Restrict access to administration or management systems to privileged users.
> - Restrict remote access, if required, to trusted/authorized systems only.
> - **Run under the principle of least privilege where possible to limit the impact of exploit by threats.**

[40] *Symantec Security Advisory, SYM07-020, Symantec Discovery Insecure File Permissions*, SYMANTEC (Jul. 27, 2007), https://www.symantec.com/avcenter/security/Content/2007.07.27a.html (emphasis added).

- **Keep all operating systems and applications updated with the latest vendor patches.**
- Follow a multi-layered approach to security. Run both firewall and anti-malware applications, at a minimum, to provide multiple points of detection and protection to both inbound and outbound threats.
- Deploy network and host-based intrusion detection systems to monitor network traffic for signs of anomalous or suspicious activity. This may aid in detection of attacks or malicious activity related to exploitation of latent vulnerabilities.
- As a best practice Symantec recommends running the same version of SEP Client and SEPM.[41]

Symantec Intelligence Report: June 2011

. . .

Best Practice Guidelines for Enterprises

. . .

- Be aggressive on your updating and patching: Update, patch and migrate from outdated and insecure browsers, applications and browser plug-ins to the latest available versions using the vendors' automatic update mechanisms. **Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field.** Be wary of deploying standard corporate images containing older versions of browsers, applications, and browser plug-ins that are outdated and insecure. **Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.**[42]

Security Advisories Relating to Symantec Products - Symantec Endpoint Protection Multiple Issues

. . .

Best Practices

As part of normal best practices, Symantec strongly recommends:

- Restrict access to administration or management systems to privileged users.

---

[41] *Security Advisories Relating to Symantec Products - Symantec Endpoint Protection File Overwrite,* SYMANTEC (Dec. 15, 2010), https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20101215_00 (emphasis added).

[42] *Symantec Intelligence Report,* SYMANTEC (Jun. 2011), https://www.symantec.com/content/dam/symantec/docs/security-center/archives/intelligence-report-june-11-en.pdf (emphasis added).

- Restrict remote access, if required, to trusted/authorized systems only.
- **Run under the principle of least privilege where possible to limit the impact of potential exploit.**
- **Keep all operating systems and applications updated with the latest vendor patches.**
- Follow a multi-layered approach to security. At a minimum, run both firewall and anti-malware applications to provide multiple points of detection and protection to both inbound and outbound threats.
- Deploy network- and host-based intrusion detection systems to monitor network traffic for signs of anomalous or suspicious activity. This may aid in the detection of attacks or malicious activity related to the exploitation of latent vulnerabilities.[43]

36. As exemplified above, key practice guidelines that Symantec has repeatedly highlighted, going as far back as 2007, include the need to follow the principle of least privilege and the importance of keeping up-to-date with the latest vendor patches. These correspond directly to the defects that Project Zero uncovered with respect to the AntiVirus Decomposer Engine. Symantec failed to follow its own longstanding advice to its consumer and enterprise users, thereby exposing millions of its customers to critical security vulnerabilities.

The Applicable Statutes of Limitations Are Tolled

37. The applicable statutes of limitations are tolled under the Discovery Rule. Through no fault or lack of diligence on their part, Plaintiff and class members were unaware of the information essential to the claims alleged herein.

38. The High Privilege Defect and the Outdated Source Code Defect were first publicly revealed on June 28, 2016 via the Project Zero Disclosures and a Symantec security advisory. Prior to June 28, 2016, these defects were completely unknown to the public, and Plaintiff and class members would not have had any reason to suspect that the Affected Products contained critical vulnerabilities, in violation of industry best practices and Symantec's own security guidelines.

---

[43] *Security Advisories Relating to Symantec Products - Symantec Endpoint Protection Multiple Issues,* SYMANTEC (Jul. 30, 2015), https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&suid=20150730_00 (emphasis added).

39. Project Zero consists of expert security engineers and analysts who specialize in finding and resolving security vulnerabilities. By contrast, Plaintiff and class members are customers without security expertise or the ability to engage in highly complex, technical investigation of antivirus products. Plaintiff and class members, therefore, could not have discovered these defects with reasonable diligence. Accordingly, the Discovery Rule applies, and any applicable statutes of limitations were tolled—and did not begin to run—until at least June 28, 2016.

40. The Fraudulent Concealment Doctrine also tolled any applicable statutes of limitations. Through no fault or lack of diligence on their part, Plaintiff and class members were unaware of the information essential to the claims alleged herein. As the proprietary owner and licensor of the Affected Products, Symantec knew, or was otherwise reckless or willfully blind in not knowing, that its AntiVirus Decomposer Engine suffered from extremely serious defects, i.e., the High Privilege Defect and the Outdated Source Code Defect. Furthermore, Symantec knew, or was otherwise reckless or willfully blind in not knowing, that its security practices diverged significantly from its own best practices recommendations.

41. Throughout the Class Period, Symantec had a duty to disclose the true character, quality, and nature of the Affected Products to Plaintiff and the class members but failed to do so. Had Plaintiff and class members known about the fundamental and longstanding defects in the AntiVirus Decomposer Engine, they would not have purchased any of the Affected Products. Symantec is therefore estopped from relying on any statutes of limitations by virtue of its knowing and active concealment of the facts alleged above.

CLASS ACTION ALLEGATIONS

42. Plaintiff brings this class action on behalf of himself and all others similarly situated as members of a proposed Class and Subclasses, defined as follows:

> Nationwide Class: All persons in the United States and its territories who purchased or licensed an Affected Product between December 21, 2005 and September 19, 2016 (the "Class Period").

43. Within the Nationwide Class, there is one subclass for purposes of Plaintiff's claims under the Consumer Legal Remedies Act and the Song-Beverly Consumer Warranty Act, defined as follows:

> Consumer Subclass: All persons in the United States and its territories who purchased or licensed a Norton Product between December 21, 2005 and September 19, 2016 (the "Class Period").

44. Excluded from the Nationwide Class and Consumer Subclass are governmental entities, Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and Consumer Subclass are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

45. This action is brought and may properly be maintained as a class action pursuant to FED. R. CIV. P. 23(b)(2) and 23(b)(3). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of these rules.

46. ***Numerosity Under Rule 23(a)(1).*** The Nationwide Class and Consumer Subclass are so numerous that the individual joinder of all members is impracticable. While the Nationwide Class and Consumer Subclass's exact numbers are currently unknown and can only be ascertained through appropriate discovery, Plaintiff, on information and belief, alleges that the Nationwide Class and Consumer Subclass include at least millions of persons.

47. ***Commonality Under Rule 23(a)(2).*** Common legal and factual questions exist that predominate over any questions affecting only individual Nationwide Class or Consumer Subclass Members. These common questions, which do not vary among Nationwide Class or Consumer Subclass Members and which may be determined without reference to any Nationwide Class or Consumer Subclass Member's individual circumstances, include, but are not limited to:

a. Whether the Affected Products are of the same quality as those generally acceptable in the market;

b. Whether the Affected Products are fit for the ordinary purposes for which the goods are used;

c. Whether the Affected Products were adequate contained, packaged, and labeled;

d. Whether Symantec represented that the Affected Products have characteristics, uses, or benefits that they do not have;

e. Whether Symantec represented that the Affected Products are of a particular standard, quality, or grade when they are of another;

f. Whether Symantec's representations and omissions regarding the Affected Products were false and misleading and constitute false advertising;

g. Whether Plaintiff and the Nationwide Class or Consumer Subclass have been damaged by the wrongs alleged and are entitled to compensatory or punitive damages

h. Whether Plaintiff and the Nationwide Class or Consumer Subclass are entitled to injunctive or other equitable relief, including restitution.

48. Each of these common questions is also susceptible to a common answer that is capable of class-wide resolution and will resolve an issue central to the validity of the claims.

49. ***Adequacy of Representation Under Rule 23(a)(4).*** Plaintiff is an adequate Nationwide Class and Consumer Subclass representative because he is a Nationwide Class and Consumer Subclass Member, and his interests do not conflict with the Nationwide Class or Consumer Subclass's interests. Plaintiff has retained counsel who are competent and experienced in consumer-protection class actions. Plaintiff and his counsel intend to prosecute this action vigorously for the Nationwide Class and Consumer Subclass's benefit and will fairly and adequately protect their interests.

50. ***Rule 23(b)(3) Predominance and Superiority.*** The Nationwide Class and Consumer Subclass can be properly maintained under Rule 23(b)(3), because the above common questions of law and fact predominate over any questions affecting individual Nationwide Class or Consumer Subclass Members. A class action is also superior to other

available methods for the fair and efficient adjudication of this litigation because individual litigation of each Nationwide Class and Consumer Subclass Member's claim is impracticable. Even if each Nationwide Class or Consumer Subclass Member could afford individual litigation, the court system could not. It would be unduly burdensome if thousands of individual cases proceed. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the courts because it requires individual resolution of common legal and factual questions. By contrast, the class-action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

CLAIM FOR RELIEF

First Claim for Relief

Violation of the California Consumer Legal Remedies Act ("CLRA"), Cal. Civ. Code §§ 1750 et seq.

51. Plaintiff, individually and on behalf of the Consumer Subclass, incorporates by reference all of the allegations contained in the preceding paragraphs of this Complaint.

52. Defendant is a "person" as defined in CAL. CIV. CODE § 1761(c).

53. Plaintiff purchased and licensed Norton Products for personal, family, or household purposes and is therefore a "consumer" as defined in CAL. CIV. CODE § 1761(d).

54. The Norton Products are "goods" as defined by CAL. CIV. CODE § 1761(a).

55. The purchases by Plaintiff and the Consumer Subclass of the goods sold by Defendant constitute "transactions" as defined by CAL. CIV. CODE §§ 1761(e) and 1770.

56. In connection with its sale of Norton Products to Plaintiff and the Consumer Subclass, Defendant violated the CLRA by:

a. Misrepresenting to Plaintiff and the Consumer Subclass that the Norton Products were equipped with industry-leading technology that provide safe

and up-to-date security, when in fact, they used outdated third-party source code and suffered from a core engine defect that exposed entire computer systems to potential malware and other untrusted files, in violation of CAL. CIV. CODE §§ 1770(a)(5), (7), (9), and (16);

b. Misrepresenting to Plaintiff and the Consumer Subclass that the Norton Products had characteristics, uses, and benefits that they did not have, in violation of CAL. CIV. CODE § 1770(a)(5).

c. Misrepresenting to Plaintiff and the Consumer Subclass that the Norton Products were of a particular standard, quality, or grade, when they were of another, in violation of CAL. CIV. CODE § 1770(a)(7).

d. Advertising the Norton Products to Plaintiff and the Consumer Subclass with the intent not to sell them as advertised, in violation of CAL. CIV. CODE § 1770(a)(9); and

e. Misrepresenting to Plaintiff and the Consumer Subclass that the subject of a transaction has been supplied in accordance with a previous representation when it had not, in violation of CAL. CIV. CODE § 1770(a)(16).

57. In addition, under California law, a duty to disclose arises in four circumstances: (1) when the defendant is in a fiduciary relationship with the plaintiff; (2) when the defendant has exclusive knowledge of material facts not known to the plaintiff; (3) when the defendant actively conceals a material fact from the plaintiff; and (4) when the defendant makes partial representations but also suppresses some material facts.

58. Defendant had a duty to disclose to Plaintiff and the Consumer Subclass that the Norton Products contained a core decomposer engine that ran on outdated third-party source code and failed to implement the principle of least privilege. Defendant had exclusive knowledge of the information at the time of sale, Defendant actively concealed this information from Plaintiff and the Consumer Subclass, and Defendant made partial representations to Plaintiff and the Consumer Subclass regarding the benefits and security features of the Norton Products.

59. Defendant violated the CLRA by supplying defective Norton Products and by further concealing the defect from Plaintiff and the Consumer Subclass.

60. Defendant's misrepresentations and omissions in violation of the CLRA were likely to mislead an ordinary consumer. Plaintiff and the Consumer Subclass reasonably understood Defendant's representations and omissions to mean that the Norton Products would provide security protections for typical consumer use and did not contain a defect that would compromise their performance.

61. Defendant's misrepresentations and omissions alleged herein were material in that a reasonable person would attach importance to the information and would be induced to act upon the information in making purchase decisions.

62. Plaintiff and the Consumer Subclass relied to their detriment on Defendant's misrepresentations and omissions in purchasing and licensing the Norton Products.

63. Plaintiff, on behalf of himself and the Consumer Subclass, demands judgment against Defendant under the CLRA for declaratory and injunctive relief.

64. Plaintiff, on behalf of himself and the Consumer Subclass, further intend to seek compensatory and punitive damages. Pursuant to CAL. CIV. CODE § 1782(a), Plaintiff will serve Defendant with notice of its alleged violations of the CLRA by certified mail return receipt requested. If, within thirty days after the date of such notification, Defendant fails to provide appropriate relief for its violations of the CLRA, Plaintiff will amend this Complaint to seek monetary damages.

65. Notwithstanding any other statements in this Complaint, Plaintiff, on behalf of himself and the Consumer Subclass, do not seek monetary damages in conjunction with his CLRA claim—and will not do so—until this thirty-day period has elapsed.

Second Claim for Relief

Violation of the California Song-Beverly Consumer Warranty Act, Cal. Civ. Code §§ 1790 et seq.

66. Plaintiff, individually and on behalf of the Consumer Subclass, incorporates by reference all of the allegations contained in the preceding paragraphs of this Complaint.

67. At all times of purchase, Defendant was in the business of manufacturing and selling network security software products, including the Norton Products.

68. The Norton Products were used and primarily bought for personal, family, or household purposes and are therefore consumer goods.

69. The Norton Products contained a core engine defect that exposed entire computer systems to potential malware and other untrusted files.

70. The Norton Products also contained outdated third-party source code that left unpatched hundreds of memory corruption bugs and other publicly known vulnerabilities.

71. These defects were present in the Norton Products when they left the exclusive control of Defendant and therefore existed during the duration of the warranty period.

72. The Norton Products were not of the same quality as those generally acceptable in the trade; were not fit for the ordinary purposes of secure antivirus protections for which the goods are used; were not adequately contained, packaged, and labeled; and did not conform to the promise and facts stated on the container and label.

73. Defendant, therefore, breached the implied warranty of merchantability, which by law is provided in every consumer agreement for the sale of goods, including for the sale of the Norton Products.

74. As a direct and proximate cause of Defendant's breach of the implied warranty of merchantability, Plaintiff and the Consumer Subclass have been damaged by receiving an inferior product from that which they were promised. Plaintiff and the Consumer Subclass, therefore, have the right to recover the purchase price of their Norton Products.

Third Claim for Relief

Violation of the California False Advertising Law ("FAL"), Cal. Bus. & Prof. §§ 17500 et seq.

75. Plaintiff, individually and on behalf of the Nationwide Class, incorporates by reference all of the allegations contained in the preceding paragraphs of this Complaint.

76. Plaintiff brings this claim individually and on behalf of the Nationwide Class against Defendant.

77. Defendant engaged in advertising and marketing to the public and offered for sale the Affected Products.

78. Defendant engaged in the advertising and marketing alleged herein with the intent to induce the sale of the Affected Products to consumers like Plaintiff.

79. Defendant's advertising and marketing representations regarding the Affected Products were false, misleading, and deceptive as set forth in detail above. Defendant also concealed the material information that the Affected Products contained a High Privilege Defect and Outdated Source Code Defect, which exposed entire computer systems to both known and unknown security vulnerabilities.

80. Defendant's misrepresentations and omissions alleged herein deceived or had the tendency to deceive the general public regarding the reliability of the Affected Products for ordinary consumer and business use.

81. Defendant's misrepresentations and omissions alleged herein were the type of misrepresentations that are material, i.e., a reasonable person would attach importance to them and would be induced to act on the information in making purchase decisions.

82. Defendant's misrepresentations and omissions alleged herein are objectively material to a reasonable purchaser of antivirus software, and therefore reliance upon such misrepresentations may be presumed as a matter of law.

83. At the time Defendant made the misrepresentations and omissions alleged herein, Defendant knew or should have known that they were untrue or misleading and acted in violation of CAL. BUS. & PROF. CODE §§ 17500 *et seq.*

84. As a result, Plaintiff and each member of the Nationwide Class has been injured, has lost money or property, and is entitle to relief. Plaintiff and the Nationwide Class seek restitution and all other relief permitted under CAL. BUS. & PROF. CODE §§ 17500 *et seq.*

Fourth Claim for Relief

Violation of the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. §§ 17200 et seq.

85. Plaintiff, individually and on behalf of the Nationwide Class, incorporates by reference all of the allegations contained in the preceding paragraphs of this Complaint.

86. Plaintiff brings this claim individually and on behalf of the Nationwide Class against Defendant.

87. Plaintiff has standing to pursue this claim because he suffered injury in fact and has lost money or property as a result of Defendant's actions as described *supra*. All Class Members overpaid for the Affected Products due to Defendant's concealment of the High Privilege Defect and the Outdated Source Code Defect.

88. Defendant's actions as alleged herein constitute an "unlawful" practice as encompassed by CAL. BUS. & PROF. CODE §§ 17200 *et seq.* because Defendant breached the CLRA, CAL. CIV. CODE §§ 1750 *et seq.* and the FAL, CAL. BUS. & PROF. CODE §§ 17500 *et seq*.

89. Defendant's actions as alleged herein constitute a "fraudulent" practice because, by representing that the Affected Products were reliable for ordinary consumer and business use but concealing the High Privilege Defect and Outdated Source Code Defect, Defendant's conduct was likely to deceive purchasers of antivirus products. Defendant's failure to disclose the defects constitutes a material omission in violation of the UCL.

90. Defendant's actions as alleged in this Complaint constitute an "unfair" practice, because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to Defendant's customers. The harm caused by Defendant's wrongful conduct outweighs any utility of such conduct and has caused substantial injury to Plaintiff and the Nationwide Class. Defendant could and should have chosen one of many reasonably available alternatives, including not selling antivirus products that contained fundamental defects with the core engine, disclosing the defects to prospective purchasers, and/or not representing that its products were suitable for ordinary consumer or business use. Additionally, Defendant's conduct was "unfair," because it violated the legislatively declared

policies reflected by California's strong consumer protection and false advertising laws, including the CLRA, CAL. CIV. CODE §§ 1750 *et seq.* and the FAL, CAL. BUS. & PROF. CODE §§ 17500 *et seq*.

91. As a result of Defendant's unlawful, fraudulent, and unfair conduct, Plaintiff and the Nationwide Class were damaged. Plaintiff and the Nationwide Class received an inferior product from that which they were promised. Had Defendant disclosed the High Privilege Defect and the Outdated Source Code Defect, Plaintiff and the Nationwide Class would not have purchased the Affected Products or would have paid substantially less.

92. Plaintiff and the Nationwide Class seek an order requiring Defendant to make full restitution of all monies they have wrongfully obtained from Class Members, as well as all other relief permitted under CAL. BUS. & PROF. CODE §§ 17200 *et seq*.

Fifth Claim for Relief

Quasi-Contract / Unjust Enrichment

93. Plaintiff, individually and on behalf of the Nationwide Class, incorporates by reference all of the allegations contained in the preceding paragraphs of this Complaint.

94. Plaintiff and Nationwide Class Members conferred non-gratuitous benefits on Defendant by purchasing and licensing the Affected Products. Defendant appreciated, accepted, and retained such benefits conferred by Plaintiff and members of the Nationwide Class with knowledge and awareness that they were receiving falsely and misleadingly advertised Affected Products which did not provide adequate security protections, as advertised.

95. Retention of such benefits under the circumstances is accordingly unjust and inequitable. Defendant profited from its unlawful, unfair, misleading, and deceptive practices at the expense of Plaintiff and members of the Nationwide Class. Absent Defendant's misleading and deceptive representations regarding the qualities and functionality of the Affected Products, Plaintiff and Nationwide Class Members would not have purchased the products at issue or would have paid substantially less for them. As such, Plaintiff and other members of the

Nationwide Class conferred an improper windfall upon Defendant, which knew of the windfall and has unjustly retained such benefits.

96. As a direct and proximate result of Defendant's unjust enrichment, under principles of equity and good conscience, Plaintiff and the Nationwide Class are entitled to full disgorgement and restitution of all amounts by which Defendant was enriched through its unlawful or wrongful conduct.

PRAYER FOR RELIEF

Plaintiff, on behalf of himself, the Nationwide Class, and the Consumer Subclass, requests that the Court order the following relief and enter judgment against Defendant as follows:

A. An order certifying the proposed Class under FED. R. CIV. P. 23;

B. An order appointing Plaintiff and his counsel to represent the Nationwide Class and the Consumer Subclass;

C. A declaration that Defendant has engaged in the illegal conduct alleged;

D. A judgment awarding Plaintiff, the Nationwide Class, and the Consumer Subclass restitution and disgorgement of all compensation obtained by Defendant from its wrongful conduct;

E. A judgment awarding Plaintiff and the Consumer Subclass compensatory and punitive damages pursuant to their breach of implied warranty claim in amounts to be proven at trial;

F. Prejudgment and postjudgment interest at the maximum allowable rate;

G. Attorneys' fees and expenses and the costs of this action; and

H. All other relief that the Court deems necessary, just, and proper.

DEMAND FOR JURY TRIAL

Pursuant to FED. R. CIV. P. 38(b), Plaintiff hereby demands a trial by jury.

Dated: April 2, 2018

SCHUBERT JONCKHEER & KOLBE LLP

BY: */s/ Willem F. Jonckheer*

Robert C. Schubert (S.B.N. 62684)
rschubert@sjk.law
Willem F. Jonckheer (S.B.N. 178748)
wjonckheer@sjk.law
Noah M. Schubert (S.B.N. 278696)
nschubert@sjk.law
Cassidy Kim (S.B.N. 315236)
ckim@sjk.law
Three Embarcadero Center, Suite 1650
San Francisco, CA 94111
Telephone: (415) 788-4220
Facsimile: (415) 788-0161

Attorneys for Plaintiff Montgomery Beyer

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
Montgomery Beyer
Individually and on Behalf of All Others Similarly Situated

(b) County of Residence of First Listed Plaintiff
(EXCEPT IN U.S. PLAINTIFF CASES)
Kent County

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Schubert Jonckheer & Kolbe LLP
Three Embarcadero Center, Suite 1650, San Francisco, CA 94111
(415) 788-4220

DEFENDANTS
Symantec Corporation

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☒ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

PRISONER PETITIONS

HABEAS CORPUS
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

OTHER
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee–Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent–Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 USC § 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation–Transfer ☐ 8 Multidistrict Litigation–Direct File

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d); Violations of Cal. Civ. Code §§1750 et seq, 1790 et seq, Cal. Bus. & Prof. Code §§ 17500 et seq., 17200 et seq.
Brief description of cause:
California Consumer Legal Remedies Act, Song-Beverly Consumer Warranty Act, California FAL and UCL, Unjust Enrichment

VII. REQUESTED IN COMPLAINT:
✔ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.
DEMAND $ > 5,000,000
CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S), IF ANY *(See instructions):*
JUDGE
DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)
(Place an "X" in One Box Only) ☐ **SAN FRANCISCO/OAKLAND** ☒ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 04/02/2018 **SIGNATURE OF ATTORNEY OF RECORD** /s/ Willem F. Jonckheer

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)."

II. Jurisdiction. The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

(4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked**.** (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Federal Rule of Civil Procedure 23.

Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. Divisional Assignment. If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of California

Montgomery Beyer, Individually and on Behalf of All Others Similarly Situated

Plaintiff(s)

v.

Symantec Corporation

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Symantec Corporation
CSC -Lawyers Incorporating Service
2710 Gateway Oaks Dr Ste 150N
Sacramento, CA 95833

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Robert C. Schubert
Willem F. Jonckheer
Schubert Jonckheer & Kolbe LLP
Three Embarcadero Center, Suite 1650
San Francisco, CA 94111

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk