`

KAPLAN FOX & KILSHEIMER LLP
Laurence D. King (SBN 206423)
lking@kaplanfox.com
Matthew B. George (SBN 239322)
mgeorge@kaplanfox.com
Mario M. Choi (SBN 243409)
mchoi@kaplanfox.com
350 Sansome Street, Suite 400
San Francisco, CA 94104
Telephone: 415-772-4700
Facsimile: 415-772-4707

KAPLAN FOX & KILSHEIMER LLP
Frederic S. Fox (*pro hac vice* to be sought)
ffox@kaplanfox.com
Donald R. Hall (*pro hac vice* to be sought)
dhall@kaplanfox.com
David A. Straite (*pro hac vice* to be sought)
dstraite@kaplanfox.com
Aaron L. Schwartz (*pro hac vice* to be sought)
aschwartz@kaplanfox.com
850 Third Avenue
New York, NY 10022
Telephone: (212) 687-1980
Facsimile: (212) 687-7714

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CITY OF PROVIDENCE, individually and on behalf of others similarly situated, Plaintiff, vs. INTEL CORP., a Delaware corporation, Defendant.	Case No. 5:18-cv-0894 **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

`

Plaintiff City of Providence ("Plaintiff" or "Providence") on behalf of itself and all other similarly situated, brings this action against Intel Corporation ("Defendant" or "Intel") based upon personal knowledge of the facts pertaining to itself, and upon information and belief as to all other matters, hereby alleges as follows:

NATURE OF THE CASE

1. This is a consumer protection action seeking injunctive relief and damages arising from Defendant Intel's sale of defective microprocessor chips to Plaintiff and Class Members for over twenty-three (23) years. Intel's microprocessor chips are defective because they possess significant security vulnerabilities that, if exploited, permit an adversary to access sensitive data stored elsewhere on the machine or in the "cloud." Defendant has been aware of these issues since at least June 2017, and thus far, is unable to offer consumers who purchased devices containing defective microprocessor chips that possess the significant security vulnerabilities described herein ("Affected Devices") an effective remedy.

2. Intel's primary business is the manufacture, sale, and supply of microprocessors for computer system manufacturers like Apple, Lenovo, HP, Dell, among others. Intel also manufactures motherboard chipsets, network interface controllers and integrated circuits, flash memory, graphics chips, embedded processors and other devices related to communications and computing. In 2016, Intel reported full-year revenue of $59.4 billion.

3. Intel's marketing scheme emphasizes its cutting-edge processor speed and security. Defendant repeatedly makes public representations that its machines meet certain performance metrics and possess security features embedded in the hardware, which provided "robust, vulnerability-resistant platforms."[1] For example, on July 11, 2017, Intel unveiled its "powerful" new Xeon Scalable processor, which broke "58 world [performance] records and counting," and was designed to offer businesses "security without compromise" while providing support to "an expanding range of existing and emerging data center, and network workloads, including cloud computing, high-performance computing

[1] Data *Protection with Hardware-Assisted Security, Ensuring Data Protection Through Innovation*, Intel.com, https://www.intel.com/content/www/us/en/data-security/security-overview-general-technology.html (last visited Jan. 31, 2018).

`

and artificial intelligence."[2] Similarly on January 19, 2016, Intel unveiled its then new 6th Gen Intel Core vPro processor for "full business productivity with up to 2.5 times the performance," which "lock[ed] the PC's Virtual Front Door with More than Password Protection."[3]

4. Unbeknownst to consumers purchasing Affected Devices, Defendant's microprocessors were defectively designed, exposing Plaintiff and Class Members' sensitive information to adversaries through at least two types of security vulnerabilities, dubbed "Meltdown" and "Spectre."

5. Meltdown affects virtually every machine that runs an Intel processor, or millions of machines world-wide, as it is imbedded in nearly all of Intel's "out-of-order" execution microprocessors manufactured since 1995.[4] Adversaries exploiting the Meltdown flaw attack the processors "out-of-order" execution to read arbitrary kernel-memory locations, including personal data and passwords. A Meltdown attack is independent of the operating system and does not rely on software vulnerabilities, which allows it to bypass security assumptions based on address space isolation and paravirtualized environments. An adversary that uses Meltdown to infect a system may readily access and read (without user permissions or privileges) the memory of other processes in that machine or the processes of linked virtual machines (*i.e.*, those in the cloud). In addition to Microsoft and other software manufacturers releasing patches, Defendant purports to have released software patches through original equipment manufacturer ("OEM") partners, which purport to protect 90 percent of machines affected by Meltdown.[5] The patches, however, are not 100 percent secure and has been shown to decrease the

[2] Press Release, Intel Unveils Powerful Intel Xeon Scalable Processors, Brining Next-Generation Business and Consumer Experiences to Life, Intel.com (July 11, 2017), *available at*: https://newsroom.intel.com/news-releases/intel-unveils-powerful-intel-xeon-scalable-processors-bringing-next-generation-business-consumer-experiences-life/ (last visited, Jan. 31, 2018).

[3] Press Release, Intel Transforms the Workplace with Latest 6th Generation Intel® Core™ vPro™ Processors, Intel.com (Jan. 19, 2016), *available at*: https://newsroom.intel.com/news-releases/intel-transforms-the-workplace-with-latest-6th-generation-intel-core-vpro-processors/ (last visited, Jan. 31, 2018).

[4] The only known exception microprocessors that do not appear to be affected by Meltdown are Intel's Itanium and pre-2013 Atoms microprocessors.

[5] Press Release, Intel Offers Security Issue Update, Intel.com (Jan. 9, 2018), *available at*: https://newsroom.intel.com/ news/intel-offers-security-issue-update/ (last visited, Feb. 7, 2018); *see also* Press Release, Intel Issues Updates to Protect Systems from Security Exploits, Intel.com (Jan. 4, 2018), *available at*: https://newsroom.intel.com/news-releases/intel-issues-updates-protect-systems-security-exploits/ (last visited, Feb. 7, 2018).

`

performance of the Intel microprocessor by as much as 30 percent. There are also growing reports that the patches are causing significant machine instability.

6. Spectre, meanwhile, exploits modern processor branch prediction and speculative execution by instructing the microprocessor to execute the destination of a branch ahead of time and then guessing the branch destination, depend on the memory value being read. The processor either discards wrong speculative guesses, or if right, commits to the speculative computation when the memory value finally arrives.[6] Speculative logic, therefore, has access to the machine's memory and registers and performs operations.[7] Spectre exploits this access. In a successful attack, the adversary induces the victim to "speculatively perform operations that would not occur during correct program execution and which leak the victim's confidential information via a side channel to the adversary."[8] Because Spectre accesses memory registers and performs software operations, securing devices affected by Spectre requires each individual software vendor update its potentially vulnerable applications. Spectre, therefore, is a difficult fix, and a problem that "will haunt us for quite some time."[9]

7. Defendant's microprocessors are defective because they expose sensitive consumer data to adversaries through the Meltdown and Spectre security vulnerabilities. Moreover, Intel has thus far been unable to offer consumers who purchased Affected Devices an effective repair or alternative solution. Intel itself admits that patches released for Meltdown and Spectre has caused instability in both newer and older machines.[10] Based on these issues, Intel has even gone so far as to advise consumers to stop installing current versions of its Spectre and Meltdown patches.[11] Defendant's defect

[6] P. Kocher et al., *Spectre Attacks: Exploiting Speculative Execution*, *available at*: https://spectreattack.com/spectre.pdf (last visited, Jan. 31, 2018).

[7] *Id.*

[8] *Id.*

[9] Meltdown and Spectre, Vulnerabilities in modern computers leak passwords and sensitive data, Graz University of Technology, available at: https://spectreattack.com//#faq-fix (last visited, Jan. 31, 2018).

[10] D. Allan, *Intel Admits that Meltdown and Spectre patch problems affect newer CPUs*, Techradar (Jan. 18, 2018), *available at*: http://www.techradar.com/news/intel-admits-that-meltdown-and-spectre-patch-problems-affect-newer-cpus (last visited, Feb. 7, 2018).

[11] N. Shenoy, *Root Cause of Reboot Issue Identified; Updated Guidance for Customers and Partners*, Intel.com (Jan. 22, 2018), *available at*: https://newsroom.intel.com/news/root-cause-of-reboot-issue-identified-updated-guidance-for-customers-and-partners/ (last visited, Feb. 7, 2018).

`

microprocessors exist in nearly every Intel central processing unit (CPU) manufactured in the last 23 years, and thus, Affected Devices include most personal computers, laptops, smartphones, tablets, and servers in use today.

8. Consumers, including Plaintiff and all members of the proposed Class, are consequently left between a rock and a hard place, forced to choose between: purchasing a new machine with a processor that does not contain the design defect; continuing to use Affected Devices with significant security vulnerabilities; or utilizing a “patched” machine that is not 100 percent secure, which also may suffer from significant performance degradation or other instability issues.

9. Intel’s conduct deprived consumers of the ability to make a meaningful choice from among competing processor products. Had consumers known of Intel’s defectively designed processors prior to purchase, consumers likely would have opted to purchase AMD or ARM processors, which are not affected by the Meltdown flaw and are often priced below comparable Intel processors.

10. Plaintiffs and the Class it seeks to represent are consumers who purchased Affected Devices. This lawsuit is brought to challenge Intel’s unfair business practices and practices pursuant to the consumer protection laws of Rhode Island, R.I. Gen. Laws § 6-13.1-2, and California, Bus. & Prof. Code. § 17200 and Civil Code § 1790. Plaintiff also brings a claim for: breach of express and implied warranty of marketability; unjust enrichment; and negligence.

11. Plaintiff requests the Court find Intel’s business practices constitute unfair business practices and enjoin Intel from selling affected machines in the future. Plaintiff further requests the Court order Defendant to: pay civil penalties pursuant to Cal. Bus. & Prof. Code § 17206 and R.I. Gen. Laws § 6-13.1-8; provide restitution to the Class of all money that may have been acquired by means of their unfair practices; award punitive damages to the extent they are justified; and pay attorneys’ fees and costs of litigation.

JURISDICTION AND VENUE

12. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed the sum value of $5,000,000, exclusive of interests and costs, and this is a class action in which more than two-thirds of the proposed plaintiff class, on the one hand, and Defendant, on the other, are citizens of different states.

`

13. This Court has personal jurisdiction over Defendant Intel Corp. because Intel's principle place of business is located in Santa Clara, California.

14. Venue is proper in this district under 28 U.S.C. § 1391 because Intel resides in this District and because a substantial portion of the actions and unfair practices described in this complaint, giving rise to Plaintiff's claims, were conducted in and orchestrated from this District by Intel, including Intel's design and marketing of the affected products. Moreover, Intel's wrongful actions harmed consumers residing in this District who purchased affected products in this District.

INTRADISTRICT ASSIGNMENT

15. Assignment is proper to the San Jose division of this District under Local Rule 3-2(c)-(e), as a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in Santa Clara County, where Intel is headquartered.

PARTIES

16. Plaintiff City of Providence is a municipal corporation with its principal address at Providence City Hall, 25 Dorrance Street, Providence, Rhode Island 02903. Providence has approximately 1400 municipal employees in over 35 departments. During the Class Period, Providence purchased hundreds of Affect Devices, including over 800 computers with defective Intel chips in the past five years.

17. Defendant Intel Corp., is a Delaware corporation with its principle place of business and corporate headquarters at 2200 Mission College Blvd. Santa Clara, CA 95052. At all relevant times, Intel was engaged in the business of designing, manufacturing, distributing, or selling electronic machine products, including the defective Intel microprocessors at issue.

FACTUAL ALLEGATIONS

18. The microprocessor is the CPU of a machine or computer system, processing system data and controlling other devices in the system. Founded in 1968, Intel created the world's first commercial microprocessor chip in 1971. Intel remains the top-selling microprocessor manufacturer, commanding in 2011, 79.3 percent of the personal computer microprocessor market and 84.4 percent of the mobile personal computer (laptop) market.

`

19. Intel offers microprocessors with one or multiple processor cores. Multi-core processors enable improved multi-tasking and energy-efficient performance by distributing computing tasks across two or more cores. Many of Intel's processor families integrate graphics functionality with the processor. Intel offers consumers a range of platforms based upon the following microprocessors:

- Intel® Quark™ Processor: Designed to integrate with applications where lower power, size, and cost take priority, including wearable technologies and the "next generation" of intelligent, connected devices;

- Intel® Atom™ x3, x5, and x7 Processors: Designed to deliver performance and mobility in tablets, and 2 in 1 systems and smartphones, as well as power-efficiency in microservers;

- Intel® Pentium® Processor: Designed to deliver quality, reliability and performance for work and play;

- Intel® Celeron® Processor: Designed to deliver quality, reliability, and performance for work and play;

- Intel® Core™ m3 Processor: Designed to deliver performance and mobility in thin, sleek, fanless devices

- Intel® Core™ i3 i5 and i7 Processors: Designed to deliver maximum performance and built-in security for the most demanding applications;

- Intel® Xenon® Processor: Designed to deliver advance performance and energy efficiency for cost effective solutions that scale to address diverse compute, network, and storage requirements;

- Intel® Xeon Phi™ Processor: Designed to deliver optimized performance for highly parallel workloads; and

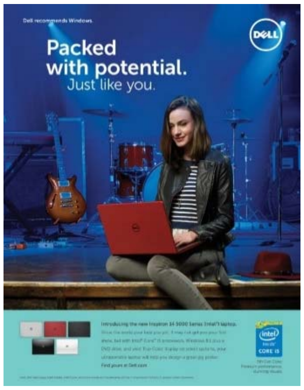
- Intel® Titanium® Processor: Designed to deliver mainframe reliability and enterprise performance on a platform sharing common characteristics of the rest of the data center.

20. Intel's microprocessors are found in a wide variety of products, including personal computer systems manufactured by Apple, Lenovo, HP, Dell, and Acer.[12] Intel ensures consumers purchasing such machines are aware that the machine is being run by an Intel processor. For example:

/ / /

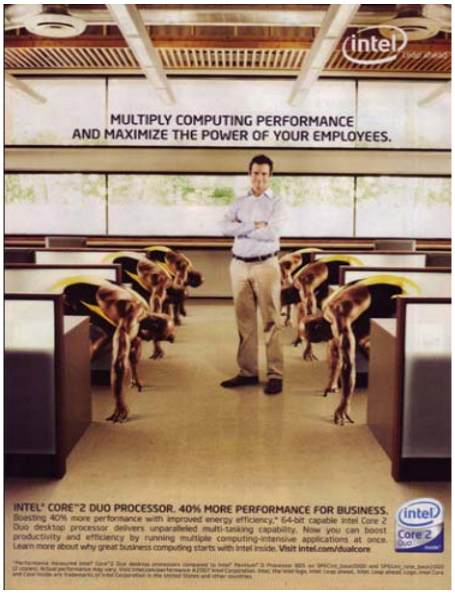
/ / /

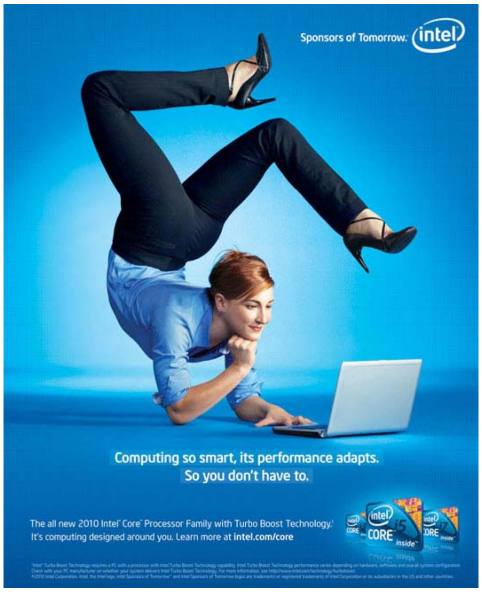
[12] In 2016, Dell accounted for 15 percent of Intel's total revenues while Lenovo accounted for 13 percent of total revenues and HP Inc. accounted for 10 percent of total revenues.


Dell recommends Windows.
Packed with potential. Just like you.
DELL
Introducing the new Inspiron 14 5000 Series Intel® laptop.
Find yours at Dell.com
intel inside CORE i5

YOGA Tab 3 Pro
A tablet with a built-in projector, so any surface can be a cinema.
Goodweird.
Lenovo
intel inside
Intel® Atom™ x5 processor
Intel Inside®. Better Experiences Outside.
Found at lenovo.com/YOGA

21. Moreover, for years, Intel has touted the performance of its processors in its marketing materials. For example, Intel broadly offers that "[w]hether you want the mobility of a tablet, the versatility of a 2 in 1, or the simplicity of an All-in-One desktop, Intel® processor technology delivers the powerful performance you need, for work and for play."[13] The performance of its processors is described as "stunning" or "[u]nlock[ing] your full potential."[14] As seen below, Intel advertisements similarly focus on processor speed and performance:


intel leap ahead
MULTIPLY COMPUTING PERFORMANCE AND MAXIMIZE THE POWER OF YOUR EMPLOYEES.
INTEL® CORE™2 DUO PROCESSOR. 40% MORE PERFORMANCE FOR BUSINESS.
Boasting 40% more performance with improved energy efficiency,* 64-bit capable Intel Core 2 Duo desktop processor delivers unparalleled multi-tasking capability. Now you can boost productivity and efficiency by running multiple computing-intensive applications at once. Learn more about why great business computing starts with Intel inside. Visit intel.com/dualcore
intel Core 2 Duo

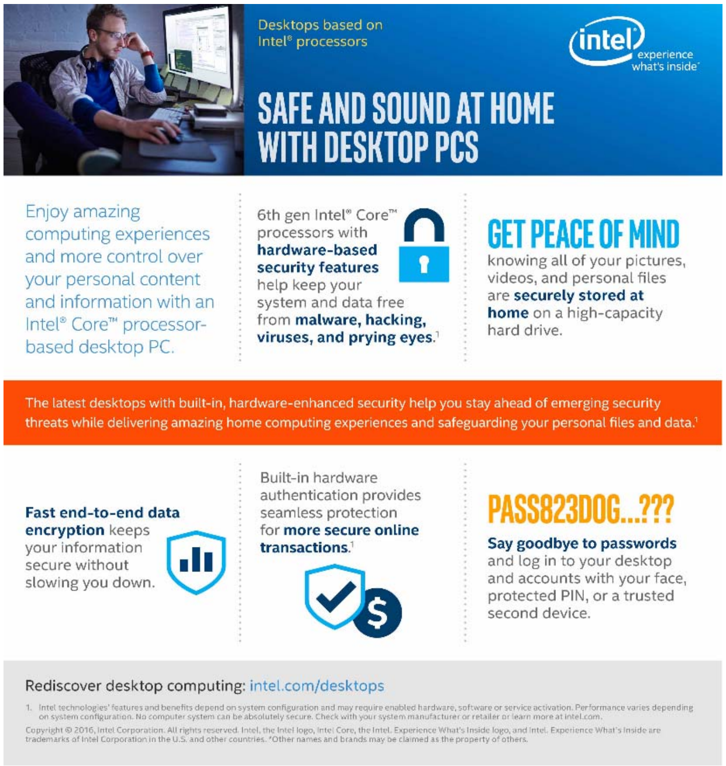

Sponsors of Tomorrow. intel
Computing so smart, its performance adapts.
So you don't have to.
The all new 2010 Intel® Core® Processor Family with Turbo Boost Technology.
It's computing designed around you. Learn more at intel.com/core
intel CORE i5 inside
intel CORE i7 inside

[13] *Performance Designed for the Way You Work and Play*, Intel.com, https://www.intel.com/content/www/us/en/ benchmarks/intel-product-performance.html (last visited, Jan. 31, 2018).

[14] *Id.*

`

22. Similarly, Intel regularly touts the security of its processors in its marketing materials. For example, Intel advertises that its processors offer "Data Protection with Hardware-assisted Security" and ensures "data protection through innovation."[15] In one instance, Intel emphasizes a "key component" of its approach to security is "providing more robust, vulnerability-resistant platforms. Security features are embedded in the hardware of Intel® processors, including three of Intel's newest server processors – the Intel® Xeon® processor E3 v3 family, the Intel® Xeon® processor E5 family, and the Intel® Xeon® processor E7 family, as well as the latest generation Intel® Core™ vPro™ processors." As seen below, Intel's advertisements routinely focus on security measures built into its processors.



Desktops based on Intel® processors

intel
experience what's inside™

SAFE AND SOUND AT HOME WITH DESKTOP PCS

Enjoy amazing computing experiences and more control over your personal content and information with an Intel® Core™ processor-based desktop PC.

6th gen Intel® Core™ processors with **hardware-based security features** help keep your system and data free from **malware, hacking, viruses, and prying eyes.**[1]

GET PEACE OF MIND knowing all of your pictures, videos, and personal files are **securely stored at home** on a high-capacity hard drive.

The latest desktops with built-in, hardware-enhanced security help you stay ahead of emerging security threats while delivering amazing home computing experiences and safeguarding your personal files and data.[1]

Fast end-to-end data encryption keeps your information secure without slowing you down.

Built-in hardware authentication provides seamless protection for **more secure online transactions.**[1]

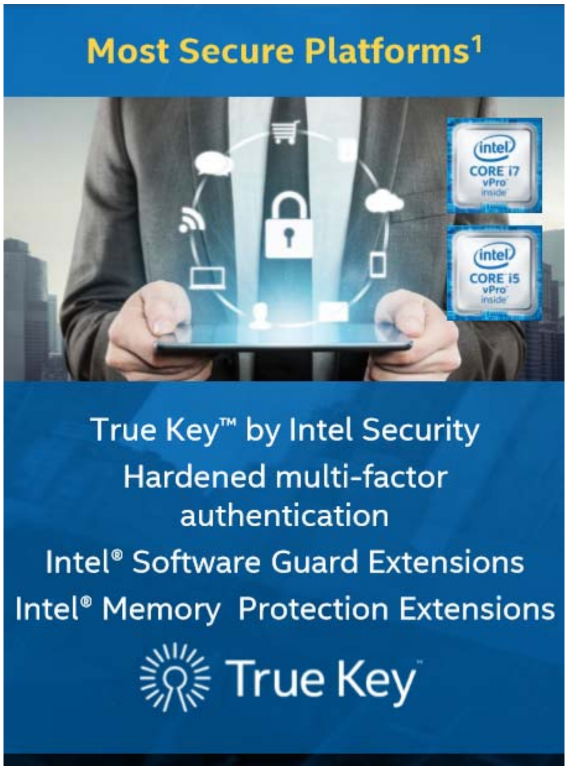
PASS823DOG...???

Say goodbye to passwords and log in to your desktop and accounts with your face, protected PIN, or a trusted second device.

Rediscover desktop computing: intel.com/desktops

1. Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Copyright © 2016, Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Core, the Intel. Experience What's Inside logo, and Intel. Experience What's Inside are trademarks of Intel Corporation in the U.S. and other countries. *Other names and brands may be claimed as the property of others.



Most Secure Platforms[1]

intel
CORE i7
vPro
inside
intel
CORE i5
vPro
inside

True Key™ by Intel Security
Hardened multi-factor authentication
Intel® Software Guard Extensions
Intel® Memory Protection Extensions

True Key

23. In June 2017, Intel learned its microprocessors suffered from several defects that allowed adversaries to access secure consumer data. These defects, colloquially known as Meltdown and Spectre, rendered Affected Devices unfit for their intended use.

[15] *Data Protection with Hardware-Assisted Security, Ensuring Data Protection Through Innovation,* Intel.com, https://www.intel.com/content/www/us/en/data-security/security-overview-general-technology.html (last visited, Jan. 31, 2018).

`

24. Intel initially sought to keep this information secret by imposing an "information embargo." The embargo was lifted January 2, 2018.

25. On January 3, 2018 Intel confirmed the presence of the design defects. It was later revealed the security flaws were discovered and reported by groups of independent researchers.[16]

A. The Meltdown Security Flaw

26. Meltdown affects nearly all machines using Intel microprocessors.[17] Meltdown exploits normal programs to read the contents of private kernel memory. Kernels are the most fundamental part of an operating system, used to manage the operation of the machine's memory and CPU time. A kernel is best understood as the program controlling all other programs in a machine. Machines never interact directly with the kernel, which runs behind-the-scenes unnoticed (except for the text logs it prints).

[16] Independent teams working on Meltdown include: Jann Horn at Google Project Zero; Werner Hass and Thomas Prescher at Cyberus Technology; and Daniel Gruss, Moritz Lipp, Stefan Mangard, and Michael Schwarz at Graz University of Technology. Independent teams working on Spectre include: Jann Horn at Google Project Zero; Paul Kocher in collaboration with Daniel Genkin at the University of Pennsylvania and University of Maryland, Mike Hamburg at Rambus, Moritz Lipp at Graz University of Technology, and Yuval Yarom at the University of Adelaide and Data61.

[17] The microprocessors affected include: Intel® Core™ i3 processor (45nm and 32nm), Intel® Core™ i5 processor (45nm and 32nm), Intel® Core™ i7 processor (45nm and 32nm), Intel® Core™ M processor family (45nm and 32nm), 2nd generation Intel® Core™ processors, 3rd generation Intel® Core™ processors, 4th generation Intel® Core™ processors, 5th generation Intel® Core™ processors, 6th generation Intel® Core™ processors, 7th generation Intel® Core™ processors, 8th generation Intel® Core™ processors, Intel® Core™ X-series Processor Family for Intel® X99 platforms, Intel® Core™ X-series Processor Family for Intel® X299 platforms, Intel® Xeon® processor 3400 series, Intel® Xeon® processor 3600 series, Intel® Xeon® processor 5500 series, Intel® Xeon® processor 5600 series, Intel® Xeon® processor 6500 series, Intel® Xeon® processor 7500 series, Intel® Xeon® Processor E3 Family, Intel® Xeon® Processor E3 v2 Family, Intel® Xeon® Processor E3 v3 Family, Intel® Xeon® Processor E3 v4 Family, Intel® Xeon® Processor E3 v5 Family, Intel® Xeon® Processor E3 v6 Family, Intel® Xeon® Processor E5 Family, Intel® Xeon® Processor E5 v2 Family, Intel® Xeon® Processor E5 v3 Family, Intel® Xeon® Processor E5 v4 Family, Intel® Xeon® Processor E7 Family, Intel® Xeon® Processor E7 v2 Family, Intel® Xeon® Processor E7 v3 Family, Intel® Xeon® Processor E7 v4 Family, Intel® Xeon® Processor Scalable Family, Intel® Xeon Phi™ Processor 3200, 5200, 7200 Series, Intel Atom® Processor C Series, Intel Atom® Processor E Series, Intel Atom® Processor A Series, Intel Atom® Processor x3 Series, Intel Atom® Processor Z Series, Intel® Celeron® Processor J Series, Intel® Celeron® Processor N Series, Intel® Pentium® Processor J Series, Intel® Pentium® Processor N Series (the "Affected CPUs"). *See Facts About the New Security Research Findings and Intel Products*, Intel.com, https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html (last visited, Jan. 4, 2018).

`

27. The central security feature of modern operating systems is memory isolation; the prevention of one application from accessing other application memory, or reading or writing kernel memory. Isolation "is a cornerstone of [the] computing environment and allows running multiple applications on personal devices or executing processes of multiple users on a single machine in the cloud."[18]

28. Meltdown overcomes memory isolation by enabling any user process to read the entire kernel memory of the machine, including all physical memory mapped in the kernel region, without exploiting any software vulnerability.

29. Meltdown exploits side-channel information available on most modern Intel microarchitectures through out-of-order execution. Out-of-order execution is used to significantly increase performance of processors by utilizing latencies of busy execution units. For example, instead of a memory fetch unit waiting for data arrival from memory, out-of-order execution looks ahead and schedules subsequent operations – *i.e.*, running machine operations out of order. Traditionally, out-of-order executions were ***not*** thought to present security issues because the processor discards the results of the memory it looks up if the instructions should not have been executed.

30. In June 2017, independent researchers discovered that out-of-order memory lookups influence the machine's cache, which may be detected through the cache side channel. Meltdown exploits the cache side channel to access the entire kernel memory through the out-of-order execution stream. The information may then be transmitted and reconstructed.

31. Meltdown may affect the entire physical memory on all the three major operating systems: Windows, Linux, and OS X.

32. In January 2018, Intel announced it has been working with its OEM partners since early December 2017 to release patches that cover 90 percent of machines sold in the last five (5) years. The patch relies on the countermeasure KAISER, variations of which have been applied to all three operating systems. However, because Meltdown bypasses the hardware-enforced isolation of security domains,

[18] Moritz Lipp *et. al*, *Meltdown*, *available at*: https://meltdownattack.com/meltdown.pdf (last visited, Jan. 31, 2018).

the KAISER software patch still leaves small amounts of memory exposed – the design of the x86 architecture permits several privileged memory locations to be mapped in user space.[19] While these memory locations do not possess "secrets," they might contain "pointers." Certain pointers may be used to again mount a side channel attack, breaking the kernel address space layout randomization ("KASLR").

33. To protect against leaking these pointers, KAISER uses a "trampoline function" – randomizing the kernel with a different offset than the remaining kernels. To be effective, however, trampoline code is required for every kernel memory mapped in user space. Thus, the proposed security fix significantly depreciates machine performance by as much as 30 percent by protecting each kernel memory with its own trampoline code. Machine slowdown has been confirmed by Microsoft.

34. Moreover, because certain information continues to remain exposed, and because trampoline code is not foolproof, some experts suggest the only means to truly secure machine memory, and thereby defeat Meltdown, is to design completely new hardware or implement a microcode update. At this time, Intel has not announced it will remedy defective products through replacing hardware or implementing a microcode update.

B. The Spectre Security Flaw

35. Researchers believe that almost every computing system, including laptops, desktops, smartphones, and cloud servers, is affected by the Spectre bug.[20]

36. Spectre is a related microarchitectural attack that exploits side channels to extract otherwise secret unavailable information. Microprocessors use "speculative execution" to increase performance by creating a checkpoint and then guessing (and prematurely executing) likely future execution paths. But for speculative execution, the microprocessor would be "idling" and waiting for the machine's memory to catch up.

[19] *Id.*

[20] S. Larson, *Major chip flaws affect billions of devices*, CNNTech (Jan. 4, 2018) *available at*: http://money.cnn.com/2018/ 01/03/technology/computer-chip-flaw-security/index.html (last visited, Jan. 31, 2018).

`

37. When the direction of control flow eventually arrives from the machine's memory, the processor checks the initial guess. If the guess is wrong, the processor discards the speculative execution by reverting the register state back to the stored checkpoint. The performance of the machine in such situations is comparable to "idling." However, if the processor guesses correctly, the speculative execution results are committed, resulting in significant performance gains.

38. Previously, speculative execution was not thought to give rise to any security implications because the processors are designed to revert the results of an incorrect speculative execution to their prior state to maintain correctness. Spectre, however, exploits speculative execution by tricking the microprocessor into speculatively executing instruction sequences that should ***not*** be executed during correct program execution.[21] Alternatively, Spectre may exploit speculative execution by executing previous sequences as "transient instruction" to read the entire memory address space of the machine.[22] Finally, Spectre attacks may be used to violate JavaScript in a website to extract login cookies for other sites from the browser's memory. In any of those three cases, Spectre allows an adversary to access sensitive security information across security domains.

39. Spectre, unlike Meltdown, cannot be fixed by a KAISER patch because an adversary may use the speculative execution of other programs and machines to exploit interactions between machines. Thus, the software of all programs must be updated to avoid being attacked by other programs. Intel has recently informed consumers and partners to stop installing recently released patches because the patches are causing devices to experience "higher than expected reboots and other unpredictable system behavior." Intel's patch issues have trickled down to other manufacturers and developers. VMWare, a cloud infrastructure company, issued a statement that it would delay microcode updates to resolve coordination issues between hardware and low-level software because of problems with Intel's firmware patches.[23] Similarly, Lenovo announced that due to stability concerns, it had to recall some firmware

[21] P. Kocher et. al. *Spectre Attacks: Exploiting Speculative Execution*, *available at*: https://spectreattack.com/spectre.pdf (last visited, Jan. 31, 2018).

[22] *Id*.

[23] L. Newman, *Meltdown and S0pectre patching has been a total train wreck*, Wired.com (Jan. 23, 2018), *available at*: https://www.wired.com/story/meltdown-spectre-patching-total-train-wreck/ (last visited, Feb. 7, 2018).

`

patches issued while Dell instructed consumers to "revert back to a previous BIOS version."[24] Linux creator Linus Torvalds has called the Intel patches for the Linux kernel "COMPLETE AND UTTER GARBAGE . . . They do things that do not make sense."[25]

C. Class Harm

40. Intel's security flaws are material and significant. The number of Affected Devices is in the millions and is thought to date back to machines manufactured in 1995. Plaintiff and Class Members would not have purchased any iterations of Affected Devices (or would not have purchased Affected Devices at the prices they did) had they known data stored on those machines may be compromised.

41. Competing processors, like AMD, are not affected by Meltdown. Moreover, AMD chips "are generally cheaper than comparable Intel chips."[26] For example, low-end, dual core AMD Sempron, Athlon, or A-series dual-core processors cost about $30, compared to low-end Intel chip, like the G3930 dual-core processor, which costs around $40.[27] Meanwhile, the price difference may be even more drastic for a higher-end processor: AMD's eight-core Ryzen 7 1700 costs $460 while Intel's cheapest eight-core processor, the Core i7-7820X costs $600.[28]

42. There is also no proposed cure to Affected Devices. Researchers suggest that because the security flaws reflect fundamental hardware defects, the only certain, 100 percent fix is through a recall. Intel has not offered a recall for devices affected by either Spectre or Meltdown.

43. Intel even admits that the Meltdown security flaws may only be "mitigated" by software or firmware upgrades – the remedy it has proposed.[29] Intel also admits that patches released to address both the Spectre and Meltdown issue impacts performance of Affected Devices, causes significant machine instability, or both. Independent analyses suggest the slowdown to Affected Devices might be

[24] *Id.*

[25] *Id.* (emphasis in original).

[26] M. Smith, *AMD v. Intel: How does tech's oldest rivalry look in 2018?* Digital Trends (Jan. 22, 2018) *available at*: https://www.digitaltrends.com/computing/here-we-explain-the-basic-differences-between-intel-and-amd-cpus/ (last visited Jan. 31, 2018).

[27] *Id.*

[28] *Id.*

[29] *Id.*

`

as high 30 percent, depending on the task and processor model.[30] Microsoft has also confirmed that updates that seek to address these issues affect device performance.

44. Intel does not challenge the presence of the microprocessor design defects or that Meltdown and Spectre expose Affected Devices to critical security vulnerabilities.

45. Intel's design defect constitutes an unfair trade practice under Rhode Island and California law. Intel's design defect also constitutes a violation breach of express and implied warranties of marketability, unjust enrichment, and negligence. Plaintiffs and members of the proposed Class have been directly and proximately harmed as a result of Intel's actions.

CLASS ACTION ALLEGATIONS

46. Plaintiff brings this action pursuant to the Federal Rules of Civil Procedure Rule 23 ("Rule 23") on behalf of itself and others similarly situated persons or entities (the "Class"), as defined below:

> All persons or entities in the United States who purchased or leased an Affected Device from: Intel; an authorized retail seller; or from a computer retail or computer manufacturer who installed an affected Intel processor inside the Affected Device

47. Plaintiff also brings this action pursuant to Rule 23 on behalf of itself and the following subclass for Class Members in Rhode Island (the" Rhode Island Subclass"):

> All persons or entities in the Rhode Island who purchased or leased an Affected Device from: Intel; an authorized retail seller; or from a computer retail or computer manufacturer who installed an affected Intel processor inside the Affected Device.

48. The nation-wide Class and the Rhode Island Subclass shall be collectively referred to as the Class throughout the complaint.

49. Excluded from the proposed class are Defendant; any entity in which Defendant has or had a controlling interest; any of Defendant's officers, directors, legal representatives, heirs, successors, and assigns; Plaintiff's counsel and anyone employed by Plaintiff's counsel; any Judge assigned to this action and his or her immediate family; and anyone who timely requests exclusion from the class.

[30] J. Leyden & C. Williams, *Kernel-memory-leaking Intel processor design flaw forces Linux*, *Windows redesign*, The Register (Jan. 2, 2018), *available at*: https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/ (last visited Jan. 31, 2018).

`

50. This action may be maintained on behalf of the class proposed above under the criteria of Rule 23 of the Federal Rules of Civil Procedure.

51. **Numerosity.** The class as presently proposed consists of owners of various affected machines, described above. Upon information and belief, the number of proposed Class Member exceeds tens of millions, and individual joinder of the purchasers of these machines would be impractical.

52. **Commonality and Predominance.** Common questions of law and fact exist as to members of the class and predominate over questions affecting only individual class members. These common questions include:

a. Whether affected processors possess the Meltdown security flaw;

b. Whether the affected processors possess the Spectre security flaw;

c. The extent to which the software updates fixed Affected Devices;

d. The extent to which the software update slowed the performance of Affected Devices;

e. Whether Defendant made any implied warranties in connection with the sale of Affected Devices;

f. Whether Defendant made any express warranties in connection with the sale of Affected Devices;

g. Whether Defendant breached any implied warranties relating to its sale of Affected Devices by failing to resolve the defects in the manner required by law;

h. Whether Defendant breached any express warranties relating to its sale of Affected Devices by failing to resolve the defects in the manner required by law;

i. Whether Defendant was unjustly enriched by the sale of Affected Devices;

j. Whether Defendant was negligent in selling Affected Devices; and

k. Whether Defendant violated applicable consumer protection laws by selling Affected Devices or by failing to disclose the design defect, and failing to provide the relief required by law.

`

53. **Typicality.** Plaintiff is a member of the proposed class and its claim is typical of the claims of the other members of the class. Plaintiff and Class Members all purchased Affected Devices. The injuries suffered by Plaintiff and members of the proposed Class flow from a common nucleus of operative facts, as set forth above. The defenses, if any, that may be asserted against Plaintiff are similar to the defenses, if any, that may be asserted against Class Members.

54. **Adequacy.** Plaintiff is an adequate representative of the Class because its interests do not conflict with the interests of the members of the Class it seeks to represent. Plaintiff has retained counsel competent and experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously. The interests of members of the Class will be fairly and adequately protected by Plaintiff and its counsel.

55. **Superiority.** The class action device is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and the Class Members. The relief sought per individual member of the Class is small given the burden and expense of individual prosecution of the potentially extensive litigation necessitated by the conduct of Defendant. Furthermore, it would be virtually impossible for the Class Members to seek redress on an individual basis. Even if the Class Members themselves could afford such individual litigation, the court system could not. Individual litigation of the legal and factual issues raised by the conduct of Defendant would increase delay and expense to all parties and to the court system. The Class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale and comprehensive supervision by a single court. Given the similar nature of the Class Members' claims and the absence of material differences in the state statutes and common laws upon which the Class Members' claims are based, a nationwide Class will be easily managed by the Court and the parties.

FIRST CAUSE OF ACTION

(For Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et. seq*.)

56. Plaintiff incorporates by reference the foregoing paragraphs.

/ / /

/ / /

`

57. Defendant's acts and practices, as alleged in this complaint, constitute unfair, unlawful and fraudulent business practices in violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et. seq*.

58. Defendant engaged and continues to engage in unfair business practices by selling microprocessor chips it designed to consumers when it knew those microprocessor chips were designed defectively as alleged herein. Moreover, the resolution offered by Intel for Meltdown security flaw still leaves the machine vulnerable to attack and significantly reduces machine performance while also causing machine instability.

59. Defendant's business practices were and are unscrupulous, unethical, and substantially injurious to consumers. There is no legitimate business reason for Defendant's business practice such that the utility of its business practice outweighs the harm to consumers. Furthermore, Defendant's business practice undermines this State's fundamental policy against unfair and sharp business practices that are likely to deceive or mislead consumers, and which undercuts trust and fair competition in the consumer marketplace.

60. Plaintiff and Class Members have standing to challenge Defendant's unfair, unlawful and fraudulent business practices on behalf of the public pursuant to California Business and Professions Code § 17204, since it suffered injury in fact and lost money or property in the form of reduced value of machine's running Intel microprocessors because of Defendant's practices. For years, Plaintiff and Class Members have purchased Affected Devices.

61. The applicable statute of limitations for the unfair competition law claim is tolled by the discovery rule and concealment.

62. Plaintiff and Class Members hereby seek money damages and restitution in an amount to be determined at trial. Plaintiff and Class Members also seek appropriate equitable relief pursuant to California Business & Professions Code § 17203, including an injunction prohibiting Defendant from engaging in the same or similar unfair business practices in the future, civil penalties, restitution of money that may have been acquired by Defendant's unfair business practices, and attorneys' fees and costs of litigation. The entry of injunctive relief is of particular importance in this matter as it is necessary to secure a fair consumer marketplace.

`

SECOND CAUSE OF ACTION

(For Violation of the Song-Beverly Consumer Warranty Act,
Cal. Civ. Code § 1790, *et. seq.*)

63. Plaintiff incorporates by reference the foregoing paragraphs.

64. Plaintiff and Class Members are "buyers," and Defendant is a "manufacturer," "distributor," or "retail seller" of a "consumer good" – *i.e.*, microprocessors – under Cal. Civ. Code § 1791.

65. Every purchase or lease of Defendant's processors or machines containing Defendant's processors to Plaintiff and Class Members included an implied warranty of merchantability whereby Defendant warranted that its processors were fit for the ordinary purpose and particular purpose for which they were used.

66. Defendant breached its implied warranty to Plaintiff and Class Members when it sold Affected Devices to Plaintiff and Class Members. Defendant knew or should have known those Affected Devices were not fit for the ordinary purpose and particular purpose for which they were used. Specifically, microprocessors sold contained certain design defects (*i.e.*, associated security, performance, and instability issues) alleged herein.

67. Defendant's actions deprived Plaintiff and Class Members of the benefit of their bargain, and caused Defendant's microprocessors to be worth significantly less than what Plaintiff and Class Members paid.

68. As a direct and proximate result of Defendant's breach of its duties, Plaintiff and Class Members received goods whose condition substantially impairs their value. Plaintiff and Class Members have been damaged by the diminished value of Defendant's microprocessors.

69. The applicable statute of limitations for violation of the Song-Beverly Consumer Warranty Act is tolled by the nature of the latent defect described herein, the discovery rule, and concealment.

70. Pursuant to Cal. Civ. Code §§ 1791.1 and 1794, Plaintiff and Class Members hereby seek money damages in an amount to be determined at trial. Plaintiff and Class Members also seek appropriate equitable relief, including: at their election, the right to revoke acceptance of Affected Devices; overpayment; diminution in value; an injunction prohibiting Defendant from engaging in the

`

same or similar business practices in the future; and other such relief that the Court may see as just and warranted. Finally, Plaintiff and Class Members seek reasonable attorney fees and costs, to which they are entitled pursuant to Cal. Civ. Code § 1794.

THIRD CAUSE OF ACTION

(For Violation of Rhode Island's Unfair Competition Law
R.I. Gen. Laws §§ 5-13.1-1, *et seq.*)

71. Plaintiff incorporates by reference the foregoing paragraphs.

72. Defendant's acts and practices, as alleged in this complaint, constitute unfair, unlawful and fraudulent business practices in violation of the Rhode Island Unfair Trade Practice and Consumer Protection Act, R.I. Gen. Laws §§ 5-13.1-1, *et seq.*

73. Defendant engaged and continues to engage in unfair business practices by selling Affected Devices to consumers when it knew those microprocessor chips have significant security, stability, and performance issues, as alleged herein. The resolution offered by Defendant for Meltdown and Spectre may still leave the machine vulnerable to attack while significantly reduces machine performance and stability.

74. Defendant's business practices are unscrupulous, unethical, and substantially injurious to consumers. There is no legitimate business reason for Intel's business practice such that the utility of its business practice outweighs the harm to consumers. Furthermore, Defendant's business practice undermines this State's fundamental policy against unfair and sharp business practices that are likely to deceive or mislead consumers, and which undercut trust and fair competition in the consumer marketplace.

75. Plaintiff and Class Members have standing to challenge Defendant's unfair, unlawful and fraudulent business practices on behalf of the public pursuant to Rhode Island's Unfair Trade Practice and Consumer Protection Act, R.I. Gen. Laws §§ 6-13.1-5.2, *et seq.*, because it suffered injury in fact and lost money or property in the form of reduced value of machine's running Defendant's microprocessors because of Defendant's practices. For years, Plaintiff and Class Members have purchased Affected Devices.

76. The applicable statute of limitations for the unfair competition law claim is tolled by the discovery rule and concealment.

`

77. Plaintiff and Class Members hereby seeks money damages and restitution in an amount to be determined at trial. Plaintiff and Class Members also seek appropriate equitable relief pursuant to Rhode Island's Unfair Trade Practice and Consumer Protection Act, R.I. Gen. Laws §§ 6-13.1-5.2, *et seq.*, including an injunction prohibiting Defendant from engaging in the same or similar unfair business practices in the future, civil penalties, restitution of money that may have been acquired by Defendant's unfair business practices, and attorneys' fees and costs of litigation. The entry of injunctive relief is of particular importance in this matter as it is necessary to secure a fair consumer marketplace.

FOURTH CAUSE OF ACTION

(For Violation of the Magnuson-Moss Warranty Act, 15 U.S.C. § 2301, *et. seq.*)

78. Plaintiff incorporates by reference the foregoing paragraphs.

79. The Magnuson-Moss Warranty Act ("MMWA") governs warranties on consumer products, and was designed to prohibit manufacturers from using unfair or misleading warranties on consumer products.

80. Plaintiff and Class Members are "consumers" under MMWA because they purchased or leased (not for the purpose of resale) a consumer product.

81. Defendant is a "supplier" because it engaged "in the business of making a consumer product directly or indirectly available to consumers." Defendant is also a "warrantor" under MMWA because, as a supplier, it is obligated under an implied warranty. Defendant impliedly warranted that Intel's chips were merchantable and fit for the ordinary and particular purpose for which they were used.

82. Defendant breached its implied warranty to Plaintiff and Class Members when it sold Affected Devices to Plaintiff and Class Members. Defendant knew or should have known Affected Devices were not fit for the ordinary purpose and particular purpose for which they were used. Specifically, microprocessors sold contained certain design defects (*i.e.*, associated security, stability, and performance issues) alleged herein.

83. Plaintiff and Class Members were directly and proximately damaged as a result of Defendant's breach of the implied warranty of merchantability.

84. It would be unconscionable to permit Defendant to disclaim, modify, or limit its implied warranties under MMWA. Defendant knowingly sold or leased defective products or machines

`

containing defective products. Defendant was notified by independent research teams that its products were defectively designed, a fact that Defendant knew or should have known much earlier. Defendant knew or should have known it was selling or leasing Affected Devices, yet it did not disclose these design defects to Plaintiff or Class Members. Affording Defendant a reasonable opportunity to cure its breach of implied warranties would be unnecessary and futile because Defendant knew and concealed the defects alleged herein, and in any event, is unable or has refused to adequately repair or replace Affected Devices at no cost to Plaintiff or Class Members.

85. The applicable statute of limitations for the MMWA claim is tolled by the discovery rule and concealment.

86. Plaintiff and Class Members hereby seek money damages and restitution in an amount to be determined at trial. Plaintiff and Class Members have complied with all obligations under the MMWA, or have otherwise been excused from performance of such obligations due to Defendant's conduct described herein.

87. Plaintiff and Class Members also seek appropriate equitable relief pursuant to MMWA, 15 U.S.C. § 2310, including an injunction prohibiting Defendant from engaging in the same or similar business practices in the future, restitution of money that may have been acquired by Defendant's breach of its implied warranty of merchantability, and other such relief that the Court may see as just and warranted.

FIFTH CAUSE OF ACTION

(For Breach of Implied Warranty)

88. Plaintiff incorporates by reference the foregoing paragraphs.

89. The Uniform Commercial Code ("U.C.C.") § 2-314 provides for an implied warranty of merchantable goods in every contract for the sale of goods between a merchant and a consumer. Defendant is and at all relevant times was a "merchant" and seller of "goods," as defined by the U.C.C.

90. Defendant impliedly warranted that its processors were in merchantable condition and fit for the ordinary purpose for which Defendant marketed its processors to be used.

91. Plaintiff and Class Members purchased or leased Affected Devices from Defendant.

/ / /

`

92. Defendant breached its implied warranty of merchantability. The Affected Devices sold or leased by Defendant to Plaintiff and Class Members was not fit for the ordinary purpose for which Defendant marketed its processors to be used due to the design defects (and associated security, stability, and performance issues) alleged herein.

93. It would be unconscionable to permit Defendant to limit or disclaim its implied warranties as it knowingly sold or leased Affected Devices. Defendant was notified by independent research teams that its products were defectively designed, a fact that Defendant knew or should have known much earlier. Defendant knew or should have known it was selling or leasing Affected Devices, yet it did not disclose these design defects to Plaintiff or Class Members. Affording Defendant a reasonably opportunity to cure its breach of implied warranties would be unnecessary and futile because Defendant knew and concealed the defects alleged herein, and in any event, is unable or has refused to adequately repair or replace Affected Devices at no cost to Plaintiff or Class Members.

94. Moreover, Defendant, as a manufacturer of consumer goods is precluded from excluded or modifying an implied warranty of merchantability or limiting customer remedies for breach of this warranty.

95. The applicable statute of limitations for the implied warranty claim is tolled by the discovery rule and concealment.

96. Defendant's warranties were designed to influence consumers purchasing Affected Devices.

97. As a direct and proximate result of Defendant's breach of its implied warranty of merchantability, Plaintiff and Class Members were damaged in an amount to be proven at trial. Plaintiff and Class Members have complied with all obligations under this warranty, or have otherwise been excused from performance of such obligations due to Defendant's conduct described herein.

SIXTH CAUSE OF ACTION

(For Breach of Express Warranty of Marketability)

98. Plaintiff incorporates by reference the foregoing paragraphs.

/ / /

/ / /

`

99. Defendant is a "merchant" within the meaning of the U.C.C. because it designed, manufactured, advertised, and distributed the defective processors at issue in this litigation. Moreover, the defective processors are "goods" within the meaning of the U.C.C.

100. In connection with the sale or lease of Affected Devices, Defendant represented that its processors were fit for the ordinary purpose for which Defendant marketed its processors to be used. However, due to the design defects (and associated security, stability, and performance issues) alleged herein, the processors were not fit for the ordinary purpose for which Defendant marketed its processors.

101. Defendant's affirmation of facts and promises relating to its defective processors became part of the bargain of sale, and created an express warranty that the processors would conform to Defendant's affirmations and promises.

102. Defendant's express warranties run to Plaintiff and Class Members either directly or as third-party beneficiaries.

103. Defendant's breached its express warranties by selling or leasing Affected Devices to Plaintiff and Class Members that did not conform to Defendant's affirmations and promises.

104. The applicable statute of limitations for the express warranty claim is tolled by the discovery rule and concealment.

105. Defendant's breach of express warranties directly and proximately caused damages, injury in fact, and ascertainable loss to Plaintiff and Class Members in an amount to be determined at trial.

106. All conditions precedent to this claim have been satisfied.

SEVENTH CAUSE OF ACTION

(For Unjust Enrichment)

107. Plaintiff incorporates by reference the foregoing paragraphs.

108. Defendant was and should have been reasonably expected to manufacture and sell microprocessors free from the design defects alleged herein. Defendant benefited from the purchase or lease of Affected Devices by Plaintiff and Class Members.

109. There is privity between Defendant and Plaintiff and Class Members because Defendant intended Plaintiff and Class Members to be purchasers or lessors of Affected Devices.

/ / /

`

110. Defendant unjustly profited from the sale and lease of Affected Devices at inflated prices due to materially deceptive advertising, marketing, false representations, omissions, and concealments. But for Defendant's materially deceptive advertising, marketing, false representations, omissions, and concealments, Plaintiff and Class Members would not have purchased or leased Affected Devices at the prices paid. As a result, Defendant received ill-gotten gains, benefits, and profits.

111. Defendant has been unjustly enriched at the expense of Plaintiff and Class Members because it did not provide the benefits represented. It would be inequitable for Defendant to retain those ill-gotten gains, benefits, and profits.

112. The applicable statute of limitations for the unjust enrichment claim is tolled by the discovery rule and concealment.

113. Due to Defendant's unlawful, unjust, and inequitable conduct, Plaintiff and Class Members are entitled to restitution of an amount to be proven at trial that represents Defendant's ill-gotten gains, benefits, and profits, including interest.

EIGHTH CAUSE OF ACTION

(For Negligence)

114. Plaintiff incorporates by reference the foregoing paragraphs.

115. Defendant owed a duty of care to Plaintiff and Class Members to exercise reasonable care to safeguard sensitive information stored on machines purchased by consumers that utilize Defendant microprocessors from foreseeable security vulnerabilities arising due to the microarchitectural design of those microprocessors.

116. Defendant's duty to Plaintiff and Class Members included, *inter alia*, designing, maintaining, monitoring, and testing microprocessors to ensure it detected microarchitectural issues, such as the design defects alleged herein, in a timely manner.

117. In marketing and selling microprocessors to consumers, Defendant also had a duty to ensure its microprocessors could reasonably function at the quality, stability, and processing speeds represented.

118. Finally, Defendant owed a duty to disclose any material defects, like the design defect alleged herein, to Plaintiff and Class Members in a timely manner.

`

119. Defendant breached each of these duties.

120. But for Defendant's breach of these duties, Plaintiff and Class Members would not have purchased or leased Affected Devices at the prices paid.

121. Plaintiff and Class Members were foreseeable victims of Defendant's wrongdoing. Defendant knew or should have known that its processors would cause damages to Plaintiff and Class Members.

122. The applicable statute of limitations for the negligence claim is tolled by the discovery rule and concealment.

123. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been damaged in an amount to be proven at trial. Damages include, but are not limited to, compensatory damages, incidental and consequential damages, punitive damages, and any other damage allowed by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays that the Court enters judgment in their favor and against Intel as follows:

A. An order certifying the proposed class, or an alternative class that the Court may find appropriate under Rule 23 of the Federal Rules of Civil Procedure, directing that Plaintiff's claims proceed on a class-wide basis, and appointing Plaintiff and her counsel to represent the class;

B. An order and/or judgement enjoining Defendant from manufacturing microprocessor chips that contain known security flaws;

C. An order and/or judgment requiring Defendant to make restitution to Plaintiff of money that may have been acquired by means of its unfair practices;

D. An order granting reasonable attorneys' fees and costs, as well as pre- and post-judgment interest at the maximum legal rate; and

/ / /

/ / /

/ / /

/ / /

`

E. Such other and further relief as this Court may deem appropriate.

Respectfully submitted,

DATED: February 12, 2018

KAPLAN FOX & KILSHEIMER LLP

By: /s/ *Laurence D. King*
Laurence D. King

Laurence D. King (SBN 206423)
lking@kaplanfox.com
Matthew B. George (SBN 239322)
mgeorge@kaplanfox.com
Mario M. Choi (SBN 243409)
mchoi@kaplanfox.com
350 Sansome Street, Suite 400
San Francisco, CA 94104
Telephone: 415-772-4700
Facsimile: 415-772-4707

KAPLAN FOX & KILSHEIMER LLP
Frederic S. Fox (*pro hac vice* to be sought)
ffox@kaplanfox.com
Donald R. Hall (*pro hac vice* to be sought)
dhall@kaplanfox.com
David A. Straite (*pro hac vice* to be sought)
dstraite@kaplanfox.com
Aaron L. Schwartz (*pro hac vice* to be sought)
aschwartz@kaplanfox.com
850 Third Avenue
New York, NY 10022
Telephone: (212) 687-1980
Facsimile: (212) 687-7714

Attorneys for Plaintiff

JS-CAND 44 (Rev. 06/17)

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

CITY OF PROVIDENCE, individually, and on behalf of all others similarly situated,

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Laurence D. King / KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400, San Francisco, CA 94104
(415) 772-4700; lking@kaplanfox.com

DEFENDANTS

INTEL 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

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

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

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. sec. 1332(d)

Brief description of cause:
Violation of the Consumer Protection Act for false representations

VII. REQUESTED IN COMPLAINT:

☑ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes □ No

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

JUDGE Edward J. Davila

DOCKET NUMBER 5:18-cv-00046-EJD

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) □ **SAN FRANCISCO/OAKLAND** ☒ **SAN JOSE** □ **EUREKA-MCKINLEYVILLE**

DATE 02/12/2018

SIGNATURE OF ATTORNEY OF RECORD /s/ Laurence D. King

Print Save As... Reset

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.