

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION**

JASON JONES , on behalf of himself)
and all others similarly situated,)
) Civil No. 1:18-CV-00029
Plaintiff,)
)
v.) CLASS ACTION COMPLAINT
)
INTEL CORPORATION ,) JURY TRIAL DEMANDED
)
Defendant.)

CLASS ACTION COMPLAINT

Plaintiff Jason Jones (“Plaintiff”), on behalf of himself and all others similarly situated, by counsel, brings this Class Action Complaint against Defendant Intel Corporation (“Intel” or “Defendant”), and alleges as follows:

INTRODUCTION

1. Plaintiff brings this action against Intel on behalf of all persons in the State of Indiana who purchased a defective Intel core processor (“CPUs”).

2. Defendant Intel’s x86-64x CPUs suffer from a security defect, which causes the CPUs to be exposed to troubling security vulnerabilities by allowing potential access to extremely secure kernel data (the “Defect”). The only way to “patch” this vulnerability requires extensive changes to the root levels of the Operating System which will dramatically reduce performance of the CPU. The Defect renders the Intel x86-64x CPUs unfit for their intended use and purpose. The Defect exists in all Intel x86-64x CPUs manufactured since at least 2008. The

x86-64x CPU is, and was, utilized in the majority of all desktop, laptop computers, and servers in the United States

3. To date, Defendant has been unable or unwilling to repair the Defect or offer Plaintiff and Class members a non-defective Intel CPU or reimbursement for the cost of such CPU and the consequential damages arising from the purchase and use of such CPUs. Indeed, there does not appear to be a true “fix” for the Defect. The security “patch,” while expected to cure the security vulnerabilities, will dramatically degrade the CPU’s performance. Therefore, the only “fix” would be to exchange the defective x86-64x processor with a device containing a processor not subject to this security vulnerability. In essence, Intel x86-64x CPU owners are left with the unappealing choice of either purchasing a new processor or computer containing a CPU that does not contain the Defect, or continuing to use a computer with massive security vulnerabilities or one with significant performance degradation.

4. The CPUs Defendant manufactured and sold to Plaintiff and Class members were not merchantable and were not fit for the ordinary and particular purposes for which such goods are used in that the CPUs suffer from a critical security defect, requiring an OS-level software patch that will degrade the performance of the CPU.

5. Having purchased a CPU that suffers from this Defect, Plaintiff and Class members suffered injury in fact and a loss of money or property as a result of Defendant’s conduct in designing, manufacturing, distributing and selling defective

CPUs. Intel has failed to remedy this harm, and has earned and continues to earn substantial profit from selling defective CPUs.

JURISDICTION & VENUE

6. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2) because this is a class action involving more than 100 class members in which matter in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, and in which at least one member of the class of plaintiffs is a citizen of a state different from a defendant.

7. Venue is proper in this Court under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

PARTIES

8. Plaintiff Jason Jones is, and at all relevant times was, a citizen of the State of Indiana. On or about November 2017, Plaintiff Jones purchased an Intel Core i7-8700KCPU from Newegg.com which he then inserted into his computer. Plaintiff Jones uses his computer for gaming and he specifically purchased the Intel Core i7-8700KCPU for a fast and ideal gaming experience. He was unaware of the CPU Defect described in this Complaint prior to his purchase. Had Defendant disclosed such material facts Plaintiff Jones would not have purchased the Intel Core i7-8700KCPU or paid the price he did.

9. Defendant Intel Corporation is, and at all relevant times was, a citizen of the State of Delaware and of the State of California, as it is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business in California.

FACTUAL ALLEGATIONS

10. For at least 10 years, Defendant has marketed, distributed, and warranted these defective Intel CPUs in Indiana and throughout the United States.

11. On or about November 21, 2017, news stories revealed that a large number of Intel processors contain a serious design flaw that creates significant security vulnerabilities for any device that uses Intel processors. The security flaw is in Intel's x86-64 hardware which was first introduced in 2004 and is still in use in the majority of today's modern-day processors.

12. The design defect is believed to exist in almost every Intel processor made since at least 2004 regardless of the operating system. Intel's x86-64x processors are the most widely-used chips in virtually all desktop and laptop computers. The Intel processors are also used in most of the large, cloud based servers such as those from Google, Microsoft and Amazon.

13. On or about January 2, 2018, it was revealed that the "patch" to this security vulnerability would lead to substantial CPU performance degradation. The "patch" would require root level changes to the Operating System resulting in a substantial decrease in CPU performance as much as 30-50% by some estimates.

The Intel CPU Defect

14. Intel CPUs have a Defect that is inherent within the CPU itself and/or the result of software or hardware design or manufacturing flaws. Fixing the Defect using an OS-level software patch causes the CPUs to slow down.

15. As *The Register* reported on January 2, 2018:

A fundamental design flaw in Intel's processor chips has forced a significant redesign of the Linux and Windows kernels to defang the chip-level security bug.

Programmers are scrambling to overhaul the open-source Linux kernel's virtual memory system. Meanwhile, Microsoft is expected to publicly introduce the necessary changes to its Windows operating system in an upcoming Patch Tuesday: these changes were seeded to beta testers running fast-ring Windows Insider builds in November and December.

Crucially, these updates to both Linux and Windows will incur a performance hit on Intel products. The effects are still being benchmarked, however we're looking at a ballpark figure of five to 30 per cent slow down, depending on the task and the processor model. More recent Intel chips have features – such as PCID – to reduce the performance hit. [...]

Similar operating systems, such as Apple's 64-bit macOS, will also need to be updated – the flaw is in the Intel x86-64 hardware, and it appears a microcode update can't address it. It has to be fixed in software at the OS level, or go buy a new processor without the design blunder.

Details of the vulnerability within Intel's silicon are under wraps: an embargo on the specifics is due to lift early this month, perhaps in time for Microsoft's Patch Tuesday next week. Indeed, patches for the Linux kernel are available for all to see but comments in the source code have been redacted to obfuscate the issue.

(See *Kernel-memory-leaking Intel processor design flaw forces Linux, Windows redesign: Speed hits loom, other OSes need fixes*, *The Register*, https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/ (last visited January 4, 2018).)

16. Subsequent reporting by *The Register* found that Apple has already provided a software patch for the defect: “Finally, macOS has been patched to counter the chip design blunder since version 10.13.2, according to operating system kernel expert Alex Ionescu.” (*Id.*)

17. The Defect’s presence is material because fixing the Defect reduces the performance of the CPUs thereby causing the CPUs to slow down from the performance specifications that Defendant promised and that consumers expected when buying a computer with an Intel CPU. The Defect is also material because of the security vulnerabilities Intel based CPUs are exposed to.

18. As *The Register* article further explains:

Impact

It is understood the bug is present in modern Intel processors produced in the past decade. It allows normal user programs – from database applications to JavaScript in web browsers – to discern to some extent the layout or contents of protected kernel memory areas.

The fix is to separate the kernel’s memory completely from user processes using what’s called Kernel Page Table Isolation, or KPTI. [...]

Whenever a running program needs to do anything useful – such as write to a file or open a network connection – it has to temporarily hand control of the processor to the kernel to carry out the job. To make the transition from user mode to kernel mode and back to user mode as fast and efficient as possible, the kernel is present in all

processes' virtual memory address spaces, although it is invisible to these programs. When the kernel is needed, the program makes a system call, the processor switches to kernel mode and enters the kernel. When it is done, the CPU is told to switch back to user mode, and reenter the process. While in user mode, the kernel's code and data remains out of sight but present in the process's page tables. [...]

These KPTI patches move the kernel into a completely separate address space, so it's not just invisible to a running process, it's not even there at all. Really, this shouldn't be needed, but clearly there is a flaw in Intel's silicon that allows kernel access protections to be bypassed in some way.

The downside to this separation is that it is relatively expensive, time wise, to keep switching between two separate address spaces for every system call and for every interrupt from the hardware. These context switches do not happen instantly, and they force the processor to dump cached data and reload information from memory. ***This increases the kernel's overhead, and slows down the computer.***

Your Intel-powered machine will run slower as a result.

(*Id.* (emphases added).)

19. In an effort to run as quickly as possible, Intel processors run something called "speculative execution." In essence, the processor attempts to guess what operation is going to be run next so that code can be standing by, ready to execute. When the processor selects what it believes is the next operation, it will fetch the code(s) needed to carry out that operation and have the code(s) on standby. However, Intel's "speculative execute" code may "fetch" secure codes without first performing a security check which would block such a request. So an innocuous program such as Javascript might be exploited to gain access to extremely secure kernel data. Or as *The Register* writes, "[t]hat would allow ring-3-level user code to read ring-0-level kernel data. And that is not good." (*Id.*)

20. The Defect is material because neither Plaintiff, Class members, nor any reasonable consumer would have purchased the defective Intel CPUs at the prices that they did had they known or had they been told by Intel or its retail agents about the Defect prior to purchase.

21. The Defect is unprecedented in scope in that it exposes millions and millions of Intel-based computers to critical security vulnerabilities and hacking and the “patch” to cure these security vulnerabilities will result in substantial performance degradation.

Intel Admits the Defect Exists and Fails to Provide a Remedy

22. Intel is aware that its CPUs suffer from the Defect that exposes the CPUs to critical security vulnerabilities and that proposed OS-level software patches will slow the performance of these CPU chips.

23. On January 3, 2018, Intel issued a press release in response to the myriad news media reports concerning the Defect, stating:

Intel Responds to Security Research Findings

Intel and other technology companies have been made aware of new security research describing software analysis methods that, when used for malicious purposes, have the potential to improperly gather sensitive data from computing devices that are operating as designed. Intel believes these exploits do not have the potential to corrupt, modify or delete data.

Recent reports that these exploits are caused by a “bug” or a “flaw” and are unique to Intel products are incorrect. Based on the analysis to date, many types of computing devices — with many different vendors’ processors and operating systems — are susceptible to these exploits.

Intel is committed to product and customer security and is working closely with many other technology companies, including AMD, ARM Holdings and several operating system vendors, to develop an industry- wide approach to resolve this issue promptly and constructively. Intel has begun providing software and firmware updates to mitigate these exploits. Contrary to some reports, any performance impacts are workload-dependent, and, for the average computer user, should not be significant and will be mitigated over time.

Intel is committed to the industry best practice of responsible disclosure of potential security issues, which is why Intel and other vendors had planned to disclose this issue next week when more software and firmware updates will be available. However, Intel is making this statement today because of the current inaccurate media reports.

Check with your operating system vendor or system manufacturer and apply any available updates as soon as they are available. Following good security practices that protect against malware in general will also help protect against possible exploitation until updates can be applied.

Intel believes its products are the most secure in the world and that, with the support of its partners, the current solutions to this issue provide the best possible security for its customers.

(Intel Refutes Chip “Bug,” “Inaccurate Media Reports,” Barrons,

<https://www.barrons.com/articles/intel-refutes-chip-bug-inaccurate-media-reports-1515010736> (last visited Jan. 4, 2018).)

24. Defendant’s press release acknowledges the existence of the Defect, claims other vendors (competitors) products also suffer from this Defect, and downplays the performance impact which it claims “will be mitigated over time.”

25. Intel has failed to cure the Defect or replace Plaintiff’s Intel CPUs with non- defective CPUs and offer full compensation required under federal and state law.

26. Any fix would require extensive changes at the root levels of the OS software, which would assuredly impact the performance of Intel processor-based machines. More importantly, any “fix” would not only directly impact the performance of a particular user’s Intel-based device, but have indirect performance impacts. Countless servers that run internet-connected services in the cloud will see a dramatic degradation in performance, which will have a downstream impact to all users of these servers. Thus, cloud-based services like Microsoft, Google, and Amazon will see performance degradation.

CLASS ACTION ALLEGATIONS

27. Plaintiff brings this action on his own behalf and as a class action on behalf of the following class:

All persons in the State of Indiana who purchased one or more Intel CPUs from Intel and/or its authorized retailer sellers and experienced the Defect or are likely to experience the Defect during the useful life of the CPU.

28. This action is properly maintainable as a class action under Fed. R. Civ. P. 23(a) and (b)(3).

29. The class consists of thousands of persons, such that joinder of all Class members is impracticable.

30. There are questions of fact and law that are common to the Class members and that predominate over any questions affecting only individual members. These questions include, but are not limited to:

- a. Whether Defendant’s CPUs possess the Defect and the nature of that Defect;

- b. Whether Defendant made any implied warranties in connection with the sale of the defective CPUs;
- c. Whether Defendant breached any implied warranties relating to its sale of defective CPUs by failing to resolve the Defect in the manner required by law;
- d. Whether Defendant was unjustly enriched by selling defective Intel CPUs;
- e. Whether Defendant violated applicable consumer protection laws by selling CPUs with the Defect and/or by failing to disclose the Defect, and failing to provide the relief required by law; and
- f. The appropriate nature and measure of Class-wide relief.

31. The claims of the Plaintiff are typical of the claims of the proposed Class because they are based on the same legal theories, and Plaintiff has no interests that are antagonistic to the interests of the Class members.

32. The Plaintiff is an adequate representative of the Class and has retained competent legal counsel experienced in class actions and complex litigation.

33. A class action is an appropriate and superior method for the fair and efficient adjudication of this controversy, as the pursuit of thousands of individual lawsuits would not be economically feasible for individual Class members and would cause a strain on judicial resources and increase the likelihood of varying outcomes, yet each Class member would be required to prove an identical set of facts in order to recover damages.

34. This action does not present any unique management difficulties.

COUNT I – INDIANA DECEPTIVE CONSUMER SALES ACT, §24-5-0.5-3

35. Plaintiff incorporates the preceding paragraphs in this Complaint as if fully set forth below.

36. Plaintiff asserts this claim individually and on behalf of all Class members under Indiana Code § 24-5-0.5-4.

37. The Indiana Deceptive Consumer Sales Act (“DCSA”) was enacted to protect consumers from suppliers who commit deceptive and unconscionable sales acts. The DCSA applies to Defendant’s acts and practices because it covers subjects of consumer transactions.

38. The General Assembly has instructed Courts to construe the DCSA liberally to promote these purposes and policies. Ind. Code § 24-5-0.5-1(a).

39. Intel is a “supplier” under Indiana Code § 24-5-0.5-2.

40. The Intel CPUs are “subjects of a consumer transaction” under Indiana Code § 24-5-0.5-2.

41. Plaintiff and Class members engaged in “consumer transactions” under Indiana Code § 24-5-0.5-2, including the purchase of Intel CPUs.

42. The DCSA states that “A supplier may not commit an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction. Such an act, omission, or practice by a supplier is a violation of this chapter whether it occurs before, during, or after the transaction.” Ind. Code § 24-5-0.5-3.

43. Under the DCSA, “An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations.” Ind. Code § 24-5-0.5-3.

44. The DCSA further provides that:

Without limiting the scope of subsection (a), the following acts, and the following representations as to the subject matter of a consumer transaction, made orally, in writing, or by electronic communication, by a supplier, are deceptive acts:

1. That such subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have.
2. That such subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not.

Ind. Code § 24-5-0.5-3.

45. Intel committed unfair and deceptive acts by representing that the Intel CPUs had performance, characteristics, or benefits which Intel knew or should reasonably have known they did not have, in violation of Indiana Code § 24-5-0.5-3.

46. Intel's violations were "incurable deceptive acts" because they were done "as part of a scheme, artifice, or device with intent to defraud or mislead." Ind. Code § 24-5-0.5-2(a)(8).

47. By designating a violation as an "*incurable* deceptive act," rather than merely a "deceptive act," the DCSA defines the violation as one in which notice is not required.

48. Defendant had exclusive knowledge of material facts, i.e. the Intel CPUs were defective, unknown to Plaintiff and Class members. If Plaintiff and Class members had known of the Defect in the Intel CPU, they would not have purchased the CPUs at the prices they did, if at all.

49. Plaintiff and Class members relied on the incurable deceptive acts of Intel and are therefore entitled to recover, in a class action, actual damages, statutory damages, treble damages, and reasonable attorneys' fees.

COUNT II – BREACH OF IMPLIED WARRANTY

50. Plaintiff incorporates the preceding paragraphs of this Complaint as if fully set forth below.

51. Defendant and its authorized agents and resellers sold Intel CPUs to Plaintiff and Class members in the regular course of business.

52. Defendant impliedly warranted to members of the general public, including Plaintiff and Class members, these CPUs were of merchantable quality (i.e., a product of a high enough quality to make it fit for sale, usable for the purpose it is made, of average worth in the marketplace, or not broken, unworkable, damaged, contaminated or flawed), was of the same quality as those generally acceptable in the trade or that would pass without objection in the trade, were free from material defects and were reasonably fit for the ordinary purposes for which they were intended or used. In addition, Defendant either was or should have been aware of the particular purposes for which such CPUs are used, and that Plaintiff and the Class members were relying on the skill and judgment of Defendant to furnish suitable goods for such purpose.

53. Pursuant to agreements between Defendant and its authorized agents and re-sellers, the stores Plaintiff and Class members purchased their defective Intel CPUs from are authorized retailers and authorized CPU service facilities.

Plaintiff and Class members are third-party beneficiaries of, and substantially benefited from, such contracts.

54. Defendant breached its implied warranties by selling Plaintiff and Class members defective Intel CPUs. The Defect renders the Intel CPUs unmerchantable and unfit for their ordinary or particular use or purpose. Defendant has refused to recall, repair or replace, free of charge, all Intel CPUs or any of their defective component parts or refund the prices paid for such CPUs.

55. The Defect in the Intel CPUs existed when the CPUs left Defendant's and their authorized agents' and retail sellers' possession and thus is inherent in such CPUs.

56. As a direct and proximate result of Defendant's breach of its implied warranties, Plaintiff and Class members have suffered damages and continue to suffer damages, including economic damages at the point of sale in terms of the difference between the value of the CPUs as warranted and the value of the CPUs as delivered. Additionally, Plaintiff and Class members either have or will incur economic, incidental and consequential damages in the cost of repair or replacement and costs of complying with continued contractual obligations as well as the cost of buying an additional CPU they would not have purchased had the CPUs in question not contained the non-repairable Defect.

57. Plaintiff and Class members are entitled to legal and equitable relief against Defendant, including damages, specific performance, rescission, attorneys' fees, costs of suit, and other relief as appropriate.

COUNT III – NEGLIGENCE

58. Plaintiff incorporates the preceding paragraphs of this Complaint as if fully set forth below.

59. Defendant was negligent in the manufacture and design of the CPUs containing the Defect, which CPUs were contained in, but also separate and apart from, the computers Plaintiff and Class members purchased.

60. Defendant's negligence was a substantial factor and reasonably foreseeable in causing harm to Plaintiff and Class members.

61. Plaintiff and Class members have been harmed, as they now own a computer with a CPU that due to such manufacturing or design defect is subject to invasion of a supposedly core protected part of the CPU and decreased performance, in an amount according to proof at trial.

COUNT IV – UNJUST ENRICHMENT/MONEY HAD AND RECEIVED

62. Plaintiff incorporates the preceding paragraphs of this Complaint as if fully set forth below.

63. Defendant has received and retained funds properly payable to the Plaintiff and Class members under such circumstances that in equity and good conscience Defendant ought not to retain those funds.

64. Defendant should be required to pay the improperly received and retained funds, with interest thereon, to the Plaintiff and Class members.

REQUEST FOR RELIEF

A. Certification of the Class requested above and appointment of the Plaintiff as the Class Representatives and his counsel as Class Counsel;

B. Awarding Plaintiff and Class members all proper measures of equitable monetary relief and damages, plus interest to which they are entitled;

C. Awarding equitable, injunctive, and declaratory relief as the Court may deem just and proper, including restitution and restitutionary disgorgement;

D. Awarding Plaintiff's reasonable costs and attorney's fees; and

E. All other relief that the Court finds just and proper.

DEMAND FOR JURY TRIAL

Plaintiff requests a jury trial on any and all counts for which trial by jury is permitted.

Dated: January 4, 2018

Respectfully submitted,

/s/Lynn A. Toops

Irwin B. Levin, #8786-49

Richard E. Shevitz, #12007-49

Vess A. Miller, #26495-53

Lynn A. Toops, #26386-49A

COHEN & MALAD, LLP

One Indiana Square, Ste. 1400

Indianapolis, IN 46204

Telephone: (317) 636-6481

Facsimile: (317) 636-2495

ilevin@cohenandmalad.com

rshevitz@cohenandmalad.com

vmiller@cohenandmalad.com

ltoops@cohenandmalad.com

*Counsel for Plaintiff and the Proposed
Plaintiff Class*