Rosemary M. Rivas (State Bar No. 209147)
Email: rrivas@zlk.com
Quentin A. Roberts (State Bar No. 306687)
Email: qroberts@zlk.com
LEVI & KORSINSKY, LLP
44 Montgomery Street, Suite 650
San Francisco, California 94104
Telephone: (415) 291-2420
Facsimile: (415) 484-1294

Courtney E. Maccarone (to be admitted *pro hac vice*)
Email: cmaccarone@zlk.com
LEVI & KORSINSKY, LLP
30 Broad Street, 24th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 636-7171

Counsel for Plaintiff Alexandr Bahcevan

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

ALEXANDR BAHCEVAN, on behalf of himself and all others similarly situated, Plaintiff, v. INTEL CORPORATION, a Delaware corporation, Defendant.	Case No. 5:18-cv-00187 **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Alexandr Bahcevan ("Plaintiff"), by and through his attorneys, makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to allegations specifically pertaining to himself and their counsel, which are based on personal knowledge, against defendant Intel Corporation ("Intel" or "Defendant").

NATURE OF THE ACTION

1. Plaintiff brings this action against Intel on behalf of all persons in the United States who purchased an Intel x86-64x series central processing unit ("CPU") either separately or as a component of another product.

2. Intel is the top-selling semiconductor company in the world. There are approximately 1.5 billion personal computers in use today and approximately 90% are powered by Intel CPUs. The x86-64x CPU is utilized in the majority of desktop, laptop computers, and servers in the United States. Products containing Intel CPUs are manufactured by companies such as Apple, Asus, Acer, Lenovo, Hewlett Packard, and Dell.

3. A CPU is the part of a computer's hardware that performs the instructions of programs and controls the operations of the system. In other words, the CPU is a computer's brain.

4. Unfortunately, nearly every single Intel CPU is defective because they were designed by Intel in a way that allows hackers and malicious programs to access highly secure information stored on the units in which they are installed.[1] The vulnerabilities have been named Spectre and Meltdown: "Meltdown" because it "melts security boundaries which are normally enforced by the hardware," and "Spectre" because its root cause is speculative execution, and "because it is not easy to fix, it will haunt us for quite some time.[2]

5. Both Meltdown and Spectre operate by manipulating different ways the CPUs optimize performance by rearranging the order of instructions or performing different instructions in parallel.

---

[1] The affected CPUs 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).

[2] *See Meltdown and Spectre*, SpectraAttack.com, https://spectreattack.com/ (last visited Jan. 5, 2018).

This means that an attacker who controls one process on a system can use the vulnerabilities to steal sensitive data from elsewhere on the computer. The vulnerability allows hackers to read information stored on a computer memory and steal sensitive data like passwords, Social Security numbers, credit card and banking information, and photographs.

6. While Intel claims that security updates will make 90% of phones and PCs that use its CPUs "immune" to the vulnerabilities,[3] experts warn that the vulnerabilities result from a design flaw which is *unfixable*. While companies that design operating systems are now scrambling to develop patches that may provide a fix, experts warn that these are only temporary fixes and a more permanent solution will have to be physically built into future CPUs. Moreover, the temporary patches will dramatically degrade CPU's performance by as much as thirty percent.

7. Defendant has not been able to offer an effective repair to its customers. A patch that dramatically cuts processor performance is not a legitimate solution, nor is any patch that does not fully address the security vulnerability.

8. Accordingly, Affected CPU owners are left with the unfortunate choice of either (1) purchasing a new processor or computer containing a CPU that does not contain the defect, (2) continuing to use a computer with massive security vulnerabilities, or (3) continuing to use a computer with significant performance degradation.

9. Defendant has admitted knowing of the design defect giving rise to the security vulnerabilities for at least six months. However, Defendant continued to manufacture, sell, and distribute its Affected CPUs without repair or disclosure of the defect.

10. Plaintiff has suffered an ascertainable injury and a loss of money or property as a result of Defendant's wrongdoing because Plaintiff would not have purchased the Affected CPUs had he known of the security vulnerabilities or would not have paid the prices he paid for the Affected CPUs.

[3] *See Intel Issues Updates to Protect Systems from Security Exploits*, Intel.com, https://newsroom.intel.com/news-releases/intel-issues-updates-protect-systems-security-exploits/ (last visited Jan. 5, 2018).

PARTIES

11. Plaintiff Alexandr Bahcevan is a citizen of the state of New York, residing in Brooklyn. Plaintiff has purchased at least one Affected CPU every year for the last five years. Had Plaintiff known that the Affected CPUs were built with a design flaw leading to security vulnerabilities, Plaintiff would not have purchased the Affected CPUs or would have paid less for them.

12. Defendant Intel Corporation is a Delaware corporation with its principal place of business located in Santa Clara, California. At all relevant times, Defendant was engaged in the business of designing, manufacturing, distributing, and/or selling electronic computer products, including the defective Intel CPUs at issue.

JURISDICTION AND VENUE

13. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class members and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest, fees, and costs, and at least one Class member is a citizen of a state different from Defendant.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant is headquartered in this District, and a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District, including Intel's design and marketing of the Affected CPUs from its headquarters in Santa Clara, California, and that Intel's wrongful actions harmed consumers who live in this District and purchased the Affected CPUs in this District.

INTRADISTRICT ASSIGNMENT

15. Pursuant to Civil L.R. 3-2(c), this civil action should be assigned to the San Jose Division, because a substantial part of the events or omissions giving rise to the claim occurred in the county of Santa Clara, where Intel is headquartered.

APPLICATION OF CALIFORNIA LAW TO THE CLASS IS APPROPRIATE

16. Based upon information and belief, Intel's actions and representations alleged herein emanated from the State of California from its headquarters located in Santa Clara and Intel's business acts and practices complained of were centered in, carried out, effectuated, and perfected within or had

their effect in the State of California, and injured Plaintiff and all Class members. Accordingly, the application of California law to the entire Class is appropriate.

FACTUAL ALLEGATIONS

17. The CPU of a computer is the piece of hardware that carries out the instructions of a computer program. It performs the basic arithmetical, logical, and input/output operations of a computer system. In other words, the CPU is like the brain of a computer. Every instruction has to go through the CPU.

18. One of the most important tasks that a CPU must perform is allowing a computer's operating system to interact with the computer's hardware. The CPU does this by dedicating some of its processing power to this task. This memory is known as kernel memory.

19. The kernel inside an operating system is an invisible process that facilitates the way applications and functions work on a computer by talking directly to the hardware. It has complete access to the operating system, with the highest possible level of permissions.

20. On January 2, 2018, it was widely reported that a design defect in the Affected CPUs exposes the CPU's kernel to vulnerabilities that allow malicious users to gain access to sensitive data that is supposed to be protected by the kernel, such as passwords, Social Security numbers, credit card and banking information, and photographs.[4]

21. At issue are two different vulnerabilities, dubbed "Meltdown" and "Spectre," that were independently discovered and reported by several security researcher groups including, but not limited to Cyberus Technology, Google, and the Graz University of Technology.

22. Meltdown affects every Intel processor shipped since 1995 (with the exception of Intel Itanium and Intel Atom before 2013), although researchers said the flaw could impact other chip makers. Spectre is a far more wide-ranging and troublesome flaw, impacting desktops, laptops, cloud servers, and smartphones from a variety of vendors.[5]

[4] *See, e.g.*, John Leyden, *Kernel-memory-leaking Intel processor design flaw forces Linux, Windows redesign*, TheRegister.co.uk, https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/ (last visited Jan. 5, 2018).

[5] *See Scary Chip Flaws Raise Spectre of Meltdown*, KrebsOnSecurity.com, https://krebsonsecurity.com/2018/01/scary-chip-flaws-raise-spectre-of-meltdown/ (last visited Jan. 5, 2018).

23. The vulnerabilities allow access to an operating system's kernel memory because of how the CPUs handle "speculative execution," which modern chips perform to increase performance.[6]

24. The *Register* reported on January 4, 2018:

> The severe design flaw in Intel microprocessors that allows sensitive data, such as passwords and crypto-keys, to be stolen from memory is real—and its details have been revealed.
>
> On Tuesday, we warned that a blueprint blunder in Intel's CPUs could allow applications, malware, and JavaScript running in web browsers, to obtain information they should not be allowed to access: the contents of the operating system kernel's private memory areas. These zones often contain files cached from disk, a view onto the machine's entire physical memory, and other secrets. This should be invisible to normal programs.
>
> Thanks to Intel's cockup—now codenamed Meltdown—that data is potentially accessible, meaning bad websites and malware can attempt to rifle through the computer's memory looking for credentials, RNG seeds, personal information, and more.[7]

25. The *Register* continued, "[t]his is, essentially, a mega-gaffe by the semiconductor industry. As they souped up their CPUs to race them against each other, they left behind one thing in the dust. Security.[8]

26. Intel is aware that its CPUs suffer from the defect that exposes the CPUs to critical security vulnerabilities, and has been for at least six months. However, before informing the public about these major security vulnerabilities, Intel's CEO Brian Krzanich sold millions of dollars in stock after the company had been informed that since 1995 almost every processor it has manufactured has two severe security vulnerabilities. Moreover, had Intel been performing proper tests and security checks of its CPUs, the vulnerabilities would have been evident far earlier. With its access to proprietary information about its CPUs, there is no reason why three independent teams working

---

[6] Speculative execution attempts to improve speed by executing multiple instructions at once (or even in a different order than when entering the CPU). To increase performance, the CPU predicts which path of a branch is most likely to be taken, and will speculatively continue execution down that path even before the branch is completed. If the prediction is wrong, speculative execution is rolled back in a way that is intended to be invisible to software.

[7] *See* Chris Williams, *Meltdown, Spectre: The password theft bugs at the heart of Intel CPUs*, TheRegister.co.uk, https://www.theregister.co.uk/2018/01/04/intel_amd_arm_cpu_vulnerability/ (last visited Jan. 5, 2018).

[8] *See id.*

separately were able to discover Meltdown and two independent teams were able to discover Spectre, but Intel did not.

27. It was only on January 3, 2018, that Intel issued a press release in response to the countless news media reports concerning the Affected CPUs, stating:

> 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.[9]

28. However, Defendant's press release is misleading because, among other reasons, while it acknowledges the existence of the defect, it claims other vendors' (competitors) products also suffer from the vulnerabilities, and downplays the performance impact which it claims "will be mitigated over time."

[9] *See Intel Responds to Security Research Findings*, Intel.com, https://newsroom.intel.com/news/intel-responds-to-security-research-findings/ (last visited Jan. 5, 2018).

29. Moreover, in a press release issued the following day on January 4, 2018, Intel claimed it has "developed and is rapidly issuing updates for all types of Intel-based computer systems—including personal computers and servers—that render those systems immune from both exploits."[10] However, key members of Google's Project Zero and data company Rambus stated that at least in Spectre's case, "this flaw is at such a level that it cannot be fixed by any old security patch. Rather, *this is a hole baked into the very chips' design*."[11]

30. Plaintiff and Class members used Intel's products and had business dealings with Intel either directly or indirectly as described above. The acts and practices of Intel have caused Plaintiff and Class members to lose money and property by being overcharged for and paying for the defective CPUs at issue, or being required to purchase an additional working CPU. Such loss was the result of the above acts of unfair competition and Intel's misconduct, and injury occurred at the point of sale.

31. Thus, the CPUs Defendant manufactured, installed, and sold in devices 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 design defect that leaves devices with an Intel CPU vulnerable to attacks by hackers.

32. Thus, Plaintiff and Class members are left with CPUs that are slower and more vulnerable than what they bargained for. They have CPUs that are not adequate for their ordinary purpose. Plaintiff and other Class members would not have purchased their CPUs, or would not have paid as much for them, had they known the truth.

CLASS ALLEGATIONS

33. Plaintiff brings this action on behalf of himself and the members of the proposed Class under Federal Rule of Civil Procedure Rule 23(b)(2) and (3). The proposed Class consists of the following:

> All persons in the United States who purchased an Affected CPU either from Intel, an authorized retail seller, or from a computer retailer or manufacturer who installed

---

[10] *See Intel Issues Updates to Protect Systems from Security Exploits*, Intel.com, https://newsroom.intel.com/news-releases/intel-issues-updates-protect-systems-security-exploits/ (last visited Jan. 5, 2018).

[11] *See* Joe Osborne, *Intel's chips to be 'immune' to Meltdown and Spectre after latest security updates*, TechRadar.com, http://www.techradar.com/news/intels-chips-to-be-immune-to-meltdown-and-spectre-after-latest-security-updates (last visited Jan. 5, 2018) (emphasis added).

an Affected CPU inside the customer's computer.

34. Plaintiff reserves the right to redefine the Class prior to certification after having the opportunity to conduct discovery.

35. Excluded from the Class are Defendant, its parents, subsidiaries, affiliates, officers and directors, any entity in which Defendant has a controlling interest, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

36. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that joinder is impractical. The Class consists of millions of members, the precise number which is within the knowledge of and can be ascertained only by resort to Defendant's records.

37. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are numerous questions of law and fact common to the Class, which predominate over any questions affecting only individual members of the Class. Among the questions of law and fact common to the Class are:

a) Whether the Affected CPUs possess the Meltdown security flaw;

b) Whether the Affected CPUs possess the Spectre security flaw;

c) Whether Defendant made any implied warranties in connection with the sale of the Affected CPUs;

d) Whether Defendant breached any implied warranties relating to its sale of the Affected CPUs;

e) Whether Defendant was unjustly enriched as a result of its acts complained of herein;

f) Whether Defendant engaged in deceptive, unfair, and/or unlawful business practices under California law; and

g) Whether Class members are entitled to damages, and in what amount.

38. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of the claims of the members of the Class. The injuries sustained by Plaintiff and the Class flow, in each instance, from a common nucleus of operative facts based on Intel's uniform conduct as set forth above. The defenses, if any, that will be asserted against Plaintiff's claims likely will be similar to the defenses that will be asserted, if any, against Class members' claims. Moreover, Plaintiff has no interests antagonistic to the interests of any other member of the Class.

39. Adequacy. Fed. R. Civ. P. 23(a)(4). Plaintiff is a representative who will fairly and adequately assert and protect the interests of the Class, and retained counsel experienced in prosecuting class actions. Accordingly, Plaintiff is an adequate representative and will fairly and adequately protect the interests of the Class.

40. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit, because individual litigation of the claims of all members of the Class is economically unfeasible and procedurally impracticable. While the aggregate damages sustained by the Class are in the millions of dollars, the individual damages incurred by each member of the Class resulting from Defendant's wrongful conduct may be too small to warrant the expense of individual lawsuits. The likelihood of individual Class members prosecuting their own separate claims is remote, and even if every member of the Class could afford individual litigation, the court system would be unduly burdened by individual litigation of such cases.

41. The prosecution of separate actions by members of the Class would create a risk of establishing inconsistent rulings and/or incompatible standards of conduct for Defendant. Additionally, individual actions may be dispositive of the interests of the Class, although certain Class members are not parties to such actions.

42. Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2). The conduct of Defendant is generally applicable to the Class as a whole and Plaintiff seeks equitable remedies with respect to the Class as a whole. As such, the systematic policies and practices of Defendant make declaratory or equitable relief with respect to the Class as a whole appropriate.

COUNT I

Violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.* "Unfair" Business Practices

(Individually and on Behalf of the Class)

43. Plaintiff incorporates and realleges by reference each and every allegation above as if set forth herein in full.

44. Plaintiff has standing to pursue this claim as Plaintiff has suffered injury in fact and lost money or property as a result of Defendant's actions, as set forth above.

45. Defendant's actions as alleged in this Complaint constitute "unfair" business practices within the meaning of California Business and Professions Code §§ 17200, *et seq.*

46. Defendant's business practices, as alleged herein, are "unfair" because they offend established public policy and/or are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to their customers. Additionally, Defendant's conduct is "unfair" because Defendant's conduct violated legislatively declared policies not to engage in misleading and deceptive conduct, or to not sell defective products. Defendant also concealed material facts from consumers.

47. As a result of Defendant's "unfair" business practices, Plaintiff and members of the Class spent money on computers containing CPUs that contained security vulnerabilities.

48. Defendant's unfair business practices alleged herein constitute a continuing course of unfair competition.

49. Plaintiff and the Class seek an order for injunctive relief to benefit the public, including a corrective advertising campaign, requiring Defendant to make full disgorgement and restitution of all monies wrongfully obtained from Plaintiff and the Class, and all other relief permitted under Bus. & Prof. Code §§ 17200, *et seq*.

COUNT II

Violation of Cal. Bus. & Prof. Code §§ 17200, *et seq*.
"Deceptive" Business Practices

(Individually and on Behalf of the Class)

50. Plaintiff incorporates and realleges by reference each and every allegation above as if set forth herein in full.

51. Defendant's actions as alleged in this Complaint constitute "deceptive" business practices within the meaning of Bus. & Prof. Code §§ 17200, *et seq*.

52. Plaintiff does not allege a claim of common law fraud nor any claim in this Cause of Action that requires proof of intent.

53. Defendant's business practices, as alleged herein, are "deceptive" because they were and are likely to deceive reasonable consumers, including Plaintiff and members of the Class, targeted by such omissions of material fact.

54. Defendant failed to disclose material information to purchasers of computers containing the Affected CPUs by concealing the material fact that these CPUs contain the security vulnerabilities.

55. As a result of Defendant's "deceptive" conduct, Plaintiff and members of the Class spent money on the Affected CPUs or on computers containing the Affected CPUs that suffer from security vulnerabilities.

56. Defendant's deceptive business practices alleged herein constituted a continuing course of unfair competition.

57. Plaintiff and the Class seek an order for injunctive relief to benefit the public, requiring Defendant to make full disgorgement and restitution of all monies that have been wrongfully obtained from Plaintiff and the Class, and all other relief permitted under Bus. & Prof. Code §§ 17200, *et seq*.

COUNT III

Breach of Implied Warranty

(Individually and on Behalf of the Class)

58. Plaintiff incorporates and realleges by reference each and every allegation above as if set forth herein in full.

59. This claim is asserted on behalf of Plaintiff and the Class.

60. Defendant is a "merchant" and the Affected CPUs are "goods" as defined under the Uniform Commercial Code.

61. Pursuant to Uniform Commercial Code § 2-314, an implied warranty that goods are merchantable is implied in every contract for a sale of goods. Defendant impliedly warranted that the Affected CPUs were of a merchantable quality.

62. Defendant breached the implied warranty of merchantability because the Affected CPUs were and are not of a merchantable quality due to the security vulnerabilities and the associated problems and failures in the Affected CPUs caused by the vulnerabilities.

63. Plaintiff's and each Class member's interactions with Defendant suffice to create privity of contract between Plaintiff and all other members of the Class, on the one hand, and Defendant, on the other hand; however, privity of contract need not be established nor is it required because Plaintiff and the absent Class members are intended third-party beneficiaries of contracts between Defendant and its resellers, authorized dealers, and specifically, of Defendant's implied warranties.

64. Defendant's resellers, dealers, and distributors are intermediaries between Defendant and consumers. These intermediaries sell the Affected CPUs to consumers and are not, themselves, consumers of the Affected CPUs, and therefore have no rights against Defendant with respect to Plaintiff's and all other Class members' purchases of Affected CPUs. Defendant's warranties were designed to influence consumers who purchased the Affected CPUs, including products that contain them.

COUNT IV

Negligence

(Individually and on Behalf of the Class)

65. Plaintiff incorporates and realleges by reference each and every allegation above as if set forth herein in full.

66. This claim is asserted on behalf of Plaintiff and the Class.

67. Defendant owed a duty of care to Plaintiff and Class members, arising from the sensitivity of the information stored on computers and the foreseeability of Affected CPU's data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding sensitive personal information. It also had a duty of care to ensure that its CPUs would function at the quality and speed levels it represented. This duty included, among other things, designing, maintaining, monitoring, and testing its CPUs to ensure that Class members' data and computers were adequately secured and that the processors would function as promised.

68. Defendant owed a duty to Plaintiff and Class members to implement processes that would detect a major defect in a timely manner.

69. Defendant also owed a duty to disclose the material fact the Affected CPUs were defective.

70. But for Intel's breach of its duties, Plaintiff and Class members would not have purchased the defective Affected CPUs or would not have paid as much for them as they did, and would not have been exposed to security risks and processor slowdowns.

COUNT V

Unjust Enrichment

(Individually and on Behalf of the Class)

71. Plaintiff incorporates and realleges by reference each and every allegation above as if set forth herein in full.

72. This claim is asserted on behalf of Plaintiff and the Class.

73. Plaintiff makes this claim in the alternative to the warranty claim set forth above.

74. As a result of Defendant's material deceptive advertising, marketing, and/or sale of its Affected CPUs, Defendant was enriched at the expense of Plaintiff and all other Class members through their purchase of the Affected CPUs, because the Affected CPUs did not provide the benefits as represented.

75. Under the circumstances, it would be against equity and good conscience to permit Defendant to retain the ill-gotten benefits it received from Plaintiff and the Class as the result of its unfair and deceptive practices. Thus, it would be unjust or inequitable for Defendant to retain the benefit without restitution to Plaintiff and the other members of the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class demand judgment against Defendant as follows:

A. An order certifying that this Action may be maintained as a class action, that Plaintiff be appointed as the Class Representative, and his counsel be appointed Class Counsel;

B. A judgment awarding Plaintiff and all members of the Class damages as alleged above incurred by Plaintiff and Class members as a result of Defendant's unlawful, deceptive, and unfair business and trade practices described herein;

C. A judgment awarding Plaintiff and all members of the Class restitution or other equitable relief, including, without limitation, disgorgement of all profits and unjust enrichment that Defendant obtained from Plaintiff and the Class as a result of their unlawful, unfair, and deceptive business

practices described herein;

D. An order enjoining Defendant from continuing to violate the laws as described herein;

E. A judgment awarding Plaintiff the costs of suit, including reasonable attorneys' fees, and pre and post-judgment interest; and

F. Such other and further relief as may be deemed necessary or appropriate.

JURY DEMAND

Plaintiff demands a trial by jury.

Dated: January 9, 2018

LEVI & KORSINSKY, LLP

By: */s/Rosemary M. Rivas*
Rosemary M. Rivas

Rosemary M. Rivas
Quentin A. Roberts
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 291-2420
Facsimile: (415) 484-1294

LEVI & KORSINSKY, LLP
Courtney E. Maccarone (to be admitted *pro hac vice*)
30 Broad Street, 24th Floor
New York, New York 10004
Telephone: (212) 363-7500
Facsimile: (212) 636-7171

Counsel for Plaintiff Alexandr Bahcevan

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
ALEXANDR BAHCEVAN, on behalf of himself and all others similarly situated

(b) County of Residence of First Listed Plaintiff Kings County, New York
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Rosemary Rivas, Levi & Korsinsky, LLP, 44 Montgomery Street, Suite 650, San Francisco, CA 94104; 415-291-2420

DEFENDANTS
INTEL CORPORATION, a Delaware corporation

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

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

Attorneys *(If Known)*

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

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

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

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

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

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

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

TORTS

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

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

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

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

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

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

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

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)
Brief description of cause:
Cal. Bus. & Prof. Code §§ 17200, et seq.; Breach of Implied Warranty; Negligence; and Unjust Enrichment

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

VIII. RELATED CASE(S), IF ANY *(See instructions):*
JUDGE van Keulen; Cousins; Lloyd DOCKET NUMBER 18cv46 and 18cv74; 18cv105; 18cv111

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

DATE 01/09/2018 **SIGNATURE OF ATTORNEY OF RECORD** /s/ Rosemary M. Rivas

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.