

1 **KESSLER TOPAZ**
2 **MELTZER & CHECK, LLP**
3 ELI R. GREENSTEIN (Bar No. 217945)
egreenstein@ktmc.com
4 JENNIFER L. JOOST (Bar No. 296164)
jjoost@ktmc.com
5 STACEY M. KAPLAN (Bar No. 241989)
skaplan@ktmc.com
6 One Sansome Street, Suite 1850
San Francisco, CA 94104
7 Tel: (415) 400-3000
8 Fax: (415) 400-3001

Attorneys for Plaintiff Zog, Inc.
[additional counsel listed on signature page]

9 **UNITED STATES DISTRICT COURT**
10 **NORTHERN DISTRICT OF CALIFORNIA**
11 **SAN JOSE DIVISION**

12 ZOG, INC., Individually and on Behalf of All
13 Others Similarly Situated,

14 Plaintiff,

15 v.

16 INTEL CORPORATION,

17 Defendant.

Civil Action No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1 Plaintiff Zog, Inc. (“Plaintiff”), on behalf of itself and all others similarly situated, hereby
2 alleges the following based on personal knowledge as to itself and its own conduct, and upon
3 information and belief as to all other matters.

4 **I. INTRODUCTION**

5 1. Defendant Intel Corporation (“Defendant” or “Intel”) is one of the largest
6 manufacturers of central processing units (“CPUs” or “processors”). Intel’s processors are
7 integrated—with Intel’s assistance and guidance—into desktop and laptop computers, servers, and
8 smartphones manufactured by, *inter alia*, Dell Inc., Lenovo Group Limited, HP Inc., Acer Inc., and
9 Apple Inc.

10 2. Given that CPUs are responsible for executing instructions provided by various
11 software programs, the processing speed of a CPU is critical to running software programs effectively
12 and efficiently. Likewise, a CPU’s ability to securely process data is critical to maintaining the
13 integrity of a user’s confidential and sensitive information.

14 3. To this end, Intel has long touted the purported speed and security of its processors in
15 marketing materials directed to business and enterprise customers. For example, when launching its
16 7th Gen Core vPro processor in January 2017, Intel emphasized that the new processor delivered a
17 “best-in-class platform for business that arms IT pros with the most advanced set of capabilities across
18 the areas they care about – security, productivity, and manageability.”¹

19 4. However, unbeknownst to Plaintiff and members of the Class (defined herein), Intel’s
20 processors are defective. Specifically, Intel processors are incapable of operating at represented
21 processing speeds without exposing users to two security vulnerabilities (the “Defects”)—known as
22 “Meltdown” and “Spectre”—which “allow programs to steal data which is currently processed on the
23 computer.”² “Although both [Defects] are based on the same general principle, Meltdown allows
24

25 ¹ Tom Garrison, *7th Gen Intel Core vPro Processors: New Levels of Performance, Security and*
26 *Manageability for Businesses*, INTEL CORPORATION, January 3, 2017, [https://itpeernetwork](https://itpeernetwork.intel.com/7th-gen-intel-core-vpro-business-performance-security-manageability/)
27 [.intel.com/7th-gen-intel-core-vpro-business-performance-security-manageability/](https://itpeernetwork.intel.com/7th-gen-intel-core-vpro-business-performance-security-manageability/) (last accessed
28 January 12, 2018).

² Graz University of Technology, *Meltdown and Spectre*, <https://meltdownattack.com/> (last
accessed January 12, 2018).

1 malicious programs to gain access to higher-privileged parts of a computer’s memory, while Spectre
2 steals data from the memory of other applications running on a machine.”³

3 5. After the Defects were publicly revealed by *The Register* on January 2, 2018,⁴ it was
4 reported that Intel had known about the Spectre Defect since *at the latest* June 1, 2017, and the
5 Meltdown Defect since *at the latest* July 28, 2017.⁵ Notwithstanding Intel’s knowledge of the
6 Defects—and the fact that Intel should have known of the Defects many years ago—Intel continued
7 to advertise, manufacture, distribute, and sell the defective processors to members of the Class
8 including Plaintiff.

9 6. The Defects are present in virtually every modern Intel processor and cannot be
10 effectively fixed through software “patches” or updates. In fact, efforts to mitigate the Defects—
11 which “impact fundamental aspects of how mainstream processors manage and silo data”—have
12 resulted in “corresponding performance slowdowns” given that “the fixes involve routing data for
13 processing in less efficient ways.”⁶

14 7. Initial estimates have suggested that software patches intended to mitigate the Defects
15 may reduce processing speed by as much as thirty percent⁷—a concern reinforced by Intel’s
16 confirmation that patched personal computers have shown a “2 percent to 14 percent” decline in
17

18
19 ³ Andy Greenberg, *A Critical Intel Flaw Breaks Basic Security for Most Computers*, WIRED,
20 January 3, 2018, <https://www.wired.com/story/critical-intel-flaw-breaks-basic-security-for-most-computers/> (last accessed January 12, 2018).

21 ⁴ See John Leyden and Chris Williams, *Kernel-memory-leaking Intel Processor Design Flaw*
22 *Forces Linux, Windows Redesign*, THE REGISTER, January 2, 2018, https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/ (last accessed January 12, 2018).

23 ⁵ See Samuel Gibbs, *Meltdown and Spectre: ‘Worst Ever’ CPU Bugs Affect Virtually All*
24 *Computers*, THE GUARDIAN, January 4, 2018, [https://www.theguardian.com/technology/2018](https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-worst-cpu-bugs-ever-found-affect-computers-intel-processors-security-flaw)
25 [/jan/04/meltdown-spectre-worst-cpu-bugs-ever-found-affect-computers-intel-processors-security-flaw](https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-worst-cpu-bugs-ever-found-affect-computers-intel-processors-security-flaw) (last accessed January 12, 2018) (“Google said it informed the affected companies about the Spectre flaw on 1 June 2017 and later reported the Meltdown flaw before 28 July 2017.”).

26 ⁶ Lily Hay Newman, *Meltdown and Spectre Fixes Arrive—But Don’t Solve Everything*, WIRED,
27 January 6, 2018, <https://www.wired.com/story/meltdown-and-spectre-vulnerability-fix/> (last
28 accessed January 12, 2018).

⁷ See John Leyden and Chris Williams, *Kernel-memory-leaking Intel Processor Design Flaw*
Forces Linux, Windows Redesign, THE REGISTER, January 2, 2018.

1 performance speed⁸ and Microsoft Corp.’s confirmation that Meltdown-related patches for computers
2 and servers running Windows operating systems with Intel processors result in potentially significant
3 slowdowns.⁹

4 8. The Defects are of significant risks to businesses given the devastating implications
5 of a cyber-attack on a business’s ability to function. Indeed, “[t]he U.S.’ National Cyber Security
6 Alliance found that 60 percent of small companies are unable to sustain their businesses over six
7 months after a cyber attack. According to the Ponemon Institute, the average price for small
8 businesses to clean up after their businesses have been hacked stands at \$690,000; and, for middle
9 market companies, it’s over \$1 million.”¹⁰

10 9. Plaintiff and members of the Class would not have purchased or leased—or would
11 have paid substantially less for—Intel processors (or devices containing Intel processors) had they
12 known of the Defects and the reduction in processing performance associated with efforts necessary
13 to mitigate the substantial security risks presented by the Defects.

14 10. Defendant’s conduct violates state common law and statutory law.

15 11. Accordingly, Plaintiff brings this class action against Defendant individually and on
16 behalf of all other persons and entities in the United States that purchased or leased one or more Intel
17 processors, or one or more devices containing an Intel processor, for business or commercial use.

18 **II. PARTIES**

19 12. Plaintiff Zog, Inc. is incorporated and headquartered in the Commonwealth of
20 Pennsylvania. Plaintiff provides information technology management, maintenance, and support
21 services to other businesses and enterprises, including the provision of secure cloud services. Plaintiff
22 purchased numerous devices containing Intel processors including, for example:

23
24 ⁸ Intel Corporation, *Intel Offers Security Issue Update*, January 9, 2018, <https://newsroom.intel.com/news/intel-offers-security-issue-update/> (last accessed January 12, 2018).

25 ⁹ Terry Myerson, *Understanding the Performance Impact of Spectre and Meltdown Mitigations on Windows Systems*, MICROSOFT CORP., January 9, 2018, <https://cloudblogs.microsoft.com/microsoftsecure/2018/01/09/understanding-the-performance-impact-of-spectre-and-meltdown-mitigations-on-windows-systems/> (last accessed January 12, 2018).

26
27
28 ¹⁰ Gary Miller, *60% of Small Companies That Suffer A Cyber Attack Are Out Of Business Within Six Months*, THE DENVER POST, October 23, 2016.

- 1 • one HP ProBook 440 G4 14” Notebook, containing an Intel Core i3-7100U processor, for \$554 on September 27, 2017;
- 2 • one HP Business Desktop ProDesk 600 G2 Desktop Computer, containing an Intel Core i5-6500 processor, for \$679 on January 18, 2017;
- 3
- 4 • one HPE (Hewlett Packard Enterprise) ML350T09 Smart Buy Server, containing an Intel Xeon E5-2640 v4 processor, for \$2339 on January 5, 2017; and
- 5 • one Intel Xeon E5-2640 v4 processor for \$993 on January 5, 2017.
- 6

7 13. Defendant Intel Corporation is a Delaware corporation with its principal place of
8 business located within this District at 2200 Mission College Boulevard, Santa Clara, California.
9 Defendant is engaged in the business of designing, manufacturing, selling, and/or distributing CPUs,
10 including the defective processors at issue here. All references herein to any act of Intel shall include
11 the acts of Intel’s directors, officers, employees, affiliates, subsidiaries, and agents where such
12 persons or entities were engaged in the management, direction, or control of Intel, or where such
13 persons or entities were acting act the direction of Intel.

14 **III. JURISDICTION AND VENUE**

15 14. This Court has general personal jurisdiction over Defendant because it resides within
16 this District.

17 15. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d) because this matter is a
18 putative class action, the Class contains members, including Plaintiff, that are citizens of a state
19 different from Defendant, there are more than 100 members of the Class, and the matter in
20 controversy, exclusive of interest and costs, exceeds the sum or value of \$5,000,000.

21 16. Venue properly lies in this District pursuant to 28 U.S.C. § 1391 because Defendant
22 maintains its principal place of business in this District, a substantial part of the events or omissions
23 giving rise to Plaintiff’s claims occurred in this District, and because Defendant conducts a substantial
24 amount of business in this District.

25 17. Assignment to the San Jose Division of this District is proper under Northern District
26 of California Civil Local Rule 3-2(c) because a substantial part of the events or omissions which give
27 rise to Plaintiff’s claims occurred, and Defendant’s principal place of business is located, in Santa
28

1 Clara, California. Pursuant to Northern District of California Civil Local Rule 3-2(e), all civil actions
2 which arise in the Santa Clara County shall be assigned to the San Jose Division.

3 **IV. FACTUAL ALLEGATIONS**

4 18. Intel is one of the world’s largest manufacturers of CPUs—the so-called “brains” of
5 computer systems (and other electronic devices)—which are responsible for processing system data
6 and controlling other devices and components connected to the system.

7 19. Intel both sells its processors to the marketplace as stand-alone components and sells
8 its processors to third-party manufacturers that—with Intel’s assistance and guidance—incorporate
9 Intel’s processors into, among other things, desktop and laptop computers, servers, and smartphones.
10 Third-party manufacturers utilizing Intel processors include household names such as Dell Inc.,
11 Lenovo Group Limited, HP Inc., Acer Inc., and Apple Inc.

12 20. Fundamental to the operation of a CPU is the operating system’s “kernel”—the
13 program responsible for directing and coordinating access to the CPU, random-access memory, and
14 other components such as keyboards, mice, disk-drives, printers, and monitors. In order to ensure
15 effective performance and maintain security, the kernel is responsible for preventing data associated
16 with one program from being accessed or overwritten by another program.

17 **A. Intel Touts the Processing Speed and Security of Its Processors**

18 21. Processing speed and security are two of the key attributes of CPUs. Without
19 sufficient processing speed, a CPU will be unable to effectively and efficiently run the computer’s
20 operating system and software programs, and utilize connected hardware and peripheral devices.
21 Similarly, without sufficient data security, a CPU will not be able to satisfy users’ needs for the
22 processing, communication, and storage of sensitive and confidential information.

23 22. Given these market demands, Intel has consistently touted the purported speed and
24 security of its processors in communications with its prospective business and enterprise customers.
25 For example, when Intel launched its 7th Gen Core vPro processor in January 2017, Intel touted the
26 processor’s “new levels of performance, security and manageability for business” and specifically
27 represented that the new processor delivered a “best-in-class platform for business that arms IT pros
28 with the most advanced set of capabilities across the areas they care about – security, productivity,

1 and manageability.”¹¹ Furthermore, Intel assured customers that “[w]ith [the] 7th Gen Core vPro
2 processor, [Intel’s] focus is to deliver customers the solutions they need to fight against identity and
3 data breaches.”¹² Ultimately, Intel claimed that “upgrading to Windows 10 and 7th Gen Core vPro
4 processor-based devices will put enterprises on the best path to safeguard identities, drive down costs
5 while future-proofing their business.”¹³

6 23. Similarly, in advertising materials for server boards equipped with Xeon-brand
7 processors, Intel represented that “[e]very Intel® Server Board is designed and engineered to deliver
8 the performance, reliability and security customers need with the quality and support they have come
9 to expect from Intel.”¹⁴ Likewise, Intel touted “the broader benefits provided by the Intel Xeon
10 Platinum processor, which is designed for scalability, security, performance, and to take businesses
11 into the future.”¹⁵

12 24. In addition to these product-line representations, Intel specifically markets each model
13 of its processors based on their respective processing speeds. For example, Intel’s website allows
14 prospective customers to directly and easily compare the processing speed (or “clock speed”) of each
15 of its processors:¹⁶

16
17
18
19
20 ¹¹ Tom Garrison, *7th Gen Intel Core vPro Processors: New Levels of Performance, Security and
Manageability for Businesses*, INTEL CORPORATION, January 3, 2017.

21 ¹² *Id.*

22 ¹³ *Id.*

23 ¹⁴ Intel Corporation, *Intel Server Boards*, [https://www.intel.com/content/www/us/en/
motherboards/server-motherboards/server-board.html](https://www.intel.com/content/www/us/en/motherboards/server-motherboards/server-board.html) (last accessed January 12, 2018).

24 ¹⁵ Tim Allen, *The Intel Xeon Platinum Processor Is Put to the Test and Comes Out Shining*,
25 INTEL CORPORATION, July 11, 2017, [https://itpeernetwork.intel.com/intel-xeon-platinum-processor-
put-to-test/](https://itpeernetwork.intel.com/intel-xeon-platinum-processor-put-to-test/) (last accessed January 12, 2018).

26 ¹⁶ See Intel Corporation, *Intel® Xeon® Processor E5-2640 v4*, [https://www.intel.com
/content/www/us/en/products/processors/xeon/e5-processors/e5-2640-v4.html](https://www.intel.com/content/www/us/en/products/processors/xeon/e5-processors/e5-2640-v4.html) (last
27 accessed January 12, 2018); Intel Corporation, *Intel® Core™ i3-7100U Processor*,
28 <https://www.intel.com/content/www/us/en/products/processors/core/i3-processors/i3-7100u.html>
(last accessed January 12, 2018).



B. The Defects

25. Rather than processing instructions in sequential order, Intel CPUs are designed to process multiple program instructions in parallel through so-called “out-of-order” or “speculative” execution.

26. As explained by the team of researchers from the Graz University of Technology that helped identify the Defects:

Speculative execution is a technique used by highspeed processors in order to increase performance by guessing likely future execution paths and prematurely executing the instructions in them. For example when the program’s control flow depends on an uncached value located in the physical memory, it may take several hundred clock cycles before the value becomes known. Rather than wasting these cycles by idling, the processor guesses the direction of control flow, saves a checkpoint of its register state, and proceeds to speculatively execute the program on the guessed path. When the value eventually arrives from memory the processor checks the correctness of its initial guess. If the guess was wrong, the processor discards the (incorrect) speculative execution by reverting the register state back to the stored checkpoint, resulting in performance comparable to idling. In case the guess was correct, however, the speculative execution results are committed, yielding a

1 significant performance gain as useful work was accomplished during
2 the delay.¹⁷

3 27. As first reported by *The Register* on January 2, 2018, because “Intel’s CPUs
4 speculatively execute code potentially without performing security checks . . . it may be possible to
5 craft software in such a way that the processor starts executing an instruction that would normally be
6 blocked – such as reading kernel memory from user mode – and completes that instruction before the
7 privilege level check occurs.”¹⁸

8 28. Stated differently, “malicious actors c[an] take advantage of speculative execution to
9 read system memory that should have been inaccessible” and may, as a result, be able to “read
10 sensitive information in the system’s memory such as passwords, encryption keys, or sensitive
11 information open in applications” through two similar security vulnerabilities known as “Meltdown”
12 and “Spectre.”¹⁹

13 **The Meltdown Defect**

14 29. As explained by the Graz University team, “Meltdown breaks the most fundamental
15 isolation between user applications and the operating system” and “allows a program to access the
16 memory, and thus also the secrets, of other programs and the operating system.”²⁰ As a result, the
17 Meltdown Defect “enables an adversary to read memory of other processes or virtual machines in the
18 cloud without any permissions or privileges, affecting millions of customers and virtually every user
19 of a personal computer.”²¹

20 ¹⁷ Paul Kocher, *et al.*, *Spectre Attacks: Exploiting Speculative Execution**, <https://spectre-attack.com/spectre.pdf> (last accessed January 11, 2018) (the “Spectre White Paper”).

21 ¹⁸ John Leyden and Chris Williams, *Kernel-memory-leaking Intel Processor Design Flaw Forces Linux, Windows Redesign*, *THE REGISTER*, January 2, 2018.

22 ¹⁹ Matt Linton, *Today’s CPU Vulnerability: What You Need to Know*, *GOOGLE SECURITY BLOG*,
23 January 3, 2018, <https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html> (last accessed January 12, 2018).

24 ²⁰ Graz University of Technology, *Meltdown and Spectre*.

25 ²¹ Moritz Lipp, *et al.*, *Meltdown*, <https://meltdownattack.com/meltdown.pdf> (last accessed
26 January 11, 2018) (the “Meltdown White Paper”); *see also* Matt Linton, *Today’s CPU Vulnerability:
27 What You Need to Know*, *GOOGLE SECURITY BLOG*, January 3, 2018 (“Testing also showed that an
28 attack running on one virtual machine was able to access the physical memory of the host machine,
and through that, gain read-access to the memory of a different virtual machine on the same host.”).

1 process. While in user mode, the kernel's code and data remains out
2 of sight but present in the process's page tables.

3 Think of the kernel as God sitting on a cloud, looking down on Earth.
4 It's there, and no normal being can see it, yet they can pray to it.

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

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

16 Your Intel-powered machines will run slower as a result.²⁵

17 33. Indeed, researchers have estimated that the software patches designed to mitigate the
18 Meltdown Defect may reduce processing speed by as much as thirty percent.²⁶ In fact, Intel has
19 admitted that patched personal computers have shown a "2 percent to 14 percent" decline in
20 performance speed in Defendant's own testing.²⁷ More recent benchmark testing by Microsoft Corp.
21 has confirmed that Meltdown patches for computers and servers running Windows operating systems
22 with Intel processors result in potentially significant slowdowns.²⁸

23 34. Further, experts have noted that the rush to roll out patches, while necessary, makes
24 the ultimate efficacy of these early fixes potentially suspect, as there has not been much time for
25

26 ²⁵ John Leyden and Chris Williams, *Kernel-memory-leaking Intel Processor Design Flaw*
27 *Forces Linux, Windows Redesign*, THE REGISTER, January 2, 2018.

28 ²⁶ *See, e.g., id.*

²⁷ Intel Corporation, *Intel Offers Security Issue Update*, January 9, 2018.

²⁸ Terry Myerson, *Understanding the Performance Impact of Spectre and Meltdown Mitigations*
on Windows Systems, MICROSOFT CORP., January 9, 2018.

1 extensive testing and refinement. Thus, these “slapdash fixes” may not offer total protection, or could
2 create other bugs and instabilities that will need to be resolved.²⁹

3 35. In fact, on January 11, 2018, it was reported that Intel’s “patches had bugs of their
4 own” and that Intel was “advis[ing] customers to ‘delay additional deployments of these microcode
5 updates.’”³⁰ As explained by Paul Kocher, one of the researchers who identified the Defects, “[i]t
6 doesn’t surprise me a lot that there would be some hiccups.”³¹

7 **The Spectre Defect**

8 36. Like the Meltdown Defect, the Spectre Defect takes advantage of design defects in
9 Intel processors’ use of speculative execution.

10 37. The research team from Graz University has explained that “Spectre breaks the
11 isolation between different applications” and “allows an attacker to trick error-free programs, which
12 follow best practices, into leaking their secrets.”³²

13 38. More specifically, “Spectre attacks involve inducing a victim to speculatively perform
14 operations that would not occur during correct program execution and which leak the victim’s
15 confidential information via a side channel to the adversary.”³³ For example, a Spectre attack can
16 “leak information within a browser (such as saved passwords or cookies) to a malicious JavaScript”—
17 which, in turn, sends the passwords or cookies back to the malicious actor.³⁴

20 ²⁹ Lily Hay Newman, *Meltdown and Spectre Fixes Arrive—But Don’t Solve Everything*, WIRED,
21 January 6, 2018.

22 ³⁰ Robert McMillan, *Intel Fumbles Its Patch for Chip Flaw*, THE WALL STREET JOURNAL,
23 January 11, 2018, <https://arstechnica.com/gadgets/2018/01/heres-how-and-why-the-spectre-and-meltdown-patches-will-hurt-performance/> (last accessed January 12, 2018).

24 ³¹ *Id.*

25 ³² Graz University of Technology, *Meltdown and Spectre*, <https://spectreattack.com/> (last
accessed January 12, 2018).

26 ³³ Spectre White Paper.

27 ³⁴ Peter Bright, *Here’s How, and Why, the Spectre and Meltdown Patches Will Hurt*
28 *Performance*, ARS TECHNICA, January 11, 2018, <https://arstechnica.com/gadgets/2018/01/heres-how-and-why-the-spectre-and-meltdown-patches-will-hurt-performance/> (last accessed January 12, 2018).

1 39. To date, at least two particular types of Spectre attacks have emerged: “[o]ne version
2 [the “branch prediction variant”] allows an attacker to ‘train’ the processor’s branch prediction
3 machinery so that a victim process mispredicts and speculatively executes code of an attacker’s
4 choosing (with measurable side-effects); the other [the “array bounds variant”] tricks the processor
5 into making speculative accesses outside the bounds of an array.”³⁵

6 40. Fixing the Spectre Defect is particularly complicated. As explained by *Ars Technica*:

7 while there may be limited ways to block certain kinds of speculative
8 execution, general techniques that will defend against any information
9 leakage due to speculative execution aren’t known.

10 Sensitive pieces of code could be amended to include ‘serializing
11 instructions’—instructions that force the processor to wait for all
12 outstanding memory reads and writes to finish (and hence prevent any
13 speculation based on those reads and writes)—that prevent most kinds
of speculation from occurring. . . . But these instructions would have
to be very carefully placed, with no easy way of identifying the correct
placement.³⁶

14 As such, “at-risk applications (notably, browsers) are being updated to include certain Spectre
15 mitigating techniques to guard against the array bounds variant” while “[o]perating system and
16 processor updates are needed to address the branch prediction version.”³⁷

17 **C. Defendant’s Knowledge of the Defects**

18 41. Although the public only became aware of the Defects in Intel processors in January
19 2018, Intel has been aware of the Spectre Defect since *at the latest* June 1, 2017, and the Meltdown
20 Defect since *at the latest* July 28, 2017, when a team from Google’s Project Zero alerted the company
21 to the existence of the Defects.³⁸ In fact, in the intervening months between Google’s discovery and

22 ³⁵ *Id.*

23 ³⁶ Peter Bright, “*Meltdown*” and “*Spectre*”: *Every Modern Processor Has Unfixable Security*
24 *Flaws*, ARS TECHNICA, January 3, 2018.

25 ³⁷ Peter Bright, *Here’s How, and Why, the Spectre and Meltdown Patches Will Hurt*
Performance, ARS TECHNICA, January 11, 2018.

26 ³⁸ See Samuel Gibbs, *Meltdown and Spectre: ‘Worst Ever’ CPU Bugs Affect Virtually All*
27 *Computers*, THE GUARDIAN, January 4, 2018, <https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-worst-cpu-bugs-ever-found-affect-computers-intel-processors-security-flaw> (last accessed January 12, 2018) (“Google said it informed the affected companies about the Spectre flaw on 1 June 2017 and later reported the Meltdown flaw before 28 July 2017.”).

1 *The Register*'s report, at least three other outside research teams alerted Intel to the existence of the
2 Defects.³⁹

3 42. Intel knew, or should have known, of the Defect in its processors many years ago
4 given that Intel was in a superior position to perform proper tests and security checks of its processors
5 and appropriate due diligence would have revealed the vulnerabilities that were uncovered by various
6 independent teams. Indeed, Defendant had actual knowledge, and access to proprietary information
7 to discover, that defects in design were causing the Defects in its processors.

8 43. As stated succinctly by Paul Kocher, "[t]here's no reason someone couldn't have
9 found this years ago instead of today."⁴⁰

10 44. Indeed, warning signs have existed since at least early 2005 when "[r]esearchers began
11 writing about the potential for security weaknesses at the heart of central processing units."⁴¹ This
12 influential work continued in 2013 when "other research papers showed that CPUs let unauthorized
13 users see the layout of the kernel, a set of instructions that guide how computers perform key tasks
14 like managing files and security and allocating resources."⁴²

15 45. These early reports ultimately prompted industry presentations at various "Black Hat"
16 and other cybersecurity conferences in 2016 and 2017, including presentations by members of the
17 Graz University team, regarding potential attacks against the kernel memory of Intel processors.⁴³

18 46. Nevertheless, rather than inform the public about the Defects, Intel continued to sell
19 its defective processors to unknowing customers at prices much higher than what customers would
20 have paid had they know about the Defects and the impact on processing speeds.

21
22
23 ³⁹ Andy Greenberg, *Triple Meltdown: How So Many Researchers Found a 20-Year-Old Chip
24 Flaw At the Same Time*, WIRED, January 7, 2018, <https://www.wired.com/story/meltdown-spectre-bug-collision-intel-chip-flaw-discovery/> (last accessed January 12, 2018).

25 ⁴⁰ *Id.*

26 ⁴¹ Ian King, *et al.*, *'It Can't Be True': Inside the Semiconductor Industry's Meltdown*, CHICAGO
27 TRIBUNE, January 10, 2018, <http://www.chicagotribune.com/bluesky/technology/ct-inside-semiconductor-meltdown-20180110-story.html> (last accessed January 12, 2018).

28 ⁴² *Id.*

⁴³ *See id.*

1 47. As a result, Plaintiff and members of the Class, have been saddled with overpriced
2 processors that are slower and more vulnerable to security risks than what they bargained for.

3 **V. TOLLING OF THE STATUE OF LIMITATIONS AND ESTOPPEL**

4 48. **Discovery Rule Tolling.** Plaintiff and members of the Class could not have
5 reasonably discovered through the exercise of reasonable diligence that their Intel processors suffered
6 from major security vulnerabilities that, if mitigated, resulted in reduced processing performance,
7 within the time period of any applicable statute of limitations.

8 49. Plaintiff and members of the Class did not discover and did not know of any facts that
9 would have caused a reasonable person to suspect that Defendant was concealing a latent defect
10 and/or that the Intel processors contained a defect that exposed them to security vulnerabilities that,
11 if mitigated, resulted in reduced processing performance.

12 50. **Fraudulent Concealment Tolling.** Throughout the time period relevant to this
13 action, Defendant concealed from and failed to disclose to Plaintiff and members of the Class vital
14 information concerning the Defects described herein, despite the fact that Defendant knew, or should
15 have known of, the Defects in its Processors well before its discovery by a third party.

16 51. Defendant kept Plaintiff and members of the Class ignorant of vital information
17 essential to the pursuit of their claims. As a result, neither Plaintiff nor members of the Class could
18 have discovered the Defects, even upon reasonable exercise of diligence.

19 52. Despite its knowledge of the Defects, Defendant failed to disclose and concealed, and
20 continues to conceal, critical information relating to the Defects from Plaintiff and members of the
21 Class, even though, at any point in time, it could have done so through individual correspondence,
22 media release, or by other means.

23 53. Plaintiff and members of the Class justifiably relied on Defendant to disclose the
24 Defects in the Intel processors they purchased or leased (either directly or as a component of, among
25 other things, a computer, server, or smartphone), because the Defects were hidden and not
26 discoverable through reasonable efforts by Plaintiff and members of the Class.

1 54. Thus, the running of all applicable statutes of limitations have been suspended with
2 respect to any claims that Plaintiff and members of the Class have sustained as a result of the defective
3 Intel processors, by virtue of the fraudulent concealment doctrine.

4 55. **Estoppel.** Defendant was under a continuous duty to disclose to Plaintiff and members
5 of the Class the true character, quality, and nature of the defective processors and associated security
6 vulnerabilities and reductions in processing performance, but concealed the true nature, quality, and
7 character of the processors.

8 56. Based on the foregoing, Defendant is estopped from relying on any statutes of
9 limitations in defense of this action.

10 **VI. CLASS ACTION ALLEGATIONS**

11 57. Plaintiff brings this proposed action pursuant to Federal Rules of Civil Procedure
12 23(a), 23(b)(2), and/or 23(b)(3) on behalf of the following Class:

13 All persons or entities in the United States that purchased or leased one
14 or more Intel processors, or one or more devices containing an Intel
15 processor, for business or commercial use.

16 58. Excluded from the Class are Defendant and any parents, subsidiaries, corporate
17 affiliates, officers, directors, employees, assigns, successors, the Court, Court staff, Defendant's
18 counsel, and all respective immediate family members of the excluded entities described above.
19 Plaintiff reserves the right to revise the definition of the Class based upon subsequently discovered
20 information and reserves the right to establish subclasses where appropriate.

21 59. This action has been brought and may be properly maintained on behalf of the Class
22 proposed herein under Federal Rule of Civil Procedure 23.

23 60. **Numerosity.** Federal Rule of Civil Procedure 23(a)(1): The Class is so numerous
24 that individual joinder of all potential members is impracticable. Plaintiff believes that there are at
25 least thousands of proposed members of the Class throughout the United States. Members of the
26 Class may be notified of the pendency of this action by recognized, Court-approved notice
27 dissemination methods, which may include U.S. Mail, electronic mail, Internet postings, and/or
28 published notice.

1 61. **Commonality and Predominance.** Federal Rule of Civil Procedure 23(a)(2) and
2 23(b)(3): This action involves common questions of law and fact, which predominate over any
3 questions affecting individual members of the Class, including, without limitation:

- 4 A. Whether Defendant engaged in the conduct alleged herein;
- 5 B. Whether Defendant’s processors are defective and contain the Meltdown
6 Defect and/or the Spectre Defect;
- 7 C. Whether the purported “patches,” “fixes,” or other remedies are ineffective
8 and/or result in reduced processing performance;
- 9 D. Whether any such reduced processing performance is material;
- 10 E. Whether Defendant knew, or should have known, that its processors were
11 defective and that, if mitigated, resulted reduced processing performance;
- 12 F. Whether Defendant had a duty to disclose, and breached its duty to disclose,
13 that its processors were defective and that, if mitigated, resulted in reduced
14 processing performance;
- 15 G. Whether Defendant intentionally, recklessly, or negligently misrepresented or
16 omitted material facts including the fact that its processors are defective and
17 that, if mitigated, resulted in reduced processing performance;
- 18 H. Whether Defendant breached its express warranties in that its processors were
19 defective with respect to manufacture, workmanship and/or design;
- 20 I. Whether Defendant breached its implied warranties in that its processors were
21 defective with respect to manufacture, workmanship and/or design;
- 22 J. Whether Defendant was unjustly enriched by the conduct alleged herein;
- 23 K. Whether Defendant violated California’s Unfair Competition Law, California
24 Business & Professions Code § 17200, *et seq.*;
- 25 L. Whether Plaintiff and members of the Class overpaid for Intel Processors;
- 26 M. Whether Plaintiff and members of the Class are entitled to equitable relief,
27 including, but not limited to, restitution or injunctive relief; and
28

1 N. Whether Plaintiff and members of the Class are entitled to damages and other
2 monetary relief and, if so, in what amount.

3 62. **Typicality.** Federal Rule of Civil Procedure 23(a)(3): Plaintiff's claims are typical
4 of the claims of the other members of the Class because, among other things, all members of the Class
5 were comparably injured through Defendant's wrongful conduct as described above.

6 63. **Adequacy.** Federal Rule of Civil Procedure 23(a)(4): Plaintiff is an adequate Class
7 representative because its interests do not conflict with the interests of the other members of the Class
8 it seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action
9 litigation; and Plaintiff intends to prosecute this action vigorously. The interests of the Class will be
10 fairly and adequately protected by Plaintiff and its counsel.

11 64. **Declaratory and Injunctive Relief.** Federal Rule of Civil Procedure 23(b)(2):
12 Defendant has acted or refused to act on grounds generally applicable to Plaintiff and the other
13 members of the Class, thereby making appropriate final injunctive relief and declaratory relief with
14 respect to the Class as a whole.

15 65. **Superiority.** Federal Rule of Civil Procedure 23(b)(3): A class action is superior to
16 any other available means for the fair and efficient adjudication of this controversy, and no unusual
17 difficulties are likely to be encountered in the management of this class action. The damages or other
18 financial detriment suffered by Plaintiff and members of the Class are relatively small compared to
19 the burden and expense that would be required to individually litigate their claims against Defendant,
20 so it would be impracticable for members of the Class to individually seek redress for Defendant's
21 wrongful conduct. Even if members of the Class could afford individual litigation, the court system
22 could not. Individualized litigation creates a potential for inconsistent or contradictory judgments,
23 and increases the delay and expense to all parties and the court system. By contrast, the class action
24 device presents far fewer management difficulties, and provides the benefits of single adjudication,
25 economy of scale, and comprehensive supervision by a single court
26
27
28

1 **VII. CLAIMS FOR RELIEF**

2 **COUNT I**

3 **BREACH OF IMPLIED WARRANTY**

4 66. Plaintiff incorporates and realleges each preceding paragraph as though fully set forth
5 herein.

6 67. Plaintiff brings this count on behalf of itself and the Class.

7 68. Plaintiff and members of the Class purchased or leased Intel processors, or devices
8 containing Intel processors, from Defendant, by and through Defendant's authorized agents for retail
9 sales, or were otherwise expected to be the eventual purchasers or lessors of Intel processors when
10 purchased or leased from a third party. At all relevant times, Defendant was the manufacturer,
11 distributor, warrantor, and/or seller of the relevant processors. Defendant knew or had reason to know
12 of the specific use for which its processors were purchased or leased.

13 69. Defendant is and at all relevant times was a "merchant" and seller of "goods" (*i.e.*,
14 Intel processors) as defined under the Uniform Commercial Code.

15 70. Intel processors are and were at all relevant times "goods" within the meaning of the
16 Uniform Commercial Code.

17 71. Pursuant to U.C.C. § 2-314, an implied warranty that goods are merchantable is
18 implied in every contract for a sale of goods. Defendant impliedly warranted that its processors were
19 in merchantable condition and fit for the ordinary purpose for which Intel processors are used.

20 72. Intel processors, when sold or leased and at all times thereafter, were not in
21 merchantable condition and are not fit for the ordinary purpose due to the Defects, and the associated
22 problems and failures caused by the Defects. Thus, Defendant breached its implied warranty of
23 merchantability.

24 73. As a direct and proximate result of Defendant's breach of its implied warranty of
25 merchantability, Plaintiff and members of the Class have been damaged in an amount to be proven at
26 trial.

27 74. Defendant cannot disclaim its implied warranties as it knowingly sold or leased a
28 defective product.

1 75. Defendant was provided notice of the defect by independent research teams, and knew,
2 or should have known, of the existence of the Defects much earlier. Affording Defendant a
3 reasonable opportunity to cure its breach of implied warranties would be unnecessary and futile here
4 because Defendant has known of and concealed the Defects and, on information and belief, has
5 refused to adequately repair or replace its processors free of charge within or outside of the warranty
6 periods despite the Defects' existence at the time of sale or lease of the processors.

7 76. Any attempt by Defendant to disclaim or limit the implied warranty of merchantability
8 vis-à-vis consumers is unconscionable and unenforceable here. Specifically, any warranty limitation
9 is unenforceable because Defendant knowingly sold or leased a defective product without informing
10 customers about the Defects. The time limits contained in Defendant's warranty periods were also
11 unconscionable and inadequate to protect Plaintiff and members of the Class. Among other things,
12 Plaintiff and members of the Class did not determine these time limitations, the terms of which
13 unreasonably favored Defendant. A gross disparity in bargaining power existed between Defendant
14 and members of the Class, and Defendant knew or should have known that its processors were
15 defective at the time of sale or lease and that its processors were defective and posed security
16 vulnerabilities that, if mitigated, resulted in reduced processing performance.

17 77. Further, as manufacturers of consumer goods, Defendant is precluded from excluding
18 or modifying an implied warranty of merchantability or limiting customers' remedies for breach of
19 this warranty.

20 78. Plaintiff and members of the Class have complied with all obligations under the
21 warranty, or otherwise have been excused from performance of said obligations as a result of
22 Defendant's conduct described herein.

23 79. Defendant's warranties were designed to influence consumers who purchased its
24 processors, including products that contain them.

25 80. Defendant is estopped by its conduct, as alleged herein, from disclaiming any and all
26 implied warranties with respect to the defective processors.

27 81. The applicable statute of limitations for the implied warranty claim has been tolled by
28 the discovery rule, concealment, and the terms of the express warranty.

COUNT II

BREACH OF EXPRESS WARRANTY

1
2
3 82. Plaintiff incorporates and realleges each preceding paragraph as though fully set forth
4 herein.

5 83. Plaintiff brings this count on behalf of itself and members of the Class.

6 84. Defendant marketed its processors as secure and of particular processing speeds. Such
7 representations formed the basis of the bargain in Plaintiff’s and members of the Class’s decisions to
8 purchase or lease Intel processors, or devices containing Intel processors.

9 85. Pursuant to U.C.C. § 2-313, an affirmation of fact, promise, or description made by
10 the seller to the buyer which relates to the goods and becomes a part of the basis of the bargain creates
11 an express warranty that the goods will conform to the affirmation, promise, or description.

12 86. Defendant is and was at all relevant times a “merchant” and seller of “goods” (*i.e.*,
13 Intel processors) as defined under the Uniform Commercial Code.

14 87. Intel processors are and were at all relevant times “goods” within the meaning of the
15 Uniform Commercial Code.

16 88. Defendant represented that its processors were secure and of particular processing
17 speeds. Intel processors were not secure—given that they were subject to the Meltdown and Spectre
18 Defects—and did not operate at stated processing speeds given that patches necessary to mitigate the
19 Defects resulted in reduced processing performance.

20 89. Plaintiff and members of the Class experienced the existence of the Defects in Intel
21 processors within the warranty periods but had no knowledge of the existence of the Defects, which
22 was known and concealed by Defendant.

23 90. Plaintiff and members of the Class could not have reasonably discovered the Defects
24 in Intel processors prior to the public disclosure of the Defects by cybersecurity experts or prior to
25 experiencing a known security hack resulting from the Defects.

26 91. Defendant breached the express warranty by selling Intel processors that were
27 defective with respect to design, workmanship, and manufacture when Defendant knew its processors
28

1 were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing
2 performance.

3 92. Intel processors were not of merchantable quality and were unfit for the ordinary
4 purposes for which Intel processors are used because of the existence of the Defects, and do not
5 perform as warranted.

6 93. Defendant was provided notice of the defect by independent research teams, and knew,
7 or should have known, of the existence of the Defects much earlier. Affording Defendant a
8 reasonable opportunity to cure its breach of express warranties would be unnecessary and futile here
9 because Defendant has known of and concealed the Defects and, on information and belief, has
10 refused to adequately repair or replace its processors free of charge within or outside of the warranty
11 periods despite the Defects' existence at the time of sale or lease of the processors.

12 94. Any attempt by Defendant to disclaim or limit the express warranties vis-à-vis
13 consumers is unconscionable and unenforceable here. Specifically, any warranty limitation is
14 unenforceable because Defendant knowingly sold or leased a defective product without informing
15 customers about the Defects. The time limits contained in Defendant's warranty periods were also
16 unconscionable and inadequate to protect Plaintiff and members of the Class. Among other things,
17 Plaintiff and members of the Class did not determine these time limitations, the terms of which
18 unreasonably favored Defendant. A gross disparity in bargaining power existed between Defendant
19 and members of the Class, and Defendant knew or should have known that its processors were
20 defective at the time of sale or lease and that its processors were defective and posed security
21 vulnerabilities that, if mitigated, resulted in reduced processing performance.

22 95. Defendant knew that its processors were inherently defective and did not conform to
23 their warranties and Plaintiff and members of the Class were induced into purchasing or leasing Intel
24 processors, or devices containing Intel processors, under false pretenses.

25 96. Plaintiff and members of the Class have been excused from performance of any
26 warranty obligations as a result of Defendant's conduct described herein.

27 97. As a direct and proximate result of Defendant's breach of express warranties, Plaintiff
28 and members of the Class have been damaged in an amount to be determined at trial, including, but

1 not limited to, repair and replacement costs, monetary losses associated with reduced processor
2 speeds, diminished value of their computer devices, and loss of use of or access to their computer
3 devices.

4 **COUNT III**

5 **NEGLIGENCE**

6 98. Plaintiff incorporates and realleges each preceding paragraph as though fully set forth
7 herein.

8 99. Plaintiff brings this count on behalf of itself and the Class.

9 100. Defendant owed a duty of care to Plaintiff and members of the Class, arising from the
10 sensitivity of information stored on computers and the foreseeability of the impact of the Defects on
11 data security, to exercise reasonable care in safeguarding sensitive information.

12 101. Defendant also had a duty to ensure that its processors would function at the quality
13 and processing speeds that it represented to customers, including Plaintiff and members of the Class.
14 This duty included, *inter alia*, designing, maintaining, monitoring, and testing its processors to ensure
15 that members of the Class's data and computers were adequately secured and that its processors
16 would function as promised.

17 102. Defendant owed a duty to Plaintiff and members of the Class to implement processes
18 that would detect major security vulnerabilities, such as the Defects, in a timely manner.

19 103. Defendant also owed a duty to disclose the material fact that its processors were
20 defective.

21 104. But for Defendant's breach of its duties, Plaintiff and members of the Class would not
22 have purchased or leased—or would have paid substantially less for—Intel processors (or devices
23 containing Intel processors) had they known of the Defects and the reduction in processing
24 performance associated with efforts necessary to mitigate the substantial security risks presented by
25 the Defects.

26 105. Plaintiff and members of the Class were foreseeable victims of Defendant's
27 wrongdoing, and Defendant knew, or should have known, that its processors would cause damages
28 to Plaintiff and members of the Class.

1 114. Plaintiff and members of the Class seek an order requiring Defendant to disgorge its
2 gains and profits to Plaintiff and members of the Class, together with interest, in a manner to be
3 determined by the Court.

4 **COUNT V**

5 **VIOLATION OF CALIFORNIA’S UNFAIR COMPETITION LAW**

6 **CALIFORNIA BUSINESS & PROFESSIONS CODE § 17200, ET SEQ.**

7 115. Plaintiff incorporates and realleges each preceding paragraph as though fully set forth
8 herein.

9 116. Plaintiff brings this count on behalf of itself and members of the Class.

10 117. California Business & Professions Code § 17200, *et seq.* (the “UCL”) prohibits “any
11 unlawful, unfair or fraudulent business act or practice.”

12 118. At all relevant times, Defendant has maintained substantial operations in, regularly
13 conducted business throughout, and engaged in the conduct described herein within the State of
14 California.

15 119. Defendant, in connection with the Defects, has engaged in unfair, unlawful, and
16 fraudulent business acts and practices in violation of the UCL in that: (1) Defendant’s conduct is
17 immoral, unethical, oppressive, unconscionable, and substantially harmful to Plaintiff and members
18 of the Class; (2) any justification for Defendant’s conduct would be outweighed by the gravity of the
19 injury to Plaintiff and members of the Class; (3) Defendant’s conduct violates the common law; and
20 (4) Defendant’s conduct deceived and defrauded Plaintiff and members of the Class.

21 120. Defendant’s unfair, unlawful, and fraudulent business practices were likely to deceive
22 a reasonable consumer. Plaintiff and members of the Class used Defendant’s products and had
23 business dealings with Defendant either directly or indirectly through third-parties, and were the
24 intended recipients of Defendant’s processors.

25 121. As a result of Defendant’s systematic unlawful, unfair, and fraudulent conduct,
26 Plaintiff and members of the Class have been injured. The harm caused by this conduct vastly
27 outweighs any legitimate business utility it possibly could have. Plaintiff and members of the Class
28

1 are entitled to restitution, including disgorgement of profits, costs, and attorneys' fees in amounts to
2 be determined at trial.

3 122. Defendant's conduct is or may well be continuing and ongoing. Accordingly, Plaintiff
4 and members of the Class are entitled to injunctive relief to prohibit or correct such ongoing acts of
5 unfair competition, in addition to obtaining equitable monetary relief.

6 **VIII. PRAYER FOR RELIEF**

7 WHEREFORE, Plaintiff, on behalf of itself and all others similarly situated, respectfully
8 request that this Court enter judgment against Defendant and in favor of Plaintiff and the Class, and
9 award the following relief:

- 10 A. An order certifying this action as a class action pursuant to Rule 23 of the Federal
11 Rules of Civil Procedure, declaring Plaintiff as the representative of the Class, and
12 Plaintiff's counsel as counsel for the Class;
- 13 B. An order awarding declaratory relief and enjoining Defendant from continuing the
14 unlawful, deceptive, harmful, and unfair business conduct and practices alleged
15 herein;
- 16 C. Appropriate injunctive and equitable relief;
- 17 D. A declaration that Defendant is financially responsible for all Class notice and the
18 administration of Class relief;
- 19 E. Costs, restitution, damages, including statutory and punitive damages, penalties, and
20 disgorgement in an amount to be determined at trial;
- 21 F. An order requiring Defendant to pay both pre- and post-judgment interest on any
22 amounts awarded;
- 23 G. An award of costs and attorneys' fees; and
- 24 H. Such other or further relief as the Court may deem appropriate, just, and equitable.

25 **IX. DEMAND FOR JURY TRIAL**

26 Plaintiff hereby demands a trial by jury.
27
28

1 DATED: January 12, 2018

Respectfully submitted,

2 **KESSLER TOPAZ MELTZER**
3 **& CHECK, LLP**

4 /s/ Eli R. Greenstein

5 ELI R. GREENSTEIN (Bar No. 217945)

6 egreenstein@ktmc.com

JENNIFER L. JOOST (Bar No. 296164)

7 jjoost@ktmc.com

8 STACEY M. KAPLAN (Bar No. 241989)

9 skaplan@ktmc.com

10 One Sansome Street, Suite 1850

11 San Francisco, CA 94104

12 Tel: (415) 400-3000

13 Fax: (415) 400-3001

14 -and-

15 JOSEPH H. MELTZER

16 jmeltzer@ktmc.com

17 SAMANTHA HOLBROOK

18 sholbrook@ktmc.com

19 280 King of Prussia Road

20 Radnor, PA 19087

21 Tel: (610) 667-7706

22 Fax: (610) 667-7056

23 *Attorneys for Plaintiff Zog, Inc.*

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

Zog, Inc.

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

(c) Attorneys (Firm Name, Address, and Telephone Number) Kessler Topaz Meltzer & Check, LLP 280 King of Prussia Road, Radnor, PA 19087 610-667-7706

DEFENDANTS

Intel Corporation

County of Residence of First Listed Defendant Santa Clara, California (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 X 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)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship: Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, Incorporated or Principal Place of Business In This State, Incorporated and Principal Place of Business In Another State, Foreign Nation.

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

Large table with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, HABEAS CORPUS, OTHER, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

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

- X 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: Breach of Implied Warranty; Breach of Express Warranty; Negligence; Unjust Enrichment; California Unfair Competition Law

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: X Yes No

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

JUDGE (see attached) DOCKET NUMBER (see attached)

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

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

DATE 01/12/2018

SIGNATURE OF ATTORNEY OF RECORD

s/ Eli R. Greenstein

| | Case Name | Case Number/ Judge | Date Filed |
|----|---|---|-------------------|
| 1. | <i>Garcia, et al. v. Intel Corporation</i> | 5:18-cv-00046-EDJ / Edward J. Davilla | January 1, 2018 |
| 2. | <i>Reis, et al. v. Intel Corporation</i> | 5:18-cv-00074-SVK / Susan van Keulen | January 4, 2018 |
| 3. | <i>Carl Jones, et al. v Intel Corporation</i> | 5:18-cv-00105-NMC / Nathanael M. Cousins | January 5, 2018 |
| 4. | <i>Rinn, et al. v. Intel Corporation</i> | 5:18-cv-00111-BLF / Beth Labson Freeman | January 5, 2018 |
| 5. | <i>West, et al. v. Intel Corporation</i> | 5:18-cv-00146-BLF / Beth Labson Freeman | January 8, 2018 |
| 6. | <i>Bahcevan, et al. v. Intel Corporation</i> | 5:18-cv-00187-SVK / Susan van Keulen | January 9, 2018 |
| 7. | <i>Dean, et al. v. Intel Corporation</i> | 5:18-cv-00210-HRL / Howard R. Lloyd | January 9, 2018 |
| 8. | <i>Lee, et al. v. Intel Corporation</i> | 5:18-cv-00235-SVK / Susan van Keulen | January 10, 2018 |