BATHAEE DUNNE LLP
Yavar Bathaee (CA 282388)
yavar@bathaeedunne.com
Andrew C. Wolinsky (CA 345965)
awolinsky@bathaeedunne.com
445 Park Avenue, 9th Floor
New York, NY 10022
Tel.: (332) 322-8835

Brian J. Dunne (CA 275689)
bdunne@bathaeedunne.com
Edward M. Grauman (*p.h.v. to be sought*)
egrauman@bathaeedunne.com
901 South MoPac Expressway
Barton Oaks Plaza I, Suite 300
Austin, TX 78746
Tel.: (213) 462-2772

Attorneys for Plaintiffs and the Proposed Classes

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

DARQUES SMITH, RENEE WALTRIP, BRIAN CAMERON, ELIZABETH CORDOVA, and MICHAEL WORLEY, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

INTEL CORPORATION, a Delaware corporation,

Defendant.

Case No. 5:23-cv-5761

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

INTRODUCTION

1. Plaintiffs are purchasers of Intel Central Processing Units ("CPUs") and computers with Intel CPUs affected by a critical vulnerability, called Downfall. Downfall, which was caused by a defect that Intel knew about since 2018 but never disclosed, can only be "fixed" according to Intel by adopting a patch that slows CPU performance by as much as 50% during certain ordinary computing tasks, including photo and video editing, gaming, and encryption.

2. Plaintiffs are left with defective CPUs that are either egregiously vulnerable to attacks or must be slowed down beyond recognition to "fix" them. At bottom, these are not the CPUs Plaintiffs and class members purchased. They perform quite differently and are worth far less. And for years, Intel has known that all this would eventually occur.

3. Plaintiffs seek redress for Intel's knowing decision to sell processors with an egregiously defective design without telling the truth, and for a supposed "fix" that destroys their CPUs' performance—a pernicious cure that rivals the (quite serious) sickness requiring it.

* * *

4. Intel's CPUs drive billions of computers throughout the world. They are designed for performance, including while multitasking.

5. In the 1990s, high-end CPUs began to incorporate a design technique called branch prediction—a speculative procedure designed to prevent the CPU from stalling while waiting for information from relatively slow system memory. This technique permitted substantial increases in computing power and efficiency, and gave rise to further "speculative execution" techniques, including subsystems that allow CPUs to execute instructions out of order and even to predict the outcome of future instructions. For more than a decade, every modern CPU has implemented these execution features. They are, in the modern era, a core functionality of every CPU that Intel and its competitors make, and sufficient, expected CPU performance cannot be achieved without them.

6. Modern CPUs also enforce "segmentation," meaning that privileged computer programs and the resources they use (*i.e.*, system memory and hardware) must be segregated from programs run by users. This too is a core functionality in every modern CPU.

7. Intel, however, defectively designed these critical systems in billions of its CPUs. When Intel's CPUs speculatively execute instructions, they are supposed to discard the results of an execution if the CPU guessed wrong. Instead, Intel's CPUs leave "side effects"—data remains in temporary buffers or in the CPU's cache memory even after the speculative execution's results are discarded. Worse yet, Intel's CPUs allow speculatively executed code to see system resources and information that only an operating system or privileged computer program should be able to see, violating segmentation.

8. This design defect manifested in catastrophic form in January 2018 when it became public that Intel's CPUs suffered from vulnerabilities called Spectre and Meltdown—attack vectors that exploited Intel's defective design. These vulnerabilities had staggering consequences, and Intel scrambled to fix them, promising both firmware and hardware mitigations in its CPUs, particularly in its then-forthcoming 9th generation of CPUs.

9. In the summer of 2018, as Intel was dealing with the fallout of Spectre and Meltdown and promising a hardware fix in future CPU generations, Intel received two separate vulnerability reports from third parties flagging a particular set of instructions on Intel's CPUs, called the Advanced Vector Extensions ("AVX"). Two separate researchers told Intel that its AVX instructions, which perform critical CPU functionality associated with encryption, media, gaming, and the execution of memory-optimized computer programs, were vulnerable to the same class of attack as Spectre and Meltdown. Intel contemporaneously acknowledged both reports.

10. However, despite promising a hardware redesign to mitigate speculative execution vulnerabilities during the exact time period researchers disclosed the vulnerabilities in Intel's AVX instructions, Intel did nothing. It did not fix its then-current chips, and over ***three successive generations***, Intel did not redesign its chips to ensure that AVX instructions would operate securely when the CPU speculatively executed them. Worse yet, Intel had implemented ***secret buffers*** associated with these instructions, which it never disclosed to anyone. These secret buffers, coupled with side effects left in CPU cache, opened what was tantamount to a backdoor in Intel's CPUs, allowing an attacker to use AVX instructions to easily obtain sensitive information from memory—including encryption keys used for Advanced Encryption Standard ("AES") encryption—by exploiting the very design flaw that Intel had supposedly fixed after Spectre and Meltdown.

11. For years, Intel knowingly sold billions of CPUs with this massive vulnerability, which imperiled the foundation of secure networking, secure communications, and secure data storage for Intel CPUs used in PCs, in cloud servers, and in embedded computers used across the country in functional MRIs, power grids, and industrial control systems.

12. On August 24, 2022, a Google engineer, who had discovered the undisclosed buffers associated with the AVX instructions, reported to Intel that a decade of its CPUs were vulnerable to the same sort of attacks that gave rise to Spectre and Meltdown through Intel's AVX instructions, and Intel responded by asking the engineer not to publish the results.

13. On August 18, 2023, approximately a year after Intel was informed of the AVX vulnerability, the Google engineer published an academic paper and a website for the first time disclosing Intel's secret AVX buffers and its CPUs' continuing vulnerability to the same category of attacks as Spectre and Meltdown, which he called "Downfall."

14. Billions of CPUs are affected, particularly Intel's 6th through 11th generation CPUs.

15. Since the release of its 9th generation CPUs in October 2018, Intel has told customers that it engineered a hardware fix for the design flaw that gave rise to Spectre and Meltdown, and that all 9th generation CPUs (and later) incorporated it. And Intel had told customers that all of its CPUs' vulnerabilities had been "mitigated"—though at a significant performance cost—to deal with Spectre and Meltdown. Yet, since 2018, before many of these supposedly fixed CPUs were released, Intel knew its AVX instructions were at risk from the same class of attacks as Spectre and Meltdown.

16. Intel—which had exclusive knowledge about the relevant instructions, the secret buffers, its CPU design, and its Spectre/Meltdown mitigation—said nothing to CPU and computer purchasers as it sold billions of knowingly flawed CPUs over the course of several years.

17. When the Downfall vulnerability became public, Intel issued a microcode update, which supposedly mitigated the Downfall vulnerability. In reality, Intel's "mitigation" had handicapped the very systems, namely speculative execution and branch prediction, that are central to the function of every modern CPU, resulting in as much as a 50% performance degradation in affected CPUs.

18. Plaintiffs are left with defective CPUs that must be severely impaired in performance and functionality to "mitigate" their vulnerability to Downfall. These are not the CPUs they purchased.

19. Plaintiffs have been injured by Intel's willful decision not to tell the truth about its processors, leaving Plaintiffs and proposed class members—people and companies that bought affected Intel CPUs, or computers incorporating them—with CPUs and computers that are worth far less than they paid for them. At the same time, these CPUs and the computers built around them perform far worse than expected during ordinary use, remain defectively designed, and are severely vulnerable to an entire class of devastating cyberattacks.

20. Intel's affected CPUs—billions of them—are to this day defectively designed, and Intel has instituted no recall, implemented no repair program, and provided no plan to fix the underlying design defect. Plaintiffs seek damages and equitable relief.

PARTIES

I. PLAINTIFFS

21. Plaintiff Darques Smith is a resident of San Diego, California. In February 2022, Mr. Smith purchased a Dell Alienware laptop with an 11th Generation Intel Core i7-11800H processor operating on a Tiger Lake H CPU architecture from BestBuy.com. Mr. Smith uses his computer for, among other things, gaming; programming and coding with Video Studio; and editing videos and photos with Photoshop.

22. Mr. Smith reviewed and relied on online discussions, reviews, and marketing materials, including on PCMag.com, Dell's website, and BestBuy's website, before deciding to purchase his laptop operating on a Tiger Lake H CPU architecture. None of the representations received and reviewed by Mr. Smith contained any disclosure relating to the defectively designed CPU in his laptop. None of the representations received and reviewed by Mr. Smith disclosed that his Intel CPU would, when integrated into his laptop, make it uniquely vulnerable based on design defects known to Intel.

23. Mr. Smith installs regular updates on his computer, as prompted by his computer's operating system. Mr. Smith has noticed, in the last few months, significant performance issues with his computer when using Photoshop and when he plays games on his laptop. Specifically, Mr. Smith's laptop operates noticeably slower when he uses Photoshop and during gameplay.

24. Mr. Smith would not have purchased his laptop with an Intel CPU at the price he paid had he known about the defect described in this Complaint. Intel has not fixed the problems with Mr. Smith's

CPU attributable to the Downfall defect. Mr. Smith would like to buy Intel products in the future, but absent relief cannot rely on Intel's statements and marketing.

25. Plaintiff Renee Waltrip is a resident of Kansas City, Kansas. In June 2020, Ms. Waltrip purchased an Intel Core i7-9700K processor operating on a Coffee Lake CPU architecture from MicroCenter. In November 2021, Ms. Waltrip purchased an Intel Core i9-9900K processor operating on a Coffee Lake CPU architecture from NewEgg.com. Ms. Waltrip built her own computers with those processors. Ms. Waltrip uses those computers for, among other things, video editing.

26. Ms. Waltrip has built her own computers for years, and selecting the right CPU is important to her. As she made her CPU purchasing decisions in 2020 and 2021, she reviewed and relied upon Intel's marketing, websites like Tom's Hardware, YouTube video reviews, and posts on Reddit, before deciding to purchase her CPUs operating on a Coffee Lake architecture. None of the representations reviewed by Ms. Waltrip disclosed that her Intel CPUs would, when integrated into the computers she built, make those computers uniquely vulnerable based on design defects known to Intel.

27. Ms. Waltrip has installed the microcode update issued by Intel that purports to mitigate the Downfall vulnerability. Since installing that update, Ms. Waltrip has noticed significant performance issues during video editing. Specifically, video editing applications have been running noticeably and unacceptably slower since Ms. Waltrip installed the microcode update.

28. Ms. Waltrip would not have purchased her Intel CPUs at the price she paid had she known about the defect described in this Complaint. Intel has not fixed the problems with Ms. Waltrip's CPU attributable to the Downfall defect. Ms. Waltrip would like to buy Intel products in the future, but absent relief cannot rely on Intel's statements and marketing.

29. Plaintiff Brian Cameron is a resident of Northbrook, Illinois. In February 2020, Mr. Cameron purchased an Intel Core i9-9900K processor operating on a Coffee Lake CPU architecture from MicroCenter. Mr. Cameron built his own computer with this processor. Mr. Cameron uses his computer for, among other things, gaming, streaming, and surfing the Internet.

30. Mr. Cameron has built computers for himself for years, and selecting the right CPU is important to him. As he made his CPU purchasing decision in 2020, he reviewed and relied upon Intel's marketing, online reviews, and the PCPartPicker.com website before deciding to purchase his CPU

operating on a Coffee Lake architecture. None of the representations reviewed by Mr. Cameron disclosed that his Intel CPU would, when integrated into the computer he built, make the computer uniquely vulnerable based on design defects known to Intel.

31. Mr. Cameron installs regular updates on his computer, as prompted by his computer's operating system. Mr. Cameron has noticed, in the last few months, significant performance issues with his computer when gaming. Specifically, when playing games like Starfield (released in 2023) and Star Wars Jedi Survivor (released in 2023), his computer operates noticeably slower. Mr. Cameron believes that the performance problems are related to an issue with his CPU, because his computer is slower even when running much older games like Team Fortress 2 (released in 2007) and Wolfenstein: The New Order (released in 2014).

32. Mr. Cameron would not have purchased his Intel CPU at the price he paid had he known about the defect described in this Complaint. Intel has not fixed the problems with Mr. Cameron's CPU attributable to the Downfall defect. Mr. Cameron would like to buy Intel products in the future, but absent relief cannot rely on Intel's statements and marketing.

33. Plaintiff Elizabeth Cordova is a resident of Orange, California. In January 2020, while she was living in Oregon, Ms. Cordova purchased a CyberPower desktop computer with an 8th Generation Intel Core i7-8700 processor operating on a Coffee Lake CPU architecture from NewEgg.com. The computer was shipped to her in Oregon, where she lived at the time. Ms. Cordova purchased her computer principally for an advertising business that she runs, which involves use of Photoshop and Microsoft Publisher to edit photos. Ms. Cordova had not been planning to buy a new computer, but, upon learning of the Downfall defect described in this complaint and the performance issues resulting from Intel's purported mitigation, is considering replacing it.

34. Ms. Cordova reviewed and relied on online discussions, reviews, and marketing materials, as well as discussions with friends, before deciding to purchase her desktop computer operating on a Coffee Lake CPU architecture. None of the representations received and reviewed by Ms. Cordova contained any disclosure relating to the defectively designed CPU in her desktop computer. None of the representations received and reviewed by Ms. Cordova disclosed that her Intel CPU would, when integrated into her desktop computer, make it uniquely vulnerable based on design defects known to Intel.

35. Ms. Cordova installs regular updates on her computer, as prompted by her computer's operating system. Ms. Cordova has noticed, in the last few months, significant performance issues with her computer when using Photoshop and Microsoft Publisher. Specifically, Ms. Cordova's computer operates noticeably slower when she uses Photoshop and Microsoft Publisher.

36. Ms. Cordova would not have purchased her desktop computer with an Intel CPU at the price she paid had she known about the defect described in this Complaint. Intel has not fixed the problems with Ms. Cordova's CPU attributable to the Downfall defect. Ms. Cordova would like to buy Intel products in the future, but absent relief cannot rely on Intel's statements and marketing.

37. Plaintiff Michael Worley is a resident of Coon Rapids, Minnesota. In June 2022, Mr. Worley purchased an MSI laptop from Get-it-Now LLC (dba Home Choice) with a 9th generation Intel Core i9-9900K processor operating on a Coffee Lake CPU architecture. Mr. Worley purchased his laptop principally for a marketing business that he runs. Mr. Worley uses the Sony Vegas application for video editing and Photoshop for photo editing, as well as other photo editing software for his DSLR camera.

38. Mr. Worley regularly comes into contact with sensitive personal identifying information of customers, and is concerned that the security issues associated with the defect described in this Complaint could compromise his customers' data. Since learning of the Downfall vulnerability, Mr. Worley has largely used his phone for business purposes.

39. Mr. Worley reviewed and relied on online discussions, reviews, and marketing materials, before deciding to purchase his desktop computer operating on a Coffee Lake CPU architecture. None of the representations received and reviewed by Mr. Worley contained any disclosure relating to the defectively designed CPU in his desktop computer. None of the representations received and reviewed by Mr. Worley disclosed that his Intel CPU would, when integrated into his desktop computer, make it uniquely vulnerable based on design defects known to Intel.

40. Before he mostly stopped using his laptop, Mr. Worley installed regular updates on his laptop, as prompted by his computer's operating system. Mr. Worley noticed significant performance issues with his laptop during startup, and the computer seemed to lag significantly when switching between programs. When Mr. Worley turned on and logged into his laptop to obtain information to provide to counsel for this Complaint, he noted that his laptop's performance was "ridiculously slow."

41. Mr. Worley would not have purchased his laptop with an Intel CPU at the price he paid had he known about the defect described in this Complaint. Intel has not fixed the problems with Mr. Worley's CPU attributable to the Downfall defect. Mr. Worley would like to buy Intel products in the future, but absent relief cannot rely on Intel's statements and marketing.

II. DEFENDANT

42. Defendant Intel Corporation ("Intel") is a Santa Clara, California-based corporation incorporated under the laws of Delaware. Intel's headquarters are located at 2200 Mission College Boulevard, Santa Clara, California 95054.

43. Intel has been based out of California for fifty-four years, providing high-tech jobs to Californians and supporting the California economy through research and development ecosystem spending, sourcing activities, and tax revenue. Intel directs its operations from California and maintains other offices within the state, including in San Jose, San Francisco, San Diego, Folsom, and Los Angeles. Intel employs approximately 13,500 employees in California as of January 2022.

44. Intel describes its Santa Clara headquarters as its "Mission" campus. The Santa Clara headquarters is involved in engineering, design, research and development, and software engineering. Intel's Mission campus houses several corporate organizations, including sales and marketing, legal, supply network, and human resources. With more than 7,000 employees, Intel is the largest employer in Santa Clara.

45. Founded in 1968 by Gordon Moore, Robert Noyce, and Arthur Rock, Intel has since been one of the most important companies in California's Silicon Valley.

46. Intel's headquarters, its Mission Campus, which was built on a pear orchard in 1970, has been the nerve center of its operations since founding. As Intel explains on its website:

> Intel purchased our first piece of property on a 26-acre pear orchard in Santa Clara, California in 1970. Santa Clara is home to Intel's headquareters and the flagship of Intel's Museum. Today, more than 13,500 employees across California design, develop, and support semiconductor products that help to secure, power and connect billions of devices and the infrastructure of the smart, connected world—from the cloud to the network to the edge and everything in between. These innovations are key to making the world safer, help builds *[sic]* healthy and vibrant communites and increases *[sic]* productivity.

47. Intel's management, core engineering, sales, marketing, accounting, distribution, and operations personnel work from its California offices. Intel designs its CPUs, including the CPUs at issue in this complaint, in California, and it markets them from California.

48. As Intel acknowledges on its website, its Mission Campus is the nerve center of its operations, engineering, sales, and communications:

> Mission campus, our Santa Clara site *[sic]* is involved in engineering, design, research and development, and software engineering, and houses several corporate organizations, including sales and marketing, legal, supply network, and human resources. With more than 7,000 employees, Intel is the largest employer in Santa Clara.

49. All of Intel's communications, including about the CPUs in this complaint, are made from its Santa Clara offices. Indeed, Intel's press releases all begin, "SANTA CLARA, Calif."

50. Intel is an Integrated Design Manufacturer that designs and manufactures, among other things, microprocessors used in computing systems, including desktops, laptops, embedded devices, and commercial/data center systems such as servers.

51. Intel sells CPUs, including the CPUs at issue in this Complaint, to original equipment manufacturers ("OEMs") and original design manufacturers, cloud service providers, and other equipment manufacturers, with certain microprocessors available in direct retail outlets.

52. Intel also sells CPUs, including the CPUs at issue in this Complaint, through authorized resellers, like MicroCenter and Newegg.com.

53. Intel's net revenue at year-end 2022 was $63.1 billion, and $79 billion in 2021. As of 2020, Intel was the largest manufacturer of microchips in the United States. Its net revenue from its PC-centric business—Client Computing Group ("CCG"), which produces hardware components used in desktop and notebook computers—was approximately $37 billion in 2018, $37.15 billion in 2019, $40.06 billion in 2020, $41.07 billion in 2021, and $31.71 billion in 2022. CCG consistently accounts for over half of Intel's total revenue.

JURISDICTION AND VENUE

54. This Court has personal and subject matter jurisdiction over all parties to and causes of action asserted in this Complaint.

55. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d), because at least one member of the proposed Classes is of diverse citizenship from Defendant Intel, the proposed Classes consist of 100 or more members, and the aggregate claims of the members of the proposed Classes exceed $5 million, exclusive of interest and costs.

56. This Court has personal jurisdiction over Intel because Intel's principal place of business is in the State of California, and Intel is therefore subject to general jurisdiction in this State. Additionally, the conduct alleged in this Complaint occurred in and/or emanated from the State of California.

57. Venue is proper in the Northern District of California pursuant to 28 U.S.C. §§ 1391(b)(1) and (2) because Intel resides in this judicial district and a substantial part of the events and/or omissions that give rise to Plaintiffs' claims occurred in this judicial district.

DIVISIONAL ASSIGNMENT

58. This action is properly assigned to the San Jose Division of this District, pursuant to Civil Local Rule 3-2(c) and (e), because Intel is headquartered in Santa Clara County (which is served by the San Jose Division) and a substantial part of the events or omissions that give rise to the claims in this action occurred there.

FACTS

I. INTEL'S CPUS ARE DEFECTIVELY DESIGNED

A. The Protection of Privileged CPU and Memory Resources

59. A central processing unit ("CPU") executes instructions and interacts with a system's memory. The CPU contains internal, high-speed memory, called registers, which it uses to process data according to instructions provided to it as part of a computer program.

60. A computer's random access memory, unlike the CPU's registers, is orders of magnitude slower. A CPU can therefore move data in and out of its internal registers far faster than it can interact with system memory.

61. A CPU has a predefined set of instructions that it understands. For example, all CPUs have an instruction that adds two numbers together and outputs the result to one of the CPU's internal registers. The combined set of instructions available on a CPU is called its instruction set, or ISA.

62. Intel CPUs generally use what is referred to as the x86 ISA. These instructions are derived from the original instructions used as part of Intel's 8086 line of microprocessors released in 1978. Later Intel CPUs are generally backwards compatible with older CPUs, as they are designed to handle prior instruction sets. This allows respective computer programs to run on most computers built around Intel and Intel-compatible CPUs.

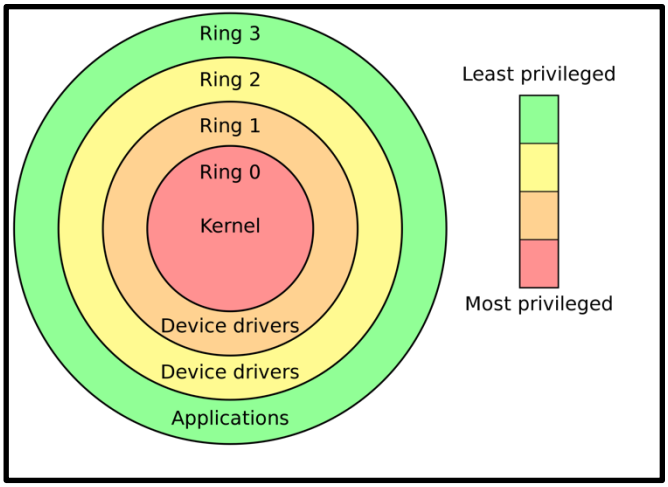
63. CPUs often run foundational instructions that comprise an operating system. An operating system is a computer program that, among other things, controls input and output for the computer; writes to and from devices; manages system resources across computer programs; and writes to and from system memory. Because an operating system interacts with sensitive system resources, a CPU is designed to ensure that only the operating system can access such resources.

64. CPUs also run computer programs executed by a system's users. These programs should not have access to memory locations outside of the program's scope—particularly memory and CPU resources used by the operating system.

65. Like most modern CPUs, Intel's CPUs divide memory and resources accessible to an operating system from those available to an ordinary computer program. An operating system operates

in a privileged space, sometimes referred to as "Kernel Space," and ordinary programs run in "User Space."

66. Specifically, Intel's CPUs provide for several "protection rings" of privilege, with the lowest number ring, ring 0, being reserved for the operating system.



67. Intel CPUs generally use only two rings—ring 0 and ring 3. Ring 3 is reserved for user space. This division is necessary for most modern computers. It allows operating systems such as Windows and Linux to ensure that ordinary user programs cannot access privileged resources that should only be available to the operating system.

68. The division between so-called "user space" and operating system (some times called kernel) space—*i.e.*, a privilege separation between user-level resources/execution and system-level resources/execution—accomplishes both security and stability. Because computers multitask, meaning they run multiple programs at once, protection rings that segment resources prevent computer programs from interfering with each other's memory and with system resources.

69. This separation also ensures that a malicious actor cannot write a user program that accesses privileged system resources, such as operating system-level memory containing encryption keys, passwords, or other sensitive information.

70. In addition to enforcing a separation of the system memory between that used by ordinary computer programs and that used by the operating system, modern CPUs also prevent ordinary programs from accessing certain of the CPU's internal registers and certain CPU instructions.

71. Intel's CPUs provide such protections as part of every modern CPU the company sells. Intel's largest competitor for x86 compatible CPUs, AMD, also implements the same protections, though its hardware implementation of them differs from Intel's.

72. In addition to registers, modern CPUs also use another high-speed memory system, called a memory cache. Specifically, frequently and/or recently accessed data is "cached"—temporarily stored in dedicated high-speed memory—so that the CPU does not have to wait for a retrieval from significantly slower system memory when it seeks such frequently accessed data.

73. Modern Intel CPUs usually have several "cores"—separate processing units—which allow the CPU to execute programs in parallel. Each core generally has its own Level 1 (or L1) cache, and higher level caches—such as Level 2 (L2) cache—that are shared across cores.

74. Certain Intel CPUs also maintain instruction "buffers" in system memory, which store data related to a particular CPU instruction.

B. Branch Prediction, Out of Order Execution, and Speculative Execution

75. Although CPUs in the 1980s and early 1990s executed instructions sequentially, modern CPUs use engineered techniques to attempt to mitigate the mismatch between CPU speeds and the speed of system memory (or even slower, a system's permanent storage).

76. In many cases, a CPU that sequentially executes instructions will encounter a conditional instruction—one dependent on a value stored in memory. The CPU must wait until that value is fetched from memory (which is relatively slow to access) to continue execution, stalling the CPU from carrying out further instructions until it is able to determine the value of data stored in memory.

77. The solution to this problem, incorporated in all modern general purpose CPUs, is to predict what a program will likely do when the processor encounters a conditional instruction (*i.e.*, an instruction dependent on some in-memory value). This is called Branch Prediction.

78. Since the mid-1990s, almost all Intel CPUs used for general purpose computers employ branch prediction; in fact, all modern CPUs do. Branch prediction became necessary for swift, stable operation as CPUs became far faster than random access memory and input/output operations.

79. Closely related to branch prediction is a technique called "speculative execution." (Indeed, branch prediction is a form of speculative execution.) All modern CPUs—including Intel's—

speculatively execute for the reasons discussed above: waiting for a value from memory is so slow in comparison to modern execution speeds that a conditional instruction (one that relies on a value) can stall a computer, and significantly impact speed and even stability systemwide when this process is multiplied over the number of conditional instructions across an entire system's control flow.

80. Speculative execution works like this: faced with a conditional instruction—*i.e.*, an instruction based on a value that must be retrieved—a CPU guesses what the value will be instead of waiting for its retrieval from memory, and executes code based on that guess. If, when the memory contents are fetched, the guess is incorrect, the CPU discards the "speculative" code. If the guess was right, the CPU has already executed past the conditional instruction (*e.g.,* conditional branch) without waiting, obviating the need to wait for memory or system input/output to continue executing.

81. As *Tech Republic* explains in a May 15, 2019 article, titled "Spectre and Meltdown explained: A comprehensive guide for professionals":

> Speculative execution allows processors to speculate on future instruction directions and proactively execute instructions along these paths before knowing if the instructions are correct. An example in the Spectre paper, "Consider an example where the program's control flow depends on an uncached value located in external physical memory. As this memory is much slower than the CPU, it often takes several hundred clock cycles before the value becomes known. Rather than wasting these cycles by idling, the CPU attempts to guess 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 arrives from memory, the correctness of the guess is checked. If correct, the results are committed, "yielding a significant performance gain as useful work was accomplished during the delay." If wrong, the speculative execution is discarded. Performance wise, this is transparent—the speeds are comparable to idling, as if the speculative execution never occurred. . . .

82. Modern Intel CPUs, including the CPUs at issue here, use speculative execution to allow the CPU to prevent stalls. Indeed, every modern general purpose CPU employs some form of branch prediction and speculative execution. They are an inherent part of a modern CPU's computation process, and modern CPU performance is not possible without them.

83. Importantly, to maintain security, a CPU must be completely cleared after speculatively executing incorrectly (*i.e.*, guessing wrong about a condition), and such execution should not change any other values stored in the CPU or in memory. It must be as if the speculatively executed code never existed—or serious security problems arise.

84. As *Tech Republic* explains:

> In terms of security, speculative execution requires executing a program in potentially incorrect ways. To maintain functional correctness, these incorrectly speculated, or transient executions, are intended to not be exposed to the program. They are not committed, and are flushed from the execution pipeline, reverting architectural effects the instructions may have had.

85. Put simply, the guessed series of instructions—referred to as transient instructions—must not create "side effects," meaning they must not alter CPU registers, cache, buffers, or other memory locations. This is because the transient instructions may be entirely erroneous, nonsensical, or may even access privileged resources the CPU would not ordinarily allow the main instruction line associated with a program to access.

86. Intel's CPUs, like all modern CPUs, also provide for out-of-order execution. Certain instruction sequences are not dependent on other instructions in a computer program and can be executed in parallel. Intel's CPUs, like those of its competitors ARM and Intel, simultaneously evaluate such independent instructions, making their result available to the program when ultimately needed.

87. *Tech Republic* explains:

> Out-of-order execution allows for the simultaneous use of all the execution units in a CPU core. As explained in the Meltdown paper, "Instead of processing instructions strictly in the sequential program order, the CPU executes them as soon as all required resources are available. While the execution unit of the current operation is occupied, the other execution units run ahead. Hence, instructions can be run in parallel as long as their results follow the architectural definition."
>
> The state of instructions processed out of order are stored in a re-order buffer, from which they are committed in order.

88. Just as with speculative execution, out-of-order execution must not have side effects—that is, buffers, CPU cache, and the contents of memory should not reflect the results of out-of-order execution once it is complete and reassembled for use by the CPU.

C. Intel's CPU Design Fails to Safeguard Privileged Resources from Side Effects Resulting from Transient Instruction Branches

89. Intel's branch prediction, speculative execution, and out-of-order execution systems are fatally flawed at the hardware level. Although the results of speculative or out-of-order instructions are discarded if a branch is incorrectly predicted, Intel fails to ensure that side effects of these instructions do not linger in various parts of the CPU accessible to the running program—or other simultaneously running programs).

90. For example, Intel's CPUs cause the CPU's cache to store memory information previously required by speculatively executed code, meaning that even if the transient code is discarded, some data remains in the CPU's cache. This means that data that may be erroneous, insecure, or malicious remains accessible by the main program or other programs even after the transient code is discarded.

91. Intel's CPUs also use instruction buffers, where transient code may store information associated with particular instructions. If a program or Intel's hardware does not flush a buffer when transient code is discarded, data may remain in the buffer that would not otherwise be accessible—and in many cases, should not be accessible—by the main program or other simultaneously running programs.

92. Intel's design does not ensure that transient code is prevented from making lingering changes to shared CPU resources, which make its CPUs vulnerable to an entire class of attacks, called transient execution attacks.

93. The vulnerability flows directly from Intel's hardware design. Its branch prediction, speculative execution, and out-of-order execution systems have access to system cache and shared buffers.

94. This design is fundamentally flawed and gives rise to many variations of attacks that exploit the same fundamental problem: transient code can leave lingering information that the main program and other programs could not have accessed due to segmentation protections.

95. In other words, Intel's speculative and out-of-order execution systems undermine the protections that users expect from modern CPUs—a CPU-enforced division between kernel and user space (between privileged and non-privileged system resources).

96. Intel's CPUs are defectively designed because they allow transient instructions to cause side effects even after discarded. This defect stems directly from Intel's hardware design, and as explained below, this design has led to catastrophic problems for purchasers of Intel's CPUs and computers with Intel CPUs.

D. Intel's Defective Design Results in the Spectre and Meltdown Class of Vulnerabilities

97. On January 3, 2018, a catastrophic set of vulnerabilities in Intel's CPUs became public for the first time. Intel's faulty hardware design had resulted in vulnerabilities of unprecedented scale, which the third-parties who had discovered them named Spectre and Meltdown, respectively.

98. As the United States Cybersecurity and Infrastructure Security Agency recounted in an article titled, "Meltdown and Spectre Side-Channel Vulnerability Guidance," dated May 1, 2018:

> On January 3, 2018, the National Cybersecurity and Communications Integration Center (NCCIC) became aware of security vulnerabilities—known as Meltdown and Spectre—that affect modern computer processors. These vulnerabilities can be exploited to steal sensitive data present in a computer system's memory.
>
> CPU hardware implementations are vulnerable to side-channel attacks, referred to as Meltdown and Spectre. Meltdown is a bug that "melts" the security boundaries normally enforced by the hardware, affecting desktops, laptop, and cloud computers. Spectre is a flaw an attacker can exploit to force a program to reveal its data. The name derives from "speculative execution"—an optimization method a computer system performs to check whether it will work to prevent a delay when actually executed. Spectre affects almost all devices including desktops, laptops, cloud servers, and smartphones.

99. Spectre and Meltdown provided an attacker with access to information stored in privileged memory, which a program in user space should never be able to access.

100. As *Tech Republic* explains in its May 15, 2019 "Spectre and Meltdown explained: A comprehensive guide for professionals" article:

> In the most basic definition, Spectre is a vulnerability allowing for arbitrary locations in the allocated memory of a program to be read. Meltdown is a vulnerability allowing a [software] process to read all memory in a given system. Spectre and Meltdown are not singular flaws—they individually represent a class of closely-related variants.
>
> Spectre and Meltdown are uniquely dangerous security vulnerabilities that allow malicious actors to bypass system security protections present in nearly every recent device with a CPU—not just PCs, servers, and smartphones, but also Internet of Things (IoT) devices like routers and smart TVs. By leveraging the duo, it is possible to read protected system memory, gaining access to passwords, encryption keys, and other sensitive information.

101. Spectre and Meltdown vulnerabilities are "transient execution" attacks, meaning that they exploit the side effects of speculative code generated during speculative execution like branch prediction. These vulnerabilities stem from Intel's defective hardware design, particularly the hardware systems responsible for much of the performance provided by modern processors.

102. *Tech Republic* explains:

> Spectre and Meltdown are representative examples of "transient execution" attacks, which rely on hardware design flaws in the implementation of speculative execution, instruction pipelining, and out-of-order execution in modern CPUs. While this trio are essential to performance optimizations inherent to modern processors, implementation of these vary between CPU manufacturers and microarchitectures; as a result, not all Spectre and Meltdown variants are exploitable on all microarchitectures.

103. Intel's CPUs incorporated hardware design choices that made many of the company's microarchitectures vulnerable to both types of exploits (Spectre and Meltdown). Other CPU manufacturers were less vulnerable to attack than Intel because of differences in their hardware implementation of speculative execution, instruction pipelining, and out-of-order execution.

104. Spectre and Meltdown vulnerabilities were particularly pernicious, as they were extremely difficult to detect. As *Tech Republic* explains:

> Exploitation of Spectre and Meltdown can be performed untraceably—that is, without leaving evidence of an exploit in system logs. This makes the pair difficult to detect in targeted malware attacks, though known malware signatures are still possible to determine by traditional means.

105. Both exploits were direct results of Intel's failure to control side effects from speculative execution, branch prediction, and out-of-order execution. Spectre, for example, exploited the fact that speculatively executed code could access parts of the system and protected memory space that a program itself could not:

> Spectre, according to the original authors of the Spectre paper, "[induces] a victim to speculatively perform operations that would not occur during strictly serialized in-order processing of the program's instructions, and which leak a victim's confidential information via a covert channel to the adversary."

(brackets in original).

106. Spectre relied on side effects left in an Intel CPU's cache as a result of speculatively executed code. The speculative code was able to access forbidden system resources and memory, and the result was residually stored in the CPU's cache, even after the transient code was discarded:

> Spectre attacks are conducted in three steps:
>
> 1. The setup phase, in which the processor is mistrained to make "an exploitable erroneous speculative prediction."
>
> 2. The processor speculatively executes instructions from the target context into a microarchitectural covert channel.
>
> 3. The sensitive data is recovered. This can be done by timing access to memory addresses in the CPU cache.

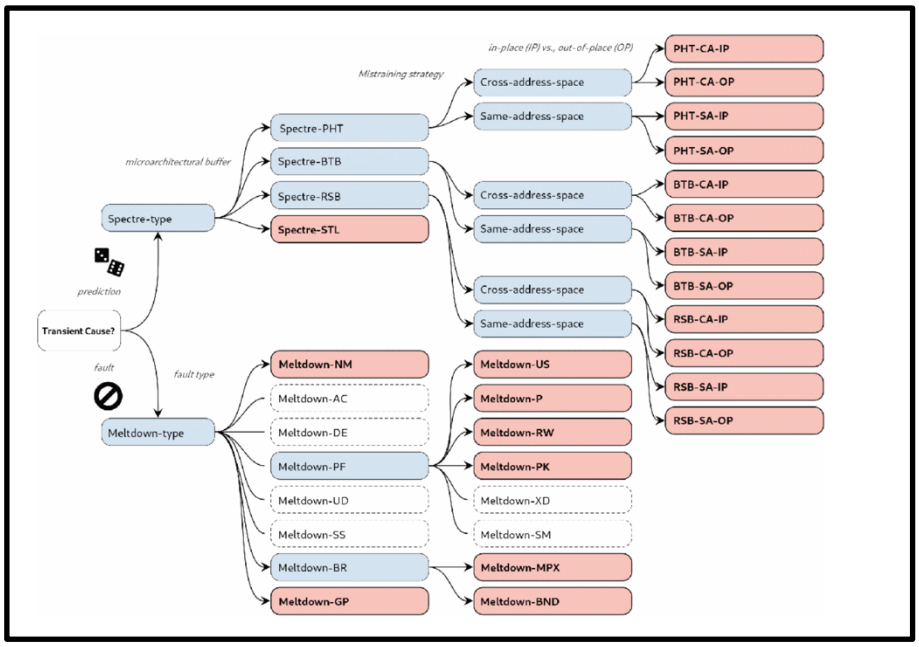
107. Meltdown exploited the same flaw in Intel's hardware design and implementation—a failure to enforce segmentation of privileged resources for speculatively executed code. Specifically, Meltdown allowed an attacker to directly access privileged memory that a user program should never be able to access:

> Meltdown exploits a race condition between memory access and privilege level checking while an instruction is being processed. In conjunction with a CPU cache side-channel attack, privilege level checks can be bypassed, allowing access to memory used by an operating system, or other running processes. In certain circumstances, this can be used to read memory in paravirtualized software containers.

108. Like Spectre, Meltdown exploited the fact that transiently executed code was accessing memory and resources that the program itself could not, and then left side effects, including within a CPU's cache system. As explained by *Tech Republic*:

> Meltdown attacks, according to the original authors of the Meltdown paper, are conducted in three steps:
>
> 1. The content of an attacker-chosen memory location, which is inaccessible to the attacker, is loaded into a register.
>
> 2. A transient instruction accesses a cache line based on the secret content of the register.
>
> 3. The attacker uses Flush+Reload to determine the accessed cache line and hence the secret stored at the chosen memory location.

109. The Spectre and Meltdown exploits were not simply discrete vulnerabilities. They were part of a large class of vulnerabilities arising from Intel's flawed design. Indeed, Spectre and Meltdown, even early after their disclosure, had given rise to many variants:



110. To mitigate the problem, Intel had to address the root cause of the entire class of vulnerabilities: speculatively executed instructions should not be allowed to access protected memory

that the program containing them cannot itself access, and more importantly, transient instructions should not leave side effects that linger after the transient instructions and results have been discarded.

111. As explained below, Intel chose not to fix the core problem, but instead provided belt-and-suspenders patches for existing CPUs, then continued to release CPUs with the same fundamentally flawed hardware.

E. Intel Fails to Fix Hardware Design that Caused Spectre and Meltdown Vulnerabilities and Pretends to Have Mitigated any Problems

112. In 2017 and 2018, Intel scrambled to provide "mitigations" for Spectre and Meltdown. What Intel provided, however, was a series of belt-and-suspenders changes to its microcode through patches—none of which addressed the hardware issue giving rise to the Spectre and Meltdown class of vulnerabilities.

113. The first supposed fix provided by Intel turned out to create severe instability in systems executing on Intel's CPUs. As ZDNet reported on January 12, 2018:

> Intel has revealed that a glitch in its patch for the Meltdown and Spectre CPU attacks is causing problems on PCs and datacenter equipment.
>
> Intel's firmware, which is delivered by hardware OEMs, is causing higher system reboots on systems with older Broadwell and Haswell CPUs.
>
> "We have received reports from a few customers of higher system reboots after applying firmware updates. Specifically, these systems are running Intel Broadwell and Haswell CPUs for both client and datacenter," Nevin Shenoy, general manager of Intel's data center group said in a statement.

114. Intel's supposed mitigation was so problematic that the company advised users of its processors not to install its patches. As *The Wall Street Journal* reported in a January 11, 2018 article, titled "Intel Fumbles Its Patch for Chip Flaw":

> Intel is quietly advising some customers to hold off installing patches that address new security flaws affecting virtually all of its processors. It turns out the patches had bugs of their own.
>
> The glitch underscores the complexity of Intel's challenge as it scrambles to fix the unprecedented vulnerabilities, which were disclosed more than a week ago.

> In a confidential document shared with some customers Wednesday and reviewed by The Wall Street Journal, Intel said it identified three issues in updates released over the past week for "microcode," or firmware—software that is installed directly on the processor. The updates are separate from patches produced by operating system companies such as Microsoft Corp.
>
> Intel advises customers to "delay additional deployments of these microcode updates," the company said in a technical advisory. "Intel will provide frequent updates."

115. Intel's first attempt to mitigate Spectre and Meltdown had failed. Notably, the first attempt at a mitigation revealed a serious problem with any fix Intel would ultimately release. Because there was a problem with the hardware—the design of Intel's branch prediction and segmentation systems—any "fix" would require handicapping the very systems on Intel's CPUs that are designed to provide performance expected of those CPUs—the processor's central function.

116. As the *Wall Street Journal* reported, the very first attempt to mitigate Spectre and Meltdown was resulting in decreased CPU performance:

> The fixes for these problems, however, have caused some performance slowdowns, particularly on older Intel systems. "With Windows 8 and Windows 7 on older silicon . . . we expect most users to notice a decrease in system performance," Microsoft said Tuesday in a blog post.

117. Intel ultimately rolled out three categories of mitigations—each impairing the branch prediction, speculative execution, and out-of-order execution systems on its CPUs.

118. By March 2018, it was clear that Intel's supposed mitigations were mostly accomplished by disabling branch prediction-related performance features in CPUs—converting modern Intel CPUs to linearly executing CPUs more in line with performance expected in processors of the early 2000s.

119. As *Wired Magazine* explained in a March 18, 2018 article titled, "Meltdown, Spectre, and the Cost of Unchecked Innovation":

> Both Meltdown and Spectre are caused by widespread use of a technique called "speculative execution" in which processors eagerly and proactively execute instructions even before they are actually needed by the program. The speculatively computed material is then faster, but the primary discovery of Meltdown and Spectre was that it is insufficiently secured, and thus provides a way to leak sensitive information. Meltdown most notably affects Intel hardware in which the speculative execution was

> previously assumed to be safe, and ***attempts to disable it at the software level can have a marked performance cost***. This is not just about sluggish laptops—many cloud service providers charge clients varying rates that reflect the computational burden of the contract, so Meltdown and Spectre may show up as an increase in technical budgets, paid out as a literal dollar amount to services that now have to run more slowly as a result of the patch.
>
> ***The only real fix for Meltdown is to eventually physically replace all the chips, a change which will take at least a full hardware generation to propagate***. Spectre is more sophisticated, and may have no real fix at all. We might not have realized until recently, but the speed and power of our computers until now has always been a lie, built atop a foundation that must now be undone if we also want to remain safe.

(emphasis added).

120. As a second version of Spectre began to propagate, Intel recommended three types of mitigations, called Indirect Branch Restricted Speculation ("IBRS"), retpoline mitigations, and an enhanced IBRS, called "EIBRS." All of these supposed mitigations essentially handicapped the functionality in Intel CPUs used to predict branches, to speculatively execute code, and to execute code out of order. The overhead from these mitigations was enormous.

121. IBRS, like the first mitigation—called an Indirect Branch Predictor Barrier ("IBPB")—restricted branch speculation when an Intel CPU switched to kernel mode. As Microsoft explained in a December 5, 2018 article, titled "Mitigating Spectre variant 2 with Retpoline on Windows":

> Our original mitigations for Spectre variant 2 made use of new capabilities exposed by CPU microcode updates to restrict indirect branch speculation when executing within kernel mode (IBRS and IBPB). While this was an effective mitigation from a security standpoint, it resulted in a larger performance degradation than we'd like on certain processors and workloads.

122. Retpoline mitigation—the follow-up to problematic IBPB and IBRS mitigations of Spectre and Meltdown—also gutted the branch prediction systems in Intel CPUs. The mitigation required the replacement of all indirect jumps in execution when a CPU was in kernel mode. Retpoline was not an option for many architectures, but for those that implemented the change, the result was again a substantial impairment of the performance expected from a modern CPU.

123. Retpoline mitigation directly impacted I/O and networking functionality on Intel's CPUs. This is because the CPU switches to kernel mode to access hardware, but in kernel mode, code could not fully exploit branch prediction and speculative execution with retpoline mitigation deployed.

124. Put simply, all of Intel's software mitigations for Spectre and Meltdown essentially resulted in disabling or handicapping core features expected of an modern CPU—branch prediction, out-of-order execution, and speculative execution. These mitigations impaired the central functionality of a modern CPU in order to patch a devastating security vulnerability. And this modern execution functionality would suffer most when the CPU was in kernel mode, interacting with privileged system resources.

125. Intel understood that its software mitigations would not fix the problem. This became readily apparent as additional variants of Spectre proliferated, including Spectre_V2 and other variants based on Branch History Injection. These variants were causing performance reductions in Intel's CPUs of up to 35% as a result of mitigation.

126. Intel promised to fix the problem in hardware in its future CPU generations. Intel CEO Brian Krzanich began a full press campaign promising a hardware fix. As *TechCrunch* reported on March 15, 2018 in an article titled, "Intel announces hardware fixes for Spectre and Meltdown on upcoming chips," an Intel press release featuring Intel's CEO (available to this day on Intel's website at https://download.intel.com/newsroom/2021/archive/2018-03-15-editorials-advancing-security-silicon-level.pdf) promised a new hardware design in future chips to finally deal with the Spectre/Meltdown class of vulnerability, including Spectre and Meltdown variants:

> "We have redesigned parts of the processor to introduce new levels of protection through partitioning that will protect against both Variants 2 and 3," Krzanich writes. Cascade Lake Xeon and 8th-gen Core processors should include these changes when they ship in the second half of 2018. Although that's a bit vague, we can be certain that Intel will prominently advertise what new chips include the mitigations as we get closer to release.

127. At the same time, *AnandTech* reported on Intel's promise of a hardware fix in future generations in a March 15, 2018 article titled, "Intel Publishes Spectre & Meltdown Hardware Plans: Fixed Gear Later This Year":

> Jumping straight to what AnandTech readers will consider the biggest news, Intel is finally talking a bit about future hardware. Intel is announcing that they have developed hardware fixes for both the Meltdown and Spectre v2 vulnerabilities, which in turn will be implemented into future processors. Both the next version of Intel's Xeon server/HEDT platform—Cascade Lake—as well as new 8th gen Core processors set to ship in the second half of this year will include the mitigations.

128. In short, in 2018, as Intel's microcode/firmware mitigations were causing severe performance problems, Intel dangled the promise of future hardware that did not suffer from the design flaw that would allow transient execution attacks such as Spectre and Meltdown.

129. However, as explained below, Intel, despite having done a deep dive into every aspect of the Spectre and Meltdown classes of vulnerabilities, never actually fixed the root cause of these vulnerabilities—the defective design of Intel's branch prediction hardware. Updated 8th generation and post-9th generation Intel chips maintained the same flawed design—transient code could access privileged resources, and speculative execution left side effects, including in the CPU cache.

F. Intel Is Directly Warned that Its AVX Instructions Are Vulnerable to Transient Execution Attacks Like Spectre and Meltdown

130. In 2018, Intel promised fully-fixed CPUs that would be even faster than prior designs, as they would operate using vector instructions, called Advanced Vector Extension (AVX) instructions.

131. A vector instruction is a CPU instruction that can perform the same type of operations on multiple data samples in a particularly efficient manner. A technological successor to so-called "single instruction, multiple data" (SIMD) scalar processing, vector instructions greatly improve CPU performance on particular workloads that involve heavy mathematical computation, including numerical simulation.

132. In modern computers, vector processing is central to the performance and function of any high-end CPU, enabling smooth performance and function of common applications like photo editing (*e.g.*, Photoshop), video processing (*e.g.*, Premiere Pro, Final Cut Pro), AI-enhanced data analysis and prediction, and image recognition. As a result, vector processing is central to the modern computing experience for both regular computer users and for businesses such as hospitals, doctor's offices, cities and governmental entities, manufacturers, and cloud providers (among many other CPU users and providers). As explained later in this Complaint, the impact of Intel's conduct in designing its post-

Spectre and Meltdown CPUs substantially impaired the basic and expected computational experience across these users and uses.

133. As *Hackaday* reported on December 12, 2018, Intel had announced new processors with AVX capabilities, stated to be based on a redesigned architecture—one understood to be patched for Spectre and Meltdown:

> Intel just announced their new Sunny Cover Architecture that comes with a lot of new bells and whistles. The Intel processor line-up has been based off the Skylake architecture since 2015, so the new architecture is a fresh breath for the world's largest chip maker. They've been in the limelight this year with hardware vulnerabilities exposed, known as Spectre and Meltdown. The new designs have of course been patched against those weaknesses.
>
> The new architecture (said to be part of the Ice Lake CPU) comes with a lot of new promises such as faster core, 5 allocation units and upgrades to the L1 and L2 caches. There is also support for the AVX-512 or Advanced Vector Extensions instructions set which will improve performance for neural networks and other vector arithmetic.

134. Evaluating its AVX instructions for Spectre-/Meltdown-like vulnerabilities was an important part of Intel's mitigation efforts in 2018. As one Google employee, Partha Ranganathan, observed at the Hotchips conference in an August 20, 2018 keynote presentation titled "Spectre/Meltdown & What it means for future design," Spectre variants posed a risk that privileged information could "leak through memory, I/O, and AVX instructions." In short, Intel's 2018 hardware redesign to overcome Spectre and Meltdown vulnerabilities would need secure its AVX instructions, along with other attack vectors.

135. In June 2018, Intel was warned by hardware enthusiast Alexander J. Yee that its AVX instructions were vulnerable to transient execution attacks such as Spectre and Meltdown class attacks. Intel acknowledged the warning and asked Yee to delay reporting on the potential vulnerability.

136. On August 7, 2018, Yee published his findings that Intel's AVX instructions were vulnerable to Spectre-class attacks in a blog post titled, "Spectre via AVX Clock Speed Throttle?":

> Note: This blog was supposed to go up in June. But rather than posting it outright, I sent it to intel and they asked me to wait.
>
> For the purpose of this, I'll call the attack described in this blog as, "AVX Clock Spectre".
>
> Since then a lot of stuff happened. Most notably, NetSpectre, a closely related exploit has been publicized. Given how similar NetSpectre is to AVX Clock Spectre, it became apparent that:
>
> 1. Given knowledge of either NetSpectre or AVX Clock Spectre, it would be trivial to derive the other.
>
> 2. The success of NetSpectre being exploitable likely means that AVX Clock Spectre is also exploitable using the same methods and/or the method described here.
>
> When I reached out to Intel again, they told me that the concepts in this blog were known both internally and to the public. Since there is no reason to further extend the information embargo, they have given me permission to publish this blog.

137. Yee described the potential vulnerability to Intel with significant detail:

> **The Exploit**
>
> High-Level Description
>
> AVX is a 256-bit SIMD instruction set extension for x86 processors. It was first introduced by Intel in 2011 with their Sandy Bridge processor line and is now widely supported by everyday hardware. AVX512 is the latest variant that extends it to 512-bit vectors.
>
> The purpose of AVX is to perform multiple operations in a single instruction. By the very nature of this, AVX instructions consume more

> power than regular instructions. In fact, they consume so much power that recent Intel processors will lower the clock speed to maintain stability and to avoid exceeding thermal limitations. It is this clock speed throttle that may be vulnerable to a Spectre side-channel attack.

138. Yee's proposed exploit worked much like the Spectre vulnerability—it exploited side effects left over from a predicted branch of execution. As Yee explained in his post:

> The original Spectre example used cache timings to expose information. Inside a mispredicted branch, you load the victim address (0 or 1) and use it to conditionally touch a cacheline. After recovering from the misprediction, you read the same cacheline manually. Then depending on how long the read takes, you can infer whether the value at the victim address is 0 or 1. This process can then be repeated to read arbitrary amounts of data. . . .
>
> The AVX Spectre exploit follows the same general approach. Inside a mispredicted branch, you load the victim address. But instead of using it to conditionally touch a cacheline, you conditionally execute an AVX instruction. If an AVX instruction was executed, the processor will reduce its clock speed. By running a benchmark to determine whether a clock speed reduction has occurred, you can infer whether the value at the victim address is 0 or 1.

139. Yee provided pseudocode[1] for the attack:

[1] Pseudocode is a simplified, part-natural language outline of a computer program, intended to allow the reader to understand what a program is logically designed/intended to do in a programming language-agnostic way.

Summary/Pseudocode of Attack:

```
bool condition = false;
uint64_t threshold;       // Some pre-calibrated number.

uint64_t run_benchmark(){
  uint64_t start = __rdtsc();
  // Do some garbage work that takes about 1 - 2 milliseconds.
  return __rdtsc() - start;
}

bool read_bit(const bool* victim_addr){

  // Step 1: Flush "condition" out of cache.
  _mm_clflush(&condition);

  // Step 2: Prefetch victim data.
  _mm_prefetch((char*)victim_addr, _MM_HINT_T0);

  // Step 3: Train branch predictor so that:
  //     Outer branch will be predicted not taken. (enter if-statement)
  //     Inner branch will be predicted taken. (skip if-statement)

  __m256d junk;

  // Step 4: Run exploit.
  if (condition){    // Outer Branch: Evaluates to false, but predicted true.
    bool victim_data = *victim_addr;
    if (victim_data){  // Inner Branch: Predicted false.
      junk = _mm256_mul_pd(junk, junk);  // Run some heavy AVX instruction.
    }
  }

  // Step 5: Wait 500 microseconds for a possible throttle to kick in.

  // Step 6: Run a benchmark.
  uint64_t score = run_benchmark();
  return score < threshold;
}
```

140. Yee's report to Intel—made in Summer 2018—made clear that its AVX instructions needed to be analyzed for potential side-channel vulnerabilities.

141. Notably, Yee had developed a means to exploit, using Intel's AVX instructions, the same underlying hardware defect that gave rise to Spectre, Meltdown, and their variants: (1) Intel's chips left side effects after the results of transient execution had been discarded, and (2) transient/speculative code was able to access privileged memory and resources its associated program could not (and should not) access. This was a significant vulnerability, and it was identified to Intel in mid-2018.

142. The AVX vulnerability that Yee identified to Intel in Summer 2018 affected several generations of Intel CPUs. As Yee explained:

> The AVX Spectre, if exploitable, requires that the processor have a measurable change in performance following an AVX instruction. These processors include:
>
> - Intel Haswell (servers and some laptops)
> - Intel Broadwell (servers and some laptops)
> - Intel Skylake (some laptops?)

- Intel Kaby Lake
- Intel Coffee Lake
- Intel Skylake X and Skylake Purley
- Intel Cannonlake

> This is basically the majority of Intel processors since 2014-ish. AMD processors aren't affected since they don't run AVX at full speed. So unlike Intel processors, AMD processors don't need to downclock to keep the thermals within limits.

143. As of June 16, 2018, when Yee reported the AVX vulnerability to Intel, Intel clearly knew that its AVX instructions created a serious transient execution vulnerability for nearly all of its modern CPUs, but Intel did nothing about it. It never recalled the many affected processors. Worse yet, it never made necessary changes to its hardware in subsequent generations of CPUs it sold.

144. Instead, Intel left a class of vulnerabilities potentially as severe as Spectre and Meltdown in its chips. As Yee explains:

> On the software side, the scope of the AVX Spectre theoretically should be largely the same as the original Spectre as described in the paper. If the attacking code is native code, it will be able to access all memory in the same address space regardless of access restrictions. Likewise, it may be possible to escape browser sandboxing. Though finding vulnerable code in libraries and VMs may be more difficult due to need for an AVX instruction.

145. Yee's warning about AVX and transient execution attacks was not the only one. Before Yee made his findings public, but after Yee raised his findings to Intel, another AVX-based transient execution exploit emerged, called NetSpectre. This attack allowed remote exploitation of the AVX instructions using Intel's defective branch prediction and segmentation hardware implementation. As *Ars Technica* reported on July 26, 2018:

> When the Spectre and Meltdown attacks were disclosed earlier this year, the initial exploits required an attacker to be able to run code of their own choosing on a victim system. This made browsers vulnerable, as suitably crafted JavaScript could be used to perform Spectre attacks. Cloud hosts were susceptible, too. But outside these situations, the impact seemed relatively limited.
>
> That impact is now a little larger. Researchers from Graz University of Technology, including one of the original Meltdown discoverers, Daniel Gruss, have described NetSpectre: a fully remote attack based on Spectre.

> With NetSpectre, an attacker can remotely read the memory of a victim system without running any code on that system.

146. NetSpectre exploited side effects both in the CPU cache and in the AVX instructions. As *Ars Technica* explained:

> Two different remote measurements were developed. The first is a variation on the cache timing approach already demonstrated with Spectre. The attacker makes the remote system perform a large data transfer (in this case, a file download), which fills the processor's cache with useless data. The attacker then calls the leak gadget to will *[sic]* speculatively load (or not load) some value in the processor's cache, followed by the transmit gadget. If the speculative execution loaded the value then the transmit gadget will be fast; if it didn't, it'll be slow.
>
> The second measurement is novel and doesn't use the cache at all. Instead, it relies on the behavior of the AVX2 vector instruction set on Intel processors. The units that process AVX2 instructions are large and power hungry. Accordingly, the processor will power down those units when it hasn't run any AVX2 code for a millisecond or two, powering them up later when needed. There's also an intermediate half powered state. Brief uses of AVX2 will use this half powered state (at the cost of lower performance); the processor will only fully enable (or fully disable) the AVX2 units after extended periods of use (or non-use). This microarchitectural feature can be measured: if the AVX2 units are fully powered down, running an AVX2 instruction will take longer than if the units are fully powered up.

147. Like AVX Spectre discovered by Yee, NetSpectre also exploited side effects from speculative execution—which should have been fully discarded—to read privileged and sensitive information from memory locations a normal user program cannot (and should not) access.

148. A July 2018 statement from Intel—quoted in *Ars Technica*—made clear the company had been informed of, and was aware of, the NetSpectre vulnerability in its CPUs.

149. By July 2018, Intel had before it a clear picture, painted through multiple publicly-acknowledged vulnerability submissions: Intel's AVX instructions were vulnerable to potentially devastating transient execution attacks. This was particularly true because Intel's AVX instructions are used for AES encryption—the national standard symmetric encryption scheme that forms the backbone of ordinary, secure CPU and computer use (including secure networking protocols such as SSL/TLS and data-at-rest disk/file encryption). A vulnerability in the AVX instructions would be tantamount to a

backdoor to PCs and other computers with Intel CPUs, as obtaining an AES key through an AVX transient execution attack would provide access to secret and sensitive information stored and transmitted by the vulnerable computer.

150. And as Intel already knew from its Spectre/Meltdown fiasco, it needed to reengineer its hardware in order to actually mitigate such a vulnerability. Indeed, Intel was doing just to mitigate Spectre and Meltdown vulnerabilities and their variants in mid-2018, when Intel was informed of the AVX vulnerabilities with AVX Spectre and NetSpectre.

151. However, despite multiple (publicly-known) vulnerability disclosures made to Intel on the subject, Intel did not carefully analyzing possible side-effects in the AVX ISA and engineering hardware solutions to fix them in 2018. Or in 2019, or 2020, or 2021, or 2022. Instead, Intel put profits first, selling defective CPUs for years after it clearly knew them to be defective, and knew that the hardware implementation of Intel's branch prediction systems needed to be addressed to prevent leaking side effects from speculative execution—specifically as to Intel's AVX instructions.

152. Repeated transient execution exploits of Intel's AVX instructions, along with the many variants of Spectre and Meltdown that had been discovered and disclosed, made clear to Intel by no later than mid-2018 that these were not one-off vulnerabilities to be mitigated with software or firmware updates. Instead, Intel's branch prediction design was broken and its AVX instructions needed careful attention and hardware-based redesign—and Intel knew it.

153. But as described below, Intel did nothing—and the inevitable eventually occurred.

II. THE DOWNFALL VUNLERABILITY REVEALS THAT INTEL NEVER FIXED ITS DEFECTIVELY DESIGNED CPUS AND IGNORED WARNINGS ABOUT ITS AVX INSTRUCTIONS

154. In August 2023, Intel publicly acknowledged another catastrophic vulnerability from the company's refusal to fix its defective speculative execution hardware. A publicly-disclosed vulnerability called "Downfall" allowed an attacker to launch a transient execution attack using Intel's AVX instructions and side effects left by Intel's defective branch prediction system.

155. As *PC World* reported on August 12, 2023:

> Well this is bad. "Downfall" is the name Daniel Moghimi, a security expert at Google, has given to a new vulnerability he has discovered in several

> generations of Intel processors. Attackers can exploit the vulnerability and read data from other programs and memory areas. The vulnerability has already been reported as CVE-2022-40982 and Intel confirmed the flaw here.
>
> Moghimi reported the vulnerability to Intel on August 24, 2022, but only made the vulnerability public on August 9, 2023 so that Intel had time to release microcode updates that can fix the vulnerability.

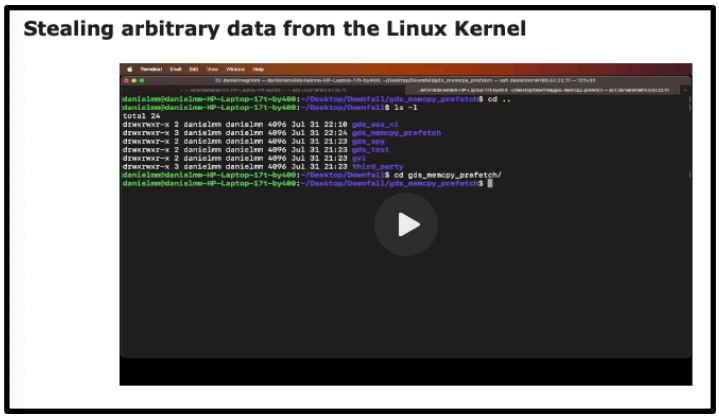
156. Moghimi created a website dedicated to the Downfall vulnerability, downfall.page. The site provided a detailed description of the vulnerability and provides examples of easily implemented code exploiting it.

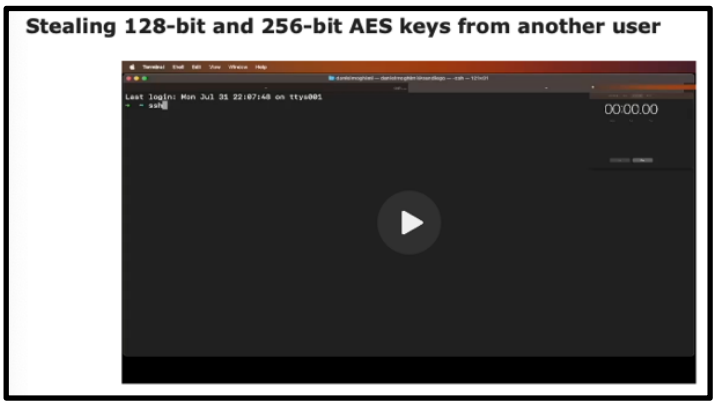
> Downfall attacks target a critical weakness found in billions of modern processors, used in personal and cloud computers. This vulnerability, identified as CVE-2022-40982, enables a user to access and steal data from other users who share the same computer. For instance, a malicious app obtained from an app store could use the Downfall attack to steal sensitive information like passwords, encryption keys, and private data such as banking details, personal emails, and messages. Similarly, in cloud computing environments, a malicious customer could exploit the Downfall vulnerability to steal data and credentials from other customers who share the same cloud computer.

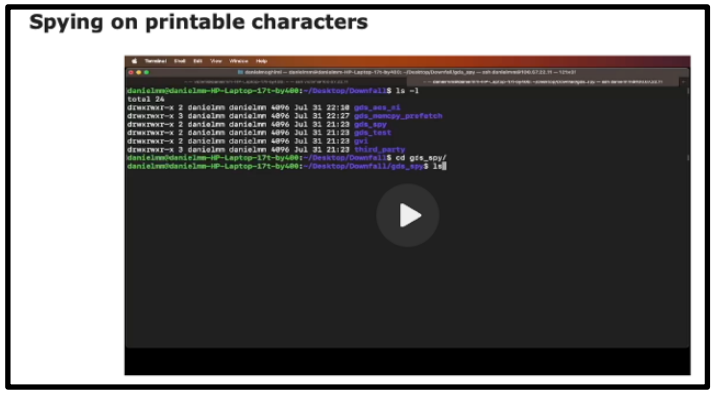
157. The vulnerability uses a "Gather" instruction, which is part of the AVX instruction set, as a key part of its implementation:

> The vulnerability is caused by memory optimization features in Intel processors that unintentionally reveal internal hardware registers to software. This allows untrusted software to access data stored by other programs, which should not normally be accessible. I discovered that the *Gather* instruction, meant to speed up accessing scattered data in memory, leaks the content of the internal vector register file during speculative execution. To exploit this vulnerability, I introduced Gather Data Sampling (GDS) and Gather Value Injection (GVI) techniques.

158. Moghimi provided a link to his academic paper describing in detail exploits of the Downfall vulnerability. The website also posted videos demonstrating exemplary exploits of the vulnerability, including stealing arbitrary data from an operating system kernel, stealing AES encryption keys from another user, and spying on printable characters.







159. The Downfall exploit, like Spectre, relies on expanding the "transient window"—the period of time the CPU runs transient code:

> Through trial and error, we observed that an attacker could prepare the transient window in a way that it does not require accessing an exotic address to leak data. . . . In this case, GDS leaks data only via accessing regular memory addresses with cacheable data without any explicit fault or microcode assist. This finding suggests that unlike MDS attacks exploiting memory accesses that experience faults or assists, *gather* can forward stale data upon normal speculative execution, ***similar to Spectre***. This finding is critical for execution environments like the *[sic]* JavaScript that sanitize addresses since the attacker does not have access to exotic addresses.

(emphasis added).

160. Moreover, just as with Spectre and Meltdown, Downfall arises from side effects left over after transient execution—this time, the AVX instruction buffer associated with the Gather instruction. As Moghimi's paper explains:

> We introduce Gather Data Sampling (GDS) that exploits the gather instruction to ***steal stale data from previously-undisclosed CPU components; SIMD register buffers***. Since various memory operations share these buffers, GDS enables attackers to steal data from other security domains (*e.g.*, across user-kernel, process, and VM boundaries). ***As a result, the latest Intel Ice Lake and Tiger Lake CPUs that claim to be resistant to data leaks expose users' data.*** Also, mitigations for earlier CPUs that rely on flushing microarchitectural buffers are ineffective since they do not flush the SIMD register buffers.

(emphasis added).

161. Notably, the buffers had not been previously disclosed by Intel. Intel, of course, knew these buffers existed. And Intel knew that its AVX instructions were vulnerable to transient execution attacks—since July 2018 at the latest. Yet Intel never redesigned its hardware.

162. Additionally, Intel had engineered its CPUs such that the Gather instruction has a temporal buffer that it shares across processor execution threads—meaning, Intel designed its CPUs to leave side effects from the use of Gather in the AVX instruction set:

> The observed data leak confirms a critical vulnerability that is exploitable from user space. The *gather* instruction appears to use a temporal buffer shared across sibling CPU threads, and it transiently forwards data to later dependent instructions, and the data belongs to a different process and *gather* execution running on the same core.

163. In other words, different computer programs running on the same CPU core share the same temporal buffer for Gather instructions. This means that if side effects remain after transient execution, lingering data can be accessed by other processes.

164. Moreover, like with Meltdown and Spectre, Intel's AVX Gather temporal buffers interact with the CPU's cache system, meaning entire lines of memory can be retained as a side effect of an AVX Gather instruction. As Moghimi explains in the Downfall paper:

> When multiple reads target the same cache line but different offsets, a temporal buffer can retain the cache line and forward different word values to the succeeding instructions independently. A temporal buffer also

facilitates out-of-order and speculative memory reads from different cache lines.

165. The Downfall exploit confirmed that Intel had again failed to design its CPUs to maintain segmentation and to eliminate lingering side effects from speculative execution. Processor components such as the CPU cache and temporal buffers were retaining stale data resulting from discarded, transient threads.

166. Indeed, the Gather Data Sampling (GDS) vulnerability published by Moghimi exploits lingering data in the CPU cache after transient execution to read what should be protected data. This is the same class of vulnerability that gave rise to catastrophic transient execution vulnerabilities like Spectre and Meltdown.

```
// Step (i): Increase the transient window
lea addresses_normal, %rdi
clflush (%rdi)
mov (%rdi), %rax
// Step (ii): Gather uncacheable memory
lea addresses_uncacheable, %rsi
mov $0b1, %rdi
kmovq %rdi, %k1
vpxord %zmm1, %zmm1, %zmm1
vpgatherdd 0(%rsi, %zmm1, 1), %zmm5{%k1}
// Step (iii): Encode (transient) data to cache
movq %xmm5, %rax
encode_eax
// Step (iv): Scan the cache
scan_flush_reload
```

Listing 2: Testing Gather Data Sampling.

167. Intel had done nothing to safeguard against the CPU's cache retaining what should have been discarded data resulting from speculative execution. It refused to learn from Spectre and Meltdown—or to reengineer its chips in the face of direct warnings Intel received in Summer 2018 about the specific AVX instruction set that gives rise to the Downfall vulnerability.

168. Moghimi discovered these vulnerabilities by systematically testing Intel's instruction set—specifically x86 instructions that "accept memory operands to see which instructions leak to GDS." Intel, of course, knew all along which instructions were vulnerable to this sort of exploit: it was warned years prior about its AVX instructions and had asymmetrically superior, and in fact exclusive, knowledge about undisclosed, shared temporal buffers.

169. Moghimi also confirmed that Intel's previous hardware mitigations had failed to flush the AVX buffers, and that even when these buffers were flushed, data leaks persisted.

> Next, we test if flushing microarchitectural buffers would mitigate the data leak within the same CPU thread. . . . We tested this across different CPU generations, and as we can see in figure 2, we can efficiently leak data on all tested CPUs even after flushing everything that we can. In fact, in some cases, we see more data leaks, likely due to changing the speculative-execution window, but it confirms that previous hardware mitigations do not flush our newly discovered buffers.

170. There was a deeper problem causing all of these transient execution vulnerabilities in Intel CPUs. Moghimi recognized this in the Downfall paper:

> Mitigating GDS without eradicating the root cause in hardware is expensive. As the size of microarchitectural data structures also grows, mitigations based on flushing buffers would also be less efficient, *i.e.*, more flushing. On the other hand, automated testing can practically find new vulnerabilities in CPUs, but such tools need to have better coverage of the hardware and the supported instructions, which are challenging due to the complexity and proprietary aspect of the hardware.

171. Software mitigation through microcode updates was becoming less and less practical. Nothing could or would be solved for its millions of defectively designed, vulnerable CPUs without a hardware redesign by Intel. This was something Intel could have always done, had it acted on information actually supplied to it several years ago. In fact, AMD CPUs do not appear vulnerable to Downfall attacks, nor are Intel's newer generation Alder Lake, Raptor Lake, and Sapphire Rapids architectures.

172. Attacks exploiting the Downfall vulnerability are highly practical. As Moghimi explained in an FAQ:

> [Q] How practical are these attacks?
>
> [A] GDS is highly practical. It took me 2 weeks to develop an end-to-end attack stealing encryption keys from OpenSSL. It only requires the attacker and victim to share the same physical processor core, which frequently happens on modern-day computers, implementing preemptive multitasking and simultaneous multithreading.

173. In other words, if an attacker can remotely run a computer program on a computer, and the program runs on the same CPU core, an attacker can obtain highly sensitive information. Moghimi

himself exploited OpenSSL, a means of remotely connecting to computers using an encrypted connection.

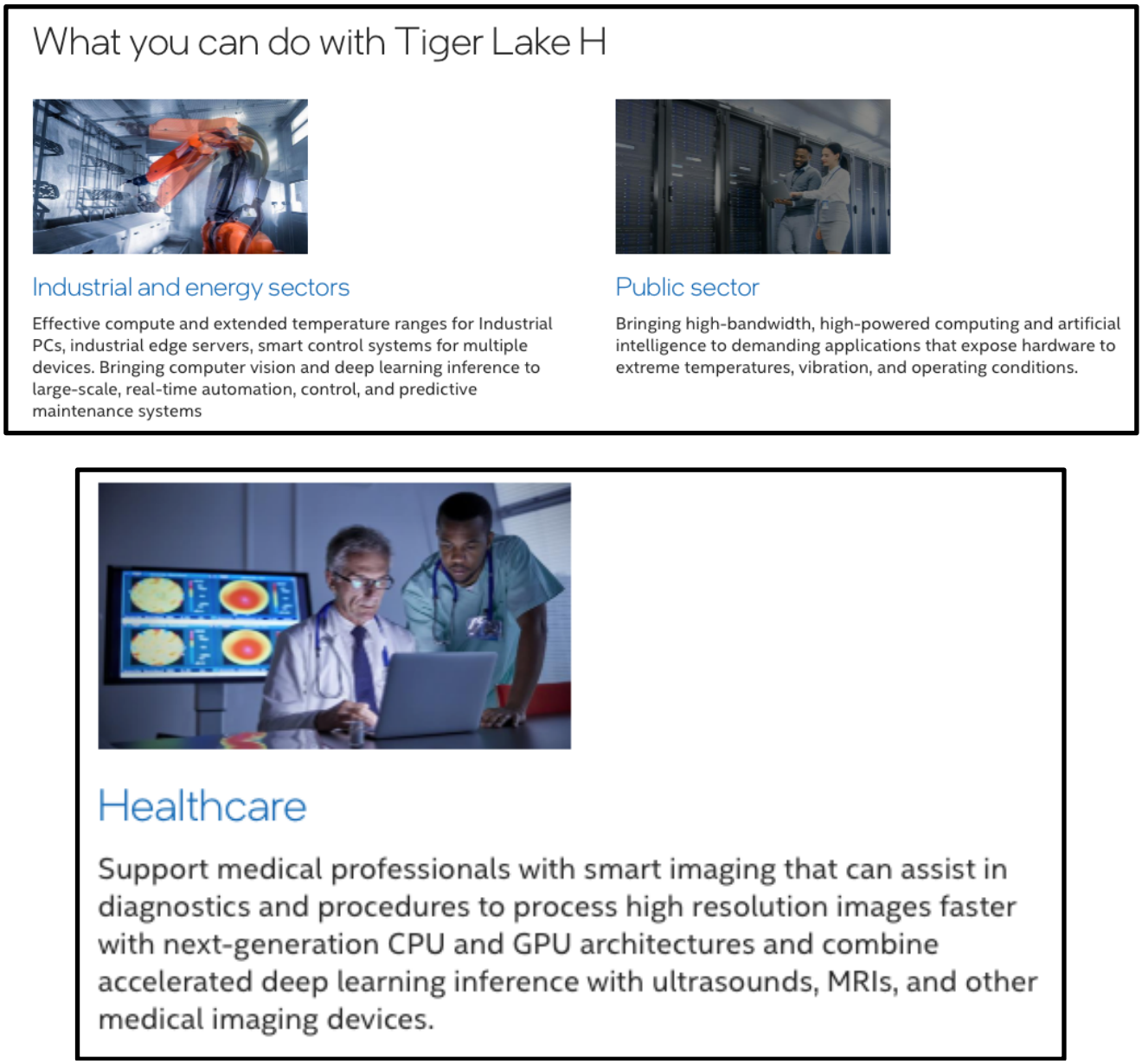
174. Downfall revealed that Intel had not fixed the design flaw that led to severe transient execution vulnerabilities—vulnerabilities like Spectre and Meltdown—in millions of CPUs across several post-Spectre/-Meltdown generations of Intel architecture. Moreover, Intel ignored direct warnings about transient execution vulnerabilities in its AVX instruction set—including publicly-known warnings about NetSpectre and AVX Spectre in the Summer of 2018.

175. Now, Intel's poor design has compromised vector processing necessary for modern performance and functionality on applications such as image editing, video gameplay, and encryption—processing tasks central to the functionality of a modern CPU during ordinary use, and to consumers' expectations of Intel's CPUs.

176. Intel disclosed that several generations of Intel CPUs were vulnerable to Downfall—from Intel's 6th generation Skylake CPUs to its 11th generation Tiger Lake CPUs. Intel's 9th through 11th generation chips, however, were supposed to have received hardware redesigns that would fix the class of vulnerabilities associated with Spectre, Meltdown, and other transient execution attacks—but Intel's engineers plainly never addressed the underlying root cause, despite repeat warnings, including about the vulnerability of Intel's AVX instructions to transient execution attacks.

177. Intel has posted a list of CPUs it considers to be vulnerable on its website. In addition to nearly every high-end consumer CPU Intel designed and manufactured for close to a decade, Intel server and embedded CPUs are also vulnerable to Downfall-type attacks. For example, Intel admits on its website that Tiger Lake U and Tiger Lake H 11th Generation Intel Core and Xeon CPUs are vulnerable to Downfall.

178. These embedded chips—admittedly vulnerable to Downfall, and designed that way by Intel despite knowing since at least mid-2018 that its AVX instructions were vulnerable to transient execution attacks—are used, according to Intel's website, in industrial, public sector, healthcare, and casino gaming applications.



179. Intel's affected CPUs are defective at the hardware level. Transiently executed code should not leave lingering side effects in shared buffers and CPU cache, and transient code should not violate the segmentation between privileged resources and user-available resources.

180. Intel had the opportunity in its 9th through 11th generation chips to redesign its hardware, knowing about its CPUs' vulnerability to AVX transient execution attacks, but it never did. In fact, Intel clearly ***could*** have made such a redesign so, as its later generations are not affected by Downfall, and its competitor AMD also appears to be immune from the Downfall vulnerability.

181. As to Intel's affected 6th through the 8th generation CPUs, Intel never bothered to recall those chips or even provide a software-based mitigation for its vulnerable AVX instructions.

III. INTEL'S PROPOSED "FIX" FOR DOWNFALL CAUSES SEVERE DECREASES IN CPU PERFORMANCE

182. Downfall, like Spectre and Meltdown before it, is an incurable vulnerability. Fixing Downfall requires significant hardware changes to Intel's CPUs as well as an update to Intel's AVX instruction set.

183. As Moghimi explained in his research paper titled, "Downfall: Exploiting Speculative Data Gathering," mitigation requires disabling the AVX instructions or changing Intel's hardware-defined instruction set:

> Intel could issue a microcode patch that disables the *gather* instruction, slowing down or breaking applications that rely on this performance feature. However, this is impractical and requires changing the ISA since *gather* is a built-in part of the AVX2.

184. Intel ultimately released supposed mitigations in late 2023, but the medicine was on par with the disease: Intel's mitigation destroyed CPU performance for certain, critical processing tasks. As Moghimi explained in his FAQ:

> [Q] Is there any mitigation for Downfall?
>
> [A] Intel is releasing a microcode update which blocks transient results of gather instructions and prevent attacker code from observing speculative data from *Gather*.
>
> [Q] What is the overhead for the mitigation?
>
> [A] This depends on whether *Gather* is in the critical execution path of a program. According to Intel, some workloads may experience up to 50% overhead.

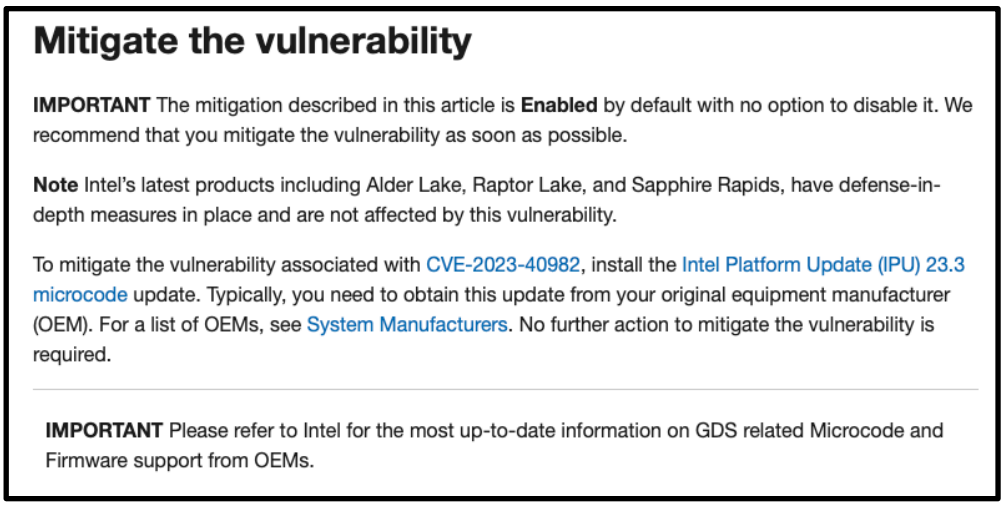
185. Users ultimately have little choice but to adopt this catastrophic mitigation. Many computer manufacturers push Intel's microcode updates through the Microsoft Windows update system.

186. For example, according to Security Week, Dell has released BIOS patches for Alienware, ChengMing, G Series, Precision, Inspiron, Latitude, OptiPlex, Vostro, and XPS computers. Lenovo and HP also began rolling out BIOS updates by the end of August 2023.

187. Dell's website confirms the release of the performance diminishing Intel 2023.3 IPU microcode for its affected products as part of its update system. *See* https://www.dell.com/support/kbdoc/en-us/000216234/dsa-2023-180-security-update-for-intel-product-update-2023-3-advisories?lang=en. HP's website states that it has also released the performance diminishing Intel 2023.3 IPU BIOS update for its affected products as part of its October 17, 2023 SoftPaq update system. *See* https://support.hp.com/ph-en/document/ish_9021973-9021997-16/hpsbhf03859. Lenovo's website provides a list of available firmware updates, including the performance debilitating firmware update for Downfall, for each affected product. https://support.lenovo.com/us/en/product_security/LEN-134879.

188. Dell (including Alienware), HP, Lenovo and other computer manufacturers with update systems will install the latest microcode update automatically if set for automatic updates or will periodically prompt the user to install the latest updates.

189. Non-OEM computers running the Windows operating system will install Intel Platform Update (IPU) 23.3 through the Windows Update system. As the Microsoft website states, the mitigation "is Enabled by default with no option to disable it":



Mitigate the vulnerability

IMPORTANT The mitigation described in this article is **Enabled** by default with no option to disable it. We recommend that you mitigate the vulnerability as soon as possible.

Note Intel's latest products including Alder Lake, Raptor Lake, and Sapphire Rapids, have defense-in-depth measures in place and are not affected by this vulnerability.

To mitigate the vulnerability associated with CVE-2023-40982, install the Intel Platform Update (IPU) 23.3 microcode update. Typically, you need to obtain this update from your original equipment manufacturer (OEM). For a list of OEMs, see System Manufacturers. No further action to mitigate the vulnerability is required.

IMPORTANT Please refer to Intel for the most up-to-date information on GDS related Microcode and Firmware support from OEMs.

190. Even if the mitigation could be disabled, the vulnerability would be significant regardless of the workload placed on the CPU, as vector registers are used to optimize common operations across most every sort of computer program—operations such as copying large parts of memory at once.

191. As Moghimi explained:

[Q] Can I disable the mitigation if my workload does not use Gather?

> [A] This is a bad idea. Even if your workload does not use vector instructions, modern CPUs rely on vector registers to optimize common operations, such as copying memory and switching register content, which leaks data to untrusted code exploiting *Gather*.

192. In other words, modern CPUs need vector instructions to execute normal operations during ordinary use, including the movement of large quantities of data and instructions to and from memory at once.

193. An Intel CPU user with an affected processor now faces a no-win choice: keeping their Intel CPU in a broken and vulnerable state or mitigating its vulnerability with a massive performance degradation. This hit to performance occurs because mitigation impairs important branch prediction functions that are an expected, and indeed, central, part of every modern CPU—and are central to the expectations of consumers that buy Intel CPUs or computer systems incorporating them.

194. Real world tests of Intel's Downfall mitigation, including those by Phoronix, yielded performance degradations in line with Intel's stated 50%, finding impairment from Intel's mitigation to be as high as 39%.

195. Intel for years sold CPUs that it knew were vulnerable to devastating attacks on central aspects of computer security—including AES (encryption) keys used for secure communication and data storage. And then when a security researcher revealed this gaping vulnerability, the company's software mitigation slowed computers by as much as 50%.

IV. INTEL'S DEFECT GOES TO THE HEART OF THE PRODUCT AND IMPAIRS ORDINARY AND EXPECTED USE

196. All modern CPUs rely on sophisticated branch prediction, speculative execution, and out-of-order execution to achieve expected performance characteristics. Without these systems, a CPU would be unmarketable.

197. Indeed, every competing CPU that rivals or is comparable to the affected Intel CPUs use extensive branch prediction, speculative execution, and out-of-order execution.

198. AMD chips that are x86 compatible—meaning compatible with Intel's chips—implement the same instruction set as Intel, including the AVX instructions.

199. Any product sold by Intel, AMD, or ARM without functioning branch prediction, speculative execution, and out-of-order execution, would be unmerchantable.

200. As AMD, Intel's primary competitor, explains in its whitepaper titled, "Software Techniques for Managing Speculation on AMD Processors":

> Speculative execution is a basic principle of all modern processor designs and is critical to support high performance hardware.

201. In other words, a CPU without a functional and safe speculative execution and branch prediction system, is not comparable to other modern CPUs—it would be unmerchantable, as would any desktop, laptop, or other computer that used it.

202. Put simply, CPUs with defective speculative execution, branch prediction, and out-of-order execution systems do not simply "compute" at slower rates. They are not saleable, as they do not come close to meeting consumer performance expectations.

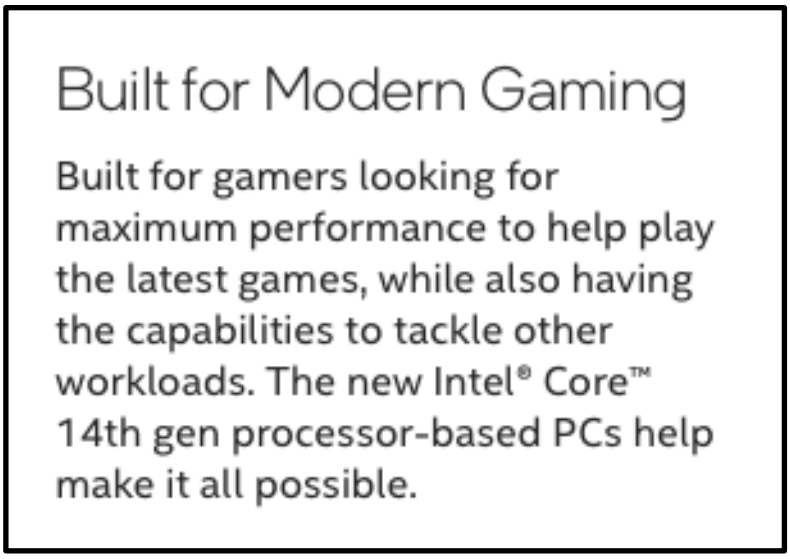
203. Vector-based instructions—in Intel and AMD's case, the AVX instructions—are also central to the operation of modern CPUs. They are necessary for everyday applications, including gaming, photo and video editing, and generally for execution of software optimized to move large amounts of data to and from system memory at once. They are also essential to encryption operations used across many applications, including AES encryption used as a backbone for common applications, including those used for secure networking, secure communication, and secure data storage.

204. Vector instructions are central components of modern CPUs, as recognized by those in the trade. As *Science Direct* explained in a 2017 article by João Cardoso and Pedro Diniz, titled "Embedded Computing for High Performance":

> Since a vector instruction can simultaneously operate on multiple pairs of operands, this technique can be used to speedup applications if data parallelism can be exploited. ***Most modern CPUs feature vector processing instructions***, including Intel x86's MMX, SSE, and AVX instructions, MIPS' MSA, SPARC's VIS, and ARM NEON extensions.

(emphasis added).

205. Intel understands that these applications are central to the function of its processors. Intel pervasively advertises that its processors are built for gaming. As its website currently states:



206. A CPU without vector functions is not a modern and merchantable CPU. Such a CPU would not come close to performance levels expected by consumers or those in the trade.

207. Intel understands that performance, including as to vector processing applications, is one of the most important, if not central, aspects of a CPU. Intel repeatedly markets its performance—using technical information that consumers and those in the trade review prior to purchase—to market its CPUs.

208. For example, Intel's website states the following about its 11th generation CPUs on its website:

> **Do More of What Matters to You with an 11th Gen Intel® Core™ Processor**
>
> 11th Generation Intel® Core™ processors redefine Intel® CPU performance for laptop and desktop PCs. New core and graphics architectures, AI-based performance boosts, best-in-class wireless and wired connectivity[1], and advanced tuning features[2] deliver higher levels of power and flow to support your aspirations.
>
> 25-watt 11th Gen Intel® Core™ U-Series laptop processors featuring Intel® Iris® Xᵉ Graphics provide discrete-level integrated graphics alongside Intel® Wi-Fi 6 — for boundary-breaking performance in thin and light laptops for everyday use. Higher-powered 35-watt 11th Gen Intel® Core™ H-Series laptop processors introduce ultraportable horsepower for gaming and creating.
>
> 11th Gen Intel® Core™ S-Series desktop processors provide higher performance to everyday desktop users, enthusiast gamers, and serious creators. Intel® Deep Learning Boost, up to DDR4-3200, 20 CPU PCIe 4.0 lanes, integrated USB 3.2 20G, enhanced UHD graphics based on the Intel® Xᵉ architecture, and greater tuning and expandability dramatically increase performance and control. High-performance overclocking for elite gaming and heavy-duty creative production is provided in unlocked 11th Gen Intel® Core™ desktop processor models.
>
> Built for business, 11th Gen Intel® Core™ vPro® processors offer all the performance gains of 11th Gen along with modern remote manageability for IT. Just what's needed for the work-from-anywhere world.
>
> Offering a range of CPU models optimized for different levels of gaming, creating, business, and everyday use, there's an 11th Gen Intel® Core™ laptop or desktop processor designed to do more of what matters to you.

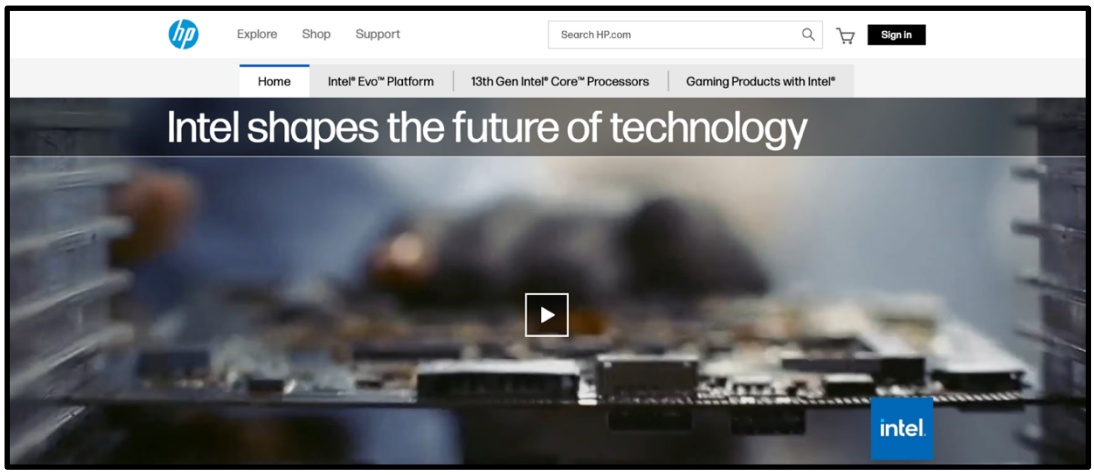
209. Intel makes clear, through its own statements including those marketing to CPU and computer purchasers, that gaming and AI applications—those that rely heavily on the AVX instructions exploited by Downfall—lie at the heart of a modern CPU's value and functionality. If Intel's CPUs did

not permit a computer built around them to perform these tasks, Intel's CPUs would not be acceptable to the ordinary consumer and would fall far short of industry standards.

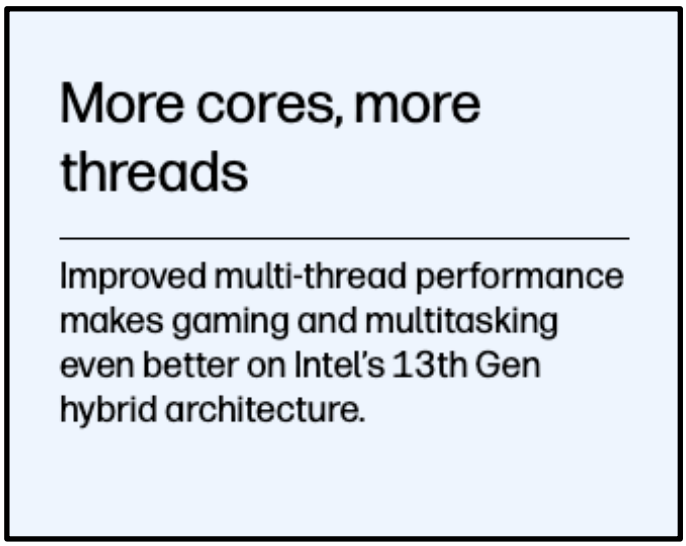
210. Indeed, the headline application in Intel's announcement of its 10th generation CPUs was performance and gaming:

> We're introducing Intel's fastest gaming processor with the 10th Gen Intel Core i9-10900k processor and you can gain a competitive edge in both work and play. Prepare to unleash your ideas like never before, enjoy and share incredible PC gaming or get work done in less time.
>
> When it comes to your desktop PC, you can't have too much speed. Whether enjoying the latest games or getting more done with the latest productivity apps, processor speed matters . . .

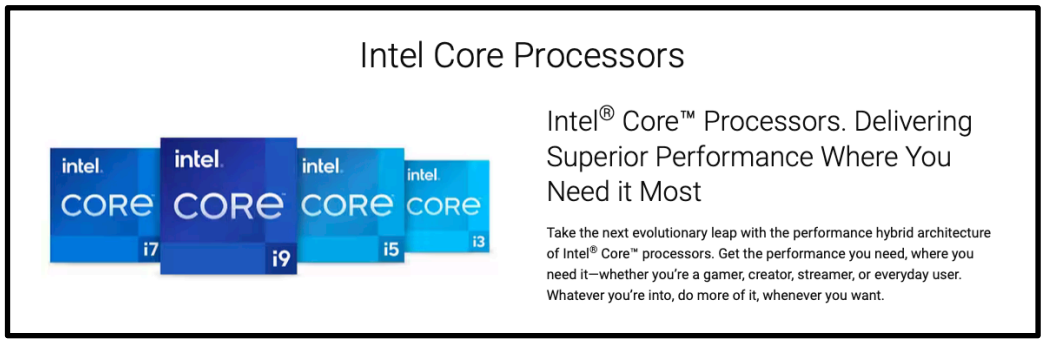
211. Intel jointly markets its CPUs with retailers and computer manufacturers/OEMs. For example, HP maintains a website showcasing Intel's products, titled "Intel and HP."



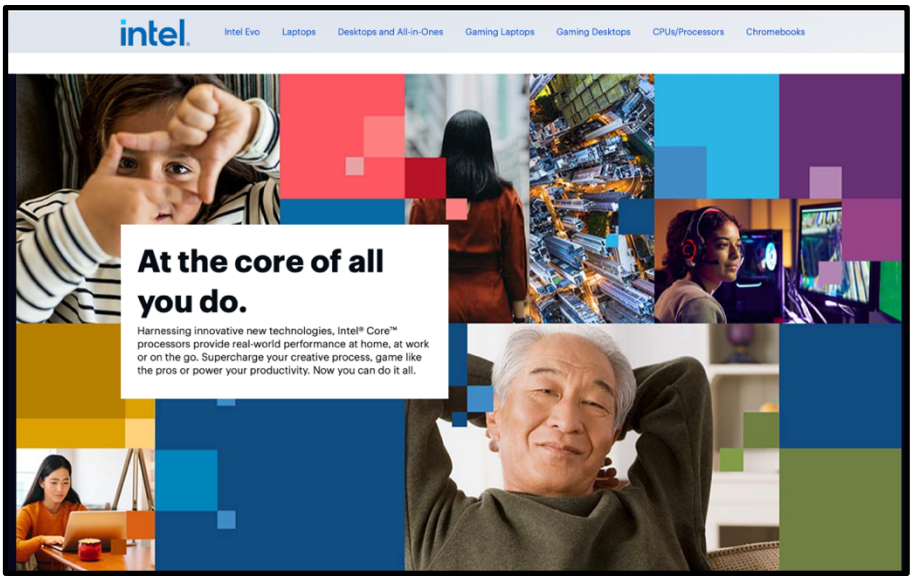
212. HP's site touts Intel CPUs' gaming and multitasking capabilities.



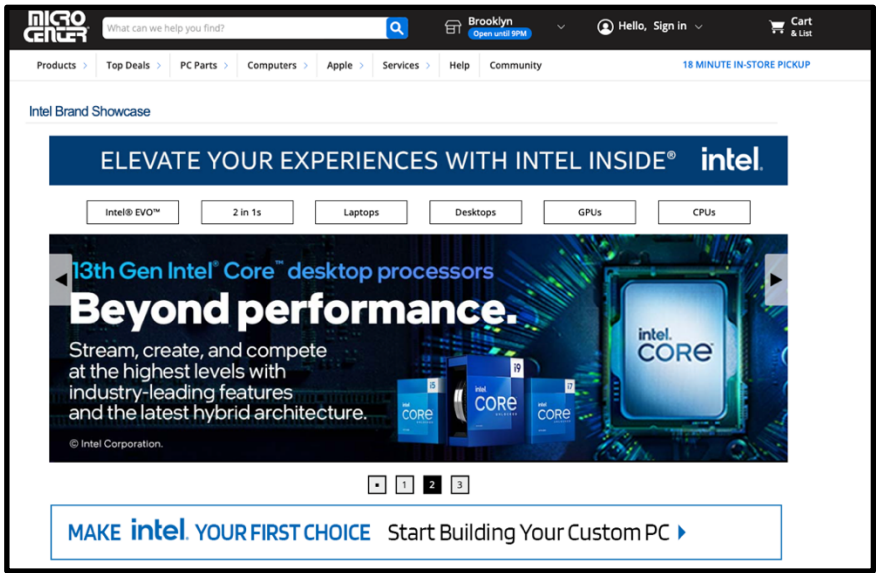
213. Dell similarly jointly markets Intel CPUs on its website:



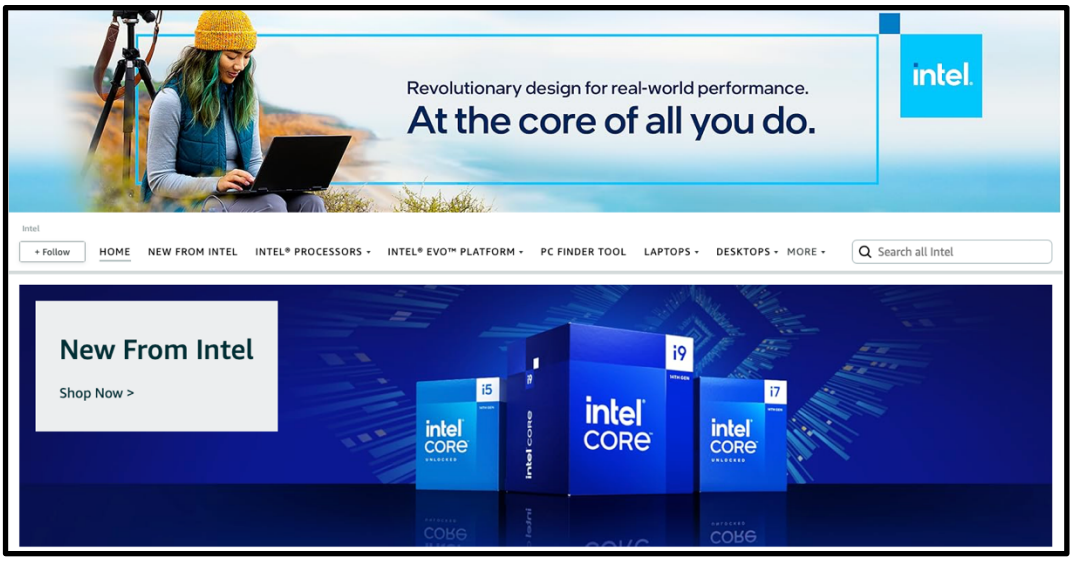
214. Retailers also display Intel's marketing next to the PCs and laptops they sell. For example, retailer BestBuy maintains a page dedicated to Intel's processors on its website:



215. Retailer MicroCenter also maintains a page on its website dedicated to Intel:



216. Online retailer Amazon.com also maintains an Intel storefront, which it uses to jointly market Intel's products, including alongside the computers it sells.



217. Put simply, wherever Intel's CPUs are sold (or computers with Intel's CPUs are sold), Intel's marketing touting performance, multitasking, gaming, and streaming is prominently displayed alongside these products.

218. When Intel sold the affected CPUs for years without disclosing that they had defective branch prediction, speculative execution, and out-of-order execution systems, Intel sold its customers CPUs that fell well below ordinary customer expectations as to the central function of a modern CPU (or of a computer with a modern CPU).

219. Intel never disclosed the defect in its CPUs in its marketing, in its jointly maintained sites with retailers and computer manufacturers, or on its website.

220. A purchaser would expect the truth to be disclosed in these sources, and if Intel made such a disclosure, it would have appeared in its marketing or on its packaging—or even as a warning by computer manufacturers. And, if the truth was disclosed, the trade press, such as *PC Magazine*, would have reported on it. Intel omitted the truth from all of these sources. It told no one that its products were defective and vulnerable, nor did it tell them that a fix would mean that Intel CPUs would be half as fast during ordinary and expected use.

V. INTEL'S DEFECTIVELY DESIGNED CPUS HAVE INJURED PLAINTIFFS AND CLASS MEMBERS AND WILL CONTINUE TO DO SO UNTIL FIXED

221. Intel's defectively designed CPUs have injured Plaintiffs and class members in several concrete ways.

222. To begin with, Plaintiffs and class members overpaid for their computers and CPUs. When the defective CPUs' devastating vulnerabilities are mitigated, those CPUs are nearly 50% slower than before. In other words, Plaintiffs paid full price for affected Intel CPUs that in fact perform approximately half as well as other modern CPUs, including those made by AMD, in order to mitigate a unique, devastating security vulnerability that Intel has known about since mid-2018. As such, Plaintiffs—purchasers of Intel CPUs or computers with Intel CPUs—have been injured through an overcharge for their purchases.

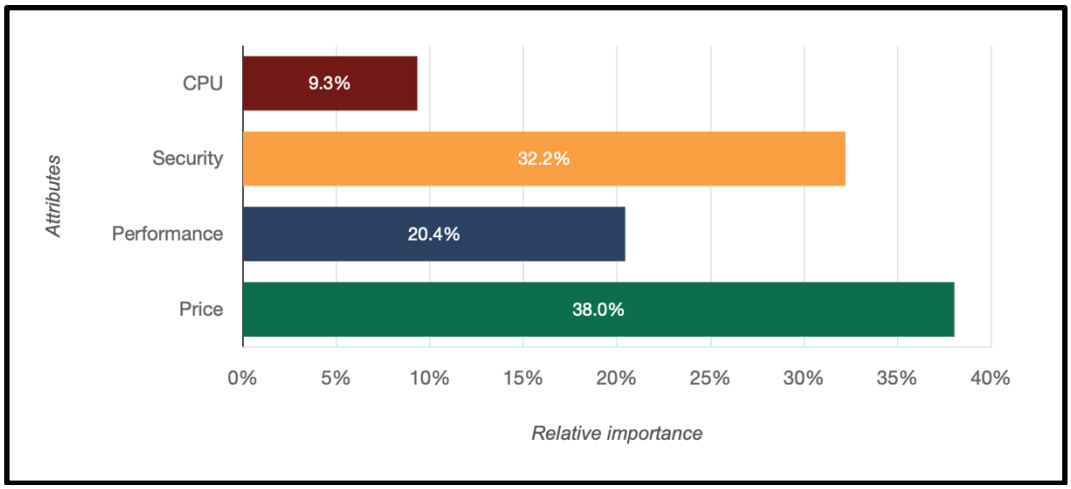
223. Likewise, computers with Intel CPUs experience a diminution in value as a result of both the security flaw and the performance impairment from Intel's mitigation.

224. Two pre-complaint conjoint studies confirm the overpayment as well as the injury to Plaintiffs' and class members' computers resulting from the design defect in affected Intel CPUs.

225. First, a conjoint study measuring the price impact on computers with affected Intel CPUs (the "Computer Conjoint"), within a 90% confidence interval, shows a material difference in marginal willingness-to-pay ("MWTP") for computers with affected Intel CPUs vs. computers with CPUs lacking the design defect.

226. The Computer Conjoint measured the relative importance, and effect on MWTP, of the performance penalty from mitigation, the security vulnerability, and various price points, and accounted for brand differences between Intel and its primary rival, AMD. The conjoint study included a survey that described the security vulnerability and the performance penalty from Intel's mitigation.

227. The Computer Conjoint makes clear that the performance and security attributes described above in this complaint were and are highly material to consumers, with the measured security flaw closely following computer price in relative importance.



228. MWTP measurements from the Computer Conjoint show that consumers are willing to pay significantly more for a computer without the Intel design flaw and the performance impairment from mitigating the security vulnerability that stems from it (and conversely, that consumers are willing to pay significantly less for a computer with an affected Intel CPU).

Attribute	Price Delta (Difference in MWTP)
Security Vulnerability	-$1,140
Performance Impairment from Mitigation	-$782.61

229. The Computer Conjoint shows that a computer with an affected Intel CPU, given a median price of $1,350, loses 85% of its value because of the security vulnerability.

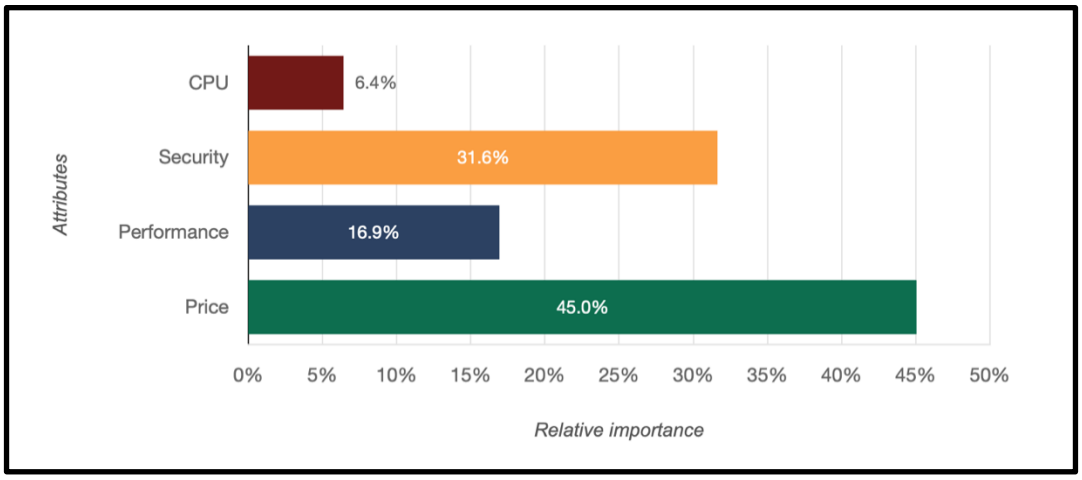
230. The Computer Conjoint also shows that a computer with an affected Intel CPU, given a median price of $1,350, loses 58% of its value because of the performance impairment from the mitigation.

231. The study shows that each Plaintiff and class member that purchased a computer with an affected Intel CPU suffered a quantifiable monetary loss from Intel's defective design and supposed mitigation. The loss is so significant as to impair most of the value of a computer with an affected Intel CPU.

232. Second, a precomplaint conjoint study measuring the price impact on standalone Intel CPUs (the "CPU Conjoint"), within a 90% confidence interval, shows a material difference in MWTP for affected Intel CPUs vs. CPUs without the design defect.

233. The CPU Conjoint measured the relative importance, and effect on MWTP, of the performance penalty from mitigation, the security vulnerability, and various price points, and accounted for brand differences between Intel and its primary rival, AMD. The conjoint study included a survey that described the security vulnerability and the performance penalty from Intel's mitigation

234. The CPU Conjoint makes clear that the performance and security attributes described above in this Complaint were and are highly material to consumers, with the measured security flaw following CPU price in relative importance.



235. MWTP measurements from the CPU Conjoint showed that consumers are willing to pay significantly more for a CPU without the Intel design flaw and the performance impairment from mitigating the security vulnerability that stems from it (and conversely, that consumers are willing to pay significantly less for an affected Intel CPU).

Attribute	Price Delta (Difference in MWTP)
Security Vulnerability	-$1,440
Performance Impairment from Mitigation	-$628

236. The CPU Conjoint shows that an Intel CPU with the defect described in this Complaint loses nearly all of its value, with negative MWTP value for a median $1,050 CPU price point.

237. The CPU Conjoint also shows that an affected Intel CPU, given a median price of $1,050, loses 60% of its value because of the performance impairment from the mitigation.

238. The CPU Conjoint shows that each Plaintiff and class member that purchased an affected Intel CPU suffered a quantifiable monetary loss from Intel's defective design and supposed mitigation. The loss is so significant as to impair most of the value of an affected Intel CPU.

239. These two conjoint studies were performed pre-complaint to confirm the impact of Intel's CPU defect on Plaintiffs and members of the Class, including on their purchases of computers with affected Intel CPUs and their purchases of affected Intel CPUs. The results confirm the allegations of injury, materiality, and damages alleged in this Complaint. Plaintiffs will measure damages during discovery through expert testimony, including, to the extent necessary and appropriate, through a more robust conjoint study.

240. Plaintiffs are also injured because their CPUs remain defective. Intel has not provided a means of addressing the root design defect of its 6th through 11th generation CPUs. Intel has never issued a recall. It has never provided replacement CPUs, such as later generation Intel CPUs that do not appear to be vulnerable to Downfall.

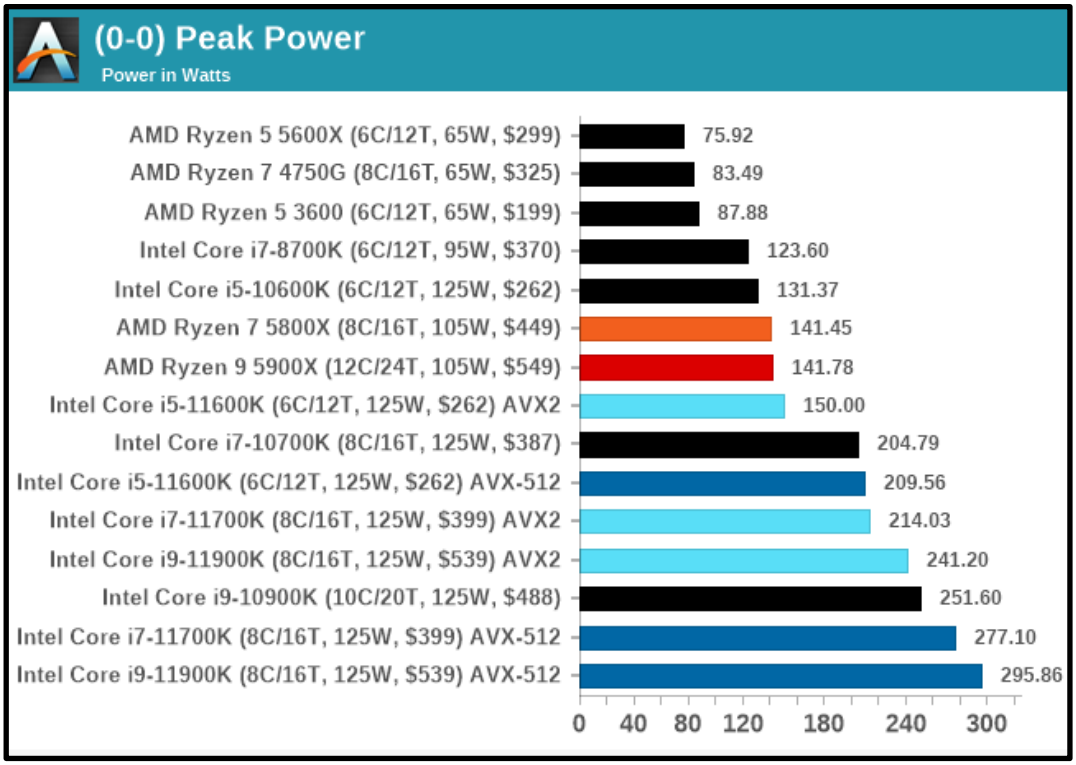
241. Plaintiffs' CPUs, and computers that incorporate them, are also now worth less given the severe Downfall vulnerability and the devastating performance drop as a result of the "mitigation" provided by Intel. If Plaintiffs had purchased a CPU from (or computer with a CPU from) one of Intel's competitors like AMD, the resale value of their CPUs (or computers) would have been higher—commensurate with what the resale value of their Intel chips (or the computers incorporating them) would have been absent Intel's fraudulent omission, unfair and unjust conduct, and intentional (certainly knowing and reckless) defective design.

242. Plaintiffs would also like to purchase Intel's CPUs, or computers incorporating them, in the future. Indeed, Intel is one of two or three CPU manufacturers that provide modern, high-performance CPUs in the United States. But Plaintiffs can no longer rely on Intel's representations, as Intel knowingly

failed to disclose that its CPUs were defectively designed. Absent an injunction, Plaintiffs are unable to rely on Intel's statements and purchase Intel's CPUs or computers with Intel's CPUs in the future.

243. Plaintiffs are also injured because a "mitigated" CPU affected by Downfall now must use more electricity and generate more heat, longer, to process the same amount of instructions and data that it did before Intel's mitigation.

244. Indeed, CPUs have distinct power-to-performance signatures. For example, for Rocket Lake Intel CPUs, the below chart, from computer hardware website Anandtech, shows their peak power consumption.



245. After mitigation, this power profile is significantly different. CPUs will have to run longer, hotter, and slower to accomplish the same task at peak power levels.

246. The defect's necessary "mitigation" also causes additional physical wear on the CPU and on batteries in battery-powered computers, such as laptops, reducing the life of the battery.

247. Moreover, operating CPUs for longer and hotter diminishes the expected life of a CPU.

248. In short, Plaintiffs have sustained physical injury to their computers, including in the form of increased heat, increased power consumption, and reduced battery life in the case of laptops (as the batteries will be drained more frequently due to slower processing time).

249. Finally, Plaintiffs are injured because Intel's defective design requires mitigation measures that may cause software incompatibilities, including with software compiled to use x86 AVX instructions.

TOLLING OF THE STATUTES OF LIMITATIONS

250. Plaintiffs and class members are entitled to tolling of the statutes of limitations applicable to the claims asserted below, as Plaintiffs and class members did not discover—and could not have reasonably discovered—that the CPUs they purchased were defective, including because of their vulnerability to the Downfall defect, until very recently.

251. Indeed, Intel did not publicly disclose even the existence of the AVX instruction buffers that are exploited as part of the Downfall vulnerability until August 2023. As such, no reasonable amount of diligence could have alerted Plaintiffs or class members to the existence of any of the asserted claims or the defect.

252. Moreover, Intel was provided specific and exclusive knowledge of the Downfall vulnerability on or about August 24, 2022, and expressly instructed Moghimi not to disclose the vulnerability to the public until August 2023. No public disclosure was permitted during the one-year embargo period.

253. Plaintiffs were alerted for the first time that their CPUs were vulnerable to Downfall well after they purchased their CPUs. They could not reasonably have known about the defect in their Intel CPUs until after the public announcement of the flaw in August 2023—and in fact, did not know about the defect or vulnerability of their Intel CPUs until after the public disclosure.

254. Intel's implementation of its branch prediction system is proprietary. In fact, Intel does not disclose the detailed workings of its branch prediction systems, including its predictive systems, even to sophisticated customers.

255. As such, no reasonable amount of diligence could have uncovered Intel's defective design and the vulnerability of its CPUs until the public announcement of the Downfall vulnerability on August 9, 2023.

256. Indeed, Moghimi, the researcher that uncovered the defect, employed highly technical methods well outside of the possession of a reasonable CPU or computer purchaser, including searching for Intel's undisclosed AVX instruction buffers. None of the methods employed by Moghimi are reasonably available to CPU or computer purchasers.

257. Because Plaintiffs and class members could not have known—and did not actually know—about the defect Intel failed to disclose, the statutes of limitations applicable to the claims they assert here are tolled until August 9, 2023, at the earliest.

258. Moreover, Plaintiffs and class members could not have known about the performance degradation resulting from Intel's "mitigation"/microcode update until it was released subsequent to the public August 9, 2023 announcement.

CLASS ACTION ALLEGATIONS

259. Plaintiffs bring this action and seek to certify and maintain it as a class action under Rules 23(a), (b)(2), (b)(3), and/or (c)(4) of the Federal Rules of Civil Procedure, on behalf of themselves and on behalf of the proposed classes of persons (collectively, the "Classes") defined below.

260. Each class's claims derive directly from a course of conduct by Intel.

261. Intel has engaged in uniform and standardized conduct toward each class. Intel did not materially differentiate in its actions or inactions toward members of the respective Classes. For each class, the objective facts on these subjects are the same for all class members.

262. Within each Claim for Relief asserted by each class, the same legal standards govern. Accordingly, Plaintiffs bring this lawsuit as a class action on their own behalf and on behalf of all other persons similarly situated as members of the proposed classes pursuant to Fed. R. Civ. P. 23.

263. Additionally, many states, and for some claims all states, share the same legal standards and elements of proof, allowing for a multistate or nationwide class or classes for some or all claims.

264. This action may be brought and properly maintained as a class action because the questions it presents are of a common or general interest, and of many persons, and also because the

parties are numerous, and it is impracticable to bring them all before the court. Plaintiffs may sue for the benefit of all as representative parties pursuant to Federal Rule of Civil Procedure 23.

The Nationwide CPU Purchaser Class

265. Plaintiffs Waltrip and Cameron bring this action and seek to certify and maintain it as a class action on behalf of themselves and all affected Intel CPU purchasers. The Nationwide CPU Purchaser Class comprises:

> All United States persons, business associations, entities, or corporations that purchased Intel CPUs from the 6th through 11th generation Core or Xeon families utilizing Affected Architectures[2] for their computers from June 16, 2018, to the present, inclusive (the "Class Period").

266. Plaintiffs Waltrip and Cameron and members of the Nationwide CPU Purchaser Class assert nationwide claims based on the uniform application of California law against Intel.

267. Excluded from the Nationwide CPU Purchaser Class are Intel, its employees, officers, directors, legal representatives, heirs, successors, and wholly or partly owned subsidiaries or affiliates; and the judicial officers and their immediate family members and associated court staff assigned to this case.

The Nationwide Computer Purchaser Class

268. Plaintiffs Smith, Cordova, and Worley bring this action and seek to certify and maintain it as a class action on behalf of themselves and a Nationwide Computer Purchaser Class. The Nationwide Computer Purchaser Class comprises:

[2] "Affected Architectures" means, based on publicly available information currently known: Haswell Server EP, Haswell Server EX, Broadwell Server E, Broadwell Server EX, Skylake Server, Skylake D, Skylake W, Skylake X, Cascade Lake Server, Cascade Lake W, Cascade Lake X, Cooper Lake, Broadwell DE V2, Broadwell DE Y0, Broadwell DE A1, Hewitt Lake, Apollo Lake, Denverton, Ice Lake Xeon-SP, Ice Lake Xeon D, Gemini Lake, Ice Lake U, Ice Lake Y, Snow Ridge, Parker Ridge, Lakefield B-step, Tiger Lake U, Tiger Lake U Refresh, Tiger Lake H35, Tiger Lake H, Amber Lake Y, Jasper Lake, Kaby Lake U, Kaby Lake U23e, Kaby Lake Y, Kaby Lake S, Kaby Lake H, Kaby Lake G, Kaby Lake X, Kaby Lake Xeon E3, Kaby Lake Refresh U, Whiskey Lake U, Ice Lake, Comet Lake-S, Comet Lake U42, Coffee Lake U23e, Coffee Lake S, Coffee Lake Xeon E, Coffee Lake S Xeon E, Coffee Lake S x/KBP, Coffee Lake H, Rocket Lake, Tiger Lake, Raptor Lake, Alder Lake-N, Alder Lake U, Alder Lake H, Alder Lake P, Alder Lake S, Elkhart Lake, and Sapphire Rapids. All CPUs affected by the Downfall vulnerability are referred to as the "Affected CPUs."

> All United States persons, business associations, entities, or corporations that purchased computers containing Intel CPUs from the 6th through 11th generation Core or Xeon families utilizing Affected Architectures from June 16, 2018, to the present, inclusive (the "Class Period").

269. Plaintiffs Smith, Cordova, and Worley and members of the Nationwide Computer Purchaser Class assert nationwide claims based on the uniform application of California law against Intel.

270. Excluded from the Nationwide Computer Purchaser Class are Intel, its employees, officers, directors, legal representatives, heirs, successors, and wholly or partly owned subsidiaries or affiliates; and the judicial officers and their immediate family members and associated court staff assigned to this case.

The California Class

271. If Plaintiffs are unable to assert claims as part of a nationwide class, Plaintiff Smith, in the alternative, brings this action and seeks to certify and maintain it as a class action on behalf of himself and a California Class. The California Class comprises:

> All California persons, business associations, entities, or corporations that purchased computers with Intel CPUs from the 6th through 11th generation Core or Xeon families utilizing Affected Architectures from June 16, 2018 to the present, inclusive (the "Class Period").

272. Excluded from the California Class are Intel, its employees, officers, directors, legal representatives, heirs, successors, and wholly or partly owned subsidiaries or affiliates; and the judicial officers and their immediate family members and associated court staff assigned to this case.

The Oregon Class

273. If Plaintiffs are unable to assert claims as part of a nationwide class, Plaintiff Cordova, in the alternative, brings this action and seeks to certify and maintain it as a class action on behalf of herself and an Oregon Class. The Oregon Class comprises:

> All Oregon persons, business associations, entities, or corporations that purchased computers with Intel CPUs from the 6th through 11th generation Core or Xeon families utilizing Affected Architectures from June 16, 2018 to the present, inclusive (the "Class Period").

274. Excluded from the Oregon Class are Intel, its employees, officers, directors, legal representatives, heirs, successors, and wholly or partly owned subsidiaries or affiliates; and the judicial officers and their immediate family members and associated court staff assigned to this case.

The Illinois Class

275. If Plaintiffs are unable to assert claims as part of a nationwide class, Plaintiff Cameron, in the alternative, brings this action and seeks to certify and maintain it as a class action on behalf of himself and an Illinois Class. The Illinois Class comprises:

> All Illinois persons, business associations, entities, or corporations that purchased Intel CPUs from the 6th through 11th generation Core or Xeon families utilizing Affected Architectures for their computers from June 16, 2018 to the present, inclusive (the "Class Period").

276. Excluded from the Illinois Class are Intel, its employees, officers, directors, legal representatives, heirs, successors, and wholly or partly owned subsidiaries or affiliates; and the judicial officers and their immediate family members and associated court staff assigned to this case.

The Kansas Class

277. If Plaintiffs are unable to assert claims as part of a nationwide class, Plaintiff Waltrip, in the alternative, brings this action and seeks to certify and maintain it as a class action on behalf of herself and a Kansas Class. The Kansas Class comprises:

> All Kansas persons, business associations, entities, or corporations that purchased Intel CPUs from the 6th through 11th generation Core or Xeon families utilizing Affected Architectures for their computers from June 16, 2018 to the present, inclusive (the "Class Period").

278. Excluded from the Kansas Class are Intel, its employees, officers, directors, legal representatives, heirs, successors, and wholly or partly owned subsidiaries or affiliates; and the judicial officers and their immediate family members and associated court staff assigned to this case.

The Minnesota Class

279. If Plaintiffs are unable to assert claims as part of a nationwide class, Plaintiff Worley, in the alternative, brings this action and seeks to certify and maintain it as a class action on behalf of himself and a Minnesota Class. The Minnesota Class comprises:

> All Minnesota persons, business associations, entities, or corporations that purchased computers with Intel CPUs from the 6th through 11th generation Core or Xeon families utilizing Affected Architectures from June 16, 2018 to the present, inclusive (the "Class Period").

280. Excluded from the Minnesota Class are Intel, its employees, officers, directors, legal representatives, heirs, successors, and wholly or partly owned subsidiaries or affiliates; and the judicial officers and their immediate family members and associated court staff assigned to this case.

Numerosity

281. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(1).

282. The members of the Classes are so numerous that a joinder of all members would be impracticable. Millions of affected Intel CPUs were sold, either on a standalone basis or as part of affected computers, during the Class Period.

Ascertainability

283. The Classes are ascertainable.

284. The defined Classes consist of persons, business associations, entities, or corporations that purchased affected Intel CPUs for use in their computers and persons, business associations, entities, or corporations that purchased computers with affected Intel CPUs in them. The identity of these purchasers can be determined through records maintained by Intel, re-sellers/merchants, OEMs, and purchasers themselves.

285. This information can be used to provide members of each class with direct notice pursuant to the requirements of Rule 23 and the Due Process Clause of the United States Constitution.

Typicality

286. Plaintiffs' claims are typical of the members of the Classes.

287. Plaintiffs' claims are the same as those asserted by members of the Classes. Each Plaintiff, like the members of the Classes, has purchased a defective Intel processor or a computer incorporating a defective Intel processor, and has been injured similarly by Intel's defective CPUs.

288. Each Plaintiff alleges injury that is not unique to them, but is typical of members of each of the Classes, including measures of damages, such as damages resulting from the diminution of value of their computers proximately caused by Intel's defective CPUs.

289. Each Plaintiff alleges that their injury flows from the common course of conduct alleged as to Intel.

290. Each Plaintiff is similarly positioned as to each member of the Classes. As such, each Plaintiff's injury can be redressed in the same manner as any redress provided to the members of the Classes (and *vice versa*).

Adequate Representation

291. Plaintiffs and their counsel will fairly and adequately protect the interests of the class members.

292. Plaintiffs are committed to putting the interest of the Classes ahead of their own and to act in the best interest of members of the Classes.

293. Plaintiffs understand their obligations to the Classes and are committed to monitoring/supervising developments in the case and class counsel.

294. Plaintiffs have retained competent counsel experienced in computer science, computer architecture, cryptography, and computer security, as well as in consumer class actions.

295. Plaintiffs have retained counsel with the resources and capital to litigate the case on behalf of the Classes.

296. Plaintiffs and their counsel intend to prosecute this action vigorously and to obtain relief, including both injunctive and monetary relief, that will remedy the design flaw and its manifestations (*e.g.*, inadequate security and performance degradation).

Superiority

297. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(2) because Intel has acted and/or refused to act on grounds generally applicable to the Classes, thereby making final injunctive and/or corresponding declaratory relief appropriate with respect to each class as a whole.

298. The class device is superior to all other available methods of adjudication, as it would make little sense for each of the millions of class members to separately prove the common conduct in which Intel has engaged.

299. Moreover, damages suffered by each individual member of the Classes may be small, meaning that the expense or burden of individual litigation would make it very difficult or impossible for individual class members to redress their injury individually.

300. Because damages may be small, individual members of the Classes may not have a rational economic interest in individually controlling the prosecution of a single action, and the burden imposed on the judicial system from having to individually adjudicate such claims will be significant in comparison to the value of individual claims.

301. Class litigation is thus superior to individual litigation and is the best procedural device to vindicate the rights of the members of the Classes.

302. In addition, class litigation will streamline the management of the litigation, such that the expense, burdens, inconsistencies, economic infeasibility, and other negative effects of individual mitigation will be lessened if not eliminated.

303. In sum, class litigation is superior because it mitigates significant inefficiencies and barriers that would result from individual litigation. In fact, absent invocation of the class device, the Classes' claims would likely not be vindicated individually, and Intel's sale of defective CPUs, and the resulting injury to purchasers, will go unaddressed.

Commonality and Predominance

304. This action and the claims asserted by the classes satisfy the requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) because there are many questions of law and fact that are common as to all of the members of the Classes.

305. These questions of fact and law concern Intel's conduct, which is common as to the members of the Classes, and answers to those questions would provide answers to issues posed by claims asserted by all members of the Classes.

306. These common issues will predominate at trial, and any individual issues that may arise would not outweigh the predominance of common issues.

307. Common issues that will predominate at trial include, without limitation, the following:

a. Whether Intel's defective design of its affected processors was reckless, negligent, and/or unlawful;

b. Whether Intel's design of its affected processors amounts to unfair competition;

c. Whether Intel's design of its affected processors should be permanently enjoined;

d. Whether Intel's design of its affected processors resulted in or is resulting in an injury to computers that incorporate those CPUs;

e. Whether the members of the Classes experienced or are experiencing out of pocket losses caused by Intel's alleged conduct;

f. Whether Intel was unjustly enriched by its conduct;

g. Whether Intel employed unlawful, unfair, deceptive, and/or fraudulent practices that harmed Plaintiffs and members of the Classes;

h. Whether Intel engaged in false advertising in contravention of California law;

i. Whether Intel violated the consumer protection laws and statutes of California, including its Unfair Competition Law and the California Consumer Legal Remedies Act;

j. Whether members of the Classes are entitled to equitable relief, including but not limited to a preliminary and/or permanent injunction and/or declaratory relief;

k. Whether aggregate amounts of statutory penalties are enough to punish and deter Intel and to vindicate statutory and public policy;

l. How such penalties should most equitably be distributed among class members;

m. Whether Intel violated the consumer protection statutes of each State, including California, Illinois, Minnesota, and Oregon;

n. Whether Intel knew or should have known about the faulty design of its CPUs when it sold them;

o. Whether purchasers of defective Intel processors are entitled to restitution for money paid for Intel's products and services due to the allegedly unlawful and/or unfair conduct by the company.

Grounds Generally Applicable to the Classes

308. Plaintiffs intend to seek injunctive relief ending Intel's sale of defective processors.

309. Plaintiffs are properly situated to seek such an injunction because Intel has acted and/or refused to act on grounds generally applicable to Plaintiffs and the members of the Classes.

310. This means that final injunctive relief or declaratory relief will redress Plaintiffs' harm as well as the harm to members of the Classes.

311. An injunction preventing Intel from continuing to sell defective CPUs will stop Intel's unlawful conduct from occurring in the future. In the alternative, an injunction requiring Intel to recall or buy back the affected CPUs (the "Affected CPUs") will stop Intel's unlawful conduct from continuing to injure the Classes.

CHOICE OF LAW

312. Plaintiffs aver that California law applies to their claims, and Plaintiffs accordingly assert their claims on behalf of a nationwide class.

313. There are no conflicts between California law and those of the several States as to the nationwide claims asserted in this Complaint on behalf of the Nationwide Class.

CLAIMS FOR RELIEF

REALLEGATION AND INCORPORATION BY REFERENCE

314. Plaintiffs reallege and incorporate by reference all the preceding paragraphs and allegations of this Complaint, as though fully set forth in each of the following Claims for Relief asserted on behalf of the classes.

A. Nationwide Claims (based on California Law)

COUNT ONE
Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On behalf of the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class, or, in the alternative, the California Class)

315. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

316. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley bring unlawful, unfair, and fraudulent prongs of this Count on behalf of themselves and the Nationwide CPU Purchaser Class and

Nationwide Computer Purchaser Class. Alternatively, Plaintiff Smith brings the unlawful, unfair, and fraudulent prongs of this Count on his own behalf and on behalf of the California Class.

317. California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq.*, proscribes acts of unfair competition, including "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Intel has engaged in unfair or deceptive acts or practices that violated the UCL, as described above and below, by, among other things, representing that the Affected CPUs have characteristics, uses, benefits, and qualities which they do not have; representing that the Affected CPUs are of a particular standard, quality and grade when they are not; advertising that the Affected CPUs are of a particular standard, quality, and grade when they are not; advertising the Affected CPUs with the intent not to sell them as advertised; and representing that the Affected CPUs had been supplied in accordance with their representations, when they had not. Intel has violated the unlawful, unfair, and fraudulent prongs of the UCL, as set forth in this Complaint and below.

318. Intel's actions constitute **"unlawful" trade practices** within the meaning of the UCL. In the course of Intel's business, Intel willfully failed to disclose and actively concealed that the Affected CPUs were defective, such that normal use of Intel's Affected CPUs would not provide (a) adequate security features, including features that reduce the risk and effect of attacks based on speculative execution; and/or (b) sufficient, expected, and promised processing speeds. Particularly in light of Intel's advertising campaign, a reasonable American consumer would expect the Affected CPUs to provide (a) adequate security features, including features that reduce the risk and effect of attacks based on speculative execution; and/or (b) sufficient, expected, and promised processing speeds. Accordingly, Intel engaged in unlawful trade practices by employing deception, deceptive acts or practices, concealment, suppression, or omission of material facts with intent that others rely upon such concealment, suppression, or omission, in connection with the sale of the Affected CPUs. Intel's actions are further unlawful because they violated (and violate) other statutes and common law prohibitions, including those recited in the other counts of this Complaint.

319. Intel's actions also constitute **"fraudulent" trade practices** within the meaning of the UCL. In purchasing the Affected CPUs, Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members were deceived

by Intel's failure to disclose that normal use of the Affected CPUs would not provide (a) adequate security features, including features that reduce the risk and effect of attacks based on speculative execution; and/or (b) sufficient, expected, and promised processing speeds.

320. Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members reasonably relied upon Intel's false misrepresentations. They had no way of knowing that Intel's representations were false and misleading, including by being knowingly and materially incomplete. As alleged here, Intel engaged in sophisticated methods of concealment, suppression, and omission about highly technical matters for which there was and is an inherent asymmetry of information. Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members did not, and could not, find out about Intel's deceptive omissions on their own, as Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and Nationwide CPU Purchaser Class and the Nationwide Computer Purchaser Class members were not aware of the defective nature of Intel's CPUs.

321. Intel's actions as set forth in this Complaint occurred in the conduct of trade or commerce.

322. Intel's deceptive concealment, suppression, and/or omission of material facts was likely to and did in fact deceive reasonable consumers.

323. Intel intentionally and knowingly misrepresented material facts regarding the Affected CPUs it manufactured and sold with intent to mislead Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members.

324. Intel knew or should have known that its conduct violated California law regarding unfair and/or deceptive acts in trade or commerce.

325. Intel owed Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members a duty to disclose the truth about the Affected CPUs because Intel:

i. Possessed exclusive knowledge of the defective design of the Affected CPUs;

ii. Intentionally concealed the above from Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members; and/or

iii. Made incomplete representations regarding the quality of the Affected CPUs, while purposefully withholding material facts from Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members that contradicted these representations.

326. Due to the specific and superior knowledge that Intel possessed, its false representations regarding the quality of the Affected CPUs, and Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members' reliance on these material representations, Intel had a duty to disclose to Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members that the Affected CPUs were defective, *i.e.*, that Intel's Affected CPUs did not and do not provide (a) adequate security features, including features that reduce the risk and effect of attacks based on speculative execution; and/or (b) sufficient, expected, and promised processing speeds. Having volunteered to provide information to Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members, Intel had a duty to disclose not just the partial truth, but the entire truth. These omitted and concealed facts were material because they directly impacted, and impact, the value of the Affected CPUs that were purchased by Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members. Adequate security features, including features which reduce the risk and effect of attacks based on speculative execution, and sufficient, expected, and promised processing speeds are material concerns to CPU and computer purchasers like (and including) Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members. Intel represented to Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members that they were purchasing CPUs or computers that were free from defect, when in fact they were or included defective CPUs.

327. Intel's conduct proximately caused injuries to Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members.

328. Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members were injured and suffered ascertainable loss, injury-in-fact, and/or actual damage as a proximate result of Intel's conduct: Plaintiffs Smith, Cordova, and Worley and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members overpaid for the Affected CPUs, and the Affected CPUs suffered a diminution in value. These injuries are the direct and natural consequence of Intel's fraudulent omissions.

329. Intel's actions constitute **"unfair" trade practices** within the meaning of the UCL. Intel's unlawful acts and practices complained of in this Complaint affect the public interest, as its actions offend public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

330. To begin with, Intel's business practice of failing to disclose that its CPUs are defective when selling them to customers and to OEMs is an unfair, unethical, oppressive, and unscrupulous practice.

331. Moreover, in addition to Intel's failure to disclose the defect, and indeed, its outright fraud, Intel's conduct is unfair because the gravity of the harm inflicted by its conduct is greater than any possible utility:

- Intel's decision not to properly redesign its hardware after Spectre and Meltdown (and the many variants), and even after Intel was warned about the same class of vulnerabilities in its AVX instructions, was willful, reckless and unreasonable. Intel could have redesigned its hardware to resolve the root design defect in its chips, but did not do so to maximize profits and minimize costs. During the entire period Intel sold defective CPUs, including to Plaintiffs and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members, it could have fixed the defect at the hardware level. Indeed, Intel's newer CPUs do not suffer from the Downfall defect, nor do the CPUs of its chief competitor, AMD. This conduct lacked any utility, and it resulted in a widespread vulnerability in millions (likely billions) of CPUs and computers. Put simply, there was no utility for Intel's conduct, and the harm to Plaintiffs and the Nationwide CPU Purchaser Class and Nationwide Computer

Purchaser Class members, who were knowingly sold defective CPUs and computers with defective CPUs worth substantially less than they paid for them, is immense.

- Intel's mitigation also lacks utility under the circumstances, while inflicting serious harm on Plaintiffs and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members. Intel's mitigation substantially impairs the central operation of its Affected CPUs—the very circuitry that allows a modern processor to process instructions and data—and the computers incorporating these Affected CPUs. As a result, Intel's Affected CPUs, and computers incorporating them, no longer perform according to merchantable and saleable standards or customer expectations, including once "mitigated" using Intel's performance- and functionality-degrading software patch. Intel's mitigation also impairs the value of Plaintiffs' and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members' CPUs and computers, as it substantially diminishes their performance and functionality beyond ordinary and reasonable commercial and industry expectations.
- Intel's decision to block publication of the Downfall defect for approximately a year while selling defective CPUs to purchasers and OEMs lacked any utility and resulted in substantial harm to billions of CPUs and computers, and as a proximate result, to Plaintiffs and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members. Intel's decision to block publication of the defect also concealed that Intel's CPUs for years had not been properly redesigned at the hardware level despite catastrophic, known-to-Intel security vulnerabilities. If the truth were publicly known, consumers and computer owners could make their own decisions about the value and utility of Intel's products, and researchers and industry participants could have devised more effective mitigations. Intel prevented them from doing so by withholding highly material information about its products—all to maximize profits.

332. All of this conduct is unfair under the UCL and proximately caused injury to Plaintiffs and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members.

333. As a direct and proximate result of Intel's violations of the UCL, Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members have suffered injury-in-fact and/or actual damage.

334. Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron would like to purchase Intel CPUs of similar design in the future, but are unable to rely on Intel's representations regarding its CPUs' performance, as they have no way of determining whether those representations are in fact true.

335. Defendant has been unjustly enriched and should be required to make restitution to Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members under Sections 17203 and 17204 of the California Business & Professions Code. Plaintiffs Smith, Cordova, Worley, Waltrip, and Cameron and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members also seek injunctive relief as deemed appropriate by the Court, including but not limited to a prohibition on falsely advertising Intel CPUs of similar design until the design defect is corrected.

COUNT TWO
Violation of the California Consumer Legal Remedies Act
Cal. Civ. Code § 1750, *et seq.*
(On behalf of the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class, or, in the alternative, the California Class)

336. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

337. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley bring this Count on their own behalf and on behalf of the Nationwide CPU Purchaser Class and the Nationwide Computer Purchaser Class. In the alternative, Plaintiff Smith brings this Count on his own behalf and on behalf of the California Class.

338. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members are "consumers" as defined in Cal. Civ. Code § 1761(d).

339. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members and Intel are "persons" as defined in Cal. Civ. Code § 1761(c).

340. Affected CPUs made by Intel, and computers incorporating Affected CPUs made by Intel, are "goods" as defined in Cal. Civ. Code § 1761(a).

341. California's Consumer Legal Remedies Act ("CLRA"), Cal. Civ. Code §§ 1750, et seq., proscribes "unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer."

342. Intel's conduct as described in this Complaint was and is in violation of the CLRA. Intel's conduct violates at least the following enumerated CLRA provisions:

i. Cal. Civ. Code § 1770(a)(5): Representing that the Affected CPUs have sponsorship, approval, characteristics, uses, benefits, or quantities that they do not have.

ii. Cal. Civ. Code § 1770(a)(7): Representing that the Affected CPUs are of a particular standard, quality, or grade although they are of another.

iii. Cal. Civ. Code § 1770(a)(9): Advertising the Affected CPUs with the intent not to sell them as advertised.

iv. Cal. Civ. Code § 1770(a)(16): Representing that the subject of a transaction involving the Affected CPUs has been supplied in accordance with a previous representation when it has not.

343. In the course of Intel's business, it willfully failed to disclose and actively concealed that the Affected CPUs were defective, such that normal use of the Affected CPUs would not provide (a) adequate security features, including features which reduce the risk and effect attacks due to speculative execution; and/or (b) sufficient processing speeds. Particularly in light of Intel's advertising campaign, a reasonable California consumer would expect the Affected CPUs to provide (a) adequate security features, including features that reduce the risk and effect of attacks based on speculative execution; and/or (b) sufficient, expected, and promised processing speeds. Accordingly, Intel engaged in unlawful trade practices by employing deception, deceptive acts or practices; fraud; misrepresentation; or

concealment, suppression, or omission of material facts with intent that others rely upon such concealment, suppression, or omission, in connection with the sale of the Affected CPUs.

344. In purchasing the Affected CPUs, Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members were deceived by Intel's failure to disclose that normal use of the Affected CPUs would not provide (a) adequate security features, including features that reduce the risk and effect of attacks based on speculative execution; and/or (b) sufficient, expected, and promised processing speeds.

345. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members reasonably relied upon Intel's false misrepresentations. They had no way of knowing that Intel's representations were false and misleading. As alleged in this Complaint, Intel engaged in sophisticated methods of deception, including about highly technical matters for which there was (and is) an inherent asymmetry of information. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members did not, and could not, discover Intel's deception on their own, as Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members were not aware of the defective nature of the Affected CPUs (and indeed, the vulnerable AVX buffers in Affected CPUs were not publicly known) prior to purchase.

346. Intel's actions as set forth above occurred in the conduct of trade or commerce.

347. Intel's deception, fraud, misrepresentation, concealment, suppression, or omission of material facts were likely to, and did in fact, deceive reasonable consumers.

348. Intel intentionally and knowingly failed to disclose material facts regarding the Affected CPUs with intent to mislead Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members.

349. Intel owed Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members a duty to disclose the truth about the Affected CPUs because Intel:

i. Possessed exclusive knowledge of the design of its CPUs, including the defective nature of its speculative execution, branch prediction, and out-of-order execution systems;

ii. Intentionally concealed the above from Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members; and/or

iii. Made incomplete representations regarding the performance of the Affected CPUs, while purposefully withholding material facts from Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members that contradicted these representations.

350. Due to its specific and superior knowledge that the Affected CPUs did not provide (a) adequate security features, including features that reduce the risk and effect of attacks based on speculative execution; and/or (b) sufficient, expected, and promised processing speeds, Intel had a duty to disclose to Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members that the Affected CPUs were defective. Moreover, Intel had a duty to disclose that its Affected CPUs did not provide (a) adequate security features, including features that reduce the risk and effect of attacks based on speculative execution; and/or (b) sufficient, expected, and promised processing speeds. Having volunteered to provide information to Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members, Intel had the duty to disclose not just the partial truth, but the entire truth. These omitted and concealed facts were material because they directly impacted, and impact, the value of the Affected CPUs or computers incorporating Affected CPUs purchased by Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members.

351. The following features are material to Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members: (a) adequate security features, including features that reduce the risk and effect of attacks based on speculative execution; and/or (b) sufficient, expected, and promised processing speeds.

352. Intel represented to Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members that they were

purchasing Intel CPUs, or computers incorporating Intel CPUs, that were free from defect, when in fact the Affected CPUs were defective.

353. Intel's conduct proximately caused injuries to Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members.

354. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members were injured and suffered ascertainable loss, injury-in-fact, and/or actual damage as a proximate result of Intel's conduct. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members overpaid for Affected CPUs or for computers incorporating Affected CPUs, and the Affected CPUs (and computers incorporating them) have suffered a diminution in value. These injuries are the direct and natural consequence of Intel's misrepresentations and omissions.

355. Intel's unlawful acts and practices complained of in this Complaint affect the public interest, as these actions offend public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

356. As a direct and proximate result of Intel's violations of the CLRA, Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members have suffered injury-in-fact and/or actual damage.

357. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members would like to purchase Affected CPUs or Intel CPUs of similar design (or computers incorporating such Intel CPUs) in the future, but are unable to rely on Intel's representations regarding its CPUs' performance, as they have no way of determining whether those representations are in fact true.

358. As a result of Intel's violations of the CLRA, Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley, the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members, and the general public of the State of California, seek injunctive relief prohibiting Intel from continuing the unlawful practices described in this Count and in this Complaint, including but not limited to a prohibition on falsely advertising the Affected CPUs or Intel CPUs of similar design until the design

defect is corrected, pursuant to Cal. Civ. Code § 1782(a)(2); equitable relief, including restitution; and a declaration that Intel's conduct violated the CLRA.

359. Pursuant to Cal. Civ. Code § 1782, on October 27, 2023, Plaintiffs Smith and Worley mailed Intel notice in writing, via certified U.S. mail, of Intel's particular violations of the CLRA and demanded that Intel rectify the actions described above by providing complete monetary relief, agreeing to be bound by its legal obligations, and giving notice to all affected customers of Intel's intent to do so.

COUNT THREE
Violation of the California False Advertising Law
Cal. Bus. & Prof. Code § 17500, *et seq.*
(On behalf of the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class, or, in the alternative, the California Class)

360. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

361. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley bring this Count on their own behalf and on behalf of the Nationwide CPU Purchaser Class and the Nationwide Computer Purchaser Class. In the alternative, Plaintiff Smith brings this Count on his own behalf and on behalf of the California Class.

362. Intel has benefitted from intentionally selling defective CPUs at artificially inflated prices due to fraudulent statements about the CPUs and their defective design. Intel has received unjust profits from this conduct, and Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members overpaid for Affected CPUs, or computers incorporating Affected CPUs, as a result of this conduct.

363. Intel publicly disseminated advertising and promotional material that was designed and intended to convey to the public that the Affected CPUs were capable of providing (a) adequate security features, including features that reduce the risk and effect of attacks based on speculative execution; and/or (b) sufficient, expected, and promised processing speeds.

364. Intel was aware of the defective design of its Affected CPUs at the time Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members purchased Affected CPUs or computers incorporating Affected

CPUs. Intel intentionally designed its Affected CPUs to defraud consumers about whether these CPUs provided (a) adequate security features, including features that reduce the risk and effect of attacks based on speculative execution; and/or (b) sufficient, expected, and promised processing speeds.

365. Moreover, Intel intentionally made representations that it corrected the vulnerabilities that led to Spectre and Meltdown, yet—due to defects Intel was aware of—did not sell Affected CPUs that conformed to the representations and promises in Intel's publicly disseminated advertisements.

366. Intel unjustly received and retained benefits from Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members.

367. It is inequitable and unconscionable for Intel to retain these benefits.

368. Because Intel wrongfully concealed its misconduct, Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members were not aware of the facts concerning the Affected CPUs and did not benefit from Intel's misconduct.

369. Intel knowingly accepted the unjust benefits of its wrongful conduct.

370. Intel had notice of its misconduct as alleged in this Complaint.

371. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley would like to purchase Intel CPUs (or computers incorporating Intel CPUs) of similar design in the future, but are unable to rely on Intel's representations regarding its CPUs' performance and security features, as they have no way of determining whether those representations are in fact true.

372. As a result of Intel's misconduct, Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members suffered an injury-in-fact and lost money and/or property in an amount to be proven at trial. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members also seek injunctive relief as deemed appropriate by the Court, including but not limited to a prohibition on falsely advertising Intel CPUs of similar design until the design defect is corrected.

COUNT FOUR
Fraud by Omission under California Law
(On behalf of the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class, or, in the alternative, the California Class)

373. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

374. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley bring this Count on behalf of themselves and the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class members. Alternatively, Plaintiff Smith brings this Count on his own behalf and on behalf of the California Class, under California law.

375. Intel fraudulently concealed and suppressed material facts regarding the Affected CPUs. Intel knew when it marketed and sold its CPUs that they were defective as to functionality central to the product's function—security and performance. Intel failed to disclose these facts to consumers, including Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members, at the time Intel marketed and sold the Affected CPUs, and jointly marketed computers incorporating Affected CPUs. Intel knowingly and intentionally engaged in this concealment in order to boost sales and revenues, maintain its competitive edge in the industry, and obtain windfall profits.

376. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members had no reasonable means of knowing that Intel had omitted to disclose material details relating to the Affected CPUs. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members did not and could not reasonably discover Intel's concealment on their own.

377. Intel had a duty to disclose, rather than conceal and suppress, the full scope and extent of the Affected CPUs' defects:

i. Intel had exclusive or far superior knowledge of the design of its CPUs, including as to the security risks in Intel's design of speculative execution and the performance issues caused through its mitigation of these risks;

ii. The details regarding these CPUs' defective design were known and/or accessible only to Intel;

iii. Intel knew that Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members did not know about Intel's defective CPUs; and

iv. Intel made representations and assurances about the qualities of the Affected CPUs, including statements about their performance, security, and quality that were misleading, deceptive, and incomplete without the disclosure of the fact that these processors were defectively designed.

378. These omitted and concealed facts were material because a reasonable consumer would rely on them in deciding to purchase an Affected CPU or a computer incorporating an Affected CPU, and because they substantially reduced the value of the Affected CPUs or computers incorporating Affected CPUs that Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members purchased. Whether the Affected CPUs were defective would have been an important factor in Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members' purchasing decisions.

379. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members trusted Intel not to sell them products that were defective.

380. Intel intentionally and actively concealed and suppressed these material facts to falsely assure purchasers that the Affected CPUs, and computers incorporating Affected CPUs, were of superior quality, performance, and security, as represented by Intel and as reasonably expected by purchasers.

381. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members are accordingly unable to rely on any representations by Intel given its fraudulent omissions.

382. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members were unaware of these omitted material

facts and would have paid less for the Affected CPUs (or computers incorporating Affected CPUs), or would not have purchased them at all, if they had known of the concealed and suppressed facts.

383. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members relied to their detriment upon Intel's reputation and material omissions in deciding to purchase Affected CPUs or computers incorporating Afffected CPUs.

384. As a direct and proximate result of Intel's fraudulent concealment, including its intentional suppression of the true facts, Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members suffered injury. They purchased CPUs, or computers incorporating CPUs, of inferior quality, performance, and security, which had a diminished value by reason of Intel's concealment of, and failure to disclose, the defect in its Affected CPUs.

385. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members sustained damages as a direct and proximate result of Intel's fraudulent concealment, in an amount to be proven at trial.

386. Intel's acts were done maliciously, oppressively, deliberately, with intent to defraud, and in reckless disregard for Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members' rights, with the aim of enriching Intel, justifying an award of punitive damages in an amount sufficient to deter such wrongful conduct in the future.

COUNT FIVE
Quasi-Contract/Restitution Under California Law
(On behalf of the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class, or in the alternative, the California Class)

387. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

388. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley bring this Count on their own behalf and on behalf of the Nationwide CPU Purchaser Class and the Nationwide Computer Purchaser

Class. In the alternative, Plaintiff Smith brings this Count on his own behalf and on behalf of the California Class.

389. This cause of action is pleaded in the alternative to the legal claims asserted.

390. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members lack an adequate remedy at law for their claims, as specifically set forth later in this Complaint.

391. Intel's conduct is unjust and requires restitution. Specifically, Intel received hundreds of millions—if not billions—of dollars in revenue from the sale of Affected CPUs.

392. This revenue was a benefit conferred upon Intel by Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members.

393. Intel was unjustly enriched through financial benefits conferred upon it by Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members in the form of the amounts paid to Intel for the Affected CPUs, through Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members's purchase of Affected CPUs or computers incorporating Affected CPUs.

394. Intel knew and understood that it would and did receive a financial benefit, and voluntarily accepted the same, from Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members when they elected to purchase Affected CPUs or computers incorporating Affected CPUs.

395. By selecting Affected CPUs or computers incorporating Affected CPUs and purchasing them at a premium price, Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members reasonably expected that the Affected CPUs would have the performance, security, and quality promoted by Intel, and be designed and manufactured with reasonable care. Instead, not only did the Affected CPUs fall short of such expectations and performance/security standards, they injured and damaged Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer

Purchaser Class Members computers by interfering with their operation. The Affected CPUs also made Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members computers less secure. Intel was enriched, while at the same time, Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members experienced a diminution of value to their computers.

396. Therefore, because Intel will be unjustly enriched if it is allowed to retain the revenues obtained through its negligence and unlawful conduct, Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members are entitled to recover the amount by which Intel was unjustly enriched at their expense.

397. Accordingly, Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members seek damages against Intel in the amounts by which Intel has been unjustly enriched at Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members' expense, and such other relief as this Court deems just and proper.

COUNT SIX
Negligence under California Law
(On behalf of the Nationwide CPU Purchaser Class and Nationwide Computer Purchaser Class, or, in the alternative, the California Class)

398. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

399. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley bring this Count on their own behalf and on behalf of the Nationwide CPU Purchaser Class and the Nationwide Computer Purchaser Class. In the alternative, Plaintiff Smith brings this claim on behalf of the California Class.

400. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members bring this negligence claim for harm to their property—their computers. This count does not state a claim for injuries, damage, or overpayment as to the Intel CPUs themselves.

401. Intel had a duty to Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members to exercise reasonable care in designing and manufacturing the Affected CPUs.

402. Intel knew, or could reasonably foresee, that Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members would incorporate or use the CPU in their computers, and that the computers would be used to edit photos and videos, play games, and perform other everyday tasks using AVX instructions.

403. Intel knew, or could reasonably foresee, that the Affected CPUs would interface with other hardware components in Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members' computers, including, for example, Random Access Memory ("RAM"), Graphical Processing Units ("GPUs"), and other peripherals.

404. Intel knew, or could reasonably foresee, that its design of its CPUs would make Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members computers susceptible to attacks due to speculative execution and cause a substantial decrease in processing speeds.

405. Intel undertook a duty of care to Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members when it designed the CPUs incorporated into, or sold for incorporation into, their computers.

406. Intel breached its duty of care by designing CPUs that were uniquely susceptible to attacks based on speculative execution, for which the only available mitigation causes a substantial decrease in processing speeds.

407. Intel's defective design fell below the standard of reasonable care, as other CPUs are not uniquely susceptible to attacks due to speculative execution and do not require a mitigation that results in substantially decreased processing speeds.

408. Intel's breach of duty proximately caused injury and damage to Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members' property—their computers. The physical wear on Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer

Purchaser Class Members computers includes diminished battery life (for laptops) and (for all computers) a diminished expected life for the CPU and nearby components due to the CPU running for longer and at hotter temperatures. This is a direct and foreseeable consequence of Intel's defective design of the Affected CPUs.

409. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members are injured and damaged by Intel's defectively designed CPUs because the Affected CPUs interfere with, damage, and/or injure the functionality of Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members' computers incorporating Affected CPUs. Plaintiffs Cameron, Cordova, Smith, Waltrip, and Worley and the Nationwide CPU Purchaser and Nationwide Computer Purchaser Class Members seek to recover damages for their injury, including the diminution of value of their computers as a result of Intel's negligence.

COUNT SEVEN
Breach of Implied Warranty under California Law
Cal. Comm. Code § 2314
(On behalf of the Nationwide CPU Purchaser Class)

410. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

411. Plaintiffs Cameron and Waltrip bring this cause of action on their own behalf and on behalf of the Nationwide CPU Purchaser Class under the law of warranties, which is materially uniform in all states. In the alternative, Plaintiffs Cameron and Waltrip bring implied warranty claims on behalf of the Illinois and Kansas Classes as set forth above in this Complaint.

412. Intel is and was at all relevant times a merchant with respect to its CPUs, including the Affected CPUs.

413. A warranty that the Affected CPUs were in merchantable condition was implied by law for Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members' purchase of Affected CPUs.

414. Intel marketed the Affected CPUs as having high quality, speed, performance, and security, that would function, at least, as reasonably expected by consumers and in accordance with

industry standards. Intel's representations formed the basis for the bargain in Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members' decision to purchase Affected CPUs.

415. Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members purchased Affected CPUs from Intel, or through retailers or resellers. At all relevant times, Intel was the manufacturer, distributor, warrantor, and/or seller of the Affected CPUs.

416. Intel knew or had reason to know of the specific use for which the Affected CPUs were purchased.

417. Because of the design defect described in this Complaint in the Affected CPUs, the Affected CPUs were not in merchantable condition when sold and were (and are) not fit for the ordinary purpose of such CPUs.

418. Intel knew about the defect in the Affected CPUs, allowing Intel to cure its breach of warranty if it so chose.

419. In its capacity as warrantor, Intel had acknowledged the inherently defective nature of the defectively designed branch prediction, speculative execution, and out-of-order execution systems in Affected CPUs, and these CPUs' vulnerability to devastating AVX speculative execution attacks. Any effort by Intel to limit the implied warranties in a manner that would exclude coverage of the Affected CPUs is unconscionable, and any such effort to disclaim or otherwise limit such liability is null and void.

420. Any limitations Intel might seek to impose on its warranties are procedurally unconscionable. There was unequal bargaining power between Intel on the one hand and Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members on the other as, at the time of purchase, Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members had no other viable option for purchasing warranty coverage other than from Intel, nor were there alternative sources of comparable CPUs that Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members could have purchased free of the unconscionable terms contained in Intel's warranties. In addition, the terms of any applicable Intel express warranties were not displayed or conspicuous to Plaintiffs Cameron and Waltrip during the process of purchasing their Intel CPUs from Microcenter and Newegg.com, respectively, and they did not review those terms prior to purchase. The time limits contained in Intel's warranty periods were also unconscionable and inadequate to protect Plaintiffs

Cameron and Waltrip and the Nationwide CPU Purchaser Class Members. Among other things, Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members had no meaningful choice in determining these time limitations, the terms of which unreasonably favored Intel.

421. Any limitations Intel might seek to impose on its warranties are also substantively unconscionable. Intel knew that the Affected CPUs' defective design would result in the vulnerability and need for debilitating mitigation as set forth above. Moreover, Intel knew that this vulnerability and need for mitigation would manifest after the warranty purportedly expired. Intel failed to disclose the defect, or the need to slow down the performance of its CPUs for mitigation, to Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members. Thus, Intel's enforcement of the durational limits on those warranties are harsh and shock the conscience.

422. To the extent a CPU purchaser plaintiff or Nationwide CPU Purchaser Class Member is not in privity with Intel, privity of contract is not required here because Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members are intended third-party beneficiaries of contracts between Intel and retailers/resellers, including (1) the written distribution and supply agreements between Intel and its authorized resellers (*e.g.*, Amazon.com, Micro Center), and the implied warranties that attach to those contracts; and (2) any express warranties provided by Intel, Intel's retailers and resellers have no rights under the warranty agreements provided with the Affected CPUs; the warranty agreements were designed for and intended to benefit consumers. Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members are also intended beneficiaries of retailer and reseller warranties.

423. Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members have complied with all obligations under the warranty, or otherwise have been excused from performance of said obligations as a result of Intel's conduct described in this Complaint. Affording Intel a reasonable opportunity to cure the breach of written warranties would be unnecessary and futile.

424. Accordingly, Intel is liable to Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members for damages in an amount to be proven at trial.

COUNT EIGHT
Breach of Implied Warranty under the Song-Beverly Consumer Warranty Act
Cal. Civ. Code § 1790, *et seq*.
(On behalf of the Nationwide CPU Purchaser Class)

425. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

426. Plaintiffs Cameron and Waltrip bring this cause of action on their own behalf and on behalf of the Nationwide CPU Purchaser Class under the law of warranties, which is materially uniform in all states. In the alternative, Plaintiffs Cameron and Waltrip bring implied warranty claims on behalf of the Illinois and Kansas Classes as set forth above in this Complaint.

427. Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class are "buyers" within the meaning of Cal. Civ. Code § 1791(b).

428. Intel is a "manufacturer" within the meaning of Cal. Civ. Code § 1791(j).

429. The Affected CPUs, including those purchased by Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members, are "consumer goods" within the meaning of Cal. Civ. Code § 1791(a).

430. Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class members purchased their Affected CPUs at retail in California within the meaning of Cal. Civ. Code § 1792. Cameron and Waltrip purchased their Affected CPUs from Intel through Microcenter and Newegg.com, respectively. Intel is headquartered in California and directs its United States sales and shipping operations from California, including with respect to the Affected CPUs purchased by Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members.

431. A warranty that the Affected CPUs were in merchantable condition was implied by law for the subject transactions.

432. Intel marketed the Affected CPUs as having high quality, speed, performance, and security, that would function, at least, as reasonably expected by consumers and in accordance with industry standards. Intel's representations form the basis of the bargain in Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members' decisions to purchase Affected CPUs.

433. Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members purchased the Affected CPUs from Intel, or through retailers or resellers. At all relevant times, Intel was the manufacturer, distributor, warrantor, and/or seller of the Affected Computers.

434. Intel knew or had reason to know of the specific use for which the Affected CPUs were purchased.

435. Because of the design defect described in this Complaint, the Affected CPUs were not in merchantable condition when sold and were (and are) not fit for the ordinary purpose of such CPUs.

436. Intel knew about the defect in the Affected CPUs, allowing Intel to cure its breach of warranty if it chose.

437. In its capacity as warrantor, Intel had knowledge of the inherently defective nature of the defectively designed CPUs. Any effort by Intel to limit the implied warranties in a manner that would exclude coverage of the Affected CPUs is unconscionable, and any such effort to disclaim or otherwise limit such liability is null and void.

438. Any limitations Intel might seek to impose on its warranties are procedurally unconscionable. There was unequal bargaining power between Intel on the one hand and Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members on the other as, at the time of purchase, Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members had no other viable options for purchasing warranty coverage other than from Intel, nor were there alternative sources of comparable CPUs that Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members could have purchased free of the unconscionable terms contained in Intel's warranties. In addition, the terms of any applicable Intel express warranties were not displayed or conspicuous to Plaintiffs Cameron and Waltrip during the process of purchasing their Intel CPUs through Microcenter and Newegg.com, respectively, and they did not review those terms prior to purchase. The time limits contained in Intel's warranty periods are also unconscionable and inadequate to protect Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members. Among other things, Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members had no meaningful choice in determining these time limitations, the terms of which unreasonably favored Intel.

439. Any limitations Intel might seek to impose on its warranties are also substantively unconscionable. Intel knew that the Affected CPUs were defective, and that their defect could only be mitigated (absent a hardware redesign) by significantly impairing processor performance. Moreover, Intel knew that selling the Affected CPUs would result in the manifestation of a vulnerability and debilitating mitigation after the warranty purportedly expired. Intel failed to disclose the defect, or the needed mitigation, to Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members. Thus, Intel's enforcement of the durational limitations on those warranties is harsh and shocks the conscience.

440. A claim for breach of implied warranty under the Song-Beverly Consumer Warranty Act does not require contractual privity between a plaintiff and a defendant. In the alternative, to the extent a CPU purchaser plaintiff or a Nationwide CPU Purchaser Class Member is not in privity with Intel, privity of contract is not required here Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members are intended third-party beneficiaries of contracts between Intel and retailers/resellers, including (1) the written distribution and supply agreements between Intel and its authorized resellers (*e.g.*, Amazon.com, Micro Center), and the implied warranties that attach to those contracts; and (2) any express warranties provided by Intel. Intel's retailers and resellers have no rights under the warranty agreements provided with the Affected CPUs; the warranty agreements were designed for and intended to benefit consumers. Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members are also the intended beneficiaries of retailer and reseller warranties.

441. Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members have complied with all obligations under the warranty, or otherwise have been excused from performance of said obligations as a result of Intel's conduct described in this Complaint. Affording Intel a reasonable opportunity to cure the breach of written warranties would be unnecessary and futile.

442. Accordingly, Intel is liable to Plaintiffs Cameron and Waltrip and the Nationwide CPU Purchaser Class Members for damages in an amount to be proven at trial.

B. Claims Brought in the Alternative on Behalf of the Oregon Class

COUNT NINE
Unjust Enrichment under Oregon Law
(On Behalf of the Oregon Class)

443. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

444. Plaintiff Cordova brings this Count, in the alternative to the nationwide claims, on her own behalf and on behalf of the Oregon Class.

445. This cause of action is pleaded in the alternative to the legal claims asserted.

446. Plaintiff Cordova and the Oregon Class Members lack an adequate remedy at law for their claims, as specifically set forth later in this Complaint.

447. Intel's conduct is unjust and requires restitution. Specifically, Intel received hundreds of millions—if not billions—of dollars in revenue from sale of the Affected CPUs.

448. This revenue was a benefit conferred upon Intel by Plaintiff Cordova and the Oregon Class Members.

449. Intel was unjustly enriched through financial benefits conferred upon it by Plaintiff Cordova and the Oregon Class Members in the form of the amounts paid to Intel for the Affected CPUs as a result of Plaintiff Cordova and the Oregon Class Members purchase of computers incorporating Affected CPUs.

450. Intel knew and understood that it would and did receive a financial benefit, and voluntarily accepted the same, from Plaintiff Cordova and the Oregon Class Members when they elected to purchase computers with Affected CPUs.

451. By selecting a computer with the Affected CPUs and purchasing it at a premium price, Plaintiff Cordova and the Oregon Class Members reasonably expected that the Affected CPUs would have the performance, security, and quality promoted by Intel, and be designed and manufactured with reasonable care.

452. Instead, not only did the Affected CPUs fall short of such expectations and performance/security standards, they injured and damaged Plaintiff Cordova and the Oregon Class Members' computers by interfering with their operation. The Affected CPUs also made Plaintiff Cordova

and Oregon Class Members' computers less secure. Intel was enriched, while at the same time, Plaintiff Cordova and the Oregon Class Members experienced a diminution of value to their computers.

453. Therefore, because Intel will be unjustly enriched if it is allowed to retain the revenues obtained through its unlawful conduct, Plaintiff Cordova and the Oregon Class Members are entitled to recover the amount by which Intel was unjustly enriched at their expense.

454. Accordingly, Plaintiff Cordova and the Oregon Class Members seek damages against Intel in the amounts by which Intel has been unjustly enriched at Plaintiff Cordova and the Oregon Class Members expense, and such other relief as this Court deems just and proper.

COUNT TEN
Oregon Unlawful Trade Practices Act
Or. Rev. Stat. §§ 646.605, *et seq.*
(On Behalf of the Oregon Class)

455. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

456. Plaintiff Cordova brings this cause of action on her own behalf and on behalf of the Oregon Class Members against Intel pursuant to the Oregon Unlawful Trade Practices Act, Or. Rev. Stat. §§ 646.605, *et seq*.

457. Intel is a person within the meaning of Or. Rev. Stat. § 605(4).

458. When incorporated into computers, the Affected CPUs, including those purchased in computers by Plaintiff Cordova and the Oregon Class Members, are "goods" obtained primarily for personal family or household purposes within the meaning of Or. Rev. Stat. § 646.605(6).

459. The Oregon Unfair Trade Practices Act ("Oregon UTPA") prohibits a person from, in the course of the person's business, doing any of the following: "(e) Represent[ing] that . . . goods . . . have . . . characteristics . . . uses, benefits, . . . or qualities that they do not have; . . . (g) Represent[ing] that . . . goods . . . are of a particular standard [or] quality . . . if they are of another; . . . (i) Advertis[ing] . . . goods or services with intent not to provide them as advertised; . . . and (u) engag[ing] in any other unfair or deceptive conduct in trade or commerce." Or. Rev. Stat. § 646.608(1).

460. In the course of its business, Intel violated the Oregon Unfair Trade Practices Act ("Oregon UTPA") and engaged in deceptive acts or practices concerning the Affected CPUs because it misrepresented and omitted material facts concerning the Affected CPUs, including that the CPUs were uniquely vulnerable based on design defects known to Intel.

461. By failing to disclose material facts concerning the Affected CPUs, Intel engaged in unfair and deceptive business practices in violation of the Oregon UTPA.

462. The true nature of the Affected CPUs would be material to a reasonable consumer, such as Plaintiff Cordova and the Oregon Class Members.

463. Intel's deceptive acts and practices described in this Complaint concerning the Affected CPUs were likely to deceive or mislead a reasonable consumer acting reasonably under the circumstances, such as Plaintiff Cordova and the Oregon Class Members, and did in fact deceive and mislead Plaintiff Cordova and the Oregon Class Members.

464. Intel failed to disclose material information about the Affected CPUs, which Intel possessed and of which consumers, like Plaintiff Cordova and the Oregon Class Members, were unaware. Intel's failure to disclose this material information about the Affected CPUs was likely to deceive or mislead a reasonable consumer acting reasonably under the circumstances, such as Plaintiff Cordova and the Oregon Class Members, and did in fact deceive and mislead Plaintiff Cordova and the Oregon Class Members.

465. Plaintiff Cordova and the Oregon Class Members could not have discovered Intel's deception until shortly before this class action was commenced.

466. Intel knew about the defects in its Affected CPUs.

467. Intel owed Plaintiff Cordova and the Oregon Class Members a duty to disclose that the Affected CPUs were defective because:

i. Intel possessed exclusive knowledge about the design of the Affected CPUs and the defective nature of its speculative execution, branch prediction, and out-of-order execution systems; and

ii. Omitted the foregoing from Plaintiff Cordova and the Oregon Class Members.

468. Intel's deceptive practices alleged in this Complaint directly and proximately caused actual damages and ascertainable monetary loss to Plaintiff Cordova and the Oregon Class Members. Because Intel omitted information about the Affected CPUs, Plaintiff Cordova and the Oregon Class Members were deprived of the benefit of their bargain since the CPUs (and computers incorporating them) were worth less than they would have been if they did not suffer from Intel's design defect in their branch prediction, speculative execution, and out-of-order execution systems.

469. Intel's violations of the Oregon UTPA present a continued risk to Plaintiff Cordova and the Oregon Class Members, and to the public. In particular and as alleged in this Complaint, Intel has yet to provide an adequate and timely fix for its defective CPUs. Intel's purported software "fix" or "mitigation" causes a significant diminution in CPU performance, as described in this Complaint.

470. Plaintiff Cordova and the Oregon Class Members are entitled to recover the greater of actual damages or $200 under Or. Rev. Stat. § 646.638(1).

C. Claims Brought in the Alternative on Behalf of the Kansas Class

COUNT ELEVEN
Kansas Consumer Protection Act
Kan. Stat. § 50-626(a), *et seq.*
(On Behalf of the Kansas Class)

471. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

472. Plaintiff Waltrip brings this cause of action on her own behalf and on behalf of the Kansas Class against Intel, under the Kansas Consumer Protection Act, Kan. Stat. § 50-626(a).

473. The Kansas Consumer Protection Act ("Kansas CPA") states that "[n]o supplier shall engage in any deceptive act or practice in connection with a consumer transaction." Kan. Stat. § 50-626(a). Deceptive acts or practices include, but are not limited to: "the willful use, in any oral or written representation, of exaggeration, falsehood, inuendo or ambiguity as to a material fact"; "the willful failure to state a material fact, or the willful concealment, suppression or omission of material fact"; and "making false or misleading representations, knowingly or with reason to know, of fact concerning the reason for, existence of or amounts of price reductions." *Id.* § 50-626(b).

474. Plaintiff Waltrip and the Kansas Class Members are "consumers" within the meaning of Kan. Stat. Ann. § 50-624(b).

475. The sale of Affected CPUs to Plaintiff Waltrip and the Kansas Class Members was a "consumer transaction" within the meaning of Kan. Stat. Ann. § 50-624(c).

476. Intel's conduct, as described in this complaint, constitutes "deceptive" practices in violation of the Kansas CPA.

477. Under Kan. Stat. Ann. § 50-634, Plaintiff Waltrip and the Kansas Class Members seek monetary relief against Intel measured as the greater of (a) actual damages in an amount to be determined at trial or (b) statutory damages in the amount of $10,000 for each plaintiff.

478. Plaintiff Waltrip and the Kansas Class Members also seek an order enjoining Intel's unfair, unlawful, and/or deceptive practices; declaratory relief; attorneys' fees; and any other just and proper relief available under Kan. Stat. Ann. § 50-623, *et seq.*

COUNT TWELVE
Unjust Enrichment under Kansas Law
(On Behalf of the Kansas Class)

479. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

480. Plaintiff Waltrip brings this cause of action on her own behalf and on behalf of the Kansas Class against Intel, under Kansas law, based on principles of unjust enrichment.

481. This cause of action is pleaded in the alternative to the legal claims asserted.

482. Plaintiff Waltrip and the Kansas Class Members lack an adequate remedy at law for their claims, as specifically set forth later in this Complaint.

483. Intel's conduct is unjust and requires restitution. Specifically, Intel received hundreds of millions—if not billions—of dollars in revenue from the sale of Affected CPUs.

484. This revenue was a benefit conferred upon Intel by Plaintiff Waltrip and the Kansas Class Members.

485. Intel was unjustly enriched through financial benefits conferred upon it by Plaintiff Waltrip and the Kansas Class Members, in the form of the amounts paid to Intel for Affected CPUs.

486. Intel knew and understood that it would and did receive a financial benefit, and voluntarily accepted the same, from Plaintiff Waltrip and the Kansas Class Members when they elected to purchase Affected CPUs.

487. By selecting Affected CPUs and purchasing them at a premium price, Plaintiff Waltrip and the Kansas Class Members reasonably expected that the affected Intel CPUs would have the performance, security, and quality promoted by Intel, and be designed and manufactured with reasonable care.

488. Instead, not only did the Affected CPUs fall short of such expectations and performance/security standards, they injured and damaged Plaintiff Waltrip and the Kansas Class Members' computers by interfering with their operation. The Affected CPUs also made Plaintiff Waltrip and the Kansas Class Members' computers less secure. Intel was enriched, while at the same time, Plaintiff Waltrip and the Kansas Class Members experienced a diminution of value to their computers.

489. Therefore, because Intel will be unjustly enriched if it is allowed to retain the revenues obtained through its unlawful conduct, Plaintiff Waltrip and the Kansas Class Members are entitled to recover the amount by which Intel was unjustly enriched at their expense.

490. Accordingly, Plaintiff Waltrip, on behalf of herself and each Kansas Class member, seeks damages against Intel in the amounts by which Intel has been unjustly enriched at Plaintiff Waltrip and the Kansas Class Members' expense, and such other relief as this Court deems just and proper.

COUNT THIRTEEN
Breach of Implied Warranty of Merchantability Under Kansas Law
Kan. Stat. Ann. § 84-2-314
(On Behalf of the Kansas Class)

491. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

492. Plaintiff Waltrip brings this cause of action on her own behalf and on behalf of the Kansas Class against Intel, under Kansas law.

493. Intel is and was at all relevant times a merchant, including with respect to the Affected CPUs.

494. A warranty that the Affected CPUs were in merchantable condition was implied by law for the subject transactions.

495. Intel marketed the Affected CPUs as having high quality, speed, performance, and security, that would function, at least, as reasonably expected by consumers and in accordance with industry standards. Intel's representations formed the basis of the bargain in Plaintiff Waltrip and the Kansas Class Members' decisions to purchase the Affected CPUs.

496. Plaintiff Waltrip and the other Kansas Class Members purchased the Affected CPUs from Intel, or through retailers or resellers. At all relevant times, Intel was the manufacturer, distributor, warrantor, and/or seller of the Affected CPUs.

497. Intel knew or had reason to know of the specific use for which the Affected CPUs were purchased.

498. Because of the defect discussed in this Complaint, the Affected CPUs were not in merchantable condition when sold and are not fit for the ordinary purpose of such CPUs.

499. Intel knew about the defect in the Affected CPUs, allowing Intel to cure its breach of warranty if it chose.

500. In its capacity as warrantor, Intel had knowledge of the inherently defective nature of the defectively designed CPUs. Any effort by Intel to limit the implied warranties in a manner that would exclude coverage of the Affected CPUs is unconscionable, and any such effort to disclaim or otherwise limit such liability is null and void.

501. Any limitations Intel might seek to impose on its warranties are procedurally unconscionable. There was unequal bargaining power between Intel on the one hand and Plaintiff Waltrip and the Kansas Class Members on the other, as at the time of purchase, Plaintiff Waltrip and the Kansas Class Members had no other viable options for purchasing warranty coverage other than from Intel, and there were no alternative sources of comparable CPUs that Plaintiff Waltrip and the Kansas Class Members could have purchased free of the unconscionable terms contained in Intel's warranties. In addition, the terms of any applicable Intel express warranties were not displayed or conspicuous during the process of purchasing the Intel CPUs. The time limits contained in Intel's warranty periods were also unconscionable and inadequate to protect Plaintiff Waltrip and the Kansas Class Members. Among other

things, Plaintiff Waltrip and the Kansas Class Members had no meaningful choice in determining these time limitations, the terms of which unreasonably favored Intel.

502. Any limitations Intel might seek to impose on its warranties are also substantively unconscionable. Intel knew that the Affected CPUs would result in the effects set forth in this Complaint. Moreover, Intel knew that the Affected CPUs would result in the effects set forth in this Complaint after the warranty purportedly expired. Intel failed to disclose the defect, or the effects stemming from it, to Plaintiff Waltrip and the Kansas Class Members. Thus, Intel's enforcement of the durational limitations on those warranties is harsh and shocks the conscience.

503. A claim for breach of implied warranty under Kansas law does not require contractual privity between the plaintiff and the defendant. In the alternative, to the extent Plaintiff Waltrip or a Kansas Class Member is not in privity with Intel, privity of contract is not required here because Plaintiff Waltrip and the Kansas Class Members are intended third-party beneficiaries of contracts between Intel and retailers/resellers, including (1) the written distribution and supply agreements between Intel and its authorized resellers, and of the implied warranties that attach to those contracts; and (2) any express warranties provided by Intel. Intel's retailers and resellers have no rights under the warranty agreements provided with the Affected CPUs; the warranty agreements were designed for and intended to benefit consumers. Plaintiff Waltrip and the Kansas Class Members are also the intended beneficiaries of retailer and reseller warranties.

504. Plaintiff Waltrip and the Kansas Class Members have complied with all obligations under the warranty, or otherwise have been excused from performance of said obligations as a result of Intel's conduct described in this Complaint. Affording Intel a reasonable opportunity to cure the breach of written warranties would be unnecessary and futile.

505. Accordingly, Intel is liable to Plaintiff Waltrip and the Kansas Class Members for damages in an amount to be proven at trial.

D. Claims Brought in the Alternative on Behalf of the Illinois Class

COUNT FOURTEEN
Illinois Consumer Fraud and Deceptive Business Practices Act
815 Ill. St. § 505/1, *et seq.*
(On Behalf of the Illinois Class)

506. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

507. Plaintiff Cameron brings this cause of action on his own behalf and on behalf of the Illinois Class against Intel, under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. St. § 505/1, *et seq*.

508. Intel committed a deceptive act or practice with a consumer transaction, marketing CPUs to Plaintiff Cameron and the Illinois Class Members.

509. Intel made representations knowingly or with reason to know that the CPUs: (1) have characteristics, uses, benefits or quantities that they do not have; (2) are of particular standard, quality, grade, style or model; and/or (3) that the use, benefit or characteristic of the CPUs have been proven or otherwise substantiated, including that they contained (a) security features, including features which reduce the risk and effect of attacks based on speculative execution; (b) sufficient, expected, and promised processing speeds; and/or (c) that Intel had repaired the defects which caused Spectre and Meltdown.

510. However, Intel intentionally made representations that it corrected the vulnerabilities that led to Spectre and Meltdown, yet—due to defects Intel was aware of—did not sell Affected CPUs that conformed to the representations and promises in Intel's publicly disseminated advertisements.

511. Intel unjustly received and retained benefits from Plaintiff Cameron and the Illinois Class.

512. It is inequitable and unconscionable for Intel to retain these benefits.

513. Because Intel wrongfully concealed its misconduct, Plaintiff Cameron and the Illinois Class Members were not aware of these material facts concerning the Affected CPUs. Plaintiff Cameron and the Illinois Class Members did not benefit from Intel's misconduct.

514. As a result of Intel's misconduct, Plaintiff Cameron and the Illinois Class Members were aggrieved in that they suffered an injury-in-fact and lost money and/or property in an amount to be proven at trial. Plaintiff Cameron and the Illinois Class Members also seek injunctive relief as deemed

appropriate by the Court, including but not limited to a prohibition on falsely advertising Intel CPUs of similar design until the design defect is corrected.

COUNT FIFTEEN
Unjust Enrichment Under Illinois Law
(On Behalf of the Illinois Class)

515. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

516. Plaintiff Cameron brings this cause of action, in the alternative to the nationwide claims, on his own behalf and on behalf of the Illinois Class against Intel, under Illinois law, based on principles of unjust enrichment.

517. This cause of action is pleaded in the alternative to the legal claims asserted.

518. Plaintiff Cameron and the Illinois Class Members lack an adequate remedy at law for their claims, as specifically set forth later in this Complaint.

519. Intel's conduct is unjust and requires restitution. Specifically, Intel received hundreds of millions—if not billions—of dollars in revenue from the sale of Affected CPUs.

520. This revenue was a benefit conferred upon Intel by Plaintiff Cameron and the Illinois Class Members.

521. Intel was unjustly enriched through financial benefits conferred upon it by Plaintiff Cameron and the Illinois Class Members, in the form of the amounts paid to Intel for Affected CPUs.

522. Intel knew and understood that it would and did receive a financial benefit, and voluntarily accepted the same, from Plaintiff Cameron and the Illinois Class Members when they elected to purchase Affected CPUs.

523. By selecting Affected CPUs and purchasing them at a premium price, Plaintiff Cameron and the Illinois Class Members reasonably expected that the Affected CPUs would have the performance, security, and quality promoted by Intel, and be designed and manufactured with reasonable care. Instead, not only did the Affected CPUs fall short of such expectations and performance/security standards, they injured and damaged Plaintiff Cameron and the Illinois Class Members' computers by interfering with their operation. The Affected CPUs also made Plaintiff Cameron and the Illinois Class Members'

computers less secure. Intel was enriched, while at the same time, Plaintiff Cameron and the Illinois Class Members experienced a diminution of value to their computers.

524. Therefore, because Intel will be unjustly enriched if it is allowed to retain the revenues obtained through its unlawful conduct, Plaintiff Cameron and the Illinois Class Members are entitled to recover the amount by which Intel was unjustly enriched at their expense.

525. Accordingly, Plaintiff Cameron, on behalf of himself and each Illinois Class member, seeks damages against Intel in the amounts by which Intel has been unjustly enriched at Plaintiff Cameron and the Illinois Class Members' expense, and such other relief as this Court deems just and proper.

COUNT SIXTEEN
Breach of Implied Warranty Under Illinois Law
(On Behalf of the Illinois Class)

526. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

527. Plaintiff Cameron brings this cause of action on his own behalf and on behalf of the Illinois Class against Intel, under Illinois law.

528. Intel is and was at all relevant times a merchant, including with respect to the Affected CPUs.

529. A warranty that the Affected CPUs were in merchantable condition was implied by law for the subject transactions.

530. Intel marketed the Affected CPUs as having high quality, speed, performance, and security, that would function, at least, as reasonably expected by consumers and in accordance with industry standards. Intel's representations formed the basis of the bargain in Plaintiff Cameron and the Illinois Class Members' decisions to purchase the Affected CPUs.

531. Plaintiff Cameron and the other Illinois Class Members purchased the Affected CPUs from Intel, or through retailers or resellers. At all relevant times, Intel was the manufacturer, distributor, warrantor, and/or seller of the Affected CPUs.

532. Intel knew or had reason to know of the specific use for which the Affected CPUs were purchased.

533. Because of the defect discussed in this Complaint, the Affected CPUs were not in merchantable condition when sold and are not fit for the ordinary purpose of such CPUs.

534. Intel knew about the defect in the Affected CPUs, allowing Intel to cure its breach of warranty if it chose.

535. In its capacity as warrantor, Intel had knowledge of the inherently defective nature of the defectively designed Affected CPUs. Any effort by Intel to limit the implied warranties in a manner that would exclude coverage of the Affected CPUs is unconscionable, and any such effort to disclaim or otherwise limit such liability is null and void.

536. Any limitations Intel might seek to impose on its warranties are procedurally unconscionable. There was unequal bargaining power between Intel on the one hand and Plaintiff Cameron and the Illinois Class Members on the other, as at the time of purchase, Plaintiff Cameron and the Illinois Class Members had no other viable options for purchasing warranty coverage other than from Intel, and there were no alternative sources of comparable CPUs that Plaintiff Cameron and the Illinois Class Members could have purchased free of the unconscionable terms contained in Intel's warranties. In addition, the terms of any applicable Intel express warranties were not displayed or conspicuous during the process of purchasing the Intel CPUs. The time limits contained in Intel's warranty periods were also unconscionable and inadequate to protect Plaintiff Cameron and the Illinois Class Members. Among other things, Plaintiff Cameron and the Illinois Class Members had no meaningful choice in determining these time limitations, the terms of which unreasonably favored Intel.

537. Any limitations Intel might seek to impose on its warranties are also substantively unconscionable. Intel knew that the Affected CPUs would result in the effects set forth in this Complaint. Moreover, Intel knew that the Affected CPUs would result in the effects set forth in this Complaint after the warranty purportedly expired. Intel failed to disclose the defect, or the effects stemming from it, to Plaintiff Cameron and the Illinois Class Members. Thus, Intel's enforcement of the durational limitations on those warranties would be harsh and shock the conscience.

538. A claim for breach of implied warranty under Illinois law does not require contractual privity between the plaintiff and the defendant. In the alternative, to the extent Plaintiff Cameron or an Illinois Class Member is not in privity with Intel, privity of contract is not required here because Plaintiff

Cameron and the Illinois Class Members are intended third-party beneficiaries of contracts between Intel and retailers/resellers, including (1) the written distribution and supply agreements between Intel and its authorized resellers, and of the implied warranties that attach to those contracts; and (2) any express warranties provided by Intel. Intel's retailers and resellers have no rights under the warranty agreements provided with the Affected CPUs; the warranty agreements were designed for and intended to benefit consumers. Plaintiff Cameron and the Illinois Class Members are also the intended beneficiaries of retailer and reseller warranties.

539. Plaintiff Cameron and the Illinois Class Members have complied with all obligations under Intel's warranty, or otherwise have been excused from performance of said obligations as a result of Intel's conduct described in this Complaint. Affording Intel a reasonable opportunity to cure the breach of written warranties would be unnecessary and futile.

540. Accordingly, Intel is liable to Plaintiff Cameron and the Illinois Class Members for damages in an amount to be proven at trial.

E. Claims Brought in the Alternative on Behalf of the Minnesota Class

COUNT SEVENTEEN
Minnesota Prevention of Consumer Fraud Act
Minn. Stat. §§ 325F.68, et seq. and Minn. Stat. § 8.31, SUBD. 3A
(On Behalf of the Minnesota Class)

541. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

542. Plaintiff Worley brings this cause of action, in the alternative to the nationwide claims, on his own behalf and on behalf of the Minnesota Class against Intel.

543. Computers incorporating Affected CPUs constitute "merchandise" within the meaning of MINN. STAT. § 325F.68(2).

544. The Minnesota Prevention of Consumer Fraud Act (the "Minnesota CFA") prohibits "[t]he act, use or employment by any person of any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby." MINN. STAT § 325F.69(1).

545. In the course of Intel's business, it willfully failed to disclose and actively concealed that the Affected CPUs were defective (despite knowing as much since at least mid-2018), such that normal use of computers incorporating the Affected CPUs would leave Plaintiff Worley and the Minnesota Class Members vulnerable to AVX speculative execution attacks, with mitigation creating a significant diminution in CPU performance. Accordingly, Intel engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentation, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission in connection with the sale of computers incorporating Affected CPUs.

546. In purchasing computers incorporating Affected CPUs, Plaintiff Worley and the Minnesota Class Members were deceived by Intel's failure to disclose that the Affected CPUs were defective.

547. Plaintiff Worley and the Minnesota Class Members did not and could not have known that the Affected CPUs were defective, including, among other reasons, because Intel did not disclose the existence of the Affected CPUs' AVX instruction buffers to the public. The defective aspects of the Affected CPUs are internal to the Affected CPUs, and Plaintiff Worley and the Minnesota Class Members were not aware of the defective nature of the Affected CPUs prior to their purchase of computers incorporating them.

548. Intel's actions as set forth in this Complaint occurred in the conduct of trade or commerce.

549. Intel's deception, fraud, misrepresentation, concealment, suppression, or omission of material facts was likely to, and did in fact, deceive reasonable consumers, including Plaintiff Worley and the Minnesota Class Members.

550. Intel intentionally and knowingly misrepresented material facts regarding the Affected CPUs, with intent to mislead Plaintiff Worley and the Minnesota Class Members.

551. Intel knew or should have known that its conduct violated the Minnesota law regarding consumer fraud and unfair or deceptive acts in trade or commerce.

552. Intel owed Plaintiff Worley and the Minnesota Class Members a duty to disclose the truth about the Affected CPUs because Intel:

i. Possessed exclusive knowledge of the design of the Affected CPUs, including that the branch prediction, speculative execution, and out-of-order execution systems were defective, including because speculative execution left exploitable side effects in CPU cache and buffers; and

ii. Intentionally concealed the foregoing from Plaintiff Worley and the Minnesota Class Members.

553. Intel's conduct proximately caused injuries to Plaintiff Worley and the Minnesota Class Members.

554. Plaintiff Worley and the Minnesota Class Members were injured and suffered ascertainable loss, injury in fact, and/or actual damage as a proximate result of Intel's conduct. Plaintiff Worley and the Minnesota Class Members overpaid for computers incorporating Affected CPUs and did not receive the benefit of their bargain, and their computers incorporating Affected CPUs have suffered a diminution in value. These injuries are the direct and natural consequence of Intel's fraudulent omissions.

555. Intel's violations present a continuing risk to Plaintiff Worley and the Minnesota Class Members as well as to the general public. Intel's unlawful acts and practices complained of in this Complaint affect the public interest as Intel's actions offend public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

556. Pursuant to MINN. STAT. § 8.31(3a), Plaintiff Worley and the Minnesota Class Members seek actual damages, attorneys' fees, and any other relief properly available under the Minnesota CFA.

557. Plaintiff Worley and the Minnesota Class Members also seek punitive damages under MINN STAT. § 549.20(1)(a), given the clear and convincing evidence that Intel's acts show deliberate disregard for the rights of others.

COUNT EIGHTEEN
Minnesota Deceptive Trade Practices Act
Minn. Stat. §§ 325D.9, *et seq.*
(On Behalf of the Minnesota Class)

558. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

559. Plaintiff Worley brings this cause of action, in the alternative to the nationwide claims, on his own behalf and on behalf of the Minnesota Class against Intel.

560. The Minnesota Deceptive Trade Practices Act (the "Minnesota DTPA") prohibits deceptive trade practices, which include "in connection with the sale of merchandise, knowingly misrepresent[ing], directly or indirectly, the true quality, ingredients or origin of such merchandise." MINN. STAT. § 325D.13. "Any person damaged or who is threatened with loss, damage, or injury by reason of a violation of sections 325D.09 to 325D.16 shall be entitled to sue for and have injunctive relief in any court of competent jurisdiction against any damage or threatened loss or injury by reason of a violation of sections 325D.09 to 325D.16 and for the amount of actual damages, if any. In order to obtain such injunctive relief, it shall not be necessary to allege or prove that an adequate remedy at law does not exist." MINN. STAT. § 325D.15.

561. Intel's actions as set forth in this Complaint occurred in the conduct of trade or commerce, and in connection with the sale of merchandise.

562. In the course of Intel's business, it willfully failed to disclose and actively concealed that the Affected CPUs were defective (despite knowing as much since at least mid-2018), such that normal use of computers incorporating Affected CPUs would leave Plaintiff Worley and the Minnesota Class Members vulnerable to AVX speculation execution attacks, with mitigation creating a significant diminution in CPU performance. Accordingly, Intel engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentation, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission in connection with the sale of the Affected CPUs.

563. In purchasing computers incorporating Affected CPUs, Plaintiff Worley and the Minnesota Class Members were deceived by Intel's failure to disclose that Affected CPUs were defective.

564. Plaintiff Worley and the Minnesota Class Members did not and could not have known that the Affected CPUs were defective, including, among other reasons, because Intel did not disclose the existence of the Affected CPUs' AVX instruction buffers to the public. The defective aspects of the Affected CPUs are internal to the Affected CPUs, and Plaintiff Worley and the Minnesota Class Members

were not aware of the defective nature of the Affected CPUs prior to their purchase of computers incorporating them.

565. Intel's actions as set forth in this Complaint occurred in the conduct of trade or commerce.

566. Intel's deception, fraud, misrepresentation, concealment, suppression, or omission of material facts was likely to, and did in fact, deceive reasonable consumers, including Plaintiff Worley and the Minnesota Class Members.

567. Intel intentionally and knowingly misrepresented material facts regarding the Affected CPUs with intent to mislead Plaintiff Worley and the Minnesota Class Members.

568. Intel knew or should have known that its conduct violated Minnesota law regarding unfair or deceptive acts in trade or commerce.

569. Intel owed Plaintiff Worley and the Minnesota Class Members a duty to disclose the truth about the Affected CPUs because Intel:

i. Possessed exclusive knowledge of the design of the Affected CPUs, including that the branch prediction, speculative execution, and out-of-order execution systems were defective, including because speculative execution left exploitable side effects in CPU cache and buffers; and

ii. Intentionally concealed the foregoing from Plaintiff Worley and the Minnesota Class Members.

570. Intel's conduct proximately caused injuries to Plaintiff Worley and the Minnesota Class Members.

571. Plaintiff Worley and the Minnesota Class Members were injured and suffered ascertainable loss, injury in fact, and/or actual damage as a proximate result of Intel's conduct. Plaintiff Worley and the Minnesota Class Members overpaid for computers incorporating Affected CPUs and did not receive the benefit of their bargain, and their computers have suffered a diminution in value due to the presence of Affected CPUs. These injuries are direct and natural consequence of Intel's deceptive trade practices, including its omissions in connection with sale of computers incorporating Affected CPUs.

572. Intel's violations present a continuing risk to Plaintiff Worley and the Minnesota Class Members as well as to the general public. Intel's unlawful acts and practices complained of in this Complaint affect the public interest, as Intel's actions offend public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

573. Pursuant to MINN STAT. § 325D.14, Plaintiff Worley and the Minnesota Class Members seek injunctive relief, actual damages, attorneys' fees, and any other just and proper relief available under the Minnesota DTPA.

COUNT NINETEEN
Unjust Enrichment under Minnesota Law
(On Behalf of the Minnesota Class)

574. Plaintiffs incorporate by reference all preceding and succeeding allegations as though fully set forth in this Count.

575. Plaintiff Worley brings this cause of action, in the alternative to the nationwide claims, on his own behalf and on behalf of the Minnesota Class against Intel under Minnesota law.

576. This cause of action is pleaded in the alternative to the legal claims asserted.

577. Plaintiff Worley and the Minnesota Class Members lack an adequate remedy at law for their claim, as specifically set forth later in this Complaint.

578. Intel's conduct is unjust and requires restitution. Specifically, Intel received hundreds of millions—if not billions—of dollars in revenue from the sale of the Affected CPUs, including for use in computers incorporating them. This revenue was a benefit conferred upon Intel by Plaintiff Worley and the Minnesota Class Members.

579. Intel was unjustly enriched through financial benefits conferred upon it by Plaintiff Worley and the Minnesota Class Members in the form of the amounts paid to Intel for the Affected CPUs, which were sold by Intel for incorporation into computers purchased by Plaintiff Worley and the Minnesota Class Members.

580. Intel knew and understood that it would and did receive a financial benefit, and voluntarily accepted the same, from Plaintiff Worley and the Minnesota Class Members when they elected to purchase computers with the Affected CPUs.

581. By selecting a computer with an Affected CPU and purchasing it at a premium price, Plaintiff Worley and the Minnesota Class Members reasonably expected that the Affected CPUs would have the performance, security, and quality promoted by Intel, and be designed and manufactured with reasonable care.

582. Instead, not only did the Affected CPUs fall short of such expectations and performance/security standards, they injured and damaged Plaintiff Worley and the Minnesota Class Members' computers by interfering with their operation. The Affected CPUs also made Plaintiff Worley and the Minnesota Class Members' computers less secure. Intel was enriched, while at the same time, Plaintiff Worley and the Minnesota Class Members experienced a diminution of value to their computers.

583. Therefore, because Intel will be unjustly enriched if it is allowed to retain the revenues obtained through its unlawful conduct, Plaintiff Worley and the Minnesota Class Members are entitled to recover the amount by which Intel was unjustly enriched at their expense.

584. Accordingly, Plaintiff Worley and the Minnesota Class Members seek damages against Intel in the amounts by which Intel has been unjustly enriched at Plaintiff Worley and the Minnesota Class Members' expense, and such other relief as this Court deems just and proper.

LACK OF ADEQUATE REMEDIES AT LAW

585. Plaintiffs lack an adequate remedy at law for their claims to the extent they seek relief that is equitable in nature.

586. ***Injunctive relief.*** Plaintiffs seek injunctive relief to enjoin Intel from continuing its campaign of false and misleading statements and omissions concerning its defective processors and its sale of defective processors and systems.

587. Intel knows that an essential part of its processors is defective. Intel has sold, and continues to sell, its processors while omitting that these processors are defectively designed and suffer from the crippling effects of that defective design.

588. An injunction is required to prevent the continued sale of Intel's processors and systems. Legal remedies, such as damages, cannot prevent such continued harm.

589. In addition, absent an injunction, Plaintiffs, who build their own computers and would like to buy Intel processors, and Plaintiffs who want to buy computers with Intel processors in the future, can

no longer rely on Intel's statements about its processors and computers incorporating them, including on Intel's website and in Intel marketing material distributed to third parties like Amazon.com, Newegg.com, and MicroCenter, or displayed on OEM websites, such as hp.com or dell.com. Thus, absent an injunction, Plaintiffs will abstain from buying Intel CPUs or computers with Intel CPUs.

590. Plaintiffs also seek an injunction requiring Intel to implement a repair or replacment program. At present, Intel's mitigation cripples performance of the Affected CPUs. For those who do not update through Windows Update or thorugh their OEM's update systems, a firmware update is required. Firmware updates, however, are risky and complicated. If a firmware update fails, it may result in damage to hardware or loss of data. Moreover, those who have updated are left with CPUs with impaired performance.

591. Any remediation by Intel of its design defect will therefore require a program to send Affected CPUs to Intel for direct repair or replacement. Indeed, Intel sells newer generation CPUs that are not affected by Downfall and do not require performance-crippling mitigation, which it can use to replace the Affected CPUs.

592. Absent such an option, Plaintiffs and the Class Members cannot obtain complete relief. Such relief is purely equitable in nature and unavailable at law.

593. Indeed, damages available at law would still leave members of the class with defective processors.

594. ***Alternative Pleading.*** Plaintiffs also plead their equitable claims in the alternative to their legal claims. Thus, for example, any equitable restitution available under the unjust enrichment and quasi-contract claims asserted in thie Complaint could not possibly duplicate Plaintiffs' legal claims, as Plaintiffs seek to press those equitable claims ***only*** if they do not prevail on claims providing legal remedies.

595. This alternative pleading is necessary to ensure that Plaintiffs retain equitable remedies if, for example, claims providing legal remedies are dismissed or judgment is rendered upon them prior to trial.

596. Moreover, if Plaintiffs prevail at trial on claims providing legal remedies, Plaintiffs' claims for equitable restitution will necessarily fail (and would not be asserted) to the extent co-extensive with monetary damages obtained at law.

597. ***Damages to Plaintiffs' Computers.*** Plaintiffs also plead equitable claims, including unjust enrichment and quasi-contract claims, because they seek redress for harm to their ***computers***, not merely their CPUs.

598. As explained above, Intel's conduct has resulted in (a) the direct diminution in value to Plaintiffs' and Class Members computers; and (b) Intel's capture of market share (and revenue) from AMD and other competitors in excess of what Intel would have had absent its inequitable and/or wrongful conduct.

599. Damage to Plaintiffs' computers will require a measure of monetary compensation beyond what is available at law for injuries relating directly to purchase of Intel's CPUs and systems. Indeed, to adequately compensate Plaintiffs, some non-restitutionary disgorgement of profits is necessary, as compensation for the overpayment for, or diminution in value of, Intel's CPUs will not compensate Plaintiffs for harm to their computers, including the loss of the full use and benefit of their computers as a result of Intel's conduct.

600. Plaintiffs thus require equitable relief to obtain disgorgement of Intel's ill-gotten profits in order to provide an adequate remedy for harm to their computers.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of members of the Proposed Classes, respectfully request that the Court enter judgment in their favor and against Intel, as follows:

A. Certification of the proposed Nationwide Classes or, alternatively, certification of the proposed State Classes, including appointment of Plaintiffs as Class Representatives and Plaintiffs' counsel as Class Counsel;

B. Injunctive relief in the form of a recall or free replacement program;

C. Injunctive relief in the form of a buyback;

D. Injunctive relief in the form of a prohibition on falsely advertising the Affected CPUs or Intel CPUs of similar design until the design defect is corrected;

E. An order temporarily and permanently enjoining Intel from continuing the unlawful, deceptive and unfair business practices alleged in this Complaint;

F. Restitution, including at the election of all Class Members, recovery of the purchase price of their Affected CPUs, and/or the overpayment for their Affected CPUs;

G. Damages for injury to Plaintiffs' and Class Members' computers;

H. Damages (including punitive damages), costs, and disgorgement in an amount to be determined at trial;

I. An order requiring Intel to pay both pre- and post-judgment interest on any amounts awarded;

J. An award of costs and attorneys' fees; and

K. Such other or further relief as may be appropriate.

JURY DEMAND

Plaintiffs demand a trial by jury on all claims so triable as a matter of right.

Dated: November 8, 2023

Respectfully submitted,

/s/ Brian J. Dunne
Brian J. Dunne (CA 275689)
bdunne@bathaeedunne.com
Edward M. Grauman (*p.h.v. to be sought*)
egrauman@bathaeedunne.com
BATHAEE DUNNE LLP
901 South Mopac Expressway
Barton Oaks Plaza I, Suite 300
Austin, TX 78746
Tel.: (213) 462-2772

/s/ Yavar Bathaee
Yavar Bathaee (CA 282388)
yavar@bathaeedunne.com
Andrew C. Wolinsky (CA 345965)
awolinsky@bathaeedunne.com
BATHAEE DUNNE LLP
445 Park Avenue, 9th Floor
New York, NY 10022
Tel.: (332) 322-8835

Attorneys for Plaintiffs and the Proposed Classes