KIRBY McINERNEY LLP
Robert J. Gralewski, Jr. (CSB# 196410)
Fatima G. Brizuela
600 B Street, Suite 1900
San Diego, CA 92101
Telephone: (619) 398-4340
bgralewski@kmllp.com
fbrizuela@kmllp.com

Attorneys for Plaintiff

[Additional counsel listed on signature page.]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

ARTESIA GENERAL HOSPITAL, a New Mexico not-for-profit corporation, individually and on behalf of all others similarly situated,

Plaintiff,

v.

INTEL CORPORATION,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Judge:

INTRODUCTION

1. General Hospital ("AGH" or "Plaintiff"), a not-for-profit health care provider in Artesia, New Mexico, brings this class action complaint against Intel Corporation ("Intel" or "Defendant"), to recover substantial damages resulting from profound, fundamental, and incurable security defects in central processing units ("CPUs") designed, manufactured and marketed by Intel that render patients' medical records and other protected information vulnerable to hacking.

2. Intel CPUs provide the "brains" of the majority of servers and personal computers ("PCs"), along with those of other devices, utilized in the health care and other industries. In January 2018, Intel disclosed that virtually every CPU it had manufactured and sold during the past decade or more suffered from a number of security vulnerabilities, known as "Meltdown" and "Spectre." While distinct, these vulnerabilities have put at risk sensitive data such as user names, passwords and encryption keys. The flaws in Defendant's CPUs were the result of Intel's decision to prioritize performance over security.

3. Health care providers such as AGH are obligated by federal law under the Health Insurance Portability and Accountability Act ("HIPAA") and the American Recovery and Reinvestment Act ("ARRA") to protect their patients' medical records and to make those records available to them in a secure manner via Internet-connected servers. AGH relied upon Intel's representations that its CPUs were secure and fit for use in servers, PCs and other devices that stored or accessed sensitive patient medical records.

4. As a result of the defects disclosed by Intel, and in order to comply with its privacy obligations, AGH has been and will be required to (a) undertake temporary measures to mitigate the security risks posed by "Meltdown" and "Spectre," which have the side effect of slowing the performance of its computing resources; (b) incur additional costs monitoring its computing resources for security breaches; and (c) replace its computing resources on an accelerated schedule and at significant expense with CPUs that, when available, are not susceptible to these vulnerabilities.

5. The enormous costs in responding to the "Meltdown" and "Spectre" vulnerabilities are being borne by thousands of entities throughout the country that, like AGH, are entrusted with

sensitive third-party data. Plaintiff brings this action individually and on behalf of a Class of all similarly situated entities in the United States that are subject to HIPAA or other federal laws or regulations imposing standards of care with respect to the protection of third-party information and that purchased servers, PCs or other devices with the defective Intel CPUs.

PARTIES

A. Plaintiff

6. Plaintiff AGH is a non-profit health care provider organized under the laws of the State of New Mexico which primarily does business in Artesia, New Mexico. Plaintiff's mission is to be a provider of high quality patient-focused health care that is readily accessible, cost effective and meets the needs of the citizens of the Southeastern New Mexico communities it serves. To that end, Plaintiff spends more than $3 million annually on information technology ("IT") capital and operations. AGH was named by *Hospitals & Health Networks* among "Health Care's Most Wired" in 2017.

7. Plaintiff has purchased servers, PCs and other devices with Intel CPUs that include the vulnerabilities described throughout this Complaint.

B. Defendant

8. Defendant Intel is a Delaware corporation with its principal place of business in Santa Clara, California. Intel designs, manufactures and markets computer products, including CPUs, worldwide.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this controversy pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because (a) the proposed Class, defined below, consists of more than one hundred members; (b) the parties are minimally diverse, as members of the proposed Class are citizens of states different than Intel's home state; and (c) the aggregate amount in controversy far exceeds $5 million, exclusive of interests and costs.

10. This Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367.

11. This Court has personal jurisdiction over both parties. AGH submits to the Court's jurisdiction. Intel's headquarters and principal place of business are located within this District.

12. Venue is proper in this District under 28 U.S.C.§1391 because Intel maintains its principal place of business within the District and a substantial part of the events giving rise to Plaintiff's claims occurred here.

INTRADISTRICT ASSIGNMENT

13. Assignment to the San Jose Division of this District is proper under Local Rule 3-2(c)-(e) because a substantial part of the acts or omissions underlying Plaintiff's claims occurred in Santa Clara County.

FACTUAL BACKGROUND

I. Federal Law Obligates Health Care Providers to Create, Maintain and Protect Patient Medical Records.

14. Health care providers such as AGH are subject to obligations under the ARRA, HIPAA, and attendant regulations and other bodies of law, which impose national standards with respect to the secure storage and handling of confidential patient information.

15. The ARRA requires health care providers like Plaintiff to make "meaningful use" of electronic health records ("EHR") to engage patients and family and to maintain privacy and security of patient health information.

16. HIPAA establishes national standards that require health care providers and their business associates, to develop and follow procedures that ensure the confidentiality and security of protected health information ("PHI"), including electronic PHI ("ePHI"), when it is transferred, received, handled, or shared.

17. Plaintiff and other health care providers are subject to fines imposed by the Office of Civil Rights ("OCR") of the United States Department of Health and Human Services ("HHS") for violations of HIPAA. OCR may impose annual fines up to $1.5 million on a health care provider for violations of the same HIPAA provision.

II. Intel CPUs Utilized by Health Care Providers and Other Class Members Contain Significant Security Flaws that Place Protected Data at Risk.

18. Health care providers like Plaintiff and other firms subject to heightened privacy standards under federal law routinely utilize Intel CPUs in their servers, PCs and other computing devices to generate, analyze and store ePHI, EHR and similar protected information.

19. Intel dominates the markets for CPUs used in servers and PCs, with shares estimated to be in excess of 90% and 80%, respectively, in 2017. Intel markets its widely-used CPUs as being fit to "prevent exposure to malicious code, viruses, cyber espionage, malware, and data theft."

20. Intel clearly understands the importance of security to health care providers and others subject to HIPAA. Intel's web site, for instance, states: "Protection of personal health information is a critical priority. Intel®-based technologies can support the need for compliance with local regulation of health care information such as the HIPAA privacy and security rule." That same web page warned that "[t]he financial impact from security breaches in the United States averaged more than USD 5.2 million per event in 2011."

21. In June 2017, a team of researchers at Google's Project Zero reportedly alerted Intel of a number of security flaws in Intel CPUs that have existed in virtually every CPU manufactured and sold by Defendant during at least the past decade. Google's researchers publicly announced these security flaws in January 2018.

22. Security researchers have publicly detailed three vulnerabilities: one called "Meltdown" and two referred to as "Spectre." These vulnerabilities are "privilege escalation" flaws, meaning that computer code running in less secure user programs (e.g., web browsers, email clients, and media applications) can surreptitiously access secure kernel or other computer memory to gain access to sensitive data such as user names, passwords, and encryption keys.

//

//

//

23. An article in *The New York Times* titled "Researchers Discover Two Major Flaws in the World's Computers," described the vulnerabilities as follows:

> Computer security experts have discovered two major security flaws in the microprocessors inside nearly all of the world's computers.
>
> The two problems, called Meltdown and Spectre, could allow hackers to steal the entire memory contents of computers, including mobile devices, personal computers and servers running in so-called cloud computer networks.

24. The vulnerabilities are the result of Intel's decision to achieve performance at the cost of security. Upon information and belief, Intel was or should have been aware of the security flaws prior to Google's disclosure.

25. "Proof of concept" sample code, which demonstrates how these vulnerabilities could be exploited, has been made available in a variety of programming languages including C++, JavaScript, and C.

B. *Intel's Modern Central Processing Units*

26. User programs are often made up of CPU instructions that are ordered to be processed and executed serially, one after the other, akin to water moving through a single pipeline. Intel's CPUs contain more than one "pipeline" for ordering and executing a user program's instructions. A single-pipeline CPU would take eight cycles to process eight instructions; a CPU with eight pipelines could, under ideal circumstances, process those same eight instructions in one cycle.

27. In order to take advantage of multiple pipelines, Intel's CPUs make "guesses" as to what CPU instructions may be executed after any particular instruction via a process known as "branch prediction." Branch prediction utilizes algorithms to determine what instructions are most likely to be executed after another instruction (the "prime instruction") gathers the predicted instructions and data inputs from memory and speculatively executes those instructions in anticipation of providing the results after execution of the prime instruction.

//

//

28. While Intel's implementation of branch prediction and speculative execution in its CPUs has greatly increased the performance of those processors, its particular design decisions have introduced grave security flaws.

C. *Intel's "Spectre" Design Flaws*

29. The "Spectre" security flaws are integral to the design of Intel CPUs and utilize speculative execution of privileged code. Computer programs generally consist of a series of repetitive and in-order operations. Intel CPUs take advantage of the repetitive nature of computer programs by analyzing patterns of past operations to predict future operations. The CPUs then speculatively gather data from system memory to execute those future operation to quickly provide the result to the underlying program. A malicious program can train the CPU to predict that otherwise protected memory will be relevant to a future operation and make that protected memory available to the malicious program.

30. In the context of PCs, malicious programs such as pretextual advertisements in web browsers can be used to obtain usernames and passwords that provide access to sensitive, valuable, and confidential data, including patient records, financial information, and client files. In addition to being attacked via web advertising, computers are susceptible to these attacks via email, instant messaging, and traditional malware.

31. The "Spectre" threat to cloud-based servers is particularly extreme. Cloud-based virtual server hosting is increasingly common with vendors such as Microsoft, Amazon, IBM, Salesforce.com, SAP, Oracle, Google, ServiceNow, Workday, VMware, and others providing shared server resources directly and indirectly to consumers like Plaintiff AGH. In this circumstance, vendors utilize a single Intel CPU to provide multiple virtual CPUs and servers to customers.

32. A malicious actor could exploit Intel's "Spectre" design flaws by, for example, purchasing a virtual server in the cloud and running a program that permits access to other virtual servers running on the same Intel CPU. Such a malicious server sharing space with servers for hospitals, banks, and law firms could gain complete access to the memory of those virtual servers and, consequently, gain complete access to all of servers' sensitive data.

D. *Intel's "Meltdown" Design Flaw*

33. "Meltdown" is a hardware vulnerability that tricks the CPU into speculatively loading data that has been marked unreadable or "privileged." This flaw potentially allows malicious programs to request protected kernel memory and to access copies of the protected memory.

34. Modern processors perform speculation around memory accesses; Intel's CPUs, however, do so in a particularly aggressive way. Metadata associated with operating system memory determines whether it can be accessed by user programs or is restricted to the kernel. Intel CPUs allow programs to speculatively use kernel data, with the access check (which verifies whether the kernel memory is accessible to a user program) occurring only sometime after the instruction starts executing. While speculative execution is blocked when the check occurs, the impact that speculation has on the CPUs cache can be used to infer the values stored in kernel memory.

35. As a result of the "Meltdown" vulnerability, Intel's CPUs are potentially susceptible to JavaScript exploits that allow attackers to obtain sensitive web browser information, including cookies, credentials, passwords, or payment information a user has entered into a browser. In the case of Plaintiff and other Class members, that browser data could also include PHI or other protected third-party information.

E. *Intel's "Meltdown" and "Spectre" Design Flaws Cannot be Completely Fixed in Existing CPUs.*

36. While the security risks associated with "Meltdown" and "Spectre" can be mitigated, they cannot be fixed in all instances.

37. Software patches have been issued for various operating systems (including Microsoft's Windows, Apple's macOS, and Linux) to mitigate against "Meltdown" and "Spectre."

38. In some instances, software running on Intel CPUs and microcode running within Intel CPUs can be modified to reduce, but not eliminate, the risk. However, when available, these techniques reduce the performance of the CPUs, particularly for CPU operations involving numerous input/output operations.

39. In other instances, no mitigation technique is available, and the Intel CPU is inherently insecure.

III. Intel's CPU Security Flaws Have Damaged and Will Damage Health Care Providers and Other Entities Subject to Heightened Privacy Standards.

40. Shortly after the "Meltdown" and "Spectre" flaws were disclosed publicly, OCR reportedly sent an email update that urged HIPAA-covered entities to mitigate the vulnerabilities as part of their risk management processes. Given the nature of the CPU flaws, failure to mitigate places at risk the confidentiality, integrity, and availability of protected health information.

41. On January 12, 2018, HHS's Health Care Cybersecurity and Communications Integration Center ("HCCIC") issued a technical report on the "Meltdown" and "Spectre" vulnerabilities, which noted "[m]ajor concerns" for the health care sector. These included, but were not limited to:

- Challenges identifying vulnerable medical devices and accessory medical equipment and ensuring patches are validated to prevent impacts to the intended use.
- Cloud Computing: Potential PHI or Personally Identifiable Information (PII) data leakage in shared computing environments
- Web browsers: Possible PHI/PII data leakage
- Patches: Potential for service degradation and/or interruption from patches[.]

42. Plaintiff and other Class members have incurred and will continue to incur costs to monitor protected information, including patient ePHI and EHR, for data breaches and other malicious activity. These monitoring costs are above and beyond the costs that would be incurred as part of their ordinary risk management processes. Because the Intel CPU flaws can be mitigated, but not completely fixed, on existing hardware, these additional monitoring costs will continue until such time as Plaintiff and Class members purchase new CPUs that are not subject to the security risks described above.

//

//

43. Additionally, Plaintiff and Class members have been required to expend resources to monitor and maintain their computing resources in connection with Intel's security flaws. By way of example, various of Intel's "patches" supposedly designed to mitigate Intel's security defects are themselves defective and cause substantial reliability issues in affected PCs and servers.

44. As the risks posed by "Meltdown" and "Spectre" to protected information become better understood, Plaintiff and other Class members will be required to engage in additional, costly mitigation techniques, including devoting increased labor to the heightened monitoring of their Intel-based systems for security breaches, the procurement and installation of software designed to avoid Intel's CPU defects, and procurement of additional computer hardware to compensate for the reduced performance of mitigated but still dangerously insecure Intel CPUs.

45. Intel has announced that future generations of its CPUs will not contain these defects. If and when Intel corrects its design defects and begins marketing CPUs without the flaws described above, Plaintiff and other Class members will be compelled to accelerate their purchases of this new equipment, prematurely and outside normal replacement cycles, to eliminate the security risk created by Intel's design decisions. Consequently, Plaintiff and other Class members will sustain additional damages by expending the costs necessary to upgrade to non-defective computers and servers.

CLASS ACTION ALLEGATIONS

46. Plaintiff brings this action on behalf of itself and as a class action under Rule 23(a) and (b)(3) of the Federal Rules of Civil Procedure seeking damages on behalf of itself and Class Members nationwide (the "Class"):

> All persons or entities in the United States that are subject to federal regulations imposing standards of care with respect to the protection of confidential third-party information and that purchased (a) one or more Intel CPU, or (b) one or more servers, PCs or other device containing Intel CPUs.

47. Excluded from the Class are Intel, including any of its subsidiaries or affiliates; any entity in which Intel has a controlling interest; and any person who is an officer or director of the aforementioned entities.

48. While Plaintiff does not know the exact number of the members of the Class, Plaintiff believes there are thousands of entities.

49. Common questions of law and fact exist as to all members of the Class. Such questions of law and fact common to the Class include, but are not limited to:

a. Whether Intel's CPUs are affected by the "Meltdown" and "Spectre" flaws;

b. Whether the "Meltdown" and "Spectre" flaws put at risk confidential third-party information entrusted to Class members;

c. Whether efforts by Class members to monitor their computing resources and take other steps to mitigate the risks caused by the "Meltdown" and "Spectre" flaws are reasonable;

d. Whether Intel made any implied warranties or other representations in connection with the sale or marketing of its vulnerable CPIs;

e. Whether Intel breached any duties owed to Class members; and

f. Whether Intel violated Cal. Bus. & Prof. Code § 17200, et seq. or the New Mexico Unfair Trade Practices Act.

50. Plaintiff's claims arise out of the same common course of conduct giving rise to the claims of the other members of the Class. Plaintiff's interests are coincident with, and not antagonistic to, those of the other members of the Class.

51. Plaintiff is represented by counsel who are competent and experienced in the prosecution of class action litigation, including matters involving high-tech markets. Moreover, Plaintiff's counsel have retained renowned technical and industry experts who have significant experience with the matters at issue in this litigation.

52. The questions of law and fact common to the members of the Class predominate over any questions affecting only individual members, including legal and factual issues relating to liability and damages.

53. Class action treatment is a superior method for the fair and efficient adjudication of the controversy, in that, among other things, such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort and expense that numerous individual

actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities with a method for obtaining redress for claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in management of this class action.

54. Absent a class action, most Class members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. Because of the relatively small size of the individual Class members' claims compared to the anticipated costs of the litigation, it is likely that only a few Class members could afford to seek legal redress for the harms caused by Intel's design defects.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Strict Liability

55. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in paragraphs 1 through 45 of this Complaint.

56. Plaintiff and Class members were harmed by the CPUs Intel manufactured and marketed, which were contained in, but also separate and apart from, the servers, PCs and other devices purchased.

57. Intel's CPUs contained manufacturing defects, or were defectively designed, for the reasons set forth above. As a result, Plaintiff and Class members now own servers, PCs and other devices with Intel CPUs that put at risk the confidential and protected third-party information and other sensitive data on their networks.

58. As a direct result of the manufacturing or design defect, Plaintiff and Class members have been harmed by having to incur mitigation and monitoring costs, in an amount to be determined at trial, and will continue to incur those expenses until their servers, PCs and other devices with defective Intel CPUs can be replaced with hardware that does not suffer from the defects.

59. Moreover, Plaintiff and Class members have been harmed because they are under compulsion, in order to protect against privacy breaches, to expedite their purchases of next-generation CPUs prior to the expiration of the reasonably expected operating life of the defective CPUs.

SECOND CLAIM FOR RELIEF

Negligence

60. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in paragraphs 1 through 45 of this Complaint.

61. Intel was negligent in the manufacture and design of the CPUs containing the defects described above, which were contained in, but also separate and apart from, the servers, PCs and other devices that Plaintiff and Class members purchased.

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

63. Plaintiff and Class members have been harmed, as they now own servers, PCs and other devices with CPU that, due to the manufacturing or design defects described above, put at risk confidential and protected third-party information and other sensitive data on their networks, thereby requiring them to incur mitigation and monitoring costs in an amount to be determined at trial, and will continue to have to do so until their servers, PCs and other devices with defective Intel CPUs can be replaced with hardware that does not suffer from the defects.

THIRD CLAIM FOR RELIEF

Breach of Implied Warranties of Merchantability and Fitness For Particular Purpose

64. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in paragraphs 1 through 45 of this Complaint.

65. Intel, as the designer, manufacturer, marketer, distributor, and/or seller of the defective CPUs at issue, provided implied warranties of merchantability and fitness for a particular purpose.

66. Intel breached the implied warranty of merchantability because: (a) the defective Intel CPUs could not pass without objection in the trade because they are missing a key promoted characteristic, namely not exposing users to critical security vulnerabilities; (b) the CPUs were not of fair average quality; (c) were not adequately advertised, packaged, and/or labeled as omitting material facts as to the presence of the defects; or (d) they did not conform to the promises or affirmations of fact made by Defendant. Plaintiff and Class members did not receive goods as impliedly warranted by Intel to be "merchantable." Moreover, as this was a latent defect that existed at time of purchase for the reasons described above, the CPUs are rendered unmerchantable.

67. Defendant also breached the implied warranty of fitness for a particular purpose as provided by law, including, inter alia, Cal. Comm. Code § 2316. Plaintiff and Class members purchased their servers, PCs and other computing devices with Intel CPUs for a particular purpose. Plaintiff and Class members could be reasonably expected to rely upon Intel's skill and judgment in properly providing the CPUs without containing critical security vulnerabilities, and furnish goods suitable for their particular purpose, and thus would have no reason to believe otherwise.

68. Intel had reason to know that Plaintiff and Class members were relying on its skill and judgment to furnish suitable goods that would satisfy their particular purpose. Intel had reason to know of the particular purpose of these purchases, and that purchasers would be relying on their skill and judgment to ensure these computers would perform adequately and not subject them to critical security vulnerabilities.

69. The CPUs were not altered by Plaintiff or Class members.

70. The CPUs did not conform to these implied warranties when they left the exclusive control of Intel.

71. Plaintiff and Class members did not receive these goods as impliedly warranted.

72. All conditions precedent to seeking liability for breach of these implied warranties have been performed by or on behalf of Plaintiff and Class members. Intel has refused to recall, repair or replace, free of charge, all Intel CPUs or refund the prices paid for the CPUs.

73. As a direct and proximate cause of Intel's breaches of implied warranties, Plaintiff and Class members have been injured and harmed, in an amount to be determined at trial.

FOURTH CLAIM FOR RELIEF

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

74. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in paragraphs 1 through 45 of this Complaint.

75. Plaintiff has standing to pursue this claim as AGH has suffered injury-in-fact and lost money or property as a result of the critical security vulnerabilities in Intel's CPUs.

76. Intel's business practices, including but not limited to its continued marketing of its defective CPUs after learning of the "Meltdown" and "Spectre" vulnerabilities, offend established public policy and/or are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to their customers. Additionally, Defendant's conduct is "unfair" because Intel engaged in misleading and deceptive conduct, or to not sell defective products. Intel also concealed material facts from Plaintiff and Class members.

77. Intel's business practices, including but not limited to its affirmative acts and material omissions are contrary to public and legislative policy and the harm it has, and continues to cause Plaintiff and members of the Class, far outweighs its utility.

78. As a result of Intel's "unfair" business practices, Plaintiff and members of the Class spent money on servers, PCs and other computing devices that contain Intel's defective CPUs.

79. Intel's unfair business practices constitute a continuing course of unfair competition.

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

FIFTH CLAIM FOR RELIEF

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

81. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in paragraphs 1 through 45 of this Complaint.

82. Plaintiff has standing to pursue this claim as AGH has suffered injury-in-fact and lost money or property as a result of the critical security vulnerabilities in Intel's CPUs.

83. Intel's business practices were "deceptive" because they were and are likely to deceive consumers, including Plaintiff and Class members, targeted by such omissions of material fact. Among other things, Intel failed to disclose material information to purchasers of servers, PCs and other computing devices containing Intel CPUs by concealing material facts relating to critical security vulnerabilities.

84. As a result of Intel's "deceptive" conduct, Plaintiff and Class members spent money on servers, PCs and other computing devices with defective CPUs.

85. Intel's deceptive business practices alleged herein constituted a continuing course of unfair competition.

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

SIXTH CLAIM FOR RELIEF

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

87. Plaintiff, individually and on behalf of the Class, incorporate by reference all of the allegations contained in paragraphs 1 through 45 of this Complaint.

88. Plaintiff has standing to pursue this claim as AGH has suffered injury-in-fact and lost money or property as a result of the critical security vulnerabilities in Intel's CPUs.

89. Intel's business practices, including but not limited to its continued marketing of its defective CPUs after learning of the "Meltdown" and "Spectre" vulnerabilities, constitute "unlawful" business practices because they violated California Civil Code § 1750, et seq., California Civil Code § 1790, et seq., 15 U.S.C. § 2301, et seq., among other laws, breached applicable warranties, and engaged in acts resulting in negligence and strict liability.

90. As a result of Intel's "deceptive" conduct, Plaintiff and Class members spent money on servers, PCs and other computing devices with defective CPUs.

91. Intel's deceptive business practices alleged herein constituted a continuing course of unfair competition.

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

SEVENTH CLAIM FOR RELIEF

Violation of the New Mexico Unfair Trade Practices Act

93. Plaintiff, individually and on behalf of the Class members operating in New Mexico, incorporate by reference all of the allegations contained in paragraphs 1 through 45 of this Complaint.

94. Defendant violated the New Mexico Unfair Trade Practices Act, N.M. Stat. Ann. § 57-12-1, et seq., which prohibits unfair or deceptive acts or practices.

95. Intel's business practices, including but not limited to its continued marketing of its defective CPUs after learning of the "Meltdown" and "Spectre" vulnerabilities, constitute unfair deceptive trade practices in that they are likely to deceive a reasonable consumer. A reasonable consumer expects or assumes that CPUs manufactured, marketed, and sold by Intel would not contain critical security vulnerabilities. Intel's misrepresentations and omissions concerning its defective CPUs are material and likely to deceive a reasonable consumer.

96. Among other things, and both before and after Google alerted Intel that it was aware of the CPU defects, Intel represented that its CPUs possessed certain characteristics and benefits

that they did not have and were fit for certain applications that they were not, Intel used exaggeration, innuendo, and ambiguity as to material facts regarding the fitness and quality of its CPUs in a manner that deceived or tended to deceive Plaintiff and New Mexico members of the Class and failed to state material facts regarding their CPUs that deceived or tended to deceive, which constitutes a deceptive trade practice within the meaning of the statute.

97. Intel also failed to deliver the quality of CPUs contracted for, in violation of the statute. Intel represented that its CPUs were fit to "prevent exposure to malicious code, viruses, cyber espionage, malware, and data theft," and Defendant knew or should have known that Plaintiff and other Class members in New Mexico would purchase those CPUs through intermediaries in order to store or access sensitive third-party information.

98. As a result of Intel's unfair and deceptive business practices, Plaintiff and Class members in New Mexico have been damaged in that they (a) purchased CPUs that they otherwise would not have purchased for the price they paid, (b) incurred substantial costs to monitor their networks and otherwise take steps to mitigate the risks to protected third-party information; and (c) will be required to replace servers, PCs and other devices with defective Intel CPUs when replacements are available that do not include the defect.

99. All of the wrongful conduct alleged herein occurred in the conduct of Intel's business. Intel's wrongful conduct is part of a pattern or generalized conduct that is still perpetuated and repeated, both in New Mexico and nationwide. Intel's use of unfair and deceptive acts and practices was willful and knowing.

100. Plaintiff and Class members are entitled to damages in the amount of three times their actual damages or $300 (whichever is greater). Plaintiff and Class members are also entitled to equitable relief, including restitution of all revenue accruing to Intel because of its unfair and deceptive practices; attorneys; fees and costs; declaratory relief; and a permanent injunction enjoining Intel from its unfair and deceptive activity.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all others similarly situated, requests the Court to enter judgment against Intel, as follows:

A. An order certifying the proposed Class, designating Plaintiff as the named representative of the Class, and designating the undersigned as Class Counsel;

B. An award of damages, including but not limited to compensatory, statutory and punitive damages, to Plaintiff and Class members in an amount to be determined at trial

C. An award of reasonable litigation expenses and attorneys' fees to Plaintiff and Class members;

D. An award of pre-judgment and post-judgment interest, as provided by law; and

E. An award of such other relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any, and all issues in this action so triable of right.

Dated: February 23, 2018

/s/ Robert J. Gralewski, Jr.

Robert J. Gralewski, Jr.

KIRBY McINERNEY LLP
Robert J. Gralewski, Jr.
Fatima G. Brizuela
600 B Street, Suite 1900
San Diego, CA 92101
Telephone: (619) 398-4340
bgralewski@kmllp.com
fbrizuela@kmllp.com

HINKLE SHANOR LLP
Thomas M. Hnasko
Michael E. Jacobs
P.O. Box 2068
Santa Fe, NM 87504
Telephone: (505) 982-4554
thnasko@hinklelawfirm.com
mjacobs@hinklelawfirm.com

HINKLE SHANOR LLP
Andrew J. Cloutier
Lucas M. Williams
P.O. Box 10
Roswell, NM 88202
Telephone: (575) 622-6510
acloutier@hinklelawfirm.com
lwilliams@hinklelawfirm.com

JS-CAND 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
Artesia General Hospital, et al.

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Kirby McInerney LLP
Robert J. Gralewski, Jr. (CSB#196410)
600 B Street, Suite 1900, San Diego, CA 92101 - (619) 398-4339

DEFENDANTS
Intel Corporation

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

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

Attorneys *(If Known)*

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

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

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

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

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

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

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

TORTS

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

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

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

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

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

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d); FRCP Rule 23(a) and (b)(3)

Brief description of cause:
Class action lawsuit related to security vulnerabilities in Intel CPUs-Strict liability, Negligence, Unfair Business Practices, Breach of Implied Warranty of Merchantability

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

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

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

JUDGE DOCKET NUMBER

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

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

DATE **SIGNATURE OF ATTORNEY OF RECORD**

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)."

II. Jurisdiction. The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

(4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked**.** (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Federal Rule of Civil Procedure 23.

Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. Divisional Assignment. If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

Date and Attorney Signature. Date and sign the civil cover sheet.