William J. Doyle II (SBN 188069)
Chris W. Cantrell (SBN 290874)
DOYLE APC
550 West B St., Fourth Floor
San Diego, CA 92101
Telephone: (619) 736-0000
Facsimile: (619) 736-1111
E-mail: bill@doyleapc.com
E-mail: chris@doyleapc.com

Adam J. Levitt (pending admission *pro hac vice*)
Amy E. Keller (pending admission *pro hac vice)*
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street, Eleventh Floor
Chicago, Illinois 60602
Telephone: (312) 214-7900
Facsimile: (440) 953-9138
Email: alevitt@dlcfirm.com
Email: akeller@dlcfirm.com

J. Gerard Stranch, IV (pending admission *pro hac vice)*
Benjamin A. Gastel (pending admission *pro hac vice*)
Tricia Herzfeld (pending admission *pro hac vice)*
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Telephone: (615) 254-8801
Facsimile: (615) 255-5419
E-mail: gerards@bsjfirm.com
E-mail: beng@bsjfirm.com

Jeffrey L. Fazio (SBN 146043)
Dina E. Micheletti (SBN 184141)
FAZIO | MICHELETTI LLP
2410 Camino Ramon, Suite 315
San Ramon, California 94583
Telephone: (925)543-2555
Facsimile: (925) 369-0344
Email: jlf@fazmiclaw.com
Email: dem@fazmiclaw.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

BRIAN SPECK, individually and on behalf of all others similarly situated;

Plaintiff,

v.

ADVANCE MICRO DEVICES, INC., a Delaware Corporation,

Defendant.

Case No.

CLASS ACTION COMPLAINT FOR DAMAGES AND EQUITABLE RELIEF

DEMAND FOR JURY TRIAL

Plaintiff Brian Speck ("Plaintiff"), individually and on behalf of all others similarly situated, by his undersigned counsel, alleges the following upon personal knowledge as to his own acts and upon information and belief as to all other matters.

INTRODUCTION

1. Plaintiff BRIAN SPECK brings this action against Defendant Advanced Micro Devices, Inc. ("AMD" or "Defendant") on behalf of all persons who purchased an AMD processor ("CPUs") manufactured, designed, marketed, licensed and/or sold by Defendant.

2. AMD's CPUs based on the x86-64x architecture ("x86"), suffer from security vulnerabilities, that allow unprivileged access to extremely secure kernel data. The x86 is a CPU architecture created by AMD in 2000. AMD released the first x86 CPU in 2003 called the Opteron. The x86 CPU architecture has been implemented by Intel and is the primary CPU design even today.

3. These security vulnerabilities are inherent to the x86 CPU as they are the result of design shortcuts intended to increase processor speed. Unfortunately, these shortcuts sacrificed security in the name of speed leaving consumers with CPUs that have inherent design flaws exposing the secure data of millions of AMD CPU users.

4. Cyber-security experts have identified two distinct methods of "attacking" the security vulnerabilities that are inherent in the design of x86 CPUs from AMD, Intel Corporation and ARM Holdings. Named "Meltdown" and "Spectre" by the individuals who discovered these flaws, these attack methods take advantage of the breakdown of the typical security protocol when accessing kernel data that occurs when the CPUs are performing speculative execution and out-of-order execution. Speculative execution and out-of-order execution are two methods used by the affected CPUs to increase processing speeds.

5. Both Meltdown and Spectre are side-channel attacks which are attacks based on information gained from some observable aspect of a computer's physical operation. For example, the observation of timing, power consumption and cache use. The observation and analysis of these behaviors can then be used to expose secure data on the computer. Unlike some software or operating system attacks, side-channel attacks do not corrupt, change or delete data.

6. AMD CPUs do not appear to be afflicted with the Meltdown flaw but do contain the more invidious, widespread and difficult to eradicate Spectre vulnerability. Any AMD CPU that implements speculative execution is vulnerable to Spectre side-channel attacks, which would include almost every modern-day AMD CPU. AMD x86 processors, are among the most widely utilized CPUs in the world and power large numbers of desktops, laptop computers, and servers in the United States. These flawed CPUs also power medical equipment such as CT scanners, ECG monitors and recorders, and pacemakers and defibrillators.

7. To date, Defendant has been unable or unwilling to repair the security vulnerabilities in the subject CPUs or offer Plaintiff and class members a non-defective CPU or reimbursement for the cost of such CPU and the consequential damages arising from the purchase and use of such CPUs. The software updates or "patches" pushed by AMD onto CPU owners does not appear to provide protection from all the variants of Spectre. At the very least, firmware updates or changes will be required. Even then, these "patches" dramatically degrade CPU performance.

8. A number of experts believe the security flaws in Defendant's CPUs cannot be completely "patched" via the use of software and firmware updates because these vulnerabilities arise from fundamental design flaws in the CPUs themselves. At best, these "patches" serve to mitigate the problem. According to these experts, the only real "fix" is a newly designed processor

free of the inherent design flaws creating the security vulnerabilities. Indeed, these vulnerabilities do not arise from malware changing how the system operates but rather take advantage of security flaws inherent in the CPU operating as it was designed to do. Currently, affected AMD CPU owners are left with the unappealing choice of either purchasing a new processor or computer containing a CPU that does not contain these vulnerabilities, or continuing to use a computer with massive security vulnerabilities or one with significant performance degradation. Any "patch" to secure the vulnerabilities requires extensive changes to the root levels of the computer operating system, which dramatically reduces CPU performance. These security vulnerabilities render AMD's CPUs unmerchantable and unfit for their intended use and purpose.

9. Defendant's conduct described herein violates state common law as well as state and federal statutory consumer protection and warranty statutes.

10. Having purchased a CPU that suffers from these security vulnerabilities, Plaintiff and class members suffered injury in fact and a loss of money or property as a result of Defendant's conduct in designing, manufacturing, distributing, licensing, marketing and selling defective CPUs. Defendant has failed to remedy this harm and has earned, and continues to earn, substantial profit from selling defective CPUs.

11. As a result, Plaintiff bring this class action against Defendant AMD on behalf of all other persons and entities in the United States that purchased an AMD CPU processor, or purchased a laptop, desktop, server or other computing device containing an AMD CPU.

THE PARTIES

12. Plaintiff Brian Speck, is an individuals and resident citizen of the State of Ohio. In 2013, Plaintiff Speck purchased a computer containing and AMD processor. Plaintiff Speck uses his computer primarily for personal purposes. He was unaware of the CPU design flaws or security

vulnerabilities described herein prior to his purchase of this computer. Had Defendant AMD disclosed such material facts, Plaintiff Speck would not have purchased a computer with an AMD CPU or would have paid substantially less for it.

13. Defendant Advanced Micro Devices, Inc., is a business incorporated under the laws of the State of Delaware. AMD's principal place of business is located at 2485 Augustine Drive., Santa Clara, California, 95054. AMD moved its headquarters to Santa Clara in November 2017. Prior to that, AMD's principal place business was One AMD Place, Sunnyvale, CA. At all relevant times, AMD was one of the world's largest manufacturers of CPUs and was engaged in the business of designing, manufacturing, distributing and/or selling electronic computer products, including the defective AMD CPUs at issue. AMD designed and marketed the sale of flawed CPUs from its headquarters in California which also served as the location where AMD made decisions to focus solely on increasing processor speed and disregard security testing of their CPUs which would have revealed the design flaws.

14. Whenever this Complaint refers to any act of Defendant, the reference shall mean (1) the acts of the directors, officers, employees, affiliates, or agents of Defendant who authorized such acts while actively engaged in the management, direction or control of the affairs of Defendant, or at the direction of Defendant, and/or (2) any persons who are the parents or alter egos of Defendant, while acting within the scope of their agency, affiliation, or employment

JURISDICTION AND VENUE

15. This Court has jurisdiction over the lawsuit under 28 U.S.C. § 1332(d), the Class Action Fairness Act, because this suit is a class action, the parties are diverse, and the amount in controversy exceeds $5 million, excluding interest and costs.

16. This Court has general personal jurisdiction over AMD as its principal place of business is in the State of California.

17. Venue is proper in this District under 28 U.S.C. §1391 because a substantial part of the events or omissions giving rise to this claim occurred in this district and Defendant maintains its principal place of business in this District.

18. Pursuant to Civil Local Rule 3-2(c), the San Jose Division of the Northern District of California is the proper venue as a substantial part of the events or omissions giving rise to this claim occurred in this District and Defendant maintains its principal place of business in this District.

FACTUAL ALLEGATIONS

19. The central processing unit ("CPU") is the core part of all computing devices and controls all basic computer functions. When the user requests a task be performed (to run a program, save a file) the CPU draws from the computer memory (Cache or RAM) the information associated with the requested task. The CPU reads this information and then begins assembling and transporting the data/code to carry out that task. This basic computer operational process is called the instruction cycle and is based on the steps of fetch—decode—execute.

20. To execute tasks, the CPU must allow the operating system ("OS") to interact with the hardware. These two modes of operation are called the "user mode" and "kernel mode." The "user mode" is the process whereby the user inputs commands to be executed, and the "kernel mode" is when those tasks are being executed. During kernel mode, there is unrestricted access to the computer and the kernel mode has control over everything occurring in the system. In kernel mode, the CPU can execute any instruction, initiate any operation, and access any and all areas of memory to the extent permitted by the CPU architecture. Because kernel mode has unrestricted

access to the computer system, including all secure data such as keystrokes, passwords and encryption keys, access to the kernel is secured. In all other modes, including user mode, certain operations are restricted, such as access to secure areas of memory. Most CPUs use ring-based security, which resembles a set of concentric rings with the kernel mode in the center. The hierarchy of privileges increases as you go from the outside ring to the inner-most ring (the kernel).

21. If a user mode action requires access to the kernel mode to execute, the restricted user mode must temporarily relinquish control of the CPU to the kernel mode to perform or execute this task. To do this, the user mode makes a system call to request the kernel mode take over and perform any operations that could damage or compromise the system. This prevents the user mode from gaining access to the privileged and restricted kernel data.

22. The speed at which a processor operates (fetches, decodes, and executes) depends on how quickly the processor can transition from user mode to kernel mode and back again. Modern processors have created various shortcuts to increase the speed of these operations. Two of these shortcuts "speculative execution" and "out-of-order" execution have flaws in design that create massive security vulnerabilities.

23. For years, cyber-researchers have suspected that processors based on the x86-64x architecture could be susceptible to direct firmware attacks due to some of these shortcuts. Since 2005 a number of white papers have been written on the subject. These vulnerabilities were never fully probed, as most researchers believed AMD would surely have tested their CPUs for the presence of such a gaping security flaw. In 2013, research papers revealed that unauthorized users could use the CPU to see the secure layout of the kernel. This flaw came to be called the KASLR break. Researchers were still skeptical that these vulnerabilities were real, again believing AMD would never have designed, marketed, and sold its CPUs with such a glaring security flaws. In

essence, these security vulnerabilities were so glaring, that researchers simply could not believe them to be true.

24. To their surprise, in late 2016 and early 2017 cyber-researchers confirmed these security flaws existed and could be exploited. In May 2017, two specific methods of attack were identified (Meltdown and Spectre). These two variants were distinctive in attacking the hardware/firmware of the CPU instead of the operating system or software. These side-channel attacks take advantage of speculative execution and out-of-order execution, both of which are embedded in the CPU itself.

25. These security vulnerabilities are believed to exist in every AMD processor that uses out-of-order and/or speculative execution, which includes almost AMD CPU made since least 2004, regardless of the operating system. The problem lies in the architecture of the CPUs. All CPUs have an "architecture" and the design of the architecture dictates the functionality of the CPU including the speed of operation as well as security. The architecture of the AMD x86 CPUs was designed solely for speed of operation with little or no thought to security.

26. AMD's processors are widely-used, found in many desktop and laptop computers. The AMD processors also are used in a variety of servers from system servers to large, cloud-based servers such as those from Google, Microsoft, and Amazon.

A. Spectre

27. On January 2, 2018, these flaws became public after the British tech newspaper *The Register* reported that certain microprocessors by Intel had massive security vulnerabilities

exposing them to the Meltdown and Spectre hardware/firmware attacks.[1] Over the following days, it was revealed that AMD and ARM processors also contain some of these vulnerabilities.

28. Meltdown leverages out-of-order execution, which allows the CPU to carry out instructions in parallel instead of sequential order, thereby avoiding any delay that may occur between the "fetch" instructions and the "execute" instructions phases. At this time, it is not believed that AMD CPUs are susceptible to Meltdown because their processors do not perform this type of out-of-order execution.

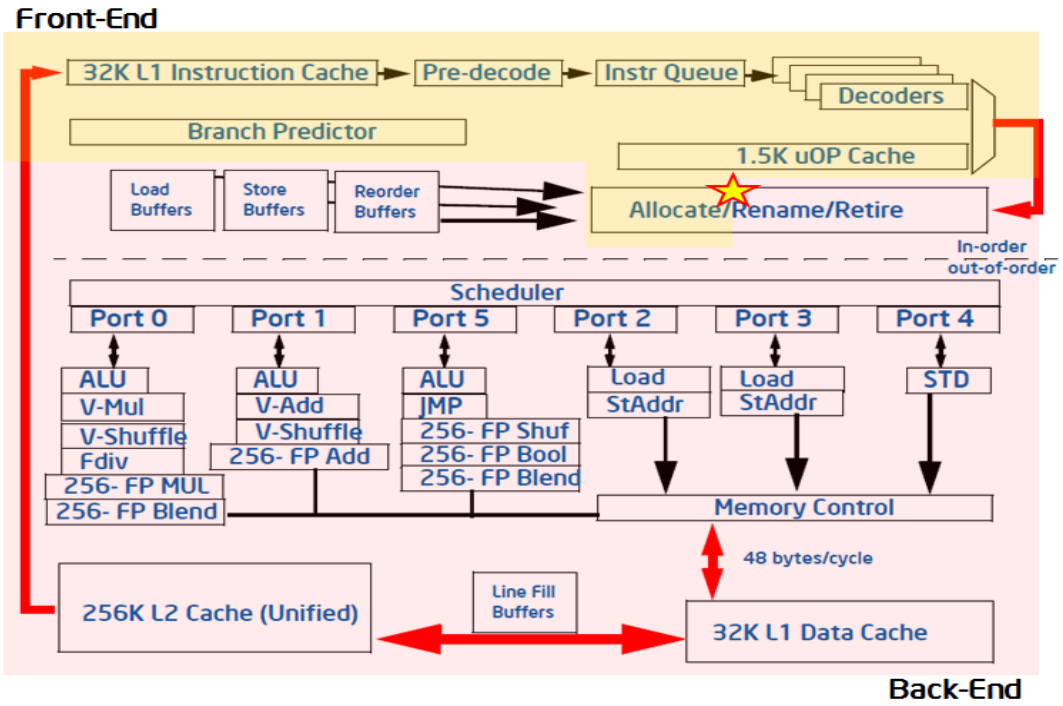
29. AMD CPUs, however, do utilize speculative execution and are vulnerable to both variants of Spectre attacks, named Variant 1 "Bounds Check Bypass" and Variant 2 "Branch Target Injection" by Google Project Zero. Both Variants of Spectre are side-channel attacks that leverage the CPU's use of speculative execution but in different ways.

30. Speculative execution increases processing speed by predicting what the next operation will be and then placing the relevant kernel data needed to carry out that predicted operation in caches where it is standing by, ready to execute. It gets rid of the lag time that would normally exist while waiting on the relevant kernel data to be accessed after the user mode requests a task be carried out by the kernel mode.

31. To execute most tasks, the kernel mode must be activated to take control of the CPU, so the kernel mode can execute the task requested. Kernel data is the most secure part of the computer storing passwords and encryption keys, and is only supposed to be accessed by secure, privileged programs or users. It is a fundamental security principle of all computing devices that access to kernel data by a low-privilege user mode program should not be allowed.

[1]John Leyden and Chris Williams, *Kernel-memory-leaking Intel processor design flaw forces Linux, Windows redesign*, (January 2, 2018), https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/

32. While the kernel data in cache are invisible to the user mode programs, the mere presence in cache can allow malware attached to a low-privilege access program to ascertain the kernel data hidden in cache and then extract the secure kernel data. In general terms, this this security flaw, can be described as allowing a low-privilege program or process to access secure, high-privilege kernel data.



Generic Diagram of Speculative Execution Process

33. Speculative Execution not only predicts the next task, so that kernel data is on stand-by; it also identifies the appropriate location or branch to place the kernel data or code. Called "branch prediction," the CPU speculatively executes instructions to the location the CPU believes it will branch to, minimizing wait time and improving CPU performance. If the proper branch is predicted, the instructions such as register and memory will be committed. If the branch is mis-predicted, the speculatively executed instructions will be discarded and the direct side-effects of the instructions are undone. This is because the normal security features protecting kernel

code/memory do not activate if the result is mis-predicted via speculative execution, for whatever process is mis-predicted is not actually executed. While the instructions are undone when a mis-prediction occurs, there are remnants of the secure kernel information remain in the CPU cache. These "indirect side-effects," such as cache changes, are not undone in a mis-prediction.

34. Both variants of Spectre leverage the branch prediction process of speculative execution to access secure data. Spectre Variant 1 ("Bounds Check Bypass") uses the cache changes from metadata that remain after a branch mis-prediction. The cache changes left behind after a mis-prediction contain certain measurable data including how long the hardware takes to retrieve the data which allows the malware to infer details of the kernel data based on this and other measurable data. So, an innocuous program, such as JavaScript, can be used to gain access to the kernel data. Or as the *The Register* writes, "[t]hat would allow ring-3-level user code to read ring-0-level kernel data. And that is not good."[2]

35. Spectre Variant 2 ("Branch Target Injection") tricks the processor into making speculative accesses outside the bounds of an array. Essentially it involves training the branch prediction hardware to favor speculatively executing pieces of kernel code desired by the malware instead of the code it should be executing. The result is the attacker has steered the secure kernel memory it wants into cache where the attacker can then access the kernel memory from the metadata that remain in cache after an indirect branch prediction.

36. While both variants of Spectre pose considerable risk, it is Variant 2 that is causing the most consternation in the industry because of the potential abuse. As one prominent tech website notes "this particular vulnerability could allow malware running in one user's virtual

[2] *See* Leyden and Williams, *supra*.

machine or other 'sandboxed' environment to read data from another – or, from the host server itself."[3]

37. The security vulnerability here is particularly troubling. Unlike the vast majority of cyber-security vulnerabilities which are usually flaws in the operating system or software, Spectre is completely independent of the computer's operating system and attacks the CPU's hardware and firmware via a side-channel attach on the CPU's cache. As one chip-level hardware security expert notes "[w]ith these glitches if there's any way an attacker can execute code on a machine, it can't be contained… For any process that untrusted and isolated, that safety is gone now…. Every process can spy on every other process and access secrets in the operating system kernel."[4]

38. Spectre impacts every AMD processor on the market. A software and/or firmware update cannot correct the Spectre defect, but can only serve to mitigate the risk from the defect. Because the flaw is such a fundamental part of the current CPU design, many cyber-researchers believe only a new generation of chips will fix the Spectre vulnerability.

39. Paul Kocher, one of the dozen or so researchers who uncovered Meltdown and Spectre stated "We've really screwed up," and continues noting that Spectre is "going to live with us for decades."[5] The cybersecurity researchers credited with discovering Spectre include:

---

[3] Sean Gallager, *The impromptu Slack War room where 'Net companies unite to file Spectre and Meltdown*, ARSTechnica (January 17, 2018), https://arstechnica.com/information-technology/2018/01/the-impromptu-slack-war-room-where-net-companies-unite-to-fight-spectre-meltdown/

[4] Andy Greenberg, *A Critical Intel Flaw Breaks Basic Security For Most Computers*, Wired (January 3, 2018), https://www.wired.com/story/critical-intel-flaw-breaks-basic-security-for-most-computers/?mbid=BottomRelatedStories

[5] Cade Metz and Nicole Perlroth, *Researchers Discover Two Major Flaws in the World's Computers*, The New York Times, (January 3, 2018), https://www.nytimes.com/2018/01/03/business/computer-flaws.html?_r=0

- Jann Horn of Google who is credited as being the first person to discover both Meltdown and Spectre;
- Paul Kocher of Cryptography Research Inc., Daniel Genkin of the University of Pennsylvania, Mike Hamburg of Rambus and Yuval Yarom of the University of Adelaide are the researchers credited with discovering Spectre; and
- Anders Fogh of G-Data Advanced Analytics is credited with being the first to actually identify the design flaw in the x86-64x as well as the connection to speculative execution.

40. Thomas Prescher, one of the researchers that uncovered Meltdown and a former Intel engineer himself, observed, "It makes you shudder … [t]he processor people were looking at performance and not looking at security."[6]

41. The security flaws are unprecedented in scope and expose millions of AMD-based computers to critical security vulnerabilities and hacking, and the alleged "patches" to cure these security vulnerabilities will cause substantial CPU performance degradation. The scope extends beyond the millions of laptops, desktops and servers utilizing AMD processors. Some of the most important and confidential work by the U.S. Government and many private companies are performed utilizing clusters of AMD processors such as simulations of rocket aerodynamics by NASA and crash simulations by Mercedes Benz.

42. The CPU is the core or brain of the computer, carrying out all instructions from all programs. Because these inherent security flaws are designed into the CPU these vulnerabilities

[6] Ian King and Jeremy Kahn, *'It Can't Be True.' Inside the Semiconductor Industry's Meltdown*, Bloomberg Technology (January 8, 2018), https://www.bloomberg.com/news/articles/2018-01-08/-it-can-t-be-true-inside-the-semiconductor-industry-s-meltdown

permeate the functionality of the entire computer system, putting every aspect of the computer system at risk.

B. Knowledge of the Security Vulnerabilities

43. Researchers have been writing papers warning of the potential security weaknesses of CPUs using speculative execution for more than a decade. Yuval Yarom, from the University of Adelaide, one of about a dozen researchers worldwide to discover Meltdown and Spectre, authored some of the early papers predicting this security vulnerability.

44. In 2013, what was thought to be only a potential security flaw became a confirmed after published research papers revealed that unauthorized users could use the CPU to see the secure layout of the kernel. This flaw from speculative execution came to be called the KASLR break and served as the basis of the discovery of Spectre and Meltdown.

45. In August 2016, a group of cyber-security researchers led by Anders Fogh and Daniel Gruss presented a research paper titled "Using Undocumented CPU Behavior to See into Kernel Mode and Break KASLR in the Process" at the Black Hat USA cyber-security conference. The paper discussed potential cyber-attacks on the CPU hardware itself instead of the usual route of software. Specifically focusing on the x86-64x architecture, the paper concluded it was possible for an attacker to access the secure kernel data via the use of low security programs such as JavaScript. Cyber-security experts had assumed such a glaring security defect would certainly have been discovered during testing by AMD and other CPU manufacturers, and the companies never would have shipped CPUs with such massive vulnerabilities.

46. In November of 2016, at the Black Hat Europe conference, Anders Fogh and others discussed this potential method of attack, but there was still no belief among researchers that such

a dangerous security vulnerability did actually exist. However, despite the lack of any belief a real flaw existed, the Graz research team continued to research the issue.

47. Two months later, in January 2017, Anders Fogh discovered the integral connection between speculative execution and the CPU design flaw. Fogh disclosed his discovery to the Graz research team who began investigating the issue more intently.

48. Around April 2017, Jann Horn, a researcher at Google's Project Zero, independently discovered both Meltdown and Spectre. In early June 2017, Jann Horn, a member of Google's Project Zero security team, advised AMD of these massive security flaws in its CPUs. Ironically, during this same period, three other teams of computer experts also contacted AMD about the ability of Spectre to exploit the security flaws in speculative execution to gain access to secure information. Immediately thereafter, the CPU manufacturers, along with Microsoft, Google, Amazon and Oracle, began to develop a purported patch.

49. In July 2017, the Graz team developed a software security patch for Linux OS called "KAISER," which was designed to fix the KASLR break. Because Linux is an open-source operating system, the software update was publicly shared. At this time, the Graz team and Fogh were not aware that AMD, Intel, ARM Holdings, Google, Microsoft, and other tech companies were already aware of these security vulnerabilities and were scrambling to find a fix

50. By November 2017, most of the large tech companies, like Google, Amazon, ARM, and Microsoft, began issuing a large number security updates for Linux OS users. The large number of these updates led cybersecurity researchers to realize something significant was taking place, especially since these companies continued to implement these patches even though they were having a terrible impact on CPU performance. Amazon discovered one of these Linux patches increased the time it took to complete certain operations by 400%. Yet despite the massive

performance diminishment, Amazon was still urging Linux users to accept the software patch, cementing the belief by cyber-researchers that a massive security issue had been discovered.

51. This belief led to a great deal of speculation on leading tech sites as to what the security issue could be. A discussion on Kernel.org, the primary distribution point for the Linux source code, centered on the KASLR break, KAISER and the possibility of side-channel attacks on CPU. Apparently monitoring these sites for evidence the security flaws had become public, on December 26, 2017, AMD VP Tom Lendacky sent an email to the Linux Kernel mailing list and proclaimed that "AMD processors are not subject to the types of attack the kernel page table isolation feature protects against."[7] This was AMD hedging its bets; hoping to keep the news of these vulnerabilities from becoming public but representing that AMD processors were not vulnerable to these types of attacks in the event it did.

52. On or about January 2, 2018, the existence of the major security vulnerabilities was publicly revealed by *The Register*.[8] The article revealed the existence of the vulnerabilities in Intel processors based on Lendacky's December 26th email to the Linux Kernel mailing list representing that AMD's processors are not subject to these security flaws. *The Register* article also credits Lendacky for providing enough detail in the email that it was possible to piece together the specifics of the design flaws in speculative execution.[9] AMD's deception helped shape the narrative that this was an "Intel only" issue as the story grabbed worldwide attention allowing AMD to avoid some of the backlash that befell Intel including a significant drop in stock price.

[7] https://patchwork.kernel.org/patch/10133447/

[8] *See* Leyden and Williams, *supra*.

[9] *See* Leyden and Williams, *supra*.

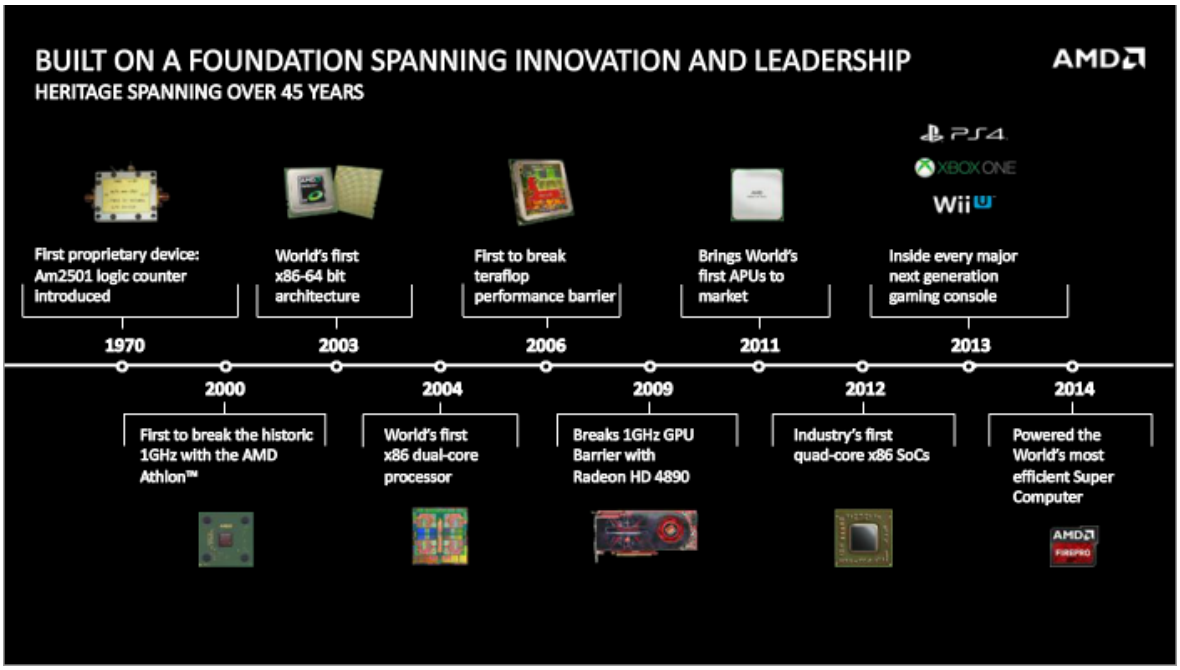
53. In the days that followed, AMD was forced to admits its CPUs contain these security flaws exposing them to Spectre type attacks. Reports also immediately disclosed that the anticipated "patches" to these security vulnerabilities would lead to substantial CPU performance degradation.[10] The "patch" would require root level changes to the operating system, resulting in a substantial decrease in CPU performance—as much as 30-50% by some estimates. In the days following, it was found that a software update to the OS would not protect the CPU from Spectre, but rather hardware or firmware changes to the CPU would be required, at the very least.

C. AMD Focuses on Speed at the Sake of Security

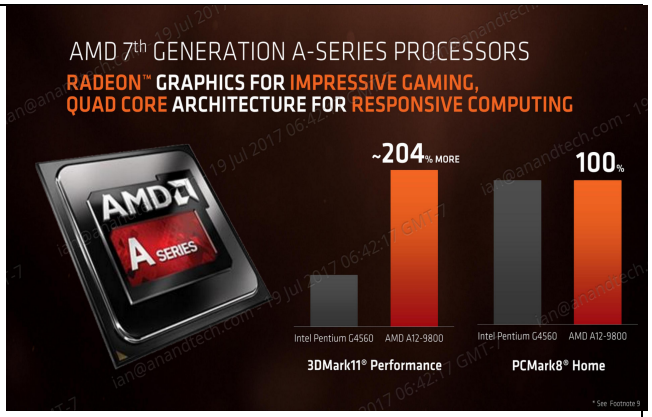
54. For years, the sole focus of the CPU industry was processing speed and how to increase it, creating an arms race of sorts within the industry to create the fastest processors. The industry reached the upper limits of what increases in speed any changes in material would bring and processor clock speeds have maxed out. At this point, "[o]ptimizations, then, become the key to speed increases."[11] AMD and others, started focusing on how to increase the speed of the instruction cycle within the CPU itself, leading to speculative execution and out-of-order execution. However, these changes were made with no thought as to the security vulnerabilities that were simultaneously created. Security was simply not part of the equation.

[10] Major Security flaw found in Intel processors, The Guardian, (January 3, 2018), https://www.theguardian.com/technology/2018/jan/03/major-security-flaw-found-intel-processors-computers-windows-mac-os-linux

[11] Larry Greenemeier, *Meltdown and Spectre Expose the Dark Side of Superfast Computers*, Scientific American (January 9, 2018), https://www.scientificamerican.com/article/meltdown-and-spectre-expose-the-dark-side-of-superfast-computers/



55. Ignoring security almost completely, AMD's marketing and promotion campaigns focused almost exclusively on processing speeds. It's CPU and GPU advertisements were replete with terms like "Most Powerful" and "Performance You Can See and Feel"



56. The Spectre vulnerabilities and its vast impact are the product of a company, and an industry, that cared only about sales and profits driven by ever-increasing processor speeds.

"Moore's law," the observation by Intel co-founder Gordon Moore that the number of transistors per square inch of an integrated circuit doubles every two years, become the industry mantra. Unfortunately, this was done at the sacrifice of security. Indeed, it doesn't appear that security was even a consideration. Writing about this very issue, *Scientific American* noted "[i]t is now clear that the insatiable need for faster processors" led CPU manufacturers to "cut corners on security, exposing potentially billions of personal computers, mobile devices and other electronics to a new crop of digital attacks for years to come."[12]

57. The cyber-researchers that uncovered Spectre had little belief that such a dangerous security vulnerability did actually exist because the CPU manufacturers would surely have tested for these flaws. As Graz researcher Michael Schwarz stated, "[t]hat would be such a major f**k up … that it can't be possible."[13]

58. Part of the disregard for security is due to the fact most cyber-security flaws today are within software or the Operating System, and not the hardware. But with society becoming more and more reliant on keeping all manner of confidential material on their computers or in cloud-storage, the need to ensure the CPU is secure is even more important.

D. AMD Fails to Provide a Remedy

59. The security flaws were not inadvertently created but rather intended to be part of the CPU and are inherent in the design of the CPU itself. AMD simply failed to perform any testing to determine if these designs would create any security vulnerabilities. A means of fixing the security vulnerabilities exposed by Spectre do not exist. "Spectre can only be mitigated – not fixed

[12] *See* Larrry Greenemeier, *supra*.

[13] *See* King and Kahn, *supra*.

– at this time" because the flaw's vast impact to "operating systems, drivers, Web servers and databases."[14] most experts agree Spectre may require an actual change to the firmware of the CPU, a far more difficult repair in addition to changes to the OS system. There are some experts that believe a fundamental change in the design of CPUs is necessary and only after a new generation of CPUs without these design flaws will these vulnerabilities be permanently removed.

60. Given these security vulnerabilities were created by AMD's desire to increase processor speed, it is not surprising any "fix" or "patch" would have the opposite effect of slowing down processing speed. As *The Register* explained in discussing the impact of the software patches:

> It allows normal user programs – from database applications to JavaScript in web browsers – to discern to some extent the layout or contents of protected kernel memory areas.
>
> The fix is to separate the kernel's memory completely from user processes using what's called Kernel Page Table Isolation, or KPTI. […]
>
> The downside to this separation is that it is relatively expensive, time wise, to keep switching between two separate address spaces for every system call and for every interrupt from the hardware. These context switches do not happen instantly, and they force the processor to dump cached data and reload information from memory. ***This increases the kernel's overhead and slows down the computer.***

See John Leyden and Chris Williams, *Kernel-memory-leaking Intel Processor design flaw forces Linux, Windows redesign*. The Register (Jan 2, 2018) https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/

61. As *The Register* reported on January 2, 2018, "[t]he effects are still being benchmarked, however we're looking at ***a ballpark figure of five to 30 per cent slow down***,

[14] *See* Greenemeier, *supra*.

depending on the task and the processor model."[15] The Register further noted, "***It has to be fixed in software at the OS level or go buy a new processor without the design blunder".***

62. Even assuming these patches were exactly as planned, it would still be improper to term these patches as "fixes." As one expert noted the patches are simply "a set of workarounds … they aren't a fix. They just change the system behavior to avoid using the bad-designed part of the CPU."[16] Spectre takes advantage of design flaws created to increase processing speed. Given any patch acts as a workaround to these design flaw, and not a true "fix," there would inevitably be a decrease in performance since the patch avoids utilizing these processes that would otherwise increase processing speed. Further, experts agree that these patches serve as mitigations to minimize the risk of attacks not as a complete protection.

63. Instead of full and honest disclosure to its customers, this entire occurrence and aftermath has been marred by AMD's continued concealment of material facts, half-truths and misleading statements. AMD, in concert with Intel, ARM, Google, Apple, Amazon and a few other tech giants, purposefully concealed these design flaws from the general public for at least six months.

64. In late December 2017, tech websites and message boards were full of speculation about a significant security flaw as well as theories about what the flaw might be. After seeing a detailed discussion on kernel.org about the KASLR break and a side-channel attack on a CPU, AMD executive Tom Lendacky saw public disclosure was imminent and sent an email to members of the discussion site telling them AMD processors are not susceptible to such attacks and

[15] *See* Leyden and Williams, *supra*

[16] Brooke Crothers, *To fix the Spectre, Meltdown Threat, it is always pretty*. Fox News (Jan. 19, 2018), http://www.foxnews.com/tech/2018/01/19/to-fix-spectre-meltdown-threat-it-isnt-always-pretty.html

explaining why in some detail. This email formed the basis for the January 2, 2018 article from *The Register* publicly disclosing the security vulnerabilities but noting only Intel CPUs were affected.[17]

65. The January 2, 2018 articles from *The Register* and *The Guardian* focused primarily on Intel CPUs based on Lendacky's email. Prior to the January 2nd article from *The Register*, there had been solidarity among the chip makers, Microsoft, Apple and others for more than six months to create a coordinated response to these flaws. When *The Register's* January 2 article implicated only Intel chips as possessing these flaws, AMD abandoned any solidarity with Intel and instead sought to capitalize on the article by creating the narrative this was an "Intel only" problem. Lendacky's email helped frame this initial perception and was followed by a January 3, 2018 press release from AMD misleadingly stating that AMD CPUs do not contain these flaws.

66. AMD's January 3rd press release stated, "[z]ero AMD vulnerability [to Meltdown] due to AMD architecture differences."[18] The press release also downplayed the exposure to Spectre Variant 1 by falsely noting it is "[r]esolved by software/OS updates …. Negligible performance impact expected" and for Variant 2 "[d]ifferences in AMD architecture mean there is near zero risk of exploitation of this variant."[19]

67. By January 11, 2018, AMD was forced to back-off these comments and admit that almost every AMD processor in use was vulnerable to both Variants of Spectre and instead of definitively representing a software patch would protect against Variant 1, AMD could only say

---

[17] *See* Leyden and Williams, *supra*.

[18] AMD Processors: Google Project Zero, Spectre and Meltdown (Jan. 24, 2018), https://www.amd.com/en/corporate/speculative-execution

[19] *See id*.

that "[w]e believe the threat can be contained with an operating system (OS) patch."[20] After a disastrous two-week period where the software and firmware updates caused a series of unintended problems including bricking and putting AMD supported devices in a continuous reboot cycle, AMD attempted to quell the outrage by asserting the flaw in design is an industry wide issue, not solely an AMD issue.[21]

68. The various patches the industry hurriedly pushed onto consumers have caused a litany of serious, unintended consequences such as putting computers into a continuous reboot cycle. This has led to some manufacturers to recommend customers stop downloading the patches until these issues can be rectified. Even more concerning is some of the patches, including Windows patches, are incompatible with some anti-virus software. Only a special registry created within the anti-virus software itself that noting compatibility between the update and the anti-virus software. Without the registry, the anti-virus software will completely block the patches as well all future patches. The patches aren't incompatible with just anti-virus software, the firmware updates from AMD have proven incompatible with many "older" processors leading AMD to warn owners of older processors not to download the patches.

69. The belief the current flawed CPU designs cannot be fixed and only a new chip without these flaws will fix the security vulnerabilities is bolstered by the fact Intel's CEO Brian Krzanich announced on January 25, 2018 that Intel expects to ship a newly designed chip without

[20] *See* fn 18.

[21] White Paper, *Software Techniques for Managing Speculation on AMD Processors,* http://developer.amd.com/wordpress/media/2013/12/Managing-Speculation-on-AMD-Processors.pdf (last visited January 26, 2018)

these flaws by the end of 2018.[22] Although, Krzanich did not specify whether these will be newly designed chips or revisions to their current generation of processors it shows the CPU manufacturers do not believe these vulnerabilities can be cured by patches, which are nothing more than attempts to bypass the security flaws and mitigate the risk. The x86 CPU manufacturers recognize these flaws are imbedded into the architecture of their CPUs and the only true fix is a newly designed CPU.

70. Indeed, many experts believe Spectre may be just the beginning of a wave of attacks leveraging these security flaws. In July 2017, Anders Fogh one of the researchers behind the discovery of these flaws, predicted that speculation execution would likely be a "Pandora's box" for future security vulnerabilities. Spectre is more a class of vulnerability than any single "security bug." Inevitably, additional security vulnerabilities will be discovered from side-channel attacks leveraging the speculative execution flaw inherent in AMD's CPUs. Plaintiff, the Class and other consumers will be dealing with Spectre and its progeny for years to come. As Paul Kocher bluntly stated, Spectre is "going to live with us for decades."[23]

71. The presence of the security vulnerabilities are material because: (1) they expose laptops, desktops, servers, smartphones, tablets, and other devices to the loss of secure and potentially confidential data and information; and (2) if any method of "patching" these vulnerabilities exists, these "patches" dramatically degrade performance speed of the CPUs which renders the performance specifications Defendant promised and consumers expected when

[22] Troy Wolverson, *Intel Plans to release chips that have built-in Meltdown and Spectre protections later this year,* (January 25, 2018) http://www.businessinsider.com/intel-says-new-spectre-and-meltdown-proof-chips-coming-this-year-2018-1

[23] Cade Metz and Nicole Perlroth, *Researchers Discovery Two Major Flaws in the World's Computers*, New York Times, (January 3, 2018), https://www.nytimes.com/2018/01/03/business/computer-flaws.html?_r=0

purchasing an AMD CPU or a device with an AMD CPU.

72. The security vulnerabilities and the lack of an adequate "patch" or "fix" are also material to a reasonable consumer because neither Plaintiff, class members, nor any reasonable consumer would have purchased the defective AMD CPUs at the prices that they did had they known or had they been told about these material facts.

73. The claims of the Plaintiff and Class are tolled under the principles of the discovery rule and fraudulent concealment tolling. Due the nature of the security flaws it was not possible for Plaintiff and Class members to have reasonably discovered through the exercise of reasonable diligence the existence of these security flaws and accompanying vulnerabilities. Nor did any facts exist that would have placed a reasonable consumer on notice as to these potential security flaws and vulnerabilities. Further, principles of fraudulent concealment tolling are applicable as AMD concealed from Plaintiff and Class information about the security flaws herein. AMD's failure to disclose this information, prevented Plaintiff and Class from discovering the security flaws until the public disclosure of these flaws on or about January 3, 2018. It would be inequitable to allow AMD to capitalize on its concealment of these material facts by asserting a statute of limitations defense.

CLASS ACTION ALLEGATIONS

74. Plaintiff brings this class action claim pursuant to Rule 23 of the Federal Rules of Civil Procedure and seeks to certify classes under Rule 23(b)(2) and (b)(3). The requirements of Rule 23 are met with respect to the class defined below.

75. Plaintiff brings his claims on his own behalf, and on behalf of the following class (the "Class"):

> All persons or entities in the United States that purchased one or more AMD CPUs from AMD and/or its authorized retailer sellers and/or purchased a desktop, laptop,

server or other computing device containing an AMD CPU with the Spectre security vulnerabilities. Excluded from the Class are Defendant, its officers and directors at all relevant times, members of immediate families and their legal representatives, heirs, successors, or assigns and any entity in which the Defendant had a controlling interest.

76. Plaintiff reserves the right to amend or modify the Class definition in connection with a motion for class certification and/or the result of discovery. This lawsuit is properly brought as a class action for the following reasons.

77. The Class is so numerous that joinder of the individual members of the proposed Class is impracticable. The Class includes thousands of persons geographically dispersed throughout the United States. The precise number and identities of Class members are unknown to Plaintiff but are known to Defendant or can be ascertained through discovery, using records of sales, warranty records, and other information kept by Defendant or their agents.

78. Plaintiff does not anticipate any difficulties in the management of this action as a class action. The Class is ascertainable, and there is a well-defined community of interest in the questions of law and/or fact alleged herein since the rights of each Class member were infringed or violated in similar fashion based upon Defendant's uniform misconduct. Notice can be provided through sales and warranty records and publication.

79. Questions of law or fact common to the Class exist as to Plaintiff and all Class members, and these common questions predominate over any questions affecting only individual members of the Class. Among these predominant common questions of law and/or fact are the following:

a. Whether Defendant's' CPUs possess the security vulnerabilities and the nature of the security flaws;

b. Whether Defendant made any implied warranties in connection with the sale of the defective CPUs;

c. Whether Defendant breached any implied warranties relating to their sale of defective CPUs by failing to resolve the security vulnerabilities in the manner required by law;

d. Whether Defendant was unjustly enriched by selling defective AMD CPUs;

e. Whether a reasonable consumer would find the failure to disclose the existence of these security flaws a material omission;

f. Whether the security flaws render the AMD CPUs unmerchantable and unfit for their particular purpose;

g. Whether Defendant's CPUs are vulnerable to the Spectre security flaws;

h. Whether Defendant's CPUs are defectively designed;

i. Whether Defendant had a duty to disclose the security flaws to purchasers of affected CPUs;

j. Whether Defendant made any express warranties in connection from the sale of its CPUs;

k. Whether Defendant breached any express warranties arising from the sale of its CPUs;

l. Whether Defendant's acts and practices would deceive a reasonable consumer;

m. Whether Defendant violated applicable consumer protection laws by selling CPUs with the security vulnerabilities and/or by failing to disclose the security flaws, and failing to provide the relief required by law; and

n. The appropriate nature and measure of Class-wide relief.

80. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff and the Class. Individual questions, if any, pale by comparison to the numerous common questions that predominate.

81. Plaintiff's claims are typical of the claims of Class members. The injuries sustained by Plaintiff and the Class flow, in each instance, from a common nucleus of operative facts based on the Defendant's' uniform conduct as set forth above. The defenses, if any, that will be asserted against Plaintiff's claims likely will be similar to the defenses that will be asserted, if any, against

Class members' claims.

82. Plaintiff will fairly and adequately protect the interests of Class members. Plaintiff has no interests materially adverse to or that irreconcilably conflict with the interests of Class members and have retained counsel with significant experience in handling class actions and other complex litigation, and who will vigorously prosecute this action.

83. A class action is superior to other available methods for the fair and efficient group-wide adjudication of this controversy, and individual joinder of all Class members is impracticable, if not impossible because a large number of Class members are located throughout the United States. Moreover, the cost to the court system of such individualized litigation would be substantial. Individualized litigation would likewise present the potential for inconsistent or contradictory judgments and would result in significant delay and expense to all parties and multiple courts hearing virtually identical lawsuits. By contrast, the conduct of this action as a class action presents fewer management difficulties, conserves the resources of the parties and the courts, protects the rights of each Class member and maximizes recovery to them.

84. Defendant has acted on grounds generally applicable to the entire Class, thereby making final injunctive relief or corresponding declaratory relief appropriate with respect to the Class as a whole.

COUNT I
Breach of Implied Warranty

85. Plaintiff hereby incorporates all the above allegations by reference as if fully set forth herein. Plaintiff asserts this count individually and on behalf of the proposed Class.

86. Defendant and its authorized agents and resellers sold AMD CPUs or desktops, laptops, servers or other computing device containing an AMD CPU to Plaintiff and Class members in the regular course of business.

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

88. Pursuant to agreements between Defendant and its authorized agents and re-sellers, the retailers from which Plaintiff and Class members purchased their defective AMD CPUs are authorized retailers and authorized CPU service facilities. Plaintiff and Class members are third-party beneficiaries of, and substantially benefited from, such contracts.

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

90. The security vulnerabilities in the AMD CPUs existed when the CPUs left Defendant's and their authorized agents' and retail sellers' possession and thus are inherent in such CPUs.

91. As a direct and proximate result of Defendant's breach of its implied warranties, Plaintiff and Class members have suffered damages and continue to suffer damages, including

economic damages at the point of sale in terms of the difference between the value of the CPUs as warranted and the value of the CPUs as delivered. Plaintiff and Class members did not receive the benefit of their bargain when purchasing the CPUs. Additionally, Plaintiff and Class members either have or will incur economic, incidental and consequential damages in the cost of repair or replacement and costs of complying with continued contractual obligations as well as the cost of buying an additional CPU they would not have purchased had the CPUs in question not contained the non-repairable security flaws.

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

COUNT II
Song-Beverly Warranty Act, California Civil Code § 1792, *et seq*.

93. Plaintiff incorporates the allegations in paragraphs 1 – 84 by reference as if fully set forth herein. Plaintiff asserts this claim individually and on behalf of all Class members.

94. Under the Song-Beverly Consumer Warranty Act, California Civil Code § 1792, *et seq.*, every sale of consumer goods in the State of California is accompanied by both a manufacturer's and retail seller's implied warranty that the goods are merchantable and an implied warranty of fitness.

95. Plaintiff and the Class members who bought at retail in California each purchased one or more AMD CPUs directly from AMD or its authorized retailers or a desktop, laptop, server or other computing device containing an AMD CPU, which are "consumer goods" within the meaning of California Civil Code § 1791.

96. Defendant is in the business of manufacturing and selling AMD CPUs to retail buyers, and therefore is a "manufacturer" and "seller" within the meaning of California Civil Code

§ 1791.

97. Defendant impliedly warranted to Plaintiff and Class members that the AMD CPUs were merchantable and fit for the ordinary and particular purposes for which the CPUs are required and used.

98. Defendant has breached implied warranties because the AMD CPUs sold to Plaintiff and Class members were not merchantable and were not fit for the ordinary and particular purposes for which such goods are used in that the CPUs suffer from critical security flaws. If these vulnerabilities can be secured it will require at a minimum an OS-level software and firmware patch that will degrade the performance of the CPU. It is not necessary for Plaintiff to prove the cause of the security vulnerabilities in the CPUs, but only that the CPUs did not conform to the applicable warranties.

99. As a direct and proximate cause of AMD's breach of the Song-Beverly Act, Plaintiff and Class members sustained damages and other losses in an amount to be determined at trial, entitling them to compensatory damages, consequential damages, statutory damages and civil penalties, diminution in value, costs, attorneys' fees and interest, as applicable.

COUNT III
Consumers Legal Remedies Act, California Civil Code § 1750 *et seq*.

100. Plaintiff incorporates the allegations in paragraphs 1 – 84 by reference as if fully set forth herein. except those allegations seeking a damages award. Plaintiffs asserts this claim individually and on behalf of all Class members.

101. Plaintiff asserts this claim individually and on behalf of all Class members under California Civil Code §1781.

102. The Consumers Legal Remedies Act ("CLRA") was enacted to protect consumers against unfair and deceptive business practices. The CLRA applies to Defendant's acts and

practices because it covers transactions involving the sale of goods to consumers.

103. The AMD CPUs are "goods" under California Civil Code §1761(a).

104. AMD is a "person" under California Civil Code §1761(c).

105. Plaintiff and the Class members are "consumers" under California Civil Code §1761(d).

106. Plaintiff and Class members engaged in "transactions" under California Civil Code §1761(e), including the purchase of AMD CPUs, or a laptop, desktop, server or other computing device with an AMD CPU, containing these security vulnerabilities.

107. AMD's unfair and deceptive business practices were intended and did result in the sale of AMD CPUs, a defective consumer product.

108. Defendant's AMD CPUs failed to perform in accordance with their expected characteristics, uses and benefits.

109. Defendant had exclusive knowledge of material facts, *i.e.* the AMD CPUs contained material security flaws, unknown to Plaintiff and Class members. If Plaintiff and Class members had known of the security flaws in the AMD CPU, they would not have purchased the CPUs at the prices they did, if at all.

110. Defendant had a duty to disclose the security vulnerabilities in the AMD CPUs for various reasons, including:

a. AMD had exclusive knowledge of the security vulnerabilities and other material facts not known to Plaintiff or the Class;

b. AMD actively concealed a material fact from Plaintiff and the Class;

c. AMD made partial representations but concealed some material facts from Plaintiff and the Class.

111. Defendant engaged in unfair and deceptive practices by misrepresenting or not disclosing the above material facts from Plaintiff and the Class, in violation of Cal. Civ. Code

§1770(a)(5), (7), (14) and (16).

112. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class members suffered injury. Plaintiff and Class members are entitled to injunctive relief, court costs and attorney fees, and other relief the Court deems proper.

113. At this time, Plaintiff only seek injunctive relief and do not seek an award of damages under the CLRA.

COUNT IV

Violation of California's Unfair Competition Law, Bus. & Prof. Code § 17200, et. seq.

114. Plaintiff incorporates the allegations in paragraphs 1 – 84 by reference as if fully set forth herein. Plaintiff asserts this claim individually and on behalf of all Class members.

115. Defendant's business acts and practices complained of were centered in, carried out, effectuated and perfected within or had their effect in the State of California, and injured Plaintiff and all Class members.

116. Beginning as early as 2008, continuing thereafter at least up through and including the date of filing this Complaint, Defendant committed acts of unfair competition, as defined by §17200, *et seq.*, of the California Business and Professions Code, by engaging in the acts and practices specified above.

117. This claim is brought pursuant to §§17203 and 17204 of the California Business and Professions Code to obtain equitable monetary and injunctive relief from Defendant for acts and practices as alleged herein that violated §17200 of the California Business and Professions Code, commonly known as the Unfair Competition Law.

118. Defendant's conduct as alleged herein violated §17200. The acts, omissions, practices and non-disclosures of Defendant constituted a common continuous course of conduct of unfair competition by means of the commission of unfair and unlawful business acts or practices

within the meaning of California Business and Professions Code, §17200, *et seq.*

119. Defendant engaged in "unlawful" business acts and practices by:

a. violating the Song-Beverly Consumer Warranty Act, California Civil Code §1792, *et seq.*;

b. breaching implied warranties; and

c. violating the Consumers Legal Remedies Act, California Civil Code §1750, *et seq.*

120. Defendant engaged in "unfair" business acts and practices by, among other things:

a. engaging in conduct where the utility of such conduct, if any, is outweighed by the gravity of the consequences to Plaintiff and the Class considering the reasonably available alternatives, based on legislatively declared policies not to sell unmerchantable and flawed products in the market without providing an adequate remedy therefor;

b. engaging in conduct that is immoral, unethical, oppressive, unscrupulous, or substantially injurious to Plaintiff and the Class; and

c. engaging in unfair business practices by refusing to repair or recall the unmerchantable and flawed AMD CPUs or providing compensation therefor.

121. Specifically, Defendant engaged in "unfair" business acts and practices by selling the AMD CPUs knowing or being aware the CPUs contained critical security vulnerabilities, where the OS-level software patch would degrade the processors performance. Defendant also engaged in unfair business acts and practices by making express and implied warranties, which it refuses to honor.

122. As such conduct is or may well be continuing and on-going, Plaintiff and each of the Class members are entitled to injunctive relief to prohibit or correct such on-going acts of unfair competition, in addition to obtaining equitable monetary relief.

123. Plaintiff and Class members used Defendant's products and had business dealings with Defendant either directly or indirectly as described above. The acts and practices of Defendant

have caused Plaintiff and Class members to lose money and property by being overcharged for and paying for the unmerchantable and flawed CPUs at issue or being required to purchase an additional working CPU. Such loss was the result of the above acts of unfair competition and Defendant's misconduct in violation of the state laws set forth above. Plaintiff are therefore entitled to seek recovery of such amounts. Such injury occurred at the time such monies were paid. Plaintiff have thus each suffered injury in fact and lost money or property as a result of such acts and practices as set forth in detail above.

124. Defendant has unjustly benefited as a result of its wrongful conduct and its acts of unfair competition. Plaintiff and Class members are accordingly entitled to equitable relief including restitution and/or restitutionary disgorgement of all revenues, earnings, profits, compensation, and benefits that have been obtained by Defendant as a result of such business acts and practices, pursuant to California Business and Professions Code §§17203 and 17204, as well as attorneys' fees and costs pursuant to, among others, California Code of Civil Procedure §1021.5.

COUNT V
Common Counts – Assumpsit, Restitution, Unjust Enrichment and/or Quasi-Contract

125. Plaintiff incorporates the allegations in paragraphs 1 – 84 by reference as if fully set forth herein. Plaintiff asserts this claim individually and on behalf of all Class members.

126. This cause of action is alleged as an alternative to the warranty claims as permitted under Rule 8(d)(2) of the Federal Rules of Civil Procedure.

127. As Plaintiff and the Class show just grounds for recovering money paid for benefits Defendant received from them, either directly or indirectly, and they have a right to restitution at law through an action derived from the common-law writ of assumpsit by implying a contract at law based on principles of restitution and unjust enrichment, or though quasi-contract.

128. Defendant, having received such benefits, is required to make restitution. The circumstances here are such that, as between the two, it is unjust for Defendant to retain such benefit based on the conduct described above. Such money or property belongs in good conscience to the Plaintiff and Class members and can be traced to funds or property in Defendant's possession. Plaintiff and Class members have unjustly enriched Defendant through payments and the resulting profits enjoyed by Defendant as a direct result of such payments. Plaintiff's detriment and Defendant's enrichment were related to and flowed from the conduct challenged in this Complaint.

129. By virtue of the purchase and sale of the CPUs in question, Defendant alternatively entered into a series of implied-at-law or quasi-contracts that resulted in money being had and received by Defendant, either directly or indirectly, at the expense of Plaintiff and Class members under agreements in assumpsit. Plaintiff and other Class members conferred a benefit upon Defendant by purchasing one of the unmerchantable and flawed CPUs. Defendant had knowledge of the general receipt of such benefits, which Defendant received, accepted and retained. Defendant owes Plaintiff and Class members these sums that can be obtained either directly from Class members, Defendant or its authorized retailers.

130. Under principles of restitution, an entity that has been unjustly enriched at the expense of another by the retention of benefit wrongfully obtained is required to make restitution to the other. In addition, under common law principles recognized in claims of common counts, assumpsit, unjust enrichment, restitution, and quasi-contract, under the circumstances alleged herein it would be inequitable for Defendant to retain such benefits without paying restitution or restitutionary damages. Such principles require Defendant to return such benefits when the retention of such benefits would unjustly enrich Defendant. They should not be permitted to retain

the benefits conferred by Plaintiff and Class members via payments for the defective CPUs. Other remedies and claims may not permit them to obtain such relief, leaving them without an adequate remedy at law.

131. Plaintiff and Class members seek appropriate monetary relief for such claims. In addition, pursuant to California Civil Code § 2224, "[o]ne who gains a thing by fraud, accident, mistake, undue influence, the violation of a trust, or other wrongful act, is, unless he or she has some other and better right thereto, an involuntary trustee of the thing gained, for the benefit of the person who would otherwise have had it." Based on the facts and circumstances alleged above, in order to prevent unjust enrichment and to prevent Defendant from taking advantage of its own wrongdoing, Plaintiff and the Class are further entitled to the establishment of a constructive trust, in a sum certain, of all monies charged and collected or retained by Defendant from which Plaintiff and Class members may seek restitution.

COUNT VI
Strict Liability

132. Plaintiff incorporates the allegations in paragraphs 1 – 84 by reference as if fully set forth herein. Plaintiff asserts this claim individually and on behalf of all Class members.

133. At all times relevant to this action, Defendant engaged in the business of designing, manufacturing, testing, marketing and/or placing into the stream of commerce AMD CPUs for sale to, and use by, members of the public, including Plaintiff.

134. Plaintiff and the Class were harmed by CPUs Defendant manufactured, designed, marketed and sold, which were contained in, but also separate and apart from, the computers they purchased.

135. Defendant's CPUs contained a manufacturing defect and/or were defectively designed for the reasons set forth above.

136. As a direct and proximate result of AMD's wrongful conduct, Plaintiff and Class members have been harmed, as they now own a computer with a CPU that contains security flaws inherent in the design of the CPU that exposes AMD CPU owners to the loss of confidential, secure information stored in kernel data. One of the core principles of the CPU is to prevent any non-privileged user from accessing secure, privileged kernel data which is exactly what these security flaws allow. Further, the "updates" from AMD that are intended to "patch" the security flaws, have caused a litany of other problems including bricking computers, causing the reboot cycle to continually reboot and significantly degrading the performance of many computer operations. The unintended damage from these "patches" was so great, AMD began advising customers not to download them.

COUNT VII
Negligence

137. Plaintiff incorporates the allegations in paragraphs 1 – 84 by reference as if fully set forth herein. Plaintiff asserts this claim individually and on behalf of all Class members.

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

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

140. Plaintiff and Class members purchased computers with CPUs that contain defects which are separate and apart from the computers, themselves.

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

COUNT VIII
Violation of Ohio Rev. Code § 1345.01(A) and (B)

142. Plaintiff incorporates the allegations in paragraphs 1 – 84 as if fully set forth herein. Plaintiff asserts this claim individually and on behalf of a subclass of Class members who reside in Ohio.

143. AMD engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code § 1345.01(A) and (B), including but not limited to the following:

a. Marketing and selling a product with a security flaw in it;

b. Knowingly and fraudulently misrepresenting that its product would perform as advertised as it relates to security and speed even though it is not possible; and

c. Omitting, suppressing, and concealing the material fact of the inadequacy of its product to be both secure and perform as intended at the same time.

144. The above unfair and deceptive acts and practices and acts by AMD were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Ohio Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

145. AMD knew or should have known that its microprocessors were inadequate to safeguard the Ohio Subclass members' personal and sensitive information and that risk of a data breach or theft was highly likely. AMD's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

146. Moreover, rather than acknowledge the Spectre security flaws in its CPUs and sell the AMD processors with the patch, AMD continued to market the CPUs as fast, despite that the patch would significantly slow down processing speeds.

147. As a direct and proximate result of these violations, the Plaintiff and Class members suffered actual damages as set forth herein.

148. Pursuant to Ohio Rev. Code § 1345.09, Plaintiff and the Ohio Subclass members seek an order enjoining AMD's unfair and/or deceptive acts or practices actual damages, trebled (to be proven at the time of trial), and attorneys' fees, costs, and any other just and proper relief, to the extent available under the Ohio Consumer Sales Practices Act, Ohio Rev. Code §§ 1345.01, *et seq*.

149. As such conduct is or may well be continuing and on-going, Plaintiff and each of the Class members are entitled to injunctive relief to prohibit or correct such on-going acts of unfair competition, in addition to obtaining equitable monetary relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and all Class members pray for judgment against Defendant as follows:

A. Declaring this action to be a proper class action pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Awarding Plaintiff and Class members all proper measures of equitable monetary relief and damages (damages excluded at this time for violations of the CLRA), plus interest to which they are entitled;

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

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

E. Granting such further and other relief this Court deems appropriate.

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of all others similarly situated, demands a trial by jury on all issues so triable.

DATED: February 4, 2018

Respectfully Submitted,

/s/ Chris W. Cantrell
William J. Doyle II (SBN 188069)
Chris W. Cantrell (SBN 290874)
DOYLE APC
550 West B St., 4th Floor
San Diego, CA 92101
Telephone: (619) 736-0000
Facsimile: (619) 736-1111
E-mail: bill@doyleapc.com
E-mail: chris@doyleapc.com

J. Gerard Stranch, IV (pending admission *pro hac vice)*
Benjamin A. Gastel (pending admission *pro hac vice)*
Tricia Herzfeld (pending admission *pro hac vice)*
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Telephone: 615/254-8801
Facsimile: 615/255-5419
E-mail: gerards@bsjfirm.com
E-mail: beng@bsjfirm.com

Adam J. Levitt (pending admission *pro hac vice*)
Amy E. Keller (pending admission *pro hac vice)*
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street, Eleventh Floor
Chicago, Illinois 60602
Telephone: (312) 214-7900
Email: alevitt@dlcfirm.com
Email: akeller@dlcfirm.com

Jeffrey L. Fazio (SBN 146043)
Dina E. Micheletti (SBN 184141)
FAZIO | MICHELETTI LLP
2410 Camino Ramon, Suite 315
San Ramon, California 94583
Telephone: (925) 543-2555
Facsimile: (925) 369-0344
Email: jlf@fazmiclaw.com
Email: dem@fazmiclaw.com

Attorneys for Plaintiff and Class