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

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

Attorneys for Plaintiffs and the Proposed Classes

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

TARAN PIETOSI and SUKHDIP RAI, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

HP, INC., a Delaware corporation,

Defendant.

Case No. 5:22-cv-4273

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

INTRODUCTION

1. Watching videos, listening to music or other audio, videoconferencing, and playing games are key—indeed, indispensable—activities on modern personal computers (PCs). Indeed, it is no stretch to say that in 2022, a desktop or laptop PC that can't play video or audio, or run videoconferencing software, or render a computer game, without experiencing intrusive stuttering, is unworthy of sale.

2. So, too, is a baseline level of hardware security—one recognized by Microsoft as necessary to mitigate the risk and effect of devastating firmware attacks—a central part of the baseline bargain expected by modern PC consumers. In a world in which virtually every aspect of an American's life is performed at least in part through their computer, a desktop or laptop that is uniquely vulnerable to known, crippling attack vectors is not a computer that consumers seek to buy.

3. Yet Defendant HP Inc. ("HP") makes, markets, and sells exactly these types of seriously flawed desktop and laptop computers. Numerous HP PCs—specifically, HP computers with AMD Ryzen or Athlon processors that have so-called "firmware TPM" ("fTPM") modules embedded within them—include a design defect that causes invasive stuttering in audio and video playback, during videoconferencing, and while playing games. At the same time, this design defect renders these HP computers uniquely vulnerable to catastrophic firmware attacks—despite the fact that a TPM is, by its very nature, supposed to *defend* against such attacks.

4. HP, however, does not acknowledge any of this. Instead, on its website and elsewhere HP specifically markets its AMD desktop and laptop computers as especially suited for watching video, for videoconferencing, and for gaming. HP also touts these computers' "enterprise-level" security.

5. The Plaintiffs in this case each purchased HP computers with AMD processors that include AMD's defective fTPM design. They have all experienced severe stuttering in media playback; in videoconferencing; and/or in gameplay. Their computers are also uniquely vulnerable to firmware attacks that could compromise not just Plaintiffs' HP computers, but potentially their home or business networks. The AMD fTPM design defect and its manifestations has significantly—perhaps totally—impaired the value of Plaintiffs' HP PCs, as they are unfit for their intended use, and their resale value is crippled. Despite this—and despite growing complaints about the performance of AMD-based HP

computers in HP forums and across the Internet—HP has done nothing to fix or replace its defective computers.

6. Plaintiffs and those similarly situated—*i.e.*, other persons who have purchased HP computers that include defective AMD processors—bring this lawsuit against HP in order to be made whole.

* * *

7. HP designs, manufactures, and sells desktop and laptop personal computers. For almost all of the PCs it sells, HP incorporates central processing units ("CPUs") from one of two manufacturers, AMD and Intel. On its website (hp.com) and elsewhere, HP touts its computers, including specifically its AMD-based PCs, as providing smooth playback of audio and video, videoconferencing, and gameplay.

8. HP also advertises and markets the security features of its AMD-based PCs, including their compliance with the security requirements of the leading PC operating system, Microsoft Windows 11. HP preinstalls Windows 11 on most of its PCs.

9. HP advertises its AMD-based PCs jointly with AMD itself, including on pages and posts within hp.com that proclaim the benefits of AMD-based PCs made by HP.

10. HP is deeply involved with the design of its PCs, including as to the CPUs it incorporates into its PCs. HP's AMD-based PCs, which include AMD Ryzen and Athlon processors, are designed and customized to fit the power consumption and use profiles suited for HP's customers.

11. Put simply, HP and AMD work hand in hand to integrate AMD CPUs into HP PCs sold to end-users.

12. In June 2021, in response to a striking increase in so-called "firmware attacks"—devastating cyberattacks that allow an attacker to compromise low-level CPU, memory, and hardware resources of computer before an operating system even loads—the leading operating system maker, Microsoft, resolved to act. Specifically, Microsoft decided to require, as a precondition for running its upcoming operating system Windows 11, a specific piece of hardware designed to separate sensitive cryptographic and other security-related resources from the main CPU and system memory—a Trusted Platform Module ("TPM").

13. Because a TPM was a separate hardware device from the system's CPU, it could protect important computer security resources—such as the system's random number generator and private keys used for encryption—from being compromised. That is, even if the system's CPU, memory, and operating system had been attacked, the secrets stored in the TPM would remain safe. For Microsoft, requiring a TPM meant implementing a broad-based minimum level of security that was uniform and consistent with a detailed specification, called the TPM 2.0 standard.

14. HP, which pre-installs Windows software on its PCs, accordingly faced a new and significant design requirement for its computers. That is, to make sure that its PCs were compatible with the newest version of Windows (Windows 11), HP had to ensure that every one of its desktop and laptop computers included an onboard TPM.

15. Faced with a potentially burdensome redesign, HP turned to AMD, which had created and implemented what was essentially a defeat device for Microsoft's new TPM requirement: a "firmware TPM," or simply "fTPM." Not an actual TPM—*i.e.*, a discrete piece of hardware to protect and segregate security-sensitive information and operations from the main system processor and memory—in any historical or computer security sense, AMD's fTPM was simply a piece of code that announced itself to the system (and critically, to Windows 11) as a "TPM." AMD implemented this firmware "TPM" as part of its Platform Security Processor (PSP)—and ARM-based embedded processor within the overall AMD CPU package. The PSP had direct access to sensitive and privileged CPU and memory resources, and as such, so did the fTPM module AMD had incorporated within it.

16. Implementing fTPM as part of the AMD PSP subsystem meant that the co-processor that ran that subsystem would be further taxed, sharing resources and memory with the fTPM. A micro-operating system called a Trusted Execution Environment ("TEE") sliced the PSP subsystem's scarce resources between the fTPM and numerous other firmware-based systems that ran as part of the PSP, including, for example, DRM software that enables the decryption of streaming video and/or audio.

17. Not only did AMD's fTPM design ironically implement a security module designed to prevent firmware attacks ***in the firmware itself***, it did so in a way that exposed sensitive system resources to the fTPM. But for HP, fTPM avoided a major hassle: HP would not need to ship new hardware with

its AMD-based PCs in order to make them compatible with Windows 11. Instead, HP could simply ensure that fTPM—a piece of code that tells the operating system it's a TPM—was enabled on its AMD-based systems, and this would satisfy Windows 11's security checks.

18. Of course, the fTPM merely checked a box for Windows 11—it was not an *actual* Trusted Platform Module. Indeed, AMD's fTPM not only failed to accomplish the very reason for being of a TPM—hardware segregation of cryptographic keys and other security-sensitive information from system resources, the CPU, and system memory, which reduces the risk and effect of firmware attacks—it made the problem of firmware attacks ***worse***. Compromising AMD's PSP subsystem, which hackers had repeatedly done since at least the end of 2018, now meant potentially compromising all the security-sensitive resources of the entire system—all conveniently grouped in one software-based module for the attacker. HP's design of its new AMD-based PCs left users ***more*** vulnerable to firmware attacks, under the guise of bolstering system security and ensuring compliance with Windows 11's system security requirements.

19. The flawed CPU design had at least two resultant effects on HP's AMD-based PCs.

20. ***First***, because the fTPM was implemented as part of the PSP, which could directly access system memory and CPU resources, particularly when users' PCs must decrypt audio and video content (*e.g.*, when streaming video from Netflix), interactions with fTPM meant potentially delaying the function of other systems implemented in the PSP that were required for smooth playback or time-sensitive memory or CPU interactions.

21. The result was the catastrophic stuttering of playback on HP PCs with AMD Ryzen and Athlon processors. Reports flooded online forums and YouTube channels describing HP and other AMD-based PCs stuttering when playing back video, when playing audio, or both. The stuttering also affected video conferencing—a staple in the post-pandemic work-from-home environment. And, with respect to gamers, whom HP directly targets for PC sales, the defective HP PCs would stutter when playing video games. In YouTube video after YouTube video, users showed the stuttering effect in various popular computer games being run (or attempting to run) on HP and other AMD-based computers. Despite HP's promises that its AMD-based PCs were suitable for ordinary uses, such as watching video, listening to

music, video conferencing, and playing games, its AMD PCs stuttered during each of these baseline applications.

22. ***Second***, the flawed fTPM design left HP's AMD-based PCs vulnerable to cyberattacks that exploit a PC's firmware. This sort of attack was (and is) especially pernicious, as it allows a hacker to access a computer system's most sensitive resources (*e.g.*, its Basic Input Output System ("BIOS")) before the operating system even comes online. Even though HP purported to make systems, particularly those running Windows 11, more secure from such attacks, the design of its AMD-based PCs did the opposite.

23. Despite the swelling of complaints over several years by HP's customers that its AMD-based PCs had significant stuttering problems, HP did nothing. It never ordered a recall of its PCs to replace the faulty CPUs (*e.g.*, with Intel CPUs that did not have the design defect) or to provide purchasers with comparable PCs that did not have the design defect. HP never as much as acknowledged the problem. It kept selling its AMD-based PCs, and indeed kept making false and misleading statements and omissions about the PCs' functionality and security.

24. On March 8, 2022, the dam broke. AMD finally recognized that there was a problem. AMD explained that systems running Windows 10 and 11 that enabled its fTPM subsystem would experience "intermittent system sutter[ing]." The release by AMD tersely blamed the stuttering on its CPUs "intermittently perform[ing] extended fTPM-related memory transactions in SPI flash memory ('SPIROM') located on the motherboard," which AMD explained led to "temporary pauses in system interactivity or responsiveness until the transaction is concluded."

25. The problem arose, however, from the flaw in the fTPM's design: it shared resources with the PSP subsystem, including flash memory (such as SPIROM), which in turn had access to the PC's CPU and memory resources. When the fTPM consumed too much of the PSP's scarce processing power and its TEE micro-operating system failed to prioritize time-sensitive needs of the overall PC, this caused the entire system to stutter. This happened in predictable—but critical—circumstances, such as media playback, videoconferencing, or gameplay.

26. The stuttering had revealed a deep flaw in the AMD-based CPUs that HP incorporated into its PCs, including desktop and laptop computers that HP designs, markets, and sells as specially adapted for media playback, videoconferencing, and gameplay.

27. AMD provided no meaningful fix for the problem, recommending that owners of AMD-based systems buy external hardware TPMs, potentially at significant additional cost. Although AMD signaled that firmware updates may be available through individual PC and hardware manufacturers (such as HP), there was no true fix possible. The flawed fTPM design, which implemented what should have been—by definition—a segregated hardware module in the CPU's firmware, remained fatally defective. No fix could cure the security problem that resulted, nor could there be a fix for the fundamental problem that had caused the stuttering—the fTPM is part of a PSP subsystem that can and frequently does access the PC's sensitive CPU and memory resources, including for DRM tasks.

28. The design flaw in AMD's CPUs—and in the HP computers incorporating them—leads to two substantial Effects: (1) intrusive stuttering during media playback, videoconferencing, and gameplay; and (2) elevated vulnerability to firmware attacks. Each of these Effects had a direct and quantifiable demand and price effect on defective AMD-based PCs sold by HP. Based on a pre-complaint statistical conjoint study (described in Section VI of this Complaint), (i) the defective HP PCs were worth less at purchase than the price Plaintiffs and Class Members paid for them, resulting in an out-of-pocket loss at purchase; (ii) each Effect caused a diminution in value of HP's AMD-based PCs owned by Plaintiffs and Class Members; and (iii) these PCs will remain defective until HP recalls and replaces the faulty AMD CPUs in Plaintiffs' and Class Members' PCs.

29. This lawsuit seeks to recover this out-of-pocket loss and diminution in value to Plaintiffs' and Class Members' HP PCs, and seeks an injunction requiring HP to replace the PCs that include the defective AMD CPUs.

PARTIES

I. PLAINTIFFS

30. Taran Pietosi is a domiciled resident of Pennsylvania, residing in West Mifflin. In 2020, Ms. Pietosi purchased a new HP All-in-One 22-df0xxx laptop with an AMD Ryzen 3 processor from

Walmart. Ms. Pietosi reviewed and relied upon marketing materials and advertisements concerning the HP laptop prior to purchasing it. Ms. Pietosi purchased her laptop for the specific purpose of working from home, including voice and video calls, web chat, and the ability to run multiple programs at once. She planned to play games on her computer as well, but has been mostly unable to do that upon realizing that her processor was unable to run tasks like gaming smoothly. Since purchasing her laptop, Ms. Pietosi has experienced stuttering during media playback, video calls, voice calls, and gameplay. Ms. Pietosi experiences stuttering on her laptop almost every time she uses any type of audio. None of the representations received and reviewed by Ms. Pietosi contained any disclosure relating to the defectively designed AMD fTPM in her computer. None of the representations received and reviewed by Ms. Pietosi disclosed that her computer would be uniquely vulnerable to firmware attacks, nor that it would experience stuttering, because of a defectively designed AMD processor. Ms. Pietosi would not have purchased her laptop at the price she paid had she known about the AMD fTPM defect described in this Complaint. HP has not fixed the problems with Ms. Pietosi's laptop attributable to the AMD fTPM defect, including its stuttering during audiovisual playback and/or gaming and its unique vulnerability to firmware attacks. Ms. Pietosi would like these problems fixed.

31. Sukhdip Rai is a domiciled resident of California, residing in Livingston. In 2019, Mr. Rai purchased a new HP Pavilion Gaming Desktop 690-00xx with an AMD Ryzen 7 processor from Amazon.com. Mr. Rai reviewed and relied upon marketing materials and advertisements concerning the HP laptop prior to purchasing it, including visiting hp.com prior to the purchase. The hp.com website boasted fast game play and clock speeds, particularly for gaming. Mr. Rai purchased his desktop specifically to play games, watch and edit video, and listen to audio. Since purchasing his desktop, Mr. Rai has experienced stuttering at least once or twice per month during video calls, gameplay, and video playback. Mr. Rai tried to troubleshoot the issue including performing virus and spyware checks, hard drive cleanups, and even factory-resetting his computer. None of these actions fixed the issue and the stuttering he experienced has not been fixed. None of the representations received and reviewed by Mr. Rai contained any disclosure relating to the defectively designed AMD fTPM in his computer. None of the representations received and reviewed by Mr. Rai disclosed that his computer would be uniquely

vulnerable to firmware attacks, nor that it would experience stuttering, because of a defectively designed AMD processor. Mr. Rai would not have purchased his laptop at the price he paid had he known about the AMD fTPM defect described in this Complaint. HP has not fixed the problems with Mr. Rai's laptop attributable to the AMD fTPM defect, including its stuttering during audiovisual playback and/or gaming and its unique vulnerability to firmware attacks. Mr. Rai would like these problems fixed.

II. DEFENDANT

32. Defendant HP, Inc. is a Palo Alto, California-based corporation incorporated under the laws of Delaware. HP's headquarters are located at 1501 Page Mill Road, Palo Alto, California, 94304.

33. According to HP's annual report filed with the SEC, it is a "global provider of personal computing and other access devices, imaging and printing products, and related technologies, solutions, and services." HP sells to individual consumers, to small- and medium-sized businesses, and to large enterprises, including to customers in the government, health and education sectors.

34. HP has three business segments: Personal Systems, Printing, and Corporate Investments. HP's Personal Systems segment is responsible for the design, manufacture, and sale of commercial and consumer desktop and notebook personal computers ("PCs"), as well as workstations and thin clients.

35. As HP explained in its 2021 Annual Report, HP develops these products using both Intel and AMD-based processors and targets the Windows and Google Chrome operating systems:

> Both commercial and consumer PCs maintain multi-operating system, multi-architecture strategies using Microsoft Windows and Google Chrome operating systems, and predominantly use processors from Intel Corporation ("Intel") and Advanced Micro Devices, Inc. ("AMD").

36. HP provides PCs for both commercial and consumer users, with varying product lines targeted to each group. HP describes its commercial PC products as follows:

> Commercial PCs are optimized for use by enterprise, public sector which includes education, and SMB customers, with a focus on robust design, security, serviceability, connectivity, reliability and manageability in the customer's environment and working remotely. Commercial PC include the HP ProBook and HP EliteBook lines of notebooks, convertibles and detachables, the HP Pro and HP Elite lines of business desktops and all-in-ones, retail POS systems, HP Thin Clients, HP Pro Tablet PCs and the HP notebook, desktop and Chromebook systems. Commercial PCs also

> include workstations that are designed and optimized for high-performance and demanding application environments including Z desktop workstations, Z all-in-ones and Z mobile workstations. Additionally, we offer a range of services and solutions to enterprise, public sector which includes education and SMB customers to help them manage the lifecycle of their PC and mobility installed base.

37. As to its consumer products, HP states:

> Consumer PCs are optimized for consumer usage, focusing on gaming, learning and working remotely, consuming multi-media for entertainment, managing personal life activities, staying connected, sharing information, getting things done for work including creating content, and staying informed and secure. These systems include HP Spectre, HP Envy, HP Pavilion, HP Chromebook, HP Stream, Omen by HP Lines of notebooks, desktops and hybrids, HP Envy, HP Pavilion desktops and all-in-one lines.
>
> Personal Systems groups its global business capabilities into the following business units when reporting business performance:
>
> - *Notebooks* consists of consumer notebooks, commercial notebooks, mobile workstations, peripherals, and commercial mobility devices;
> - *Desktops* includes consumer desktops, commercial desktops, thin clients, displays, peripherals, and retail POS systems;
> - *Workstations* consists of desktop workstations, displays and peripherals; and
> - *Other* consists of consumer and commercial services as well as other Personal Systems capabilities.

38. HP's PC business is highly dependent on central processing units created by AMD and Intel. As HP explained in its 2021 Annual Report:

> We are dependent upon Intel and AMD as suppliers of x86 processors and Microsoft and Google for various software products. We believe that disruptions with these suppliers would have industry-wide ramifications, and therefore would not disproportionately disadvantage us relative to our competitors.

39. HP discloses AMD and Intel as its single-source CPU suppliers, meaning that its PCs are dependent on processors from these two companies:

> Single-source suppliers. We obtain a significant number of components from a single source due to technology, availability, price, quality or other

> considerations. . . . We also rely on both Intel and AMD to provide us with a sufficient supply of processors for the majority of our PCs and workstations. Some of those processors may be customized for our products.

40. Because HP relies on processors from Intel and AMD, it must maintain a strong relationship with these two companies to avoid adverse affects to its business:

> In certain circumstances, we purchase components from single-source suppliers under short-term agreements that contain favorable pricing and other terms, but that may be unilaterally modified or terminated by the supplier with limited notice and with little or no penalty. The performance of single-source suppliers under those agreements (and the renewal or extension of those agreements upon similar terms) may affect the quality, quantity and price of our components. The loss of, deterioration of our relationship with, or limits in allocation by, a single-source supplier, or any unilateral modification to the contractual terms under which we are supplied components by a single-source supplier could adversely affect our business and financial performance.

41. HP's Personal Systems division made approximately $43.3 billion in 2021, with notebook PCs constituting the bulk of the revenue—$30.5 billion. Desktops were responsible for approximately $9.3 billion, and workstations approximately $1.7 billion, of reported 2021 revenue.

42. HP has over 50,000 employees worldwide, including at its offices in Palo Alto, California.

JURISDICTION AND VENUE

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

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

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

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

DIVISIONAL ASSIGNMENT

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

FACTS

I. THE TRUSTED PLATFORM MODULE (TPM)

A. The Advent of TPM

48. As Internet access and use proliferated in the late 1990s, computers increasingly required cryptographic operations in everyday use—including to interact with websites; to store and retrieve sensitive information; and to verify information about computer configurations, software, and content.

49. For example, secure http protocols central to e-commerce websites and online authentication; hard-drive and tape backup encryption relied upon by Enterprise IT; and digital rights management systems like iTunes and Windows Media Player, all relied upon encryption not just for added security, but for their very use. As a result, with the dawn of the 21st century came an increasing need in personal computers—both at work and at home—for a permanent (and secure place) to store encryption keys and assist the main hardware of a computer with cryptographic and other security-related operations.

50. In addition, with cryptography underpinning an ever-growing swath of everyday operations in Internet-connected personal computers, these systems increasingly relied on the soundness and integrity of random number generation to function securely. The cryptosystems used in standard Internet and other network protocols around the world rely for their security on the unpredictability (*i.e.*, randomness) of certain values; as a result, a weak or insecure random number generation can compromise the security of an entire, otherwise secure, computer system.

51. Early means of providing needed security functionality—secure key storage, secure random number generation, and often secure computation of the certain commonly-used cryptographic algorithms—relied on so-called "smart cards" or "smart chips." These devices, effectively small integrated circuits embedded in physical cards or wafers, were designed to securely store relevant cryptographic keys and identifiers associated with a particular user; the user would insert a given smart card or smart chip into a computer to facilitate secure cryptographic operations.

52. Smart cards or smart chips interacted with independently-implemented subsystems in a given computer that ensured (or more accurately, were meant to ensure) that cryptography was performed securely—*i.e.*, that cryptographic keys were securely segregated from the rest of a computer system; that a random number generator produced truly pseudo-random numbers with a particular statistical distribution[1]; and other cryptographic security requirements were met.

53. A major drawback was that respective computer manufacturers each implemented these subsystems differently, creating widespread compatibility and consistency issues for cryptographic and other security-sensitive processing operations, particularly in large companies that deployed thousands of computers across their workforce.

54. The logical solution was to create a standardized, modular hardware subsystem that facilitated secure performance of increasingly essential cryptographic and security-related computing functions—a hardware subsystem that was purpose-built for storing cryptographic secrets, for securely generating random numbers, and for securely validating other components of a computing system prior to allowing it access to security-sensitive operations and information. By necessity, this standardized hardware subsystem would need to be narrow in scope and strictly segregated from the rest of the system, so that it could serve as a root of trust for a decidedly insecure Internet-connected personal computer.

55. In 2003—following an abortive attempt from 1999-2001—a group of microprocessor and computer manufacturers including Intel, AMD, IBM, Microsoft, and Cisco formed an entity called the Trusted Computing Group to define a standard for trusted computer hardware in computers and mobile

[1] Computers cannot generate truly random numbers, but algorithms can be designed to generate pseudo-random numbers, which are for most applications sufficiently random.

devices. The result of this effort was the Trusted Platform Module ("TPM"), a standardized hardware subsystem meant to enable trusted computing features in computers and mobile devices

56. The first versions of TPM specified a hardware subsystem—in practice, a discrete hardware chip—that provided a common set of cryptographic- and trust-related functions that would increase the security of frequent, security-sensitive operations in modern personal computers particularly those connected to the Internet.

57. Among the goals of the TPM standard was the ability to identify devices with a unique identifying number, key, or letter-number sequence; the ability to generate new cryptographic keys that were secure; the ability to store cryptographic keys to be used in applications, including hard drive encryption; a separate memory system, NVRAM, which allowed persistent information to be stored when storage on the computer was wiped or lost; and a system to attest to device health—that is, whether a system was running genuine, secure, and up-to-date security-sensitive software (*e.g.,* operating system software and/or organization-mandated software).

58. Early versions of TPM hardware—deployed in laptops, desktop computers, and even some mobile devices in the mid-to-late 2000s—achieved many of these goals, but were inflexible. Changes and/or vulnerabilities in hard-wired encryption algorithms left large number of TPM-equipped systems suddenly vulnerable, without the ability to adopt new technology to be used in the TPM.

59. With that said, over a billion computers were using some form of TPM by 2005, such that any changes to the TPM standard would have to maintain existing TPM goals and features, even while adding new ones. As the first decade of the new millennium came to a close, the Trusted Computing Group set out to define a major revision to the original TPM standard—what would become TPM 2.0.

60. Initially chaired by Intel's David Grawrock, the Trusted Computing Group ultimately included HP's David Wooten and AMD's Julian Hammersly.

61. TPM 2.0 was meant to add significant additional functionality to the original TPM standard. Chief among the new additions for TPM 2.0 was algorithm agility—the ability to accommodate new or revised encryption technologies and algorithms. TPM 2.0 also ensured better resource identification systems, and faster key loading.

62. The TPM 2.0 standard solved many of the problems of the first standard, but left the implementation of particular TPM subsystems to computer and microprocessor manufacturers.

B. The TPM as an External System

63. One of the principal security features of the TPM standard was that it was generally implemented as part of a separate hardware system on a computer's motherboard. This ensured that a TPM did not commingle system memory and could not easily be tampered with through the system itself.

64. A discrete hardware TPM meant that cryptographic keys used by a system were stored in a physically separate subsystem—away from the system's main processor and memory systems. The TPM would serve as a neutral oracle, providing keys, random numbers, and device identification on demand.

65. The TPM also allowed for external control over a system's resources—a method of maintaining a trusted over-system to facilitate, for example, "trusted" booting, memory access, or disk drive access on an otherwise untrustworthy system. That is, a TPM would stand as a trusted oracle to evaluate whether the *rest* of the system was as the TPM expected it to be, at boot or in other security-sensitive contexts: the TPM could store trusted authentication and/or measurement values for other aspects of a computer system, and disable boot, memory access, or disk drive access if the general system was not as the TPM expected it to be. The fact that these "trusted" values were stored in a physically discrete, segregated hardware subsystem was, in essence, the entire reason they could be trusted.

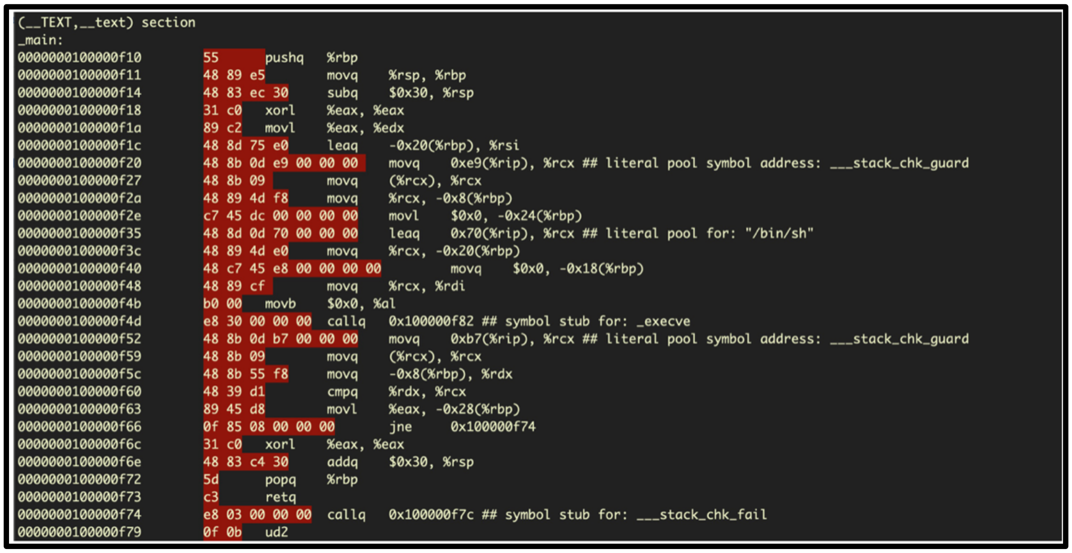
66. The most secure implementation of TPM was the "discrete TPM," a distinct hardware module physically separate from the CPU and thus less immune to attack. As the Trusted Computing Group explained:

> Discrete TPM provides the highest level of security, as might be needed for a TPM used to secure the brake controller in a car. The intent of this level is to ensure that the device it's protecting does not get hacked via even sophisticated methods. To accomplish this, a discrete chip is designed, built and evaluated for the highest level of security that can resist tampering with the chip, including probing it and freezing it with all sorts of sophisticated attacks.

67. A separate, hardware TPM module provided the highest fidelity to the TPM standard, as well as its very premise. Moreover, separate hardware that was independent of the CPU, the operating system, and system memory meant that no matter the sophistication of an attack, the odds of reaching the TPM's guarded secrets were far lower.

68. Indeed, many attacks and security vulnerabilities rely on tricking the operating system into allowing access to trusted parts of a computer's memory and then running arbitrary code. Often, a hacker will focus on inserting a payload into memory—called "shell code"—then tricking the operating system into jumping to a memory location where the payload is stored to run the code. That code will then, in many cases, provide an attacker privileged access to the computer system—*e.g.*, allowing an attacker to interact with the operating system through a shell as a super user or in trusted memory space.

69. Shell code, like the code below, can be disassembled into lower-level code, called assembly code, then the "op codes," or instructional code can be encoded into a string of text.



```
(__TEXT,__text) section
_main:
0000000100000f10        55      pushq   %rbp
0000000100000f11        48 89 e5        movq    %rsp, %rbp
0000000100000f14        48 83 ec 30     subq    $0x30, %rsp
0000000100000f18        31 c0   xorl    %eax, %eax
0000000100000f1a        89 c2   movl    %eax, %edx
0000000100000f1c        48 8d 75 e0     leaq    -0x20(%rbp), %rsi
0000000100000f20        48 8b 0d e9 00 00 00    movq    0xe9(%rip), %rcx ## literal pool symbol address: ___stack_chk_guard
0000000100000f27        48 8b 09        movq    (%rcx), %rcx
0000000100000f2a        48 89 4d f8     movq    %rcx, -0x8(%rbp)
0000000100000f2e        c7 45 dc 00 00 00 00    movl    $0x0, -0x24(%rbp)
0000000100000f35        48 8d 0d 70 00 00 00    leaq    0x70(%rip), %rcx ## literal pool for: "/bin/sh"
0000000100000f3c        48 89 4d e0     movq    %rcx, -0x20(%rbp)
0000000100000f40        48 c7 45 e8 00 00 00 00         movq    $0x0, -0x18(%rbp)
0000000100000f48        48 89 cf        movq    %rcx, %rdi
0000000100000f4b        b0 00   movb    $0x0, %al
0000000100000f4d        e8 30 00 00 00  callq   0x100000f82 ## symbol stub for: _execve
0000000100000f52        48 8b 0d b7 00 00 00    movq    0xb7(%rip), %rcx ## literal pool symbol address: ___stack_chk_guard
0000000100000f59        48 8b 09        movq    (%rcx), %rcx
0000000100000f5c        48 8b 55 f8     movq    -0x8(%rbp), %rdx
0000000100000f60        48 39 d1        cmpq    %rdx, %rcx
0000000100000f63        89 45 d8        movl    %eax, -0x28(%rbp)
0000000100000f66        0f 85 08 00 00 00       jne     0x100000f74
0000000100000f6c        31 c0   xorl    %eax, %eax
0000000100000f6e        48 83 c4 30     addq    $0x30, %rsp
0000000100000f72        5d      popq    %rbp
0000000100000f73        c3      retq
0000000100000f74        e8 03 00 00 00  callq   0x100000f7c ## symbol stub for: ___stack_chk_fail
0000000100000f79        0f 0b   ud2
```

70. The code above would therefore become a string of hexadecimal numbers, such as "x55x48x89xe5x48x83xecx30x31xc0x89xc2x48x8dx75xe0x48x8bx3bx0dxe9x . . . ." Once this string is stored in memory, the operating system will run the code if it is tricked to jump to the part of memory where the code is stored.

71. The degrees of freedom for attacks on personal computers are extremely high—nearly infinite, given the complexity and breadth of modern systems and the ways in which they are used. The example above is just one of many potential "attack vectors" for a modern computer.

72. The above example is, however, illustrative of a fundamental (and serious) security problem in modern computers that hardware-based TPM specifically addresses. A hardware TPM is not part of the CPU of a computer, and is not simply mapped to the computer's general memory address space. Thus, an attack on the operating system that provides privileged access to the CPU—and such attacks are not merely widespread, but indeed pervasive—would not, in many cases, mean that a hardware TPM would also be compromised.

73. This is in part because the hardware TPM does not share memory with the CPU, and therefore it does not share memory with the computer's operating system. Its secrets are simply out of reach, even if the operating system is tricked into jumping to particular memory locations or running arbitrary instructions as in the example above.

74. Separate physical memory space in a hardware TPM also means that a malfunction in the operation of the CPU or the operating system will not generally compromise a hardware TPM. And, *vice versa*, memory access by the hardware TPM is not accomplished through the same data pipelines used by the CPU to communicate with system memory.

75. The strict, physical separations between the trusted locations and functions in a hardware-based TPM and the untrusted rest of a modern computer system are in many ways the raison d'être of the TPM standard.

76. Additionally, a hardware TPM can be designed to disable itself, erase itself, or even self-destruct, without damaging the CPU or other expensive hardware—yet still disable access to security-sensitive operations across the computing system by doing so. For example, repeated attempts to access the TPM's data or to tamper with the TPM, if the module is implemented in separate hardware, can result in a shutoff of TPM functions, securing the computer from further attack until a trusted administrator of the system regains control.

II. MICROSOFT FORCES TPM ADOPTION AS PART OF WINDOWS 11

A. The Growing Risk of Firmware Attacks and the Need for Hardware Security Solutions

77. In March 2021, Microsoft concluded its "security signals" study, which targeted cybersecurity attacks on the Windows operating system as well as enterprise cybersecurity practices. As Microsoft explained, the goal of the study was to "provide up-to-date research on the state of security, across countries and industries in order to better serve our customers and partners, and enable security decision makers to further their development of security strategies within their organizations."

78. One of the primary conclusions reached by Microsoft was that "security frameworks" were an important means by which security could be achieved at an enterprise level and across contexts in which the Windows operating system was used.

79. A broader security "framework" was necessary, Microsoft determined, because most enterprise administrators were bogged down with individual security problems, which they addressed *ad hoc* and separately. As Microsoft's report explained:

> While companies' security strategies are clearly important to their business, more than half the decision makers we surveyed said their staff is currently too busy to spend enough time on strategic work. Instead, they are focusing on "table stakes" security issues such as software and firmware patches, hardware upgrades, and internal and external security vulnerabilities.

80. The study further showed that "firmware attacks" were a significant problem across enterprises. Firmware refers to software that is seldom modified and that is used by low-level computer hardware. The firmware is often foundational code run by the computer, including at bootup time. Obtaining control over BIOS firmware, for example, can mean controlling the system's hardware before the operating system or even the CPU comes fully online.

81. Microsoft's study found that more than 80% of enterprises had experienced at least one firmware attack in the past two years, but only 29% of security budgets were allocated to protect firmware.

82. In other words, firmware was a massive and under-protected vulnerability for most systems, particularly laptops and PCs provided to employees—even more so after the onset of the global

COVID-19 pandemic, as employees in even the most sensitive industries were forced to work from home. Moreover, Microsoft found, enterprises were increasingly allowing employees to purchase or use their own computer hardware, creating further security complexity.

83. For computers without hardware-based protection, firmware was a centralized point of vulnerability. If hacked, many of a computer's secrets would be revealed to the hacker. As Microsoft explained in a March 30, 2021, post on its website:

> Firmware, which lives below the operating system, is emerging as a primary target because it is where sensitive information like credentials and encryption keys are stored in memory. Many devices in the market today don't offer visibility into that layer to ensure that attackers haven't compromised a device prior to the boot process or at runtime below the kernel. And attackers have noticed.

84. The National Institute of Standards and Technology (NIST), which maintains a National Vulnerability Database (NVD), reported that there had been a five-fold increase in attacks against firmware in the four years prior to 2021, and attackers "have used this time to further refine their techniques ahead of software-only protections."

85. Microsoft concluded that it would need to adopt a broader security framework that it could enforce across many Windows devices at once. Its solution was to require specialized hardware to run its operating system—hardware immune from a firmware attack: a TPM.

B. The Onslaught of Firmware Attacks

86. Years prior to Microsoft's March 2021 report, a new and extremely dangerous form of cyberattack was taking hold: the "firmware" attack. These cyberattacks focus not on the programs running on the computer or on its operating system, but instead target the hardcoded software stored in flash memory or read-only memory as part of the computer's hardware.

87. While historically, most firmware was stored in a read-only memory that could not be modified once the data was "burned" into a memory chip, the lack of flexibility became problematic. Important firmware needed to be modified from time to time, including to address security threats unforeseen at the time a computer system or hardware peripheral was released.

88. The solution was to use non-volatile flash memory—a semi-permanent, but not immutable, memory that can store foundational instructions or data for hardware. Flash memory could be "flashed" with data, then later updated with a "re-flashing." The memory would not be accessed randomly, such as with local memory on computer systems (*i.e.*, random access memory ("RAM")); flashed memory would remain largely static, updated only for important reasons.

89. Nonetheless, such flash memory *could* be updated, and that meant hardware-level instructions and data could be tampered with. This created a new threat vector to computer systems.

90. The most important information stored in non-volatile flash memory pertains to the computer's Basic Input/Output System ("BIOS"). Hardcoded instructions in a computer's BIOS—usually stored on a computer's motherboard—handle the computer's bootup process, including bringing the microprocessor's full functionality online and setting up input-output systems to communicate with hardware peripherals.

91. In the late 1990s and early 2000s, the legacy BIOS used on most Intel-based PCs began to be replaced in new computers by an extensible interface that handled the same bootup functions—an extensible interface that could be modified after the initial manufacturing of the computer.

92. Originally developed by Intel and eventually migrated to an industry consortium comprised of twelve "promoter" companies including AMD, HP, Intel, Dell, Lenovo, and Microsoft, this standardized, extensible system was called the Unified Extensible Firmware Interface (UEFI), which was released as a version 2.0 specification in 2006. Other computing systems had recently moved in a similar direction, with Apple's PowerPC systems using the OpenFirmware system. There was an unmistakable trend: hardcoded instructions for bootup and hardware-OS communication were giving way to updatable instructions stored in on-board flash memory.

93. The flexibility of firmware, including UEFI firmware, came at a cost. A hardcoded BIOS stored on a ROM could only be modified with physical access to a computer. Flashed firmware, however, could be altered through software, and in later devices, remotely over a network or Internet connection.

94. It was not long before hackers discovered ways to compromise computer systems by tampering with foundational firmware, including the UEFI firmware that had become standard across PCs around the world.

95. For example, in 2018, it was publicly revealed that the state-sponsored hacking group Fancy Bear had developed an exploit to UEFI firmware that gave an attacker privileged access to most modern PCs. The malicious code worked by rewriting the firmware stored in a computer's SPI flash memory. As ZDNet reported on September 27, 2018:

> Researchers have uncovered what appears to be the first case of a UEFI rootkit in the wild, changing the concept of active UEFI exploit from a conference topic to reality.
>
> The UEFI rootkit was found bundled together with a toolset able to patch a victim's system firmware in order to install malware at this deep level, ESET researchers said on Thursday.
>
> In at least one recorded case, the threat actors behind the malware were able to write a malicious UEFI module into a system's SPI flash memory—leading to the drop and execution of malicious code on disk during the boot process.

96. The danger of such an exploit was that it obtained access to a computer system at the lowest of levels—code directly instructing and interacting with critical system hardware, even before an operating system comes online. As ZDNet explained:

> Not only do such methods circumvent operating system reinstall, but also hard disk replacement. The only way to remove such malware—assuming victims know they have been compromised in the first place—is to flash the firmware, a process not often conducted by typical users.

97. The exploit was almost impossible for an unsophisticated user to detect. It could not be removed by erasing or even changing out the computer's hard disk. It was in the most persistent storage possible—the memory ancillary to the foundational hardware systems of the computer, its firmware.

98. In May 2020, another massive firmware attack vector emerged. With this attack, the firmware governing Thunderbolt ports shipped on computers since 2011 could be maliciously modified. ZDNet reported on this threat vector on May 11, 2020:

> A Dutch researcher has detailed nine attack scenarios that work against all computers with Thunderbolt shipped since 2011 and which allow an attacker with physical access to quickly steal data from encrypted drives and memory.
>
> Researcher Bjorn Ruytenberg detailed the so-called Thunderspy attacks in a report published Sunday, warning that the attacks work even when users follow security best practice, such as locking an unattended computer, setting up Secure Boot, using strong BIOS and operating system account passwords, and enabling full disk encryption.

99. This newly-revealed firmware attack was extremely pernicious. It was an attack upon the underlying communication channels between a computer's hardware peripherals and its operating system.

100. Most operating systems map hardware memory onto system memory, allowing interaction with the hardware through direct memory read and write instructions. Because these memory read and writes are time-sensitive, an operating system often allows certain hardware Direct Memory Access ("DMA") to facilitate peripheral communication. Firmware attacks, such as Thunderspy, targeted this mechanism:

> Ruytenberg notes that Thunderspy differs to [Thunderclap, a 2019-disclosed Thunderbolt attack vector], which relied on tricking users into accepting a malicious device as a trusted one. Thunderspy on the other hand breaks Thunderbolt hardware and protocol security.
>
> While all Thunderbolt-equipped computers are vulnerable to Thunderspy, Intel, which develops Thunderbolt technology, says the attacks were mitigated at the operating system level with Kernel Direct Memory Access (DMA) protection, but this technology is limited to computers sold since 2019.

101. The Thunderspy attack vector illustrated a significant vulnerability common to firmware attacks: the exploit facilitated access to what is typically a read-only part of the operating system's memory. Modern operating systems had implemented DMA protections, but this circumvented most of those protections entirely.

102. In October 2020, the U.S. Department of Transportation sounded an alarm regarding firmware exploits of transportation systems, such as cars. So-called Over-the-Air systems, which allow manufacturers to, for example, update automobile software remotely, created a massive threat vector:

> The importance of software in computer system architecture makes it an attractive target for attackers. Software modification attacks on various embedded systems have been demonstrated repeatedly at hacking conferences and in academic publications. The capability of OTA updates for vehicle software only widens the attack vector, making it possible for hackers to distribute malware to millions of vehicles simultaneously.

103. The same problem was manifesting across industries, applications, and enterprises: firmware attacks could hijack the remote update systems built into most computers to replace foundational code, capturing the system before operating system protections even came online.

104. A discrete TPM—a distinct piece of hardware physically separate from the computer system's firmware or operating system—appeared to be a viable antidote to firmware attacks designed to reach cryptographically sensitive systems of a computer.

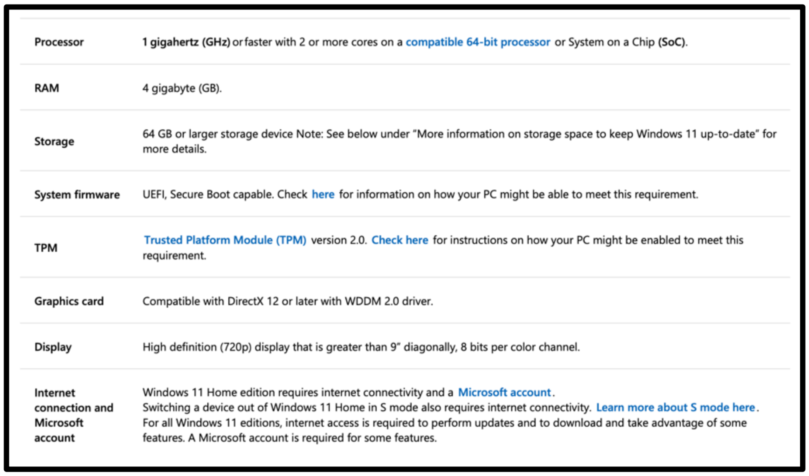
105. A hardware TPM insulated the computer system from, for example, having its random number generator tampered with (which would be disastrous for the safety of encryption systems), having cryptographic keys stolen or replaced, or having a system's authentication mechanisms hijacked.

106. To Microsoft—maker of the dominant operating system for personal computers, and whose Windows OS was the target of many firmware attacks—it was the next logical step to require systems running Windows to adopt TPMs. Indeed, there was little Microsoft's operating system could itself do to prevent or control firmware attacks, which by design capture a computer system before the operating system even comes online.

C. Microsoft Requires a TPM to Run Windows 11

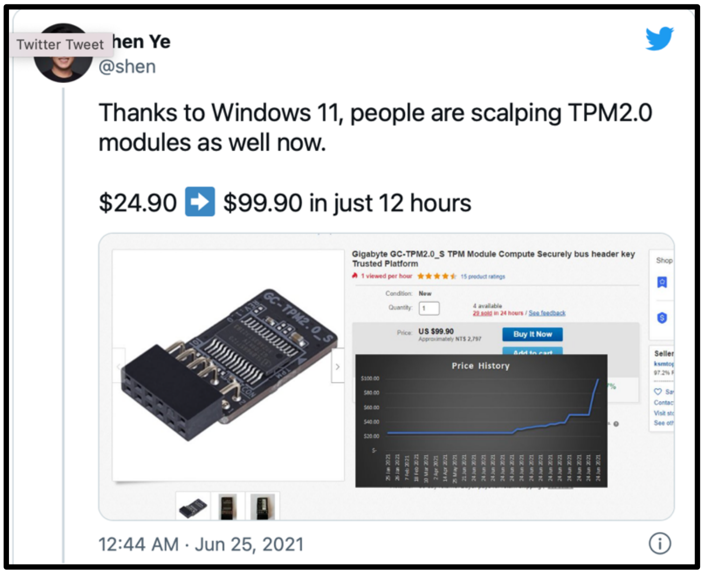
107. In 2015, Microsoft released Windows 10 as the then-latest version of its dominant operating system. Microsoft pushed OEMs pre-installing Windows 10 to ship TPMs with their computers, but had stopped short of requiring a TPM to run Windows.

108. That changed with the operating's next major release. In June 2021, Microsoft published minimum system requirements for its forthcoming Windows 11 operating system. The system requirements stated for the first time that TPM 2.0 hardware was required to run Windows.



Processor	1 gigahertz (GHz) or faster with 2 or more cores on a compatible 64-bit processor or System on a Chip (SoC).
RAM	4 gigabyte (GB).
Storage	64 GB or larger storage device Note: See below under "More information on storage space to keep Windows 11 up-to-date" for more details.
System firmware	UEFI, Secure Boot capable. Check here for information on how your PC might be able to meet this requirement.
TPM	Trusted Platform Module (TPM) version 2.0. Check here for instructions on how your PC might be enabled to meet this requirement.
Graphics card	Compatible with DirectX 12 or later with WDDM 2.0 driver.
Display	High definition (720p) display that is greater than 9" diagonally, 8 bits per color channel.
Internet connection and Microsoft account	Windows 11 Home edition requires internet connectivity and a Microsoft account. Switching a device out of Windows 11 Home in S mode also requires internet connectivity. Learn more about S mode here. For all Windows 11 editions, internet access is required to perform updates and to download and take advantage of some features. A Microsoft account is required for some features.

109. The newly published Windows 11 system requirements led to an immediate run on hardware TPMs. Reports were widespread of TPM modules being "scalped" at inflated prices.



Twitter Tweet hen Ye
@shen

Thanks to Windows 11, people are scalping TPM2.0 modules as well now.

$24.90 ➡️ $99.90 in just 12 hours

Gigabyte GC-TPM2.0_S TPM Module Compute Securely bus header key Trusted Platform

1 viewed per hour ★★★★½ 15 product ratings

Condition: New

Quantity: 1 4 available
29 sold in 24 hours / See feedback

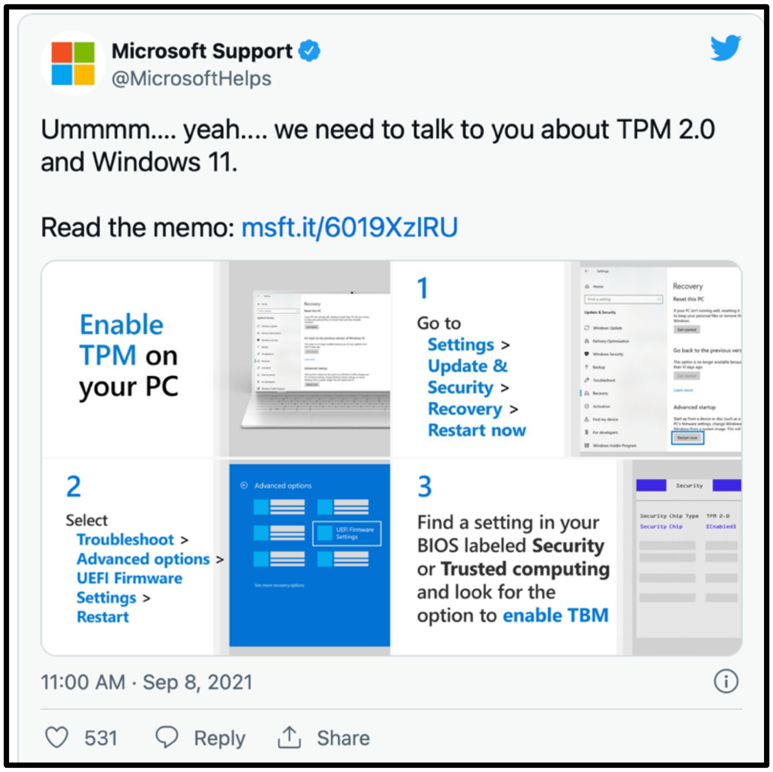
Price: US $99.90
Approximately NT$ 2,797

12:44 AM · Jun 25, 2021

110. Microsoft also had recently released software that would check whether a particular computer was eligible to upgrade to Windows 11, called the Windows Health Check app. For the first time, that utility was flagging computers without TPMs, or without enabled TPMs, as incompatible with the next version of Windows.

111. In September 2021, after a long summer of confusion and price-gouging, Microsoft expressly confirmed that it was requiring TPM 2.0 compliance going forward: a computer was required to have a TPM in order to run Windows 11.

112. On September 8, 2021, Microsoft tweeted the following from its verified Microsoft Support account:



Microsoft Support
@MicrosoftHelps

Ummmm.... yeah.... we need to talk to you about TPM 2.0 and Windows 11.

Read the memo: msft.it/6019XzIRU

Enable TPM on your PC

1 Go to Settings > Update & Security > Recovery > Restart now

2 Select Troubleshoot > Advanced options > UEFI Firmware Settings > Restart

3 Find a setting in your BIOS labeled **Security** or **Trusted computing** and look for the option to enable TBM

11:00 AM · Sep 8, 2021

113. On its website and elsewhere, Microsoft provided instructions as to how users could check their computers for TPMs and how to enable the TPMs on their systems.

114. In October 2021, just ahead of Windows 11's public launch, David Weston, Microsoft's Director of OS and Enterprise Security, explained why Microsoft had transitioned from optional TPMs in Windows 10 to mandatory TPMs in Windows 11:

> What we learned from 10 is, if you make things optional, people don't turn them on . . . . They assume that if it was necessary, it would be on. And so I think that's a big learning. What we put into 11 is [that] we are going to secure you by default. . . .

> Ultimately, we could have chosen many lines. But we used data analysis around reliability, performance, and security to get there, and that is how we landed on that particular bar.

115. Microsoft had, in a sweeping move, implemented the new security framework it had envisioned in its mid-2021 study. With Windows 11, it had decided to enforce a minimum level of hardware security by default to protect its operating system's users from firmware attacks.

116. Microsoft's move, at least at first glance, meant that most modern computers would have segregated hardware that ensured a computer's security, including with respect to the integrity of the computer's firmware.

III. AMD IMPLEMENTS A DEFEAT DEVICE—A FIRMWARE TPM BUILT ON A PLATFORM WITH DIRECT ACCESS TO PRIVILEGED SYSTEM RESOURCES

A. The AMD Platform Security Processor

117. In 2013, AMD introduced a separate co-processor and system that functioned alongside its CPUs. This new system was called the AMD Platform Security Processor ("PSP").

118. The goal of the PSP is to perform security functions before the CPU comes online and while the CPU functions. As AMD explains in its Developer Guide:

> The PSP is a standalone complex within AMD Family 16h Models 30h-3Fh processors that is responsible for creating, monitoring and maintaining the security environment. Its functions include managing the boot process, initializing various security related mechanisms, and monitoring the system for any suspicious activity or events and implementing an appropriate response.

119. The PSP uses a separate CPU of its own, with an architecture designed not by AMD, but by ARM—a British semiconductor design company. The PSP also contains a cryptographic coprocessor (CCP); local memory registers; and dedicated interfaces to interact with the system memory, input/output devices, and configuration registers.

120. The PSP's ARM CPU and supporting subsystem has direct access to an AMD-based computer system's most privileged and sensitive resources. The PSP can directly read and write to a computer system's memory, and it can directly interact with an AMD system's hardware.

121. Notably, the PSP can generate what are called “interrupts” to the AMD CPU. An interrupt is the ability to send a priority message to the CPU to handle a particular task that requires attention. Interrupts are typically used to convey high-priority or time-sensitive events related to hardware. This means that the PSP has a privileged and direct line of communication to the AMD CPU.

122. The PSP has its own local memory, and some resources are stored on flash memory or read-only memory connected through a Serial Peripheral Interface (“SPI”).

123. The ARM CPU in the PSP is controlled by its own separate micro-operating system, called a Trusted Execution Environment (“TEE”). Various functions related to security run on the co-processor’s TEE, sharing the PSP’s local memory and flash memory.

124. The ARM processor in the PSP can generally execute instructions one at a time. To allow it to run multiple programs at once, the TEE uses a program called a “scheduler,” which allows the ARM CPU to time-slice its work. By rapidly switching between programs, called a context switch, the ARM processor looks like it is executing multiple tasks at once.

125. The TEE running the PSP’s ARM processor, supporting hardware, and memory, is called Kinibi, which is made by a largely obscure company called Trustonic, which guards most workings of its micro-operating system from public access.

126. Many TEEs use a scheduling algorithm called “round robin.” Under a round robin scheduling system, or a system like it, the CPU allocates equal time slices to various tasks without priority, which is also known as cyclic execution.

127. A benefit of round robin scheduling is that it is simple to implement. And for simple tasks sharing a single CPU, the algorithm is usually more than sufficient to prevent individual resources from being starved for processor time while other programs operate.

128. However, Kinibi operating system modifies this scheduling method by assigning programs priority values and executing them accordingly. This is called preemptive scheduling. The scheduling system in Kinibi is also designed to stop execution of one program for a lower priority program when a time-sensitive task that must be completed by the lower priority program.

129. One reason the special scheduling algorithm was necessary for the ARM processor running in the PSP is because that processor is designed to concurrently run processes in two different security modes—"secure mode" and "non-secure mode"—each with its own set of registers and memory maps. Using an ARM security framework called "TrustZone," the ARM processor in the PSP effectively runs two sets of processing "worlds" at once, and repeatedly switches back and forth between them using a special processing bit and special "secure interrupts." Because of the TrustZone functionality, every security-related context switch in the ARM processor in the AMD PSP requires zeroing out a program's memory state prior to transitioning to another program, among other significant processor transitions. Otherwise, data lingering in memory could be compromised by other processes.

130. The PSP is essentially a separate computer system that sits on top of an AMD-based system. It boots up first; it controls the booting of the AMD CPU; and it routinely interacts with the system's AMD CPU, system memory, and hardware to (supposedly) ensure that only trusted programs have access to privileged resources.

131. This creates a significant problem. If the PSP is compromised by an attacker, the entire AMD-based system can be trivially compromised as well—including direct access to system memory and hardware. As explained earlier in this Complaint, such a compromise could mean tricking the AMD CPU to run arbitrary code that provides privileged access to the system.

132. The PSP has been the source of many vulnerabilities in AMD computer systems, particularly in computers running AMD Ryzen CPUs.

133. For example, in late 2017, a Google security researcher discovered a stack overflow vulnerability in the PSP—specifically, within its firmware TPM implementation—that would allow an attacker to take full control of the PSP (which would then, by the PSP's design, allow escalation to compromise of the AMD CPU and system itself). Google's security researcher noted: "As far as we know, general exploit mitigation technologies (stack cookies, NX stack, ASLR) are not implemented in the PSP environment."

134. As another example, in June 2019, security researchers discovered another flaw in the AMD PSP that allowed hackers to capture an AMD CPU and system's protected memory and resources.

135. Then in December 2021, another exploit was publicly revealed in which the AMD PSP could be compromised such that an attacker would have access to uninitialized memory on the system, again leaving data and privileged memory in the system open to being compromised. Since its inception, AMD's PSP has been attacked and compromised repeatedly.

136. One use for the PSP is Digital Rights Management ("DRM"), which is implemented through software systems designed to authenticate, decrypt, and monitor protected media content, such as movies, music, and video games. To facilitate DRM, the PSP uses its privileged access to the AMD CPU and to the system's hardware to ensure that only those with rights to watch a movie, play a game, or listen to a song can play the media on their computers. If the DRM blocks access, the PSP is able to block access to the media at the hardware level, with even more access to the system than the operating system running the AMD processor.

137. The PSP runs many programs in addition to those implementing various standardized DRM systems. The ARM processor used as part of the PSP is shared among these programs. When a program reads or writes to memory or to slower hardware, it may delay or stall a change in context to another program, delaying execution of other programs on the ARM processor until the slow memory or hardware read or write is complete. Many of the programs running on the PSP share the same bank of SPIROM or other forms of "flash memory," which is generally far slower than other memory used by CPUs. When the ARM processor reads from the SPIROM, for example, it may stall out other programs running on the ARM processor from executing.

B. AMD Shoehorns a Software-Based TPM into the PSP as Firmware

138. As TPMs initially became ubiquitous, hardware TPMs were the primary implementations of the TPM 2.0 standard. Separate hardware TPMs, however, were costly, ranging between $20 to $150 dollars depending on functionality and speed.

139. Microsoft, for its part, was pressuring Original Equipment Manufacturers ("OEMs"), such as HP or Dell, to add TPMs to their systems. By 2015, as the release of Windows 10 was imminent, OEMs were pre-installing the new Windows OS—which encouraged, but did not yet require, TPM 2.0

compliance—to their computers. However, Microsoft (and industry observers) signaled that TPM compliance could become a requirement in the near future.

140. Faced with an added and potentially significant cost to their systems, OEMs that used AMD Athlon or Ryzen processors sought a solution from AMD. AMD's response was an addition to the PSP: a so-called "firmware TPM," referred to by AMD as fTPM.

141. AMD implemented the fTPM as part of its PSP—as another program that ran on its ARM co-processor and Kinibi operating system. AMD's fTPM shared resources with other programs running on the PSP, including those responsible for DRM tasks relating to media, including video, music, and video games.

142. The AMD fTPM read its instructions from read-only memory ("ROM") connected to the PSP's SPI—so-called SPIROM. Reading from the SPIROM, which was shared among programs running on the PSP, was costly in time. It took orders of magnitude longer to read from the SPIROM than from local memory.

143. TPMs were designed to stand apart from the CPU, memory, and hardware of a computer system in order to provide trusted security-sensitive subsystems and services, including cryptography. The TPM's separation from the rest of the computer system was central to its trustworthiness, and its ability to serve as a hardware "root of trust" for an otherwise untrustworthy computer system. AMD, however, implemented the fTPM as part of its PSP subsystem, which had virtually ***unfettered*** access and connections to precisely the resources a TPM was meant to stand apart from.

144. AMD's fTPM was plainly not about providing actual hardware-based security according to the TPM standard. This fTPM was shoehorned into the existing PSP system, which was designed to directly access hardware resources, including as part of execution of DRM processes protecting media.

145. In other words, AMD's implementation of fTPM shared resources and SPIROM access with other privileged programs, proving the mere illusion of hardware-based security.

146. When Windows 11 ended up requiring a TPM, AMD-based systems could simply enable the fTPM subsystem. No separate hardware was required—or provided. The problem, unfortunately, was that the AMD fTPM, which provided none of the protections a hardware TPM was designed to provide,

merely satisfied the letter of the Windows 11 requirement without providing any substantive, structural (and much-needed) hardware protections to the subject computer system.

147. fTPM was a Potemkin TPM, designed the check a box—and more to the point, satisfy a Windows compliance check—for Windows 11's security framework requirements without actually providing the hardware-based security and trust that Microsoft had determined was necessary in the face of spiraling low-level security vulnerabilities, including firmware attacks.

148. In short, when Windows 11 looked for a TPM to evaluate compliance with Microsoft's security framework, it found AMD's "defeat device." AMD's onboard fTPM was merely a piece of software designed to look and act like a hardware TPM. Its firmware was stored among other data in shared flash memory; it ran on top of an operating system that time-sliced a single ARM co-processor; and it was part of a subsystem that had privileged and high-priority access to AMD CPU-based systems, hardware, and memory.

149. As explained below, implementing the fTPM in software and as a program running on AMD's PSP proved to be problematic. AMD had cut corners, and the OEMs let it do so. It was, however, obvious to both AMD and OEMs, including HP, that a software-based TPM that ran as part of a subsystem with privileged access to the overall CPU and hardware was not a TPM at all.

IV. AMD'S FLAWED DESIGN RESULTS IN PLAYBACK AND GAMING STUTTERING

A. AMD-Based System Users Flood the Internet with Complaints of Stuttering When Watching Video, Listening to Music, Playing Video Games, and Even Videoconferencing

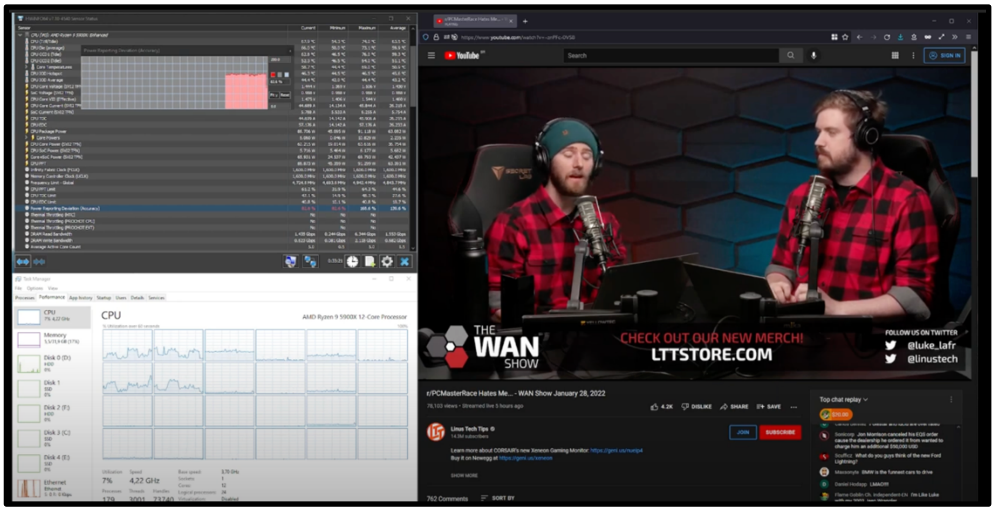
150. AMD's implementation of fTPM as part of the PSP had serious implications for the performance of AMD-based systems, particular Ryzen processors touted by OEMs, including HP, for their speed and security.

151. The AMD fTPM shared resources with PSP programs that controlled video, audio, and other hardware, including the CPU itself. When PSP programs sent interrupts to the ARM processor, the processor had to turn its attention to whatever task was being signaled—and PSP programs often had a priority lane, particularly those controlling DRM and other media-based functionality.

152. This meant that if the fTPM software was accessed, it would have to complete its work rapidly, such that it would not stall out other PSP programs running at the same time via the Kinibi TEE's time slicing. And, to the extent an operation required repeated fTPM access, that access could potentially stall out the entire PSP's array of running programs, some of which were responsible for the function of the computer's CPU and hardware peripherals.

153. This flaw became apparent as early as the middle of 2021, when reports poured in that AMD Ryzen systems were stuttering when playing streaming video or video games.

154. One January 29, 2022, YouTube post from the user "José Ribeiro" demonstrated the stuttering by showing the playback of streaming video on his AMD system with fTPM.



r/PCMasterRace Hates Me... - WAN Show January 28, 2022

78,103 views • Streamed live 5 hours ago

Linus Tech Tips

14.3M subscribers

Learn more about CORSAIR's new Xeneon Gaming Monitor: https://geni.us/nueip4

Buy it on Newegg at https://geni.us/xeneon

Sonicorp Jon Morrison canceled his EQS order cause the dealership he ordered it from wanted to charge him an additional $50,000 USD

Scufficz What do you guys think of the new Ford Lightning?

Maxsonyte BMW is the funnest cars to drive

Daniel Hodapp LMAO!!!

762 Comments

155. Notably, as pictured above in the graph in the top left corner, the stuttering triggered a significant power consumption spike signified by a red region in the graph—an almost wall-like increase in power usage by the AMD processor. This occurred at the same time as the fTPM stutter.

156. As "José Ribeiro" explained:

> The issue happens on 0:11. You can definitely see a lot of values jumping for a second and Power Reporting Deviation having a new minimum. Also, it sounds way worse on my headphones than the OBS recording. The sound freezes for a second like Windows is about to BSOD.
>
> I've been having this stuttering issue since July last year, when I enabled fTPM for the first time. It happens while listening to music, watching videos, editing videos and during gaming also. It happens for about 3 or 4 times a day and doesn't seem to be affecting performance or anything else.

> One thing I noticed though… [*sic*] While the stutter is happening, the Power Reporting Deviation on HWiNFO reports a low percentage and switches to red for the duration of the stutter.

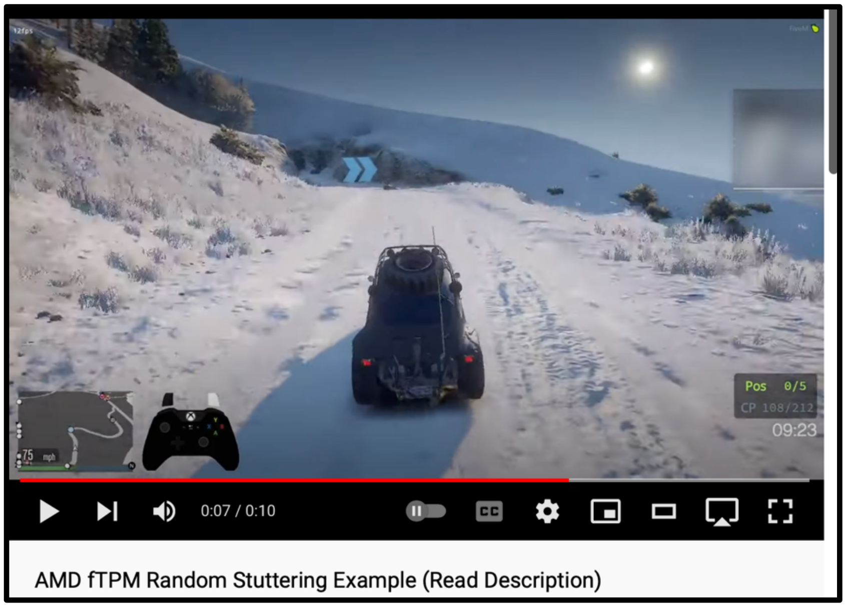
157. User comments confirmed the same behavior—user after user. As one user recounted:

> Thank you for the example, this confirms that my system is suffering from the same problem. I've been wondering what this annoying issue was and today I read about it. Didn't think I was affected, cause I'm still on Windows 10, but I guess this was never related to 11 specifically.

158. Another YouTube comment confirmed that video games, video, and even video conferencing on an AMD system resulted in stuttering:

> Same here! If you're either watching a video, playing a game, or video conferencing, stuttering will occur on AMD cpu or apu regardless of generation of cpu & apu you have! On dual core cpu or apu, I'll notice a stutter every now and then which is annoying when doing normal tasks!

159. Another YouTube video posted by user "Harrison S" demonstrated the stuttering in a video game.



AMD fTPM Random Stuttering Example (Read Description)

160. The post's description explained:

> Enabling the 'firmware TPM' causes system wide stuttering on a growing number of AMD based PC's, as seen in this video. Personally, I have now had 4 consecutive PC's with AMD CPU's that have this problem. Both on Windows 10 and Windows 11. . . .

> In my case, I had this type of stutter 3-4 times a day. Regardless of what programs I was running. Having a TPM is a requirement for Windows 11, and apparently without it your system has a chance of not installing Windows Updates properly. However, sometimes the fTPM can also be automatically enabled on Windows 10 through updates.

161. Reddit posts echoed the same problem, with some users purchasing separate TPMs to stop the stuttering. Again and again, users of AMD-based systems reported stuttering when they watched video, listened to music, played video games, or even videoconferenced.

162. The same reports rolled in on the Linus Tech Tips forum, a forum for computer hardware enthusiasts. One post lamented:

> Recently I turned on the fTPM on my asus B550 wifi motherboard because of the new Windows 11 TPM 2.0 requirements, after I did that I started getting random stuttering on everything, heavy cpu or gpu load don't seem to trigger it, I tried running the heaven benchmark and doing some heavy renders in blender but nothing happened, its just random and everything stutters, discord calls, games, YouTube, it happens randomly at least 3 times a day.

163. Another post echoed the same problem:

> I'm having the exact same issue with my 3900x and MSI MEG Unify x570 motherboard. I don't know if fTPM triggered it but I don't remember it happening before turning it on so I'm assuming it's that. . . .

164. There was an unmistakable pattern. The stuttering appeared when users viewed media, played video games, or ran video- or audio-intensive programs.

B. HP's Forums Receive Repeated Complaints of Stuttering

165. OEM forums were deluged with requests for help. For example, the HP support forum included pleas to help with AMD-based systems that stuttered. As one HP Omen gaming laptop user posted on the HP support forum:

> My god, so probably the weird stutters I can get on my computer be this I have a stutter that has been happening 50000 times a day, the audio is when you click or do something make weird static for a second or when you boot windows in loading screen when you plug headset you will hear weird static sound and when I log in with my password in windows I start using my mouse the mouse freezes for a second. im running ryzen 9 5900hx + rtx 3070 the video has an apparent reduction in frames that last 1 of 2 seconds.

166. Another owner of an HP Pavilion gaming laptop, who likely had his fTPM enabled by a Windows update, echoed the same sort of problem in a reddit post:

> From the last 3 days all games that I have played like the GTA V or red dead 2 have given me stutters every 5 seconds and it's impossible to play now. I don't know what happened because for the last two months I have been playing these games at smooth framerates with no stutters.

167. The repeated posts were met with silence by HP. There was no fix yet. AMD would have to first acknowledge that there was even a problem.

C. AMD Acknowledges the Stuttering Problem and Recommends Its Users Purchase Hardware TPMs as a "Workaround"

168. On March 8, 2022, AMD finally acknowledged that there was a problem. In a post on its website called, "Intermittent System Stutter Experience with fTPM Enabled on Windows 10 and 11," AMD explained:

> AMD has determined that select AMD Ryzen system configurations may intermittently perform extended fTPM-related memory transactions in SPI flash memory ("SPIROM") located on the motherboard, which can lead to temporary pauses in system interactivity or responsiveness until the transaction is concluded.

169. AMD never mentioned the obvious pattern—that the stuttering came during media playback and gaming. Additionally, AMD never explained why the fTPM's access of the SPIROM resulted in "transactions" that caused stuttering.

170. AMD also provided no meaningful workaround. AMD's solution was to buy an external TPM hardware module:

> Workaround: As an immediate solution, affected customers dependent on fTPM functionality for Trusted Platform Module support may instead use a hardware TPM ("dTPM") device for trusted computing. Platform dTPM modules utilize onboard non-volatile memory (NVRAM) that supersedes the TPM/SPIROM interaction described in this article.

171. Purchasing a TPM module, however, is costly. Modules can range in price from $20 to $150 depending on functionality and speed.

172. As for a more permanent fix, AMD promised a firmware update in early May, which AMD never posted on its page. Notably, AMD also explained that any update for OEM computers, such as HP, would have to be performed through the manufacturer. That process, AMD explained, "depends on the testing and integration schedule of your manufacturer. Flashable updates for motherboards will be based on AMD AGESA 1207 (or newer)."

173. HP has never ordered a recall of its PCs to fix the problem.

D. The Stuttering Was Caused by a Serious Design Flaw that Cannot Be Fixed through a Firmware Update

174. The stuttering left an important clue as to the problem. It happened when AMD-based system owners watched video, listened to music, played video games, or communicated on video chats. This was not a coincidence.

175. As explained above, AMD's fTPM was implemented as a program running as part of the PSP subsystem developed by AMD to sit in a privileged position above the most critical system resources, including the AMD CPUs themselves.

176. Some of the programs running on the PSP relate to DRM, which provides for the decryption of multimedia content and the authentication and monitoring of the person accessing the content.

177. Because the PSP's TEE operating system divides time among the programs running on its ARM processor, it forces the fTPM to share resources with programs that relate to multi-media access, including at the hardware level.

178. Moreover, the PSP has direct access to the system's hardware, to the AMD CPU, and even to protected system memory.

179. When the AMD fTPM read from slow SPIROM, it likely forced all other programs to wait until its read was completed, causing multimedia or gaming playback to "stutter."

180. Thus, AMD was in some ways correct: the stuttering was caused by "fTPM-related memory transactions in SPI flash memory," but that was the narrowest possible explanation for the problem. It was a mere symptom of a broader design blunder—the implementation of a firmware TPM

as part of the privileged PSP system, where resources would be shared by the fTPM and other programs addressed to time-sensitive tasks.

181. This flawed design had caused (and continues to cause) damage to the computer systems that used AMD's processors. The stuttering was a symptom of a design that was never an earnest way to secure Windows-compatible computers from firmware attacks (and other serious, low level threats that would be addressed by a real, hardware TPM). Ironically, AMD implemented the TPM—a system designed to thwart firmware attacks—***in firmware***. Worse yet, it implemented this fTPM as part of an already-cluttered system with direct access to system resources.

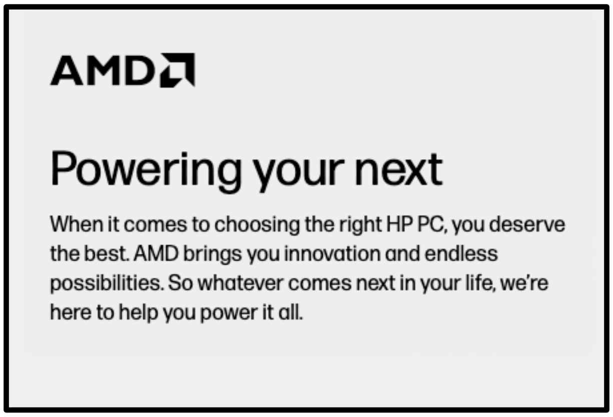
182. AMD's fTPM was not (and is not) a TPM. It was designed as a defeat device to placate the Windows operating system, which requires that a TPM be present and enabled. And AMD's defeat device not only woefully fails to provide the security provided by the TPM 2.0 standard, it causes the system itself to malfunction during ordinary—and in fact, intended—operation.

V. HP JOINTLY MARKETS AMD'S CPUS AND KNEW ABOUT THE FTPM'S FLAWED DESIGN

A. HP Jointly Markets Its PCs and Laptops with AMD, Touting AMD Processors for Multimedia, Gaming, and Security Applications

183. AMD has long jointly marketed its PCs with AMD, touting AMD's processors. For example, the HP website dedicates an entire page to joint marketing: https://www.hp.com/us-en/amd.html.

184. That page opens up by touting AMD processors as the "best":



AMD

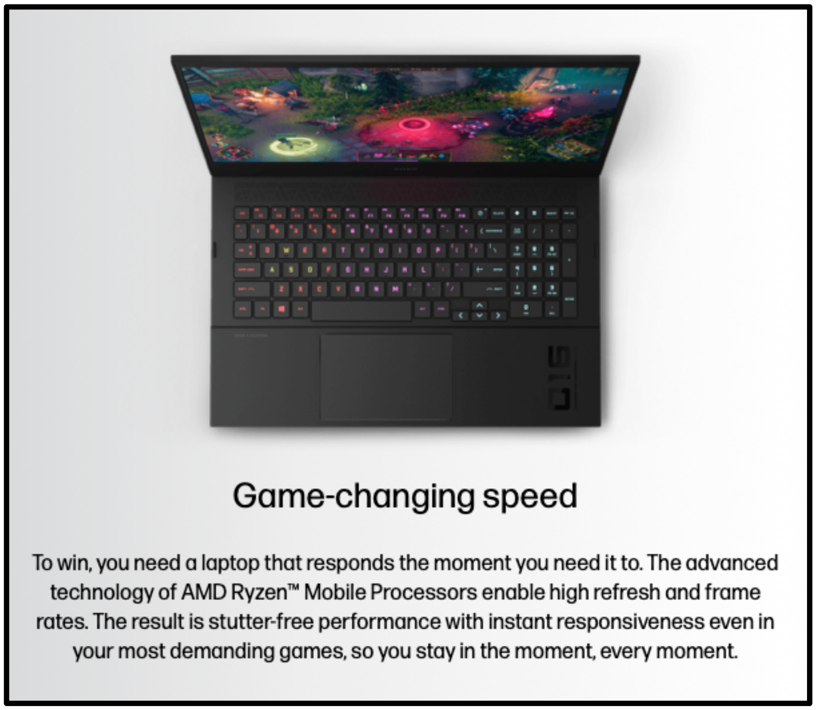
Powering your next

When it comes to choosing the right HP PC, you deserve the best. AMD brings you innovation and endless possibilities. So whatever comes next in your life, we're here to help you power it all.

185. Most representations about AMD processors by HP are, however, far more specific, designed to target precisely the applications affected by the flawed AMD fTPM design.

186. For example, HP represents that AMD-based systems are suited for video chats and video playback. HP represents that AMD-based systems allow users to "capture every detail of your video chats, shows or movies," and that AMD processors allow HP PC users to "[d]ive into immersive multimedia and gaming experiences" at "lightning-fast speeds." The AMD PSP/fTPM flaw, however, causes a decided lack of immersion—the stuttering of playback and video games.

187. HP makes specific representations about the AMD Ryzen processors, including as to gaming on HP PCs:



Game-changing speed

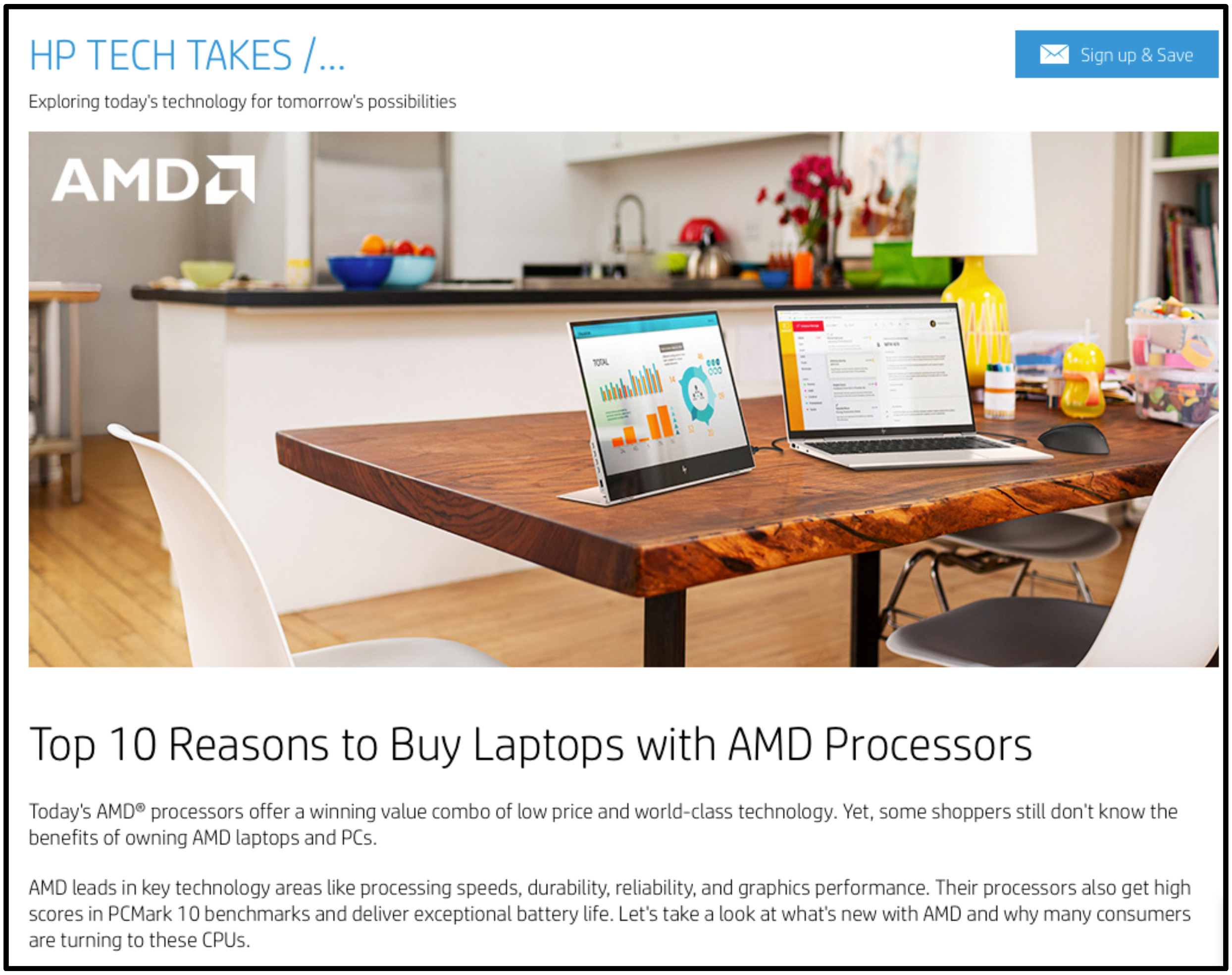
To win, you need a laptop that responds the moment you need it to. The advanced technology of AMD Ryzen™ Mobile Processors enable high refresh and frame rates. The result is stutter-free performance with instant responsiveness even in your most demanding games, so you stay in the moment, every moment.

188. HP's website touts Ryzen processors as maintaining "high refresh and frame rates" and claims "instant responsiveness" for the "most demanding games." The representation is false and misleading, because it fails to disclose that the flawed AMD PSP/fTPM design results in jarring stuttering when running games—the opposite of "responsiveness" and steady "frame rates."

189. HP promises that AMD systems provide "[p]erfect visuals, every time," including when "video chatting with friends or watching your favorite movies and shows." HP states that the multimedia

playback quality keeps a user "immersed in the moment." Stuttering during playback, however, is the opposite of immersion, making the statement false and misleading.

190. In another marketing page, HP provides its "Top 10 Reasons to Buy Laptops with AMD Processors." That page promises speed, durability, reliability, and graphics performance.



HP TECH TAKES /...

Exploring today's technology for tomorrow's possibilities

Top 10 Reasons to Buy Laptops with AMD Processors

Today's AMD® processors offer a winning value combo of low price and world-class technology. Yet, some shoppers still don't know the benefits of owning AMD laptops and PCs.

AMD leads in key technology areas like processing speeds, durability, reliability, and graphics performance. Their processors also get high scores in PCMark 10 benchmarks and deliver exceptional battery life. Let's take a look at what's new with AMD and why many consumers are turning to these CPUs.

191. In this marketing release, branded as part of HP's "HP Tech Takes" series, HP specifically touts the AMD Ryzen's ability to handle gaming and other demanding workloads:

> Models like the Ryzen 4800U are prized for their high-end gaming chops and creative work muscle. Meanwhile, the Ryzen 7 Pro 4750U outclasses the competition with up to 211% multi-thread performance to make short work of demanding workloads. AMD's family of laptop processors have come into their own with a bang.

192. Again and again, HP represents smooth playback of media and gameplay:

- "[AMD] Zen 2 architecture delivers up to 15% more instructions per cycle, improving efficiency for cloud computing, gaming, and streaming. More cores mean you're saving the world better in Fortnite or rendering a 4K video project without overheating or loud fan noise."
- "At every price point, AMD delivers either more cores or more threads. And more threads means your machine can handle more tasks at once. So when you've got 15 tabs open and you're streaming Seinfeld episodes, AMD can do it for less."
- "Plus, AMD Ryzen processors are trusted by eSports players around the globe, and by create pros with heavy rendering."
- "Graphics support matters to laptop users of all stripes; for telework, photo and video editing, gaming, design, and streaming the latest episode of the Mandalorian. AMD's integrated Radeon graphics win out handily with zippy image-crunching speeds."
- "For instance, the AMD Ryzen 7 4700U features 7 graphics processing cores, with core clock speeds of 1600 MHz. That makes it easy to churn out your next Maya or KeyShot project without waiting, or battle ghosts while playing Oxenfree."
- "The AMD Ryzen 4000 H-Series mobile processor with Radeon Graphics is the new gold standard for pro gaming performance. Because they're smaller and they use less power, they make big, clunky gaming laptops a thing of the past. AMD CPUs can handle gaming with less fan noise and less heat, while fitting in a slim, light laptop chassis. "

193. These representations were (and are) factually incomplete, incorrect, false, and misleading. To begin with, representations about media playback omit that AMD's PSP subsystem, which directly interacts with the CPU, system memory and other resources when playing back protected media (*e.g.*, DRM-protected media), shares resources with the system's fTPM. A stalled-out memory operation by the fTPM with respect to the SPIROM or flash memory could stall out more time-sensitive interactions between the PSP and the main system.

194. This means that playback of movies is not smooth; video games do not maintain immersion or frame rate; eSport professionals could not (and cannot) depend on an AMD system during critical matches; and videoconferences would not (and do not) result in smooth video and audio. AMD systems stuttered (and stutter)—routinely—during these gaming, playback, and communications activities. And AMD laptops could not (and cannot) "do more for less"—they would need an additional hardware TPM, priced at approximately $20-$150, to compensate for the AMD's flawed PSP/fTPM design.

195. On the same page, HP also touted (and touts) the security and enterprise features of its AMD-based laptops:

> **8. Modernize security**
>
> Today's internet is a digital cat-and-mouse game where the stakes get higher every day. Cybercriminals aren't standing still, so you can't either. Laptops with AMD processors keep you a step ahead with a multi-layered, modern security approach. Security is built into the design of "Zen" processor architecture, but it doesn't stop there.
>
> ***AMD collaborates with Microsoft and HP*** to unlock enterprise-level security features. Also, AMD Memory guard delivers real-time encryption to shield your system memory from prying eyes. If your laptop is lost or stolen, your laptop is a mystery machine, and mum's the word.

(emphasis added).

196. HP is clear that its computers are designed at the processor level to implement security features such as those handled by the PSP and the fTPM, including real-time encryption and shielding sensitive system memory from attack.

197. The reality, however, is that the PSP, which contains the programs that implement these features, has direct access to sensitive memory and hardware—and indeed, in a way that supersedes any operating system protections. What's more, the AMD fTPM is built into this subsystem, eliminating the very purpose of a TPM—independent security functionality segregated from the computer's firmware, CPU, and operating system.

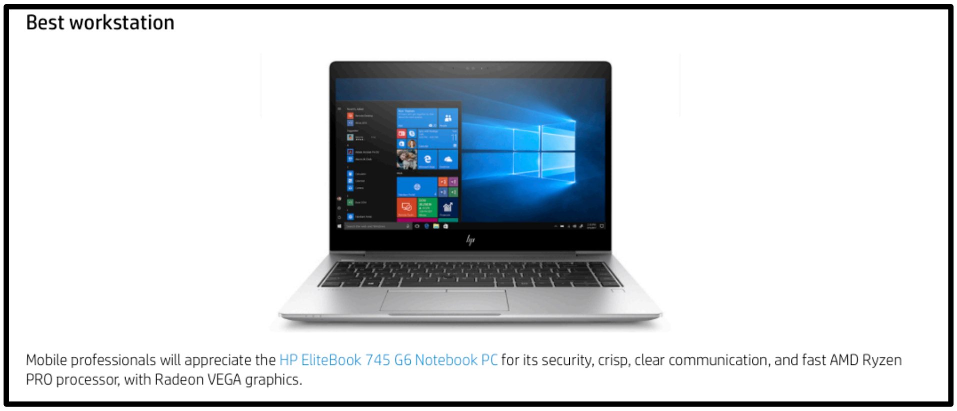
198. Put simply, the security features touted in HP's marketing page are incomplete, materially false, and misleading, as they make affirmative representations that are false and misleading and materially fail to disclose that the very design by AMD of its PSP and fTPM subsystems ***increases***, not decreases, the risk of improper access to critical hardware, access to sensitive and protected system memory, and firmware attacks.

199. HP had (and has) a duty to speak fully and truthfully when it spoke (and speaks) on the subject of the AMD processors in its computer products, but it has said things that were false and misleading and has failed to tell the whole truth—that it was (and is) selling AMD-based computers with a flawed design that made those computers less secure ***in the specific ways HP represented (and represents) these computers were (and are) secure***. The flawed PSP and AMD fTPM design provided (and, to this day provide) a firmware attacker access to protected areas of memory, to hardware attached to the computer, and to the lowest-level and most privileged workings of the AMD CPU.

200. The AMD fTPM is not, from a computer security perspective, a TPM at all—it is a firmware system, purportedly designed to mitigate firmware attacks, that is ***itself*** vulnerable to firmware attacks.

201. HP made—and continues to make—specific claims, including on its hp.com website about its AMD-based PCs, identifying its EliteBook line as the best "AMD business laptop," its Envy line the best "AMD Convertible," its Elitebook 745 line as the best "workstation," its Pavilion line as the best "best for gaming," and its HP Laptop 14 as the "[b]est budget laptop."

202. With respect to its "best workstation model," HP represents on its website that its Ryzen Pro system ensures that communications will be "crisp" and "clear" and that its "security" is suited to "professionals."



Best workstation

Mobile professionals will appreciate the HP EliteBook 745 G6 Notebook PC for its security, crisp, clear communication, and fast AMD Ryzen PRO processor, with Radeon VEGA graphics.

203. Likewise, HP has represented that "immersive video and sound" is a distinct strength of its AMD-based gaming PCs.

204. These specific representations about HP AMD-based PCs were (and remain) false and misleading, as they affirmatively mislead about the particular security and multimedia/gaming aspects and features of these computers, as well as omit the truth and speak only partially about those same aspects and features, while touting them to market and sell HP AMD-based PCs. The reality is that AMD's flawed PSP and fTPM designs made (and continue to make) HP AMD PCs less secure, and render multimedia playback and gaming on those PCs prone to intrusive stuttering.

205. HP and AMD also jointly market, including on hp.com, HP AMD-based PCs for hybrid workers—those that work both in person and at home. The touted use cases for such hybrid users—written up in joint marketing materials like an HP press release titled "New HP Business PCs Deliver Meaningful Experiences for Hybrid Work" currently posted on the hp.com website—focus on HP AMD computers' (supposed) prowess in videoconferencing and their (supposed) ability to maintain enterprise-level security while away from the physical office.

206. HP and AMD target this demographic with marketing for AMD-based HP EliteBook laptops and PCs. For example, a joint press release on hp.com features a quote from HP's General

Manager, Global Head of Commercial Systems & Display Solutions, Andy Rhodes, speaking about HP laptops "[p]owered by the latest AMD Ryzen™ Processors":

> The hybrid world has proven we have the ability to work and learn in the way that works best for us . . . . HP makes hybrid work, work through breakthrough experiences that empower people to collaborate at their best, wherever they are. With our latest offerings, HP is delivering premium performance, security, and collaboration experiences for businesses everywhere.

207. In the same press release on HP's website, AMD's counterpart to Rhodes, Jason Banta, AMD CVP and General Manager, OEM Client Computing, states:

> AMD is proud to partner with HP to create devices that deliver the performance and efficiency needed in today's hybrid work environments . . . . The new AMD Ryzen Pro 6000 Series processors offer incredible performance with multiple layers of enterprise-class security features, flexible manageability options and impressive battery life.

208. Neither speaker—nor the HP press release featuring their quotes—mentions the flawed design of the AMD PSP and fTPM subsystems, which leave AMD-based HP computers vulnerable to devastating firmware attacks (among other low-level vulnerabilities not present in "enterprise-class security" systems). Indeed, the flawed AMD PSP/fTPM design is not only unsuited for enterprise or hybrid work purposes because of stuttering (including during videoconferencing) caused by the flawed design, it is also a fundamentally insecure design whose low-level insecurity could facilitate enterprise-wide attacks, potentially comprising many other computers all at once.

209. HP's website, including its joint press release regarding AMD-based "HP Business PCs . . . for Hybrid Work" The page specifically discusses BIOS-level security—the very point uniquely vulnerable to firmware attack in an AMD-based HP computer as a result of the PSP/fTPM defect:

> To protect PCs from modern threats, HP Wolf Security for Business creates a hardware-enforced, always-on, resilient defense—from BIOS to browser, above, in, and below the OS—giving IT peace of mind. AMD PRO manageability now supports out-of-band and remote management without the need of a dongle so IT administrators have a unified set of tools to manage systems across organizations.

210. HP's representation that its AMD-based systems are secure "from BIOS to browser, above, in, and below the OS," is patently false—belied by the flawed PSP/fTPM design HP incorporates into its systems in collaboration with AMD.

211. HP has repeated and repeats similar hardware-based security claims on other pages and press releases on its website and elsewhere, including in marketing (including on hp.com) for HP's Wolf Security framework. An HP white paper on the hp.com website explains precisely why firmware attacks, particularly those affecting a PC's BIOS, are dangerous—yet says nothing about the flawed AMD PSP/fTPM design, included in HP's products, that leaves HP's AMD-based PCs open to firmware attacks:

> Managing PC firmware (BIOS) settings and controlling access to those settings is an important part of security management for any organization. If left unprotected, BIOS security settings that provide protection against an attacker with physical access to a device can be defeated by simply disabling those settings. For example, if Secure Boot is disabled, an attacker can install a root kit on the device that would be undetectable by the OS. An attacker could also disable Direct Memory Access (DMA) attack protections that prevent them from reading secrets directly from the OS memory via an external port. An attacker might even enable firmware- or hardware-based remote management technologies to obtain remote access to the PC. Therefore it is critical to protect and control access to BIOS settings.

212. HP AMD-based PCs, however, implement TPM in firmware, and they make that fTPM subsystem share a single co-processor with other programs running on AMD's PSP—which in turn has access to precisely the protected resources a real TPM is meant to be carefully siloed from.

B. HP Knew and Knows About the AMD PSP/fTPM Design Flaw, Including Its Stuttering Manifestation

213. HP represents that it collaborates with AMD on security and design. Indeed, HP tests AMD-based configurations and motherboards before packaging them into its computers and computer systems.

214. HP is aware of the overall design of AMD's PSP system, including that the PSP has direct access to protected memory regions, to privileged CPU functionality, and to system hardware. HP is also

aware of AMD's fTPM implementation of TPM 2.0, including that fTPM is implemented as a program running on AMD's PSP system.

215. Indeed, HP has released security advisories and alerts relating to the AMD fTPM system. In doing so, it described the fTPM system on AMD-based HP computers. For example, in a September 28, 2018 advisory, HP stated:

> A security vulnerability has been identified in specific versions of the AMD firmware-based Trusted Platform Module (fTPM). ***The fTPM is used only on AMD platforms (see platform list below) in place of a discrete hardware-based Trusted Platform Module (TPM).*** This vulnerability can potentially compromise applications that utilize the fTPM.

(emphasis added).

216. Even after AMD announced the stuttering issues related to the fTPM and its SPIROM access time, HP continued and continues to sell PCs without any disclosure as to the fTPM's defects or the security vulnerability inherent in the PSP/fTPM design.

217. To the contrary, to this day HP continues to affirmatively tout the supposed video streaming and immersive gaming prowess of its AMD-based computers, including through the specific representations shown and referenced earlier in this Complaint.

218. Even though HP has detailed knowledge and specifications concerning AMD's PSP and fTPM subsystems, it has never disclosed that these subsystems—and computers that contain them—are, because of these subsystems' flawed design, significantly vulnerable to firmware attacks, and that the fTPM is not a discrete module from the AMD CPU's and system's memory, defeating the very purpose of having a TPM in the first place.

219. Put simply, HP knew the truth and made (and, as of the date of this Complaint, continues to make) repeatedly incomplete, false, and misleading statements and omissions about its AMD-based systems' security and performance, including specific misleading statements and omissions regarding these computers' ability to smoothly play music, watch movies, play games, and videoconference.

VI. HP OVERCHARGED CONSUMERS FOR PCS WITH AMD CPUS AS A RESULT OF ITS FALSE AND MISLEADING STATEMENTS AND OMISSIONS

220. Because the AMD fTPM module is integrated into AMD Ryzen and Athlon CPUs as firmware running within AMD's PSP subsystem, it shares memory and resources with the main CPU, including privileged and sensitive CPU functions and system memory. That same integration requires the PSP to share its co-processor and memory resources with other PSP functions, *e.g.*, DRM-related processing. There are at least two substantial, consumer-facing effects of AMD's flawed design.

221. First, because AMD's fTPM is a firmware solution that is implemented as part of the PSP, it leaves the main CPU itself vulnerable to firmware attacks. These are attacks on foundational system software that run even before the operating system comes online, and such attacks are particularly pernicious because they can provide the attacker with broad, low-level access to a computer's hardware, software, and peripheral systems. Moreover, these attacks are difficult to protect against at the operating system level, and as a result they are usually mitigated by hardware-based security—principally, TPMs implemented as discrete hardware modules or subsystems on a computer. AMD's implementation, however, does not provide such hardware-based separation or security, and leaves PCs vulnerable to firmware attacks because of the flawed AMD fTPM and PSP design. The net effect is that affected Ryzen and Athlon CPUs are more vulnerable to firmware attacks than other comparable CPUs, including those provided by AMD's chief competitor, Intel.

222. Second, because the AMD fTPM shares resources with the main CPU and the PSP ARM co-processor (and its TEE operating system), a system's interactions with the fTPM can stall out or occupy important system resources, including the resources of the PSP ARM co-processor (and TEE operating system) that houses the fTPM firmware. The result of this AMD design choice is that users running Ryzen and Athlon CPUs may experience intrusive stuttering during the playback of audio and video, during video conferencing, and while playing games.

223. Both effects (collectively referred to as the "Effects") result in direct harm to Plaintiffs and the Classes. Because of these Effects, the economic value of the PCs purchased from HP by Plaintiffs and Class Members was lower at the time of purchase than the price Plaintiffs and Class Members paid for their PCs, resulting in an immediate out-of-pocket loss. Moreover, because of the Effects, the value

of the PCs Plaintiffs and Class Members purchased from HP is and remains lower than it otherwise would have been, including upon resale, resulting in additional injury because of the diminution of value of Plaintiffs' and Class Members' HP PCs.

224. Plaintiffs and Class Members were able to identify and quantify these injuries with a pre-complaint survey-based statistical analysis, called a conjoint analysis. This analysis allows Plaintiffs and Class Members to pinpoint relative values of the Effects as well as price and brand features of PCs. The results of this pre-complaint analysis, which was based on a survey sample size of 150 U.S. respondents, clearly show that Plaintiffs and Class Members have suffered injury through an overcharge and/or the diminution of value of their PCs.

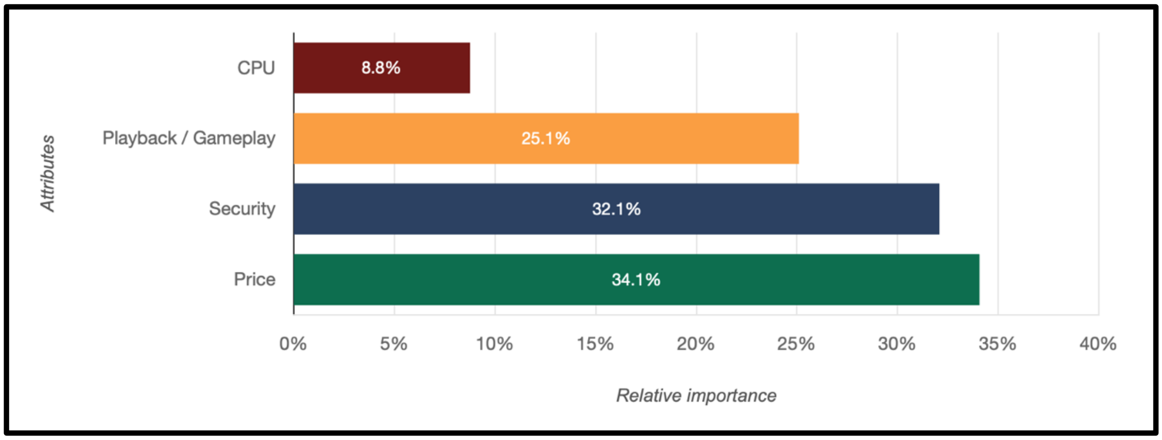
225. To begin with, the conjoint analysis identified a negative price effect for PCs with AMD CPUs given each of the Effects. As described below, each of the Effects results in a significant negative value under the marginal willingness-to-pay metric ("MWTP"), which measures the amount of money purchasers are willing to pay for each feature tested. The calculated MWTP for each Effect is set forth below compared to the baseline of PCs without any of the Effects. The MWTP measured for PCs with a given CPU brand is also set forth below and is based on the baseline of a PC with an AMD-branded CPU.

Product Attribute / Effect	Marginal Willingness to Pay (MWTP)	90% Confidence Interval MWTP
Stuttering audio/video playback, video conferencing, or gameplay	-$915.66	-$716.32 to -$1085.64
Increased vulnerability to firmware attacks	-$1088.49	-$807.42 to -$1398.76
Intel Brand (vs. AMD baseline)	$104.40	$53.30 to $146.06

226. The conjoint results, summarized above, indicate that purchasers are willing to purchase PCs at a discount of $915.66 and $1088.49 for stuttering and increased vulnerability to firmware attacks, respectively. In other words, the Effects have a quantifiable negative value on the AMD-based PCs

purchased and owned by Plaintiffs and Class Members. Indeed, the negatively valued 90% confidence intervals set forth above confirm that almost all, if not all, of the Plaintiffs or Class Members actually experienced an overcharge at purchase and/or a diminution in value as to their PCs.

227. The conjoint study also identified each of the measured Effects as highly material to purchasers. A breakdown of consumer preferences as to security, playback, and brand features tested above is shown below:



228. The study identified an increased vulnerability to firmware attacks, described as the "Security" feature in the above graphic, as nearly as important as a PC's price, with 32.1% of survey respondents valuing that attribute as the most important feature. As to stuttering in playback of audio and video, videoconferencing, and gameplay, which is identified as the "Playback / Gameplay" feature in the above graphic, 25.11% of users identified that Effect as the most important feature. In contrast, the CPU brand, identified above as the "CPU" feature, was the least important to survey respondents, with only 8.8% valuing that feature as most important.

229. The relative importance of features described above indicates that increase vulnerability to a firmware-based attack on a PC is highly material to users and that this Effect, when present, impairs, and deprives the owner of, a PC's ordinary use—*i.e.*, functionality without disproportionate vulnerability to firmware attacks. Indeed, purchasers identified this Effect as nearly as important as one of the central features of a PC product—its price.

230. Likewise, the study's relative importance metric also indicates that stuttering in audio and video playback, videoconferencing playback, and/or gameplay are also highly material to purchasers, and that when the Effect related to this feature is present, it significantly impairs, and deprives the owner of, the PC's ordinary use—*i.e.*, the smooth playback of audio and video, videoconferencing, and gameplay.

231. Moreover, the negatively valued MWTP figures revealed in the study—summarized above—indicate that a significant amount of the value of a PC is lost given each of the Effects. For example, as to the median price-point for a PC measured by the conjoint analysis and survey, $1750, the playback Effect results in an approximately 52% loss of value, and as to the firmware vulnerability Effect, 62% of the PC's value is lost.

232. Finally, the conjoint analysis shows that HP received significant benefit from selling its defective PCs with AMD CPUs. Indeed, based on simulations run given the results of the conjoint analysis, each Effect would have significant effects on AMD's revenue shares with respect to its main competitor for x86 microprocessors, Intel. HP could not have sold nearly as many of its PCs if AMD's revenue shares accurately reflected its true standing in the market given the defective CPUs it sold, including because demand for AMD-based computers would have been far less.

233. Simulations run based on the results of the conjoint analysis show that for a market in which purchasers knew *ex ante* that AMD-based PCs had the playback/gameplay Effect, PC revenue shares for AMD-based PCs compared to Intel-based PCs would have dropped from 45.5% to 17.3%.

234. Simulations run based on the results of the conjoint analysis show that for a market in which purchasers knew *ex ante* that AMD-based PCs had the increased firmware vulnerability Effect, AMD's revenue share would have dropped from 45.5% to 15.3%.

235. HP received the benefit of selling more PCs, at a higher price, than it would have if the AMD design Effects were known by would-be PC purchasers at the time of their purchase. Plaintiffs and the Class Members conferred that benefit on HP by paying an inflated price for AMD Ryzen- and Athlon-based HP PCs at purchase.

CLASS ACTION ALLEGATIONS

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

237. Each class's claims derive directly from a course of conduct by HP.

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

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

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

241. This action may be brought and properly maintained as a class action because the questions it presents are of a common or general interest, and of many persons, and also because the parties are numerous, and it is impracticable to bring them all before the court. Plaintiffs may sue for the benefit of all as representative parties pursuant to Federal Rule of Civil Procedure 23.

The Nationwide Class

242. Plaintiffs Pietosi and Rai bring this action and seek to certify and maintain it as a class action on behalf of themselves and a Nationwide Class. The Nationwide Class comprises:

> All persons, business associations, entities, or corporations that purchased HP notebooks or desktops with AMD Ryzen or AMD Athlon processors with fTPM modules from January 1, 2019, to the present, inclusive (the "Class Period").

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

The California Subclass

244. Plaintiff Rai brings this action and seeks to certify and maintain it as a class action on behalf of himself and a California Subclass. The California Subclass comprises:

> All California persons, business associations, entities, or corporations that purchased HP notebooks or desktops with AMD Ryzen or AMD Athlon processors with fTPM modules from January 1, 2019, to the present, inclusive (the "Class Period").

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

The California Consumer Subclass

246. Plaintiff Rai brings this action and seeks to certify and maintain it as a class action on behalf of himself and a California Consumer Subclass. The California Consumer Subclass comprises:

> All California consumers, as that term is defined in Cal. Civ. Code § 1799.201, who purchased HP notebooks or desktops with AMD Ryzen or AMD Athlon processors with fTPM modules from January 1, 2019, to the present, inclusive (the "Class Period").

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

The Pennsylvania Subclass

248. Plaintiff Pietosi brings this action and seeks to certify and maintain it as a class action on behalf of herself and a Pennsylvania Subclass. The Pennsylvania Subclass comprises:

> All Pennsylvania persons who purchased HP notebooks or desktops with AMD Ryzen or AMD Athlon processors with fTPM modules from January 1, 2019 to the present, inclusive (the "Class Period").

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

Numerosity

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

251. The members of the Classes are so numerous that a joinder of all members would be impracticable. HP has sold its customers millions of defective computers with AMD processors during the Class Period.

Ascertainability

252. The Classes are ascertainable.

253. The defined Classes consist of individuals who purchased HP computers. This identity of these individuals can be determined through records maintained by HP, re-sellers, and purchasers.

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

Typicality

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

256. Plaintiffs' claims are the same as those asserted by members of the Classes. Each Plaintiff, like the members of the Classes, has purchased a defective computer with an AMD Ryzen or Athlon processor, and has been harmed by overpaying for such computer in a manner typical of each of the Classes.

257. Each Plaintiff alleges injury that is not unique to them, but is typical of members of each of the Classes, including measures of damages, such as benefit of the bargain damages, out-of-pocket losses, and/or nominal damages.

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

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

Adequate Representation

260. Plaintiffs will fairly and adequately protect the interests of the class members.

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

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

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

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

265. Plaintiffs and their counsel intend to prosecute this action vigorously and to obtain relief, including both injunctive and monetary relief, that will remedy the design flaw and its manifestations (*e.g.*, stuttering in audiovisual playback and gameplay).

Superiority

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

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

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

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

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

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

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

Commonality and Predominance

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

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

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

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

a. Whether HP's design and sale of defective computers with AMD processors is reckless, negligent, and/or unlawful;

b. Whether HP's design and sale of defective computers with AMD processors amounts to unfair competition;

c. Whether HP's sale of defective computers with AMD processors should be permanently enjoined;

d. Whether HP's sale of defective computers with AMD processors resulted or is resulting in an overcharge for PCs for which members of the Classes paid or are paying;

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

f. Whether HP was unjustly enriched by its conduct;

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

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

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

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

k. Whether HP violated the consumer protection statutes of each State, including California and Pennsylvania;

l. Whether HP knew or should have known about the faulty design of AMD processors when HP designed and sold computers with AMD processors;

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

Grounds Generally Applicable to the Classes

277. Plaintiffs intend to seek injunctive relief ending HP's sale of defective computers with AMD processors.

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

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

280. An injunction preventing HP from continuing to sell defective computers with AMD processors will stop HP's unlawful conduct from occurring in the future. In the alternative, an injunction requiring HP to recall the affected PCs will stop HP's unlawful from continuing to injure the Classes.

CLAIMS FOR RELIEF

REALLEGATION AND INCORPORATION BY REFERENCE

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

A. Nationwide Claims

<u>COUNT ONE</u>
Violation of the Magnuson-Moss Warranty Act
15 U.S.C. § 2301, *et. seq*.
(On behalf of the Nationwide Class)

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

283. Plaintiffs Pietosi and Rai bring this Count on their own behalf and on behalf of the Nationwide Class (collectively for the purposes of this Count, the "Magnuson-Moss Class").

284. This Court has jurisdiction to decide claims brought under 15 U.S.C. § 2301 by virtue of 28 U.S.C. § 1332(a)-(d).

285. The HP PCs are "consumer products" within the meaning of the Magnuson-Moss Warranty Act, 15 U.S.C. § 2301(3). The Plaintiffs and Magnuson-Moss Class Members are consumers because they are persons entitled under applicable state law to enforce against the warrantor the obligations of its implied warranties.

286. HP is a "supplier" and "warrantor" within the meaning of the Magnuson-Moss Warranty Act, 15 U.S.C. § 2301(4)-(5).

287. 15 U.S.C. § 2301(d)(1) provides a cause of action for any consumer who is damaged by the failure of a warrantor to comply with an implied warranty.

288. HP provided Plaintiffs and Magnuson-Moss Class members with an implied warranty of merchantability in connection with the purchase of the PCs with affected AMD processors (the "Affected PCs") that is an "implied warranty" within the meaning of the Magnuson-Moss Warranty Act, 15 U.S.C. § 2301(7). As part of the implied warranty of merchantability, HP warranted that the Affected PCs were fit for their ordinary purpose as PCs that provided (a) smooth playback of audio and video; (b) smooth gameplay; and/or (c) a secure TPM module that maintained a separation from privileged system memory, general system memory, and CPU resources, reducing the risk and effect of firmware attacks; and that the Affected PCs would pass without objection in trade as designed, manufactured, and marketed, and were adequately contained, packaged, and labeled.

289. HP breached its implied warranty, as described above, and is therefore liable to Plaintiffs and Class Members pursuant to 15 U.S.C. § 2310(d)(1). Without limitation, the Affected PCs share a common defect in that they are all equipped with the defectively designed AMD CPUs and fTPM subsystem described in this Complaint. This defective design impaired (a) smooth playback of audio and video, and (b) smooth gameplay. In addition, it failed to provide Plaintiffs and Magnuson-Moss Class Members with a secure TPM module that maintained a separation from privileged system memory, general system memory, and CPU resources, resulting in an increased vulnerability to firmware attacks.

290. As a result of the resulting Effects, the Affected PCs, when sold, and at all times thereafter were unmerchantable and unfit for their ordinary use.

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

292. Any limitations HP might seek to impose on their warranties are procedurally unconscionable. There was unequal bargaining power between HP and Plaintiffs (and Magnuson-Moss Class Members), as, at the time of purchase, Plaintiffs had no other viable options for purchasing warranty coverage other than from HP.

293. Any limitations HP might seek to impose on their warranties are substantively unconscionable. HP knew that the Affected PCs would result in the Effects set forth above and that the fTPM module was defectively designed and faulty. Moreover, HP knew that the Affected PCs would result in the Effects after the warranty purportedly expired. HP failed to disclose this defect to Plaintiffs. Thus, HP's enforcement of the durational limitations on those warranties is harsh and shocks the conscience.

294. To the extent a Plaintiff or Class Member is not in privity with HP, Privity of contract is not required here because Plaintiffs are intended third-party beneficiaries of contracts between AMD and HP, and specifically, of HP's implied warranties. HP's retailers and resellers have no rights under the warranty agreements provided with the Affected PCs; the warranty agreements were designed for and intended to benefit consumers. Plaintiffs are also the intended beneficiaries of retailer and reseller warranties.

295. Pursuant to 15 U.S.C. § 2310(e), Plaintiffs are entitled to bring this class action and are not required to give HP notice and an opportunity to cure until such time as the Court determines the representative capacity of Plaintiffs pursuant to Rule 23 of the Federal Rules of Civil Procedure.

296. Plaintiffs would suffer economic hardship if they returned their Affected PCs but did not receive the return of all payments made by them. Because HP has refused to acknowledge any revocation of acceptance and return immediately any payments made, Plaintiffs have not re-accepted their Affected PCs by retaining them.

297. The amount in controversy of Plaintiffs' individual claims meets or exceeds the sum of $25. The amount in controversy of this action exceeds the sum of $50,000, exclusive of interest and costs, computed on the basis of all claims to be determined in this lawsuit. Plaintiffs, individually and on behalf of all other Magnuson-Moss Class members, seek all damages permitted by law, including diminution in value of their PCs, in an amount to be proven at trial. In addition, pursuant to 15 U.S.C. § 2310(d)(2), Plaintiffs are entitled to recover a sum equal to the aggregate amount of costs and expenses (including attorneys' fees based on actual time expended) determined by the Court to have reasonably been incurred

by Plaintiffs and the other Magnuson-Moss Class Members in connection with the commencement and prosecution of this action.

298. Plaintiffs also seek the establishment of an HP-funded program for Plaintiffs and Magnuson-Moss Class members to recover out-of-pocket costs incurred in attempting to rectify and/or mitigate the effects of the defective AMD processors and the fTPM modules in the Affected PCs.

COUNT TWO
Fraud
(On behalf of the Nationwide Class)

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

300. Plaintiffs Pietosi and Rai bring this cause of action on their own behalf and on behalf of Nationwide Class Members against HP under the common law of fraud, which is materially uniform in all states. In the alternative, Plaintiffs bring this claim on behalf of the California and Pennsylvania Subclasses.

301. As described above, HP defrauded Plaintiffs and the Class Members by knowingly and intentionally misrepresenting to them and to the public at large that its PCs and laptops had superior design, security, performance, and quality, including as to the playback of audio/video, fitness for gaming, and security from attack, including a firmware attack.

302. As described above, HP carried out its fraudulent and deceptive conduct through affirmative misrepresentations, omissions, suppressions, and concealments of material facts to Plaintiffs and the Class Members, as well as to the public at large.

303. These representations were false, as detailed in this Complaint. HP knew that the representations were false and acted, with knowledge of their falsity, intentionally to induce Plaintiffs and Class Members to buy the Affected PCs, as well as to achieve windfall profits at the expense of Plaintiffs and the Class Members.

304. HP's actions constitute actual fraud and deceit because HP did the following with the intent to deceive Plaintiffs and the Class Members and to induce them to purchase the Affected PCs:

a. Suggesting that the Affected PCs were of superior quality, performance, and security, including as to audio/video playback and gaming, and as to the security of the incorporated CPU;

b. Positively asserting that that the Affected PCs were of superior quality, performance, and security, including as to audio/video playback and gaming, and as to the security of the incorporated CPU.

305. HP's misrepresentations were material in that they would affect a reasonable consumer's decision to purchase the Affected PCs. Plaintiffs and the Class Members paid a premium for the Affected PCs precisely because they were purported by HP to offer superior quality, performance, and security—including superior quality and performance in video and audio playback and gameplay. Whether HPs devices were defective would have been an important factor in Plaintiffs' and the Class Members' decision to purchase or obtain the Affected PCs.

306. HP's intentionally deceptive conduct induced Plaintiffs and the Class Members to purchase the Affected PCs and resulted in harm and damage to Plaintiffs and the Class Members.

307. Plaintiffs believed and relied to their detriment upon HP's affirmative misrepresentations. Class Members may be presumed to have believed and relied upon HP's misrepresentations because the facts to which those misrepresentations pertained were and are material to a reasonable consumer's decision to purchase the Affected PCs.

308. HP also fraudulently concealed and suppressed material facts regarding the Affected PCs. HP knew when it marketed and sold its PCs that they were not superior in quality, performance, and security as represented. HP failed to disclose these facts to consumers at the time it marketed and sold the Affected PCs. HP knowingly and intentionally engaged in this concealment in order to boost sales and revenues, maintain its competitive edge in the industry, and obtain windfall profits.

309. Plaintiffs and the Class Members had no reasonable means of knowing that HP's misrepresentations were false and misleading, or that HP had omitted to disclose material details relating to the Affected PCs. Plaintiffs and the Class Members did not and could not reasonably discover HP's concealment on their own.

310. HP had a duty to disclose, rather than conceal and suppress, the full scope and extent of the Affected PCs' defects, including the defective design of their AMD-based processors and incorporated fTPM subsystem:

a. HP had exclusive or far superior knowledge of the design of its AMD-based computer systems, including as to its onboard fTPM module;

b. The details regarding these computers' defective design and defective products were known and/or accessible only to HP;

c. HP knew Plaintiffs and the Class Members did not know about HP's defective PCs, including the defective design of the AMD processors incorporated in HP's PCs; and

d. HP made representations and assurances about the qualities of the Affected PCs, including statements about their performance, security, and quality that were misleading, deceptive, and incomplete without the disclosure of the fact that the AMD processors incorporated in HP's PCs were defectively designed.

311. These omitted and concealed facts were material because a reasonable consumer would rely on them in deciding to purchase the Affected PCs, and because they substantially reduced the value of the Affected PCs that Plaintiffs and the Class Members purchased. Whether the Affected PCs were defective would have been an important factor in Plaintiffs' and the Class Members' decisions to purchase or obtain the Affected PCs.

312. Plaintiffs and the Class Members trusted HP not to sell them products that were defective.

313. HP intentionally and actively concealed and suppressed these material facts to falsely assure consumers that the Affected PCs were of superior quality, performance, and security, as represented by HP and as reasonably expected by consumers.

314. Plaintiffs and the Class Members were unaware of these omitted material facts and would have paid less for the Affected PCs, or would not have purchased them at all, if they had known of the concealed and suppressed facts.

315. Plaintiffs and the Class Members relied to their detriment upon HP's reputation, fraudulent misrepresentations, and material omissions in deciding to purchase the Affected PCs.

316. As a direct and proximate result of HP's deceit and fraudulent concealment, including its intentional suppression of the true facts, Plaintiffs and the Class Members suffered injury. They purchased PCs of inferior quality, performance, and security, which had a diminished value by reason of HP's concealment of, and failure to disclose, the defects.

317. Plaintiffs and the Class Members sustained damages as a direct and proximate result of HP's deceit and fraudulent concealment in an amount to be proven at trial.

318. HP's acts were done maliciously, oppressively, deliberately, with intent to defraud, and in reckless disregard for Plaintiffs' and the Class Members' rights, with the aim of enriching HP, justifying an award of punitive damages in an amount sufficient to deter such wrongful conduct in the future.

COUNT THREE
Fraud by Concealment
(On behalf of the Nationwide Class)

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

320. Plaintiffs Pietosi and Rai bring this cause of action on their own behalf and on behalf of the Nationwide Class Members against HP under the common law of fraudulent concealment, which is materially uniform in all states. In the alternative, Plaintiffs bring this claim on behalf of the California and Pennsylvania Subclasses.

321. As alleged in this Complaint, HP intentionally concealed, suppressed, and omitted material facts regarding the defective Affected PCs, specifically that the Affected PCs did not provide (a) smooth playback of audio and video; (b) smooth gameplay; and/or (c) a secure TPM module that maintained a separation from privileged system memory, general system memory, and CPU resources, which (if provided) would reduce the risk and effect of firmware attacks.

322. HP also misrepresented the performance, quality, and security of the Affected PCs. These representations were false because, unbeknownst to Class Members, the Affected PCs contained defective and/or defectively designed AMD processors and on-board fTPM modules, rendering them less secure from firmware attacks and less capable of streaming audio/video or running games without stuttering.

323. HP's misrepresentations and omissions about the Affected PCs were material because the misrepresentations and omissions alleged in this Complaint induced Plaintiffs and the Class Members to purchase the Affected PCs when, had they known about the defective AMD processors and on-board fTPM modules, they would not have purchased the Affected PCs or they would have paid less for them.

324. HP knew about the defective AMD processor design, including as to the on-board fTPM module, before creating the false impression that the Affected PCs were of superior quality, security, and performance, including with respect to the provision of (a) smooth playback of audio and video; (b) smooth gameplay; and/or (c) a secure TPM module that maintained a separation from privileged system memory, general system memory, and CPU resources, reducing the risk and effect of firmware attacks. In truth and in fact, the Affected PCs did not comport with the impression created by HP.

325. Reasonable consumers, such as Plaintiffs and the Class Members, would not know the truth about the defective PCs, including about their defective AMD processors and on-board fTPM modules. Plaintiffs and the Class members did not know these facts, which were concealed from them by HP. Moreover, as ordinary consumers, Plaintiffs and the Class Members did not, and could not, unravel the deception on their own.

326. HP concealed the truth about the defective PCs, including as to the defective AMD processors and on-board fTPM modules, intending for Plaintiffs and the Class Members to rely on their misrepresentations and omissions. Plaintiffs and the Class Members relied on Defendant's misrepresentations and omissions in choosing to purchase the Affected PCs, believing them to be of superior quality, security, and performance, including as to the provision of (a) smooth playback of audio and video; (b) smooth gameplay; and/or (c) a secure TPM module that maintained a separation from privileged system memory, general system memory, and CPU resources, thereby reducing the risk and effect of firmware attacks. Plaintiffs and Class Members were reasonable and justified in their reliance on HP's representations about the PCs and its omissions about their defective nature because HP is a multinational PC designer and manufacturer well-versed in the design, manufacture, and service of devices like the PCs purchased by Plaintiffs and Class Members.

327. HP had a duty to disclose the defective nature of the PCs, including the defective AMD processors and on-board fTPM modules, because HP knew these facts were not known to or reasonably discoverable by Plaintiffs and the Class Members unless and until AMD acknowledged the defect. Plaintiffs and Class Members could not—and did not—discover HP's deception and the truth about their PCs on their own.

328. HP's omissions were made with knowledge of their falsity, and with the intent that Plaintiffs and the Class Members rely on them.

329. Plaintiffs and Class Members were entitled to rely on HP's misrepresentations and omissions because they are purchasers of HP's PCs, and Defendant has been enriched by the sales of these PCs.

330. Plaintiff and the Class Members reasonably relied on HP's misrepresentations and omissions, and suffered injury and monetary damages as a direct and proximate result. Had HP not concealed material facts regarding the Affected PCs, including as to the defective AMD computers and on-board fTPM modules incorporated within them, Plaintiffs and the Class Members would not have purchased the Affected PCs or would have paid less for them. Plaintiffs and the Class Members have also incurred out-of-pocket costs related to the Affected PCs; loss of use of their PCs; and diminished value in their Affected PCs because of HP's fraud and the growing public awareness about the Affected PCs' defect, including the incorporated AMD processors and on-board fTPM modules. Accordingly, HP is liable to Plaintiffs and the Class Members for damages in an amount to be proven at trial.

331. HP's acts were committed wantonly, maliciously, oppressively, deliberately, with intent to defraud; in reckless disregard of the rights of Plaintiffs and the Class Members; and in order for HP to enrich itself. HP's misconduct in this regard warrants an assessment of punitive damages in an amount sufficient to deter such conduct in the future, and such amount shall be determined according to proof at trial.

COUNT FOUR
Unjust Enrichment/Quasi-Contract
(On behalf of the Nationwide Class)

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

333. Plaintiffs Pietosi and Rai bring this cause of action on their own behalf and on behalf of the Nationwide Class Members against HP under the common law of unjust enrichment/quasi-contract, which is materially uniform in all states. In the alternative, Plaintiffs bring this claim on behalf of the California and Pennsylvania Subclasses.

334. Plaintiffs bring this claim as an alternative to the contractual warranty claims asserted in this Complaint and/or due to HP's intentional and deceptive efforts to conceal the defects in the Affected PCs and avoid its warranty obligations.

335. HP received hundreds of millions—if not billions—of dollars in revenue from the sale of Affected PCs.

336. This revenue was a benefit conferred upon HP by Plaintiffs and the Class Members.

337. HP was unjustly enriched through financial benefits conferred upon it by Plaintiffs and the Class Members, in the form of the amounts paid to HP for the Affected PCs.

338. Plaintiffs and the Class Members elected to purchase the Affected PCs based upon HP's misrepresentations, deception, and omissions. HP knew and understood that it would and did receive a financial benefit, and voluntarily accepted the same, from Plaintiffs and the Class Members when they elected to purchase the Affected PCs.

339. By selecting the Affected PCs and purchasing them at a premium price, Plaintiffs and the Class Members reasonably expected that the Affected PCs would have the performance, security, and quality promoted by HP.

340. Therefore, because HP will be unjustly enriched if it is allowed to retain the revenues obtained through falsehoods, deception, and misrepresentations, Plaintiffs and the Class Members are entitled to recover the amount by which HP was unjustly enriched at their expense.

341. Accordingly, Plaintiffs, on behalf of themselves and each Class Member, seek damages against HP in the amounts by which HP has been unjustly enriched at Plaintiffs' and the Class Members' expense, and such other relief as this Court deems just and proper.

COUNT FIVE
Breach of Implied Warranty of Merchantability
(On behalf of the Nationwide Class)

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

343. Plaintiffs Pietosi and Rai bring this cause of action on their own behalf and on behalf of the Nationwide Class under the law of warranties, which is materially uniform in all states. In the alternative, Plaintiffs bring this claim on behalf of the California and Pennsylvania Subclasses.

344. HP is and was at all relevant times a merchant with respect to its PCs, including the Affected PCs.

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

346. HP marked the Affected PCs as having high quality, speed, performance, and security, that would function, at least, as reasonably expected by consumers and in accordance with industry standards. HP's representations formed the basis of the bargain in Plaintiffs' and Class Members' decisions to purchase the Affected PCs.

347. Plaintiffs and other Class Members purchased the Affected PCs from HP, or through retailers or resellers. At all relevant times, HP was the manufacturer, distributor, warrantor, and/or seller of the Affected PCs.

348. HP knew or had reason to know of the specific use for which the Affected PCs were purchased.

349. Because of the defective AMD-based CPUs and integrated fTPM subsystems in the Affected PCs, the Affected PCs were not in merchantable condition when sold and are not fit for the ordinary purpose of such PCs.

350. HP knew about the defect in the Affected PCs, allowing HP to cure its breach of warranty if it chose.

351. HP's attempt to disclaim or limit the implied warranty of merchantability vis-à-vis consumers is unconscionable and unenforceable here. Specifically, HP's warranty limitation is unenforceable because it knowingly sold a defective product without informing consumers about the defect. The time limits contained in HP's warranty periods were also unconscionable and inadequate to protect Plaintiffs and the Class Members. Among other things, Plaintiffs and the Class Members had no meaningful choice in determining these time limitations, the terms of which unreasonably favored HP. A gross disparity in bargaining power existed between HP and Plaintiffs/Class Members, and HP knew of the defect at issue in this Complaint at the time in sold PCs to Plaintiffs and Class Members.

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

353. Accordingly, HP is liable to Plaintiffs and the Class Members for damages in an amount to be proven at trial.

B. Claims Brought on Behalf of the California Subclass or the California Consumer Subclass

<u>COUNT SIX</u>
Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On behalf of the California Subclass)

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

355. Plaintiff Rai brings this Count on his own behalf and on behalf of the California Subclass.

356. California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq.*, proscribes acts of unfair competition, including "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." HP has engaged in unfair or deceptive

acts or practices that violated the UCL, as described above and below, by, among other things, representing that the Affected PCs have characteristics, uses, benefits, and qualities which they do not have; representing that the Affected PCs are of a particular standard, quality and grade when they are not; advertising that the Affected PCs are of a particular standard, quality, and grade when they are not; advertising the Affected PCs with the intent not to sell them as advertised; and representing that the Affected PCs had been supplied in accordance with their representations, when they had not. HP has violated the unlawful, unfair, and fraudulent prongs of the UCL, as set forth in this Complaint and below.

357. In the course of HP's business, it willfully failed to disclose and actively concealed that the Affected PCs were defective, such that normal use of HP's Affected PCs would not provide (a) smooth playback of audio and video; (b) smooth gameplay; and/or (c) a secure TPM module that maintained a separation from privileged system memory, general system memory, and CPU resources, reducing the risk and effect of a firmware attack. Particularly in light of HP's advertising campaign, a reasonable American consumer would expect the Affected PCs to provide (a) smooth playback of audio and video; (b) smooth gameplay; and/or (c) a secure TPM module that maintained a separation from privileged system memory, general system memory, and CPU resources, reducing the risk and effect of a firmware attack. Accordingly, HP engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of material facts with intent that others rely upon such concealment, suppression, or omission, in connection with the sale of the Affected PCs.

358. In purchasing the Affected PCs, Plaintiffs and the Class members were deceived by HP's failure to disclose that normal use of the Affected PCs would not provide (a) smooth playback of audio and video, (b) smooth gameplay, and/or (c) a secure TPM module that maintained a separation from privileged system memory, general system memory, and CPU resources, reducing the risk of a firmware attack.

359. Plaintiff and the Class members reasonably relied upon HP's false misrepresentations. They had no way of knowing that HP's representations were false and misleading. As alleged herein, HP engaged in sophisticated methods of deception, including about highly technical matters for which there

is an inherent asymmetry of information. Plaintiff and the Class members did not, and could not, find out about HP's deception on their own, as Plaintiffs and the Class members were not aware of the defective nature of HP's PCs and laptops.

360. HP actions as set forth above occurred in the conduct of trade or commerce.

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

362. HP intentionally and knowingly misrepresented material facts regarding the Affected PCs it manufactured and sold with intent to mislead Plaintiff Rai and the California Subclass Members.

363. HP knew or should have known that its conduct violated California law regarding unfair or deceptive acts in trade or commerce.

364. HP owed Plaintiff Rai and the California Subclass Members a duty to disclose the truth about the Affected PCs because HP:

a. Possessed exclusive knowledge of the design of the Affected PCs with defective AMD processors and fTPM modules;

b. Intentionally concealed the above from Plaintiff Rai and the California Subclass Members; and/or

c. Made incomplete representations regarding the quality of the Affected PCs, while purposefully withholding material facts from Plaintiff Rai and the California Subclass Members that contradicted these representations.

365. Due to the specific and superior knowledge that HP possessed, its false representations regarding the quality of the Affected PCs, and Plaintiff Rai and the California Subclass Members' reliance on these material representations, HP had a duty to disclose Plaintiff Rai and the California Subclass Members that the Affected PCs were defective, *i.e.*, that HP's Affected PCs do not provide (a) smooth playback of audio and video; (b) smooth gameplay; and/or (c) a secure TPM module that maintains a separation from privileged system memory, general system memory, and CPU resources, reducing the risk and effect of a firmware attack. Having volunteered to provide information to Plaintiff Rai and the California Subclass Members, HP had the duty to disclose not just the partial truth, but the entire truth.

These omitted and concealed facts were material because they directly impact the value of the Affected PCs that were purchased by Plaintiff Rai and the California Subclass Members. Smooth audio/video playback, smooth gameplay, and a secure TPM module that reduces the risk and effect of a firmware attack are material concerns to PC consumers like (and including) Plaintiff Rai and the California Subclass Members. HP represented to Plaintiff Rai and the California Subclass Members that they were purchasing PCs that were free from defect, when in fact they were defective.

366. HP's conduct proximately caused injuries to Plaintiff Rai and the California Subclass Members.

367. Plaintiff Rai and the California Subclass Members were injured and suffered ascertainable loss, injury-in-fact, and/or actual damage as a proximate result of HP's conduct: Plaintiff Rai and the California Subclass Members overpaid for Affected PCs, and the Affected PCs suffered a diminution in value. These injuries are the direct and natural consequence of HP's misrepresentations and omissions.

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

369. As a direct and proximate result of HP's violations of the UCL, Plaintiff Rai and the California Subclass Members have suffered injury-in-fact and/or actual damage.

370. Defendants have been unjustly enriched and should be required to make restitution to Plaintiff Rai and the California Subclass Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code. Plaintiff Rai and the California Subclass Members also seek injunctive relief as deemed appropriate by the Court.

COUNT SEVEN
Violation of the California Consumer Legal Remedies Act
Cal. Civ. Code § 1750, *et seq*.
(On behalf of the California Consumer Subclass)

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

372. Plaintiff Rai brings this Count on his own behalf and on behalf of the California Consumer Subclass.

373. Plaintiff Rai and other members of the California Consumer Subclass are "consumers" as defined in Cal. Civ. Code § 1761(d), and Plaintiff Rai, the California Consumer Subclass Members, and HP are "persons" as defined in Cal. Civ. Code § 1761(c).

374. The PCs made by HP are "goods" as defined in Cal. Civ. Code § 1761(a).

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

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

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

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

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

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

377. In the course of HP's business, it willfully failed to disclose and actively concealed that the Affected PCs were defective, such that normal use of the Affected PCs would not provide (a) smooth playback of audio and video; (b) smooth gameplay; and/or (c) a secure TPM module that maintains a separation from privileged system memory, general system memory, and CPU resources, thereby reducing the risk and effect of firmware attacks. Particularly in light of HP's advertising campaign, a reasonable California consumer would expect the Affected PCs to provide (a) smooth playback of audio

and video; (b) smooth gameplay; and/or (c) a secure TPM module that maintains a separation from privileged system memory, general system memory, and CPU resources, reducing the risk and effect of a firmware attack. Accordingly, HP engaged in unlawful trade practices by employing deception, deceptive acts or practices; fraud; misrepresentation; or concealment, suppression, or omission of material facts with intent that others rely upon such concealment, suppression, or omission, in connection with the sale of the Affected PCs.

378. In purchasing the Affected PCs, Plaintiff Rai and the California Consumer Subclass Members were deceived by HP's failure to disclose that normal use of the Affected PCs would not provide (a) smooth playback of audio and video; (b) smooth gameplay; and/or (c) a secure TPM module that maintains a separation from privileged system memory, general system memory, and CPU resources, thereby reducing the risk and effect of a firmware attack.

379. Plaintiff Rai and the California Consumer Subclass Members reasonably relied upon HP's false misrepresentations. They had no way of knowing that HP's representations were false and misleading. As alleged in this Complaint, HP engaged in sophisticated methods of deception, including about highly technical matters for which there was (and is) an inherent asymmetry of information. Plaintiff Rai and the California Consumer Subclass Members did not, and could not, discover HP's deception on their own, as Plaintiff Rai and the California Consumer Subclass Members were not aware of the defective nature of the Affected PCs prior to purchase.

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

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

382. HP intentionally and knowingly misrepresented material facts regarding the Affected PCs with intent to mislead Plaintiff Rai and the California Consumer Subclass Members.

383. HP owed Plaintiff Rai and the California Consumer Subclass Members a duty to disclose the truth about the Affected PCs because HP:

a. Possessed exclusive knowledge of the design of its PCs, including the defective nature of the AMD processors and onboard fTPM modules that HP incorporated into the Affected PCs;

b. Intentionally concealed the above from Plaintiff Rai and the California Consumer Subclass Members; and/or

c. Made incomplete representations regarding the performance of the Affected PCs, while purposefully withholding material facts from Plaintiff Rai and the California Consumer Subclass Members that contradicted these representations.

384. Due to its specific and superior knowledge that the Affected PCs did not provide (a) smooth playback of audio and video; (b) smooth gameplay; and/or (c) a secure TPM module that maintained a separation from privileged system memory, general system memory, and CPU resources (reducing the risk and effect of a firmware attack), HP had a duty to disclose to Plaintiff Rai and the California Consumer Subclass Members that the Affected PCs were defective. Moreover, HP had a duty to disclose that its PCs and laptops did not provide (a) smooth playback of audio and video, (b) smooth gameplay, and/or (c) a secure TPM module that maintained a separation from privileged system memory, general system memory, and CPU resources that would reduce the risk and effect of firmware attacks. Having volunteered to provide information to Plaintiff Rai and the California Consumer Subclass Members, HP had the duty to disclose not just the partial truth, but the entire truth. These omitted and concealed facts were material because they directly impacted, and impact, the value of the Affected PCs purchased by Plaintiff Rai and the California Consumer Subclass Members.

385. The following features are material to Plaintiff Rai and the California Consumer Subclass Members: (a) smooth playback of audio and video, (b) smooth gameplay, and/or (c) a secure TPM module that maintains a separation from privileged system memory, general system memory, and CPU resources, reducing the risk and effect of firmware attacks.

386. HP represented to Plaintiff Rai and the California Consumer Subclass Members that they were purchasing PCs that were free from defect, when in fact the PCs were defective.

387. HP's conduct proximately caused injuries to Plaintiff Rai and the California Consumer Subclass Members.

388. Plaintiff Rai and the California Consumer Subclass Members were injured and suffered ascertainable loss, injury-in-fact, and/or actual damage as a proximate result of HP's conduct. Plaintiff Rai and the California Consumer Subclass Members overpaid for the Affected PCs, and the Affected PCs have suffered a diminution in value. These injuries are the direct and natural consequence of HP's misrepresentations and omissions.

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

390. As a direct and proximate result of HP's violations of the CLRA, Plaintiff Rai and the California Consumer Subclass Members have suffered injury-in-fact and/or actual damage.

391. As a result of HP's violations of the CLRA, Plaintiff Rai, on behalf of himself, the California Consumer Subclass Members, and the general public of the State of California, seeks injunctive relief prohibiting HP from continuing the unlawful practices described in this Count and in this Complaint, pursuant to Cal. Civ. Code § 1782(a)(2); equitable relief, including restitution; and a declaration that HP's conduct violated the CLRA.

392. Pursuant to Cal. Civ. Code § 1782, on July 22, 2022, Plaintiff Rai, on behalf of himself, the California Consumer Subclass, and the general public of the State of California, mailed HP notice in writing, via certified U.S. mail, of HP's particular violations of the CLRA and demanded that HP rectify the actions described above by providing complete monetary relief, agreeing to be bound by HP's legal obligations, and giving notice to all affected customers of HP's intent to do so.

393. If HP fails to respond to the letter within 30 days and to take the actions demanded to rectify its violations of the CLRA, Plaintiff Rai will amend this Complaint to seek damages and attorneys' fees as allowed by the CLRA, including actual and punitive damages under the CLRA pursuant to Civil Code § 1780(a), and an additional award of up to $5,000 to each Plaintiff and California Consumer

Subclass Member who is a "senior citizen," as well as any other remedies the Court may deem appropriate under the CLRA.

COUNT EIGHT
Violation of the California False Advertising Law
Cal. Bus. & Prof. Code § 17500, et seq.
(On behalf of the California Subclass)

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

395. Plaintiff Rai brings this Count on his own behalf and on behalf of the California Subclass.

396. HP has benefited from intentionally selling defective PCs at artificially inflated prices due to fraudulent statements about the PCs and about the defective design of AMD processors incorporated in those PCs. HP has received unjust profits from this conduct, and Plaintiff Rai and the California Subclass Members overpaid for Affected PCs made by HP as a result of this conduct.

397. HP publicly disseminated advertising and promotional material that was designed and intended to convey to the public that the Affected PCs were capable of providing (a) smooth playback of audio and video; (b) smooth gameplay; and/or (c) a secure TPM module that maintained a separation from privileged system memory, general system memory, and CPU resources, reducing the risk and effect of a firmware attack.

398. HP was aware of the defective AMD processors and fTPM modules in the Affected PCs at the time Plaintiff Rai and the California Subclass Members purchased the Affected PCs. HP intentionally designed its Affected PCs to defraud consumers about whether those PCs provided (a) smooth playback of audio and video; (b) smooth gameplay; and/or (c) a secure TPM module that maintained a separation from privileged system memory, general system memory, and CPU resources, reducing the risk and effect of a firmware attack.

399. However, HP intentionally made representations in advertisements about the superior performance (including for video and audio playback and gameplay) and security of its Affected PCs yet—due to defects HP was aware of in the AMD processors and fTPM modules in those PCs—did not

sell Affected PCs that conformed to the representations and promises in HP's publicly disseminated advertisements.

400. HP unjustly received and retained benefits from Plaintiff Rai and the California Subclass Members.

401. It is inequitable and unconscionable for HP to retain these benefits.

402. Because HP wrongfully concealed its misconduct, Plaintiff Rai and the California Subclass Members were not aware of the facts concerning the Affected PCs and did not benefit from HP's misconduct.

403. HP knowingly accepted the unjust benefits of its wrongful conduct.

404. HP had notice of conduct as alleged in this Complaint.

405. As a result of HP's misconduct, Plaintiff Rai and the California Subclass Members suffered an injury-in-fact and lost money and/or property in an amount to be proven at trial.

COUNT NINE
Breach of Implied Warranty of Merchantability
Cal. Comm. Code §§ 2314 and 10212
(On behalf of the California Subclass)

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

407. Plaintiff Rai brings this Count individually and on behalf of the California Subclass against HP.

408. As set forth above, Plaintiff Rai and the California Subclass Members have suffered from a defect that existed in the Affected PCs—the defective AMD processors and fTPM modules described in this Complaint—which were defective upon the first use of the Affected PCs. Plaintiff Rai and the California Subclass Members seek to recover for this manifested defect and any and all consequential damages stemming from the defect.

409. A warranty that the Affected PCs were in merchantable condition and fit for the ordinary purpose for which the Affected PCs are used is implied by law pursuant to Cal. Comm. Code §§ 2314 and 10212. To be merchantable and fit for ordinary purpose, the Affected PCs should have been

substantially free from defects. As explained in this Complaint, the Affected PCs were not substantially free from defects: the Affected PCs contain existing, manifested defects, including that the Affected PCs fail to provide (a) smooth audio and video playback; (b) smooth gameplay; and (c) a secure TPM module that maintains a separation from privileged system memory, general system memory, and CPU resources, which (if provided) would reduce the risk and effect of firmware attacks. These Effects render the Affected PCs unmerchantable and unreliable.

410. HP is and was at all times a "merchant" with respect to the Affected PCs under Cal. Comm. Code §§ 2104(1) and 10103(c), and a "seller" of PCs under § 2103(1)(d).

411. The Affected PCs are and were at all relevant times "goods" within the meaning of Cal. Comm. Code §§ 2105(1) and 10103(a)(8).

412. A warranty that the Affected PCs were in merchantable condition and fit for the ordinary purpose for which the Affected PCs are used is implied by law pursuant to Cal. Comm. Code §§ 2314 and 10212.

413. The Affected PCs when sold, and at all times thereafter, were not in merchantable condition and are not fit for the ordinary purpose for which they are used. Specifically, the Affected PCs fail to provide (a) smooth audio and video playback; (b) smooth gameplay; and (c) a secure TPM module that maintains a separation from privileged system memory, general system memory, and CPU resources, which would (if provided) reduce the risk and effect of firmware attacks.

414. It was reasonable to expect that Plaintiff Rai and the California Subclass Members may use, consume, or be affected by the defective PCs, regardless of contractual privity with HP.

415. The Affected PCs contained an inherent defect that was substantially certain to result in malfunction during the useful life of the product.

416. Plaintiff Rai and the California Subclass Members were and are third-party beneficiaries to HP's contracts with AMD and with retailers who sold the Affected PCs.

417. HP was provided notice of these issues within a reasonable time of Plaintiff Rai's knowledge of the non-conforming or defective nature of the Affected PCs, including by letter from

Plaintiff's counsel sent to HP; by complaints from California Subclass Members, including on HP's message boards; and/or by the allegations contained in this Complaint.

418. As a direct and proximate result of HP's breach of the implied warranty of merchantability, Plaintiff Rai and the California Subclass Members have been damaged in an amount to be proven at trial.

COUNT TEN
Breach of Implied Warranty of Merchantability
Cal. Civ. Code § 1791, *et seq.*
(On behalf of the California Subclass)

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

420. Plaintiff Rai brings this claim on his own behalf and on behalf of the California Subclass.

421. The Affected PCs are "consumer goods" and Plaintiff Rai and the California Subclass Members are "buyers" within the meaning of Cal. Civ. Code § 1791. HP is also a "manufacturer," "distributor," or "retail seller" under Cal. Civ. Code § 1791.

422. The implied warranty of merchantability included with the sale of each PC means that HP warranted that each Affected PC (a) would pass without objection in trade under the contract description; (b) was fit for the ordinary purposes for which the Affected PC would be used; and (c) conformed to the promises or affirmations of fact made on the container or label.

423. The Affected PCs would not pass without objection in the PC trade because the Affected PCs fail to provide (a) smooth audio and video playback; (b) smooth gameplay; and (c) a secure TPM module that maintains a separation from privileged system memory, general system memory, and CPU resources, thereby reducing the risk and effect of firmware attacks. This makes the Affected PCs unfit for the ordinary purpose for which they would be used.

424. The Affected PCs are not adequately labeled because their labeling fails to disclose the defect and risks, and does not advise Rai or other members of the proposed California Subclass of the existence of the defect and the resulting Effects prior to experiencing the Effects firsthand in their Affected PCs.

425. HP's actions have deprived Plaintiff Rai and the California Subclass Members of the benefit of their bargains and have caused their Affected PCs to be worth less than what Plaintiff Rai and the California Subclass Members paid.

426. As a direct and proximate result of HP's breach of implied warranty, Plaintiff Rai and the California Subclass Members received goods whose condition substantially impairs their value. Plaintiff Rai and the California Subclass Members have been damaged by the diminished value of their Affected PCs.

427. Under Cal. Civ. Code §§ 1791.1(d) and 1794, Plaintiff Rai and the California Subclass Members are entitled to damages and other legal and equitable relief, including at their election, the right to revoke acceptance of the Affected PCs or to recover for the overpayment or diminution in value of their Affected PCs. They are also entitled to all incidental and consequential damages resulting from HP's breach, as well as reasonable attorneys' fees and costs.

C. Claims Brought on Behalf of the Pennsylvania Subclass

<u>COUNT ELEVEN</u>
Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law
73 PA. Cons. Stat. § 201-1, *et seq*.
(On behalf of the Pennsylvania Subclass)

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

429. Plaintiff Pietosi brings this Count on her own behalf and on behalf of the Pennsylvania Subclass against HP.

430. Defendant HP qualifies as a "person" within the meaning of 73 PA. Const. Stat. § 201-2(2).

431. Plaintiff Pietosi and the Pennsylvania Subclass Members are "persons" under 73 PA. Cons. Stat. § 201-2(2). Plaintiff Pietosi and the Pennsylvania Subclass Members purchased Affected PCs for personal, family, or household purposes within the meaning of 73 PA. Cons. Stat. § 201-9.2, and HP's actions as set forth in this Complaint occurred in the conduct of trade or commerce within the meaning of 73 PA. Cons. Stat. § 201-2(3).

432. The Pennsylvania Unfair Trade Practices and Consumer Protection Law (the "Pennsylvania CPL") prohibits unfair or deceptive acts or practices, including representing that goods or services have characteristic, benefits or qualities that they do not have; representing that goods or services are of a particular standard, quality or grade if they are of another; advertising goods or services with intent not to sell them as advertised and certified; and engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or misunderstanding. 73 PA. Cons. Stat. § 201-2(4). HP committed deceptive acts or practices in the conduct or trade or commerce, by, among other things: (a) engaging in unconscionable acts; (b) representing that the Affected PCs have characteristics, uses, benefits, and qualities which they not have; and (c) representing that the Affected PCs are of a particular standard, quality, and grade when they are not.

433. In the course of HP's business, it willfully failed to disclose and actively concealed that the Affected PCs were defective, and that as a result of the defective AMD processors and incorporated fTPM modules, the Affected PCs failed to provide (a) smooth audio and video playback; (b) smooth gameplay; and (c) a secure TPM module that maintains a separation from privileged system memory, general system memory, and CPU resources, thereby (if provided) reducing the risk and effect of firmware attacks. Particularly in light of HP's advertising campaign, a reasonable American consumer would expect the Affected PCs to be fully functional (including with respect to smooth audio, video, and game playback) and secure (including through hardware-based protection against firmware attacks). They were not. Accordingly, and as set forth in this Complaint, HP has engaged (and continues to engage) in unlawful trade practices by employing deception; deceptive acts or practices; fraud, misrepresentations, or concealment, suppression; and/or omission of material facts with intent that others rely upon such concealment, suppression, or omission in connection with the sale of the Affected PCs.

434. In purchasing the Affected PCs, Plaintiff Pietosi and the Pennsylvania Subclass Members were deceived by HP's failure to disclose that normal use of the Affected PCs does not provide (a) smooth audio and video playback; (b) smooth gameplay; and (c) a secure TPM module that maintains a separation from privileged system memory, general system memory, and CPU resources, thereby reducing the risk and effect of firmware attacks.

435. Plaintiff Pietosi and the Pennsylvania Subclass Members reasonably relied upon HP's false representations. They had no way of knowing that HP's representations were false and gravely misleading. As alleged in this Complaint, HP engaged in technically sophisticated methods of deception. Plaintiff Pietosi and the Pennsylvania Subclass Members did not, and could not, unravel HP's deception on their own, and were not aware of the defective condition of the Affected PCs.

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

437. HP's deception, fraud, misrepresentation, concealment, suppression, and/or omission of material facts was likely to—and did in fact—deceive reasonable consumers, including Plaintiff Pietosi and the Pennsylvania Subclass Members.

438. HP intentionally and knowingly misrepresented material facts regarding the Affected PCs, with intent to mislead Plaintiff Pietosi and the Pennsylvania Subclass Members.

439. HP knew or should have known that its conduct violated the Pennsylvania CPL.

440. HP owed Plaintiff Pietosi and the Pennsylvania Subclass Members a duty to disclose the truth about the defective PCs because HP:

a. Possessed exclusive knowledge of the design of the Affected PCs, including as to the incorporation of defective AMD processors that contained defective AMD fTPM subsystems;

b. Intentionally concealed the foregoing from Plaintiff Pietosi and the Pennsylvania Subclass Members; and/or

c. Made incomplete representations regarding the quality, performance and durability of the Affected PCs, while purposefully withholding material facts from Plaintiff Pietosi and the Pennsylvania Subclass Members that contradicted these representations.

441. Due to HP's (a) specific and superior knowledge that the AMD processors incorporated in the Affected PCs were defective, including that they included defectively designed AMD fTPM subsystems; (b) HP's false representations regarding the performance, durability, security, and functionality of the Affected PCs; and (c) Plaintiff Pietosi and the Pennsylvania Subclass Members' reliance on these material representations, HP had a duty to disclose to Plaintiff Pietosi and the

Pennsylvania Subclass Members that the Affected PCs were defective. Having volunteered to provide information to Plaintiff Pietosi and the Pennsylvania Subclass Members, HP had the duty to disclose not just the partial truth, but the entire truth. The facts that HP omitted and concealed were material because they directly impact the value of the Affected PCs purchased by Plaintiff Pietosi and the Pennsylvania Subclass Members. Functionality, performance, and security—including, specifically, smooth audio, video, and game playback, and hardware security against firmware attacks—are material concerns to PC consumers, including Plaintiff Pietosi and the Pennsylvania Subclass Members. HP represented that the Affected PCs were free from defect, when in fact they included defective AMD-based processors and fTPM subsystems.

442. HP's conduct proximately caused injuries to Plaintiff Pietosi and the Pennsylvania Subclass Members.

443. Plaintiff Pietosi and the Pennsylvania Subclass Members members were injured and suffered ascertainable loss, injury in fact, and/or actual damage as a proximate result of HP's conduct. Plaintiff Pietosi and the Pennsylvania Subclass Members overpaid for their PCs and did not receive the benefit of their bargain, and their Affected PCs have suffered a diminution in value. These injuries are direct and natural consequences of HP's misrepresentations and omissions.

444. HP's violations present a continuing risk to Plaintiff Pietosi and the Pennsylvania Subclass Members, as well as to the general public. HP's unlawful acts and practices complained of in this Complaint affect the public interest; they offend public policy; and they are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers (including to Plaintiff Pietosi and the Pennsylvania Subclass Members).

445. HP is liable to Plaintiff Pietosi and the Pennsylvania Subclass Members for treble their actual damages or $100—whichever is greater—and for attorneys' fees and costs. 73 PA Cons. Stat. § 201-9.2(a). Plaintiff Pietosi and the Pennsylvania Subclass Members are also entitled to an award of punitive damages given that HP's conduct was malicious, wanton, willful, oppressive, and/or exhibited a reckless indifference to the rights of others.

COUNT TWELVE
Breach of Implied Warranty of Merchantability
13 PA. Stat. Ann. § 2314
(On behalf of the Pennsylvania Subclass)

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

447. Plaintiff Pietosi brings this Count on her own behalf and on behalf of the Pennsylvania Subclass Members against HP.

448. HP is a merchant with respect to PCs within the meaning of 13 PA. Stat. Ann. § 2104.

449. Pursuant to 13 PA. Stat. Ann. § 2-314, a warranty that the Affected PCs were in merchantable condition was implied by law in the transactions in which Plaintiff Pietosi and the Pennsylvania Subclass Members purchased their Affected PCs.

450. The Affected PCs, when sold and at all times thereafter, were not in merchantable condition, and are not fit for the ordinary purpose for which the Affected PCs are used. Specifically, the Affected PCs resulted in the Effects described in this Complaint.

451. Plaintiff Pietosi and the Pennsylvania Subclass Members did not receive or otherwise have the opportunity to review, at or before the time of sale, a written warranty containing purported exclusions and limitations of remedies. Accordingly, any such exclusions and limitations of remedies are unconscionable and unenforceable, and Plaintiffs are entitled to all remedies available under Article 2 of the Uniform Commercial Code and other state laws of each Subclass. Any purported warranty disclaimers, exclusions, and limitations were unconscionable and unenforceable.

452. As a direct and proximate result of HP's breach of the implied warranty of merchantability, Plaintiff and Pennsylvania Subclass Members have been damaged in an amount to be proven at trial.

REQUEST FOR RELIEF

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

A. Certification of the proposed Nationwide and State Subclasses, including appointment of Plaintiffs' counsel as Class Counsel;

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

C. Injunctive relief in the form of a buy-back;

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

E. Restitution, including at the election of the Class and Subclass Members, recovery of the purchase price of their Affected PCs, or the overpayment for their Affected PCs;

F. Damages, costs, and disgorgement in an amount to be determined at trial;

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

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

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

JURY DEMAND

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

Dated: July 24, 2022

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

Respectfully submitted,

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

Attorneys for Plaintiffs