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
Barton Oaks Plaza I, Suite 300
Austin, TX 78746
Tel.: (213) 462-2772

Attorneys for Plaintiff and the Proposed Classes

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

STEPHEN STEWART, individually and on behalf of all others similarly situated,

Plaintiff,

v.

ACER INC., a Taiwanese Corporation, and ACER AMERICA CORPORATION, a California corporation,

Defendants.

Case No. 5:22-cv-04684

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 Defendants Acer Inc. and Acer America Corporation (collectively, "Acer") make, market, and sell exactly these types of seriously flawed computers. Numerous Acer PCs—specifically, Acer 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 Acer 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. Acer, however, does not acknowledge any of this. Instead, on its website and elsewhere Acer specifically markets its AMD desktop and laptop computers as especially suited for watching video, for videoconferencing, and for gaming. Acer also touts these computers' "robust," "multi-layered" security.

5. The Plaintiff in this case—like many other similarly situated Americans—purchased an Acer personal computer with an AMD processor that includes AMD's defective fTPM design. He has experienced severe stuttering in media playback and in videoconferencing. Like other members of the putative classes, Plaintiff's computer is also uniquely vulnerable to firmware attacks that could compromise not just Plaintiff's Acer computer, but potentially his home or business networks. The AMD fTPM design defect and its manifestations has significantly—perhaps totally—impaired the value of

Plaintiff's and class members' Acer 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 Acer computers in Acer forums and across the Internet—Acer has done nothing to fix or replace its defective computers.

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

* * *

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

8. Acer 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. Acer preinstalls Windows 11 on most of its PCs.

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

10. Acer is deeply involved with the design of its PCs, including as to the CPUs it incorporates into its PCs. Acer'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 Acer's customers.

11. Put simply, Acer and AMD work hand in hand to integrate AMD CPUs into Acer 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. Acer, 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), Acer had to ensure that every one of its desktop and laptop computers included an onboard TPM.

15. Faced with a potentially burdensome redesign, Acer 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)—an 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 Acer, fTPM avoided a major hassle: Acer would not need to ship new hardware with its AMD-based PCs in order to make them compatible with Windows 11. Instead, Acer 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. Acer'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 Acer'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 Acer PCs with AMD Ryzen or Athlon processors. Reports flooded online forums and YouTube channels describing Acer 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 Acer directly targets for PC sales, the defective Acer 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 Acer and other AMD-based computers. Despite Acer's promises that its AMD-based PCs were suitable for ordinary uses, such as watching video, listening to music, videoconferencing, and playing games, its AMD PCs stuttered during each of these baseline applications.

22. ***Second***, the flawed fTPM design left Acer'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 Acer 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 Acer's customers that its AMD-based PCs had significant stuttering problems, Acer 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. Acer 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 Acer incorporated into its PCs, including laptop computers that Acer 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 Acer), 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 Acer 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 Acer. Based on a pre-complaint statistical conjoint study (described in Section VI of this Complaint), (i) the defective Acer PCs were worth less at purchase than the price Plaintiff and Class Members paid for them, resulting in an out-of-pocket loss at purchase; (ii) each Effect caused a diminution in value of Acer's AMD-based PCs owned by Plaintiff and Class Members; and (iii) these PCs will remain defective until Acer recalls and replaces the faulty AMD CPUs in Plaintiff's and Class Members' PCs.

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

PARTIES

I. PLAINTIFF

30. Stephen Stewart is a domiciled resident of Florida, residing in Cape Coral. In 2021, Mr. Stewart purchased a new Acer Aspire 5 laptop from Amazon.com with an AMD Ryzen processor. Mr. Stewart reviewed and relied upon marketing materials and advertisements concerning the Acer laptop prior to purchasing it, including materials on the Acer.com website regarding the processor, graphics package, video play capabilities, and provided warranties. Mr. Stewart purchased his laptop specifically to use multiple applications at the same time; for video- and audioconferencing; and to stream video and audio, including online—all features of his Acer laptop that had been advertised to him, including on Acer.com. Since purchasing his laptop, Mr. Stewart has experienced stuttering during video and audio calls, as well as while streaming video and audio. The stuttering issue occurs at least three to four times per month, typically during heavy processor usage. All the materials Mr. Stewart reviewed and relied upon before purchasing his Acer laptop were positive, and none of the representations received and reviewed by Mr. Stewart contained any disclosure relating to the defective AMD CPU and onboard fTPM module in his Acer computer. Mr. Stewart would not have purchased his Acer laptop at the price he paid had he known about the AMD fTPM defect described in this Complaint. Acer has not fixed the problems with Mr. Stewart's laptop attributable to the AMD fTPM defect, including its stuttering during audiovisual playback and its unique vulnerability to firmware attacks. Mr. Stewart would like these problems fixed.

II. DEFENDANTS

31. Defendant Acer Inc. is a foreign corporation organized and existing under the laws of Taiwan, with its principal place of business at 8F, 88, Sec. 1, Xintai 5th Road, Xizhi, New Taipei City 221, Taiwan.

32. Defendant Acer America Corporation ("Acer America") is a corporation organized and existing under the laws of the State of California, with its principal place of business located at 1730 N. 1st Street, Suite 400, San Jose, California 95112.

33. Acer is a global provider of personal computing devices, including laptops and desktop computers specifically designed to run Microsoft's Windows operating system, as well as so-called "Chromebooks" that run Google's Chrome operating system.

34. For example, Acer sells Windows-based laptops under the Acer Aspire, Acer Nitro, Acer Swift, and Acer TravelMate product lines.

35. The central processing units (CPUs) in Acer's Windows-based personal computers come from two—and only two—sources: Intel and AMD.

36. Acer sells AMD-based computers in, among other things, its Acer Aspire, Acer Nitro, Acer Swift, and Acer TravelMate laptop computer lines.

37. In 2021, Acer Inc. reported consolidated revenues of NT$319.01 billion (approximately $10.63 billion USD), and net profits of NT$10.90 billion (approximately $360 million).

38. At the end of 2021, Acer had over 7,700 employees worldwide, with several hundred employees in the United States, including at Acer America's headquarters in San Jose, California.

JURISDICTION AND VENUE

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

40. 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 the Acer Defendants, 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.

41. This Court has personal jurisdiction over Defendant Acer America because Acer America is incorporated in and has its principal place of business is in the State of California, and Acer America 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.

42. This Court has personal jurisdiction over Defendant Acer Inc. because it has, along with Acer America, directly and/or through their agents and/or intermediaries, designed, produced, marketed,

sold, and serviced products, including the Affected PCs, in the this judicial district, establishing minimum contacts with this district such that the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice. As stated above, Acer's substantial United States operations are headquartered within this judicial district, and these operations lead to the design, marketing, and selling of the Affected PCs described in this Complaint to persons across the United States, including computer buyers in this judicial district.

43. As described above, both Defendants regularly conduct business in California, including in this judicial district. Defendants have placed and continue to place the Affected PCs into the stream of commerce, via an established distribution channel headquartered in this judicial district, with the knowledge and understanding that these products are sold in the United States, including in California and specifically including in this judicial district.

44. On information and belief, Defendants derive substantial revenue from sale of the Affected PCs distributed within California, including within this judicial district, and otherwise expect or should reasonably expect their complained-of actions to have consequences in California, and specifically in this judicial district.

45. Defendants' complained-of conduct, including that emanating from this judicial district (which is the locus of Acer's substantial United States operations), has led to foreseeable harm and injury to Plaintiff and to members of the Proposed Classes.

46. Venue is proper in the Northern District of California pursuant to 28 U.S.C. § 1391(b)(1) and (2) because Defendant Acer America resides in this judicial district and a substantial part of the events and/or omissions that give rise to Plaintiff's claims occurred in this judicial district. Venue is proper in the Northern District of California under 28 U.S.C. § 1391(c)(3) because Defendant Acer Inc. is not resident in the United States.

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 Defendant Acer America 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 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.

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

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, as well as representatives from Dell, Microsoft, and Lenovo.

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.

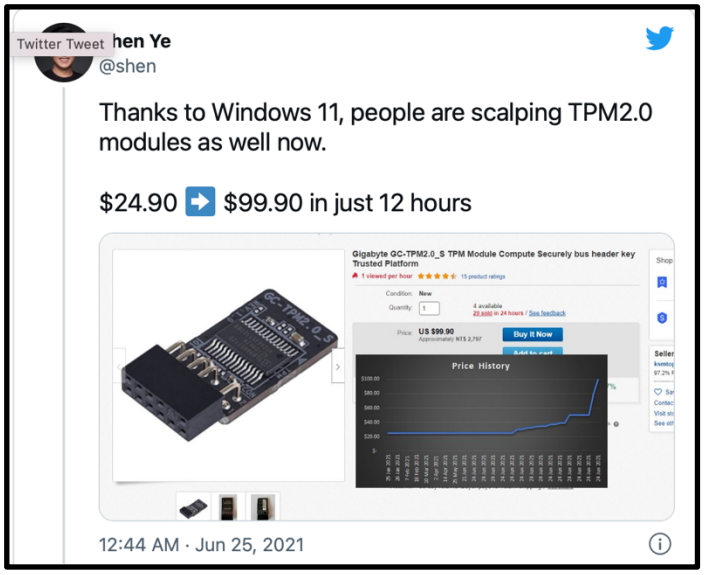
C. Microsoft Requires a TPM to Run Windows 11

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.

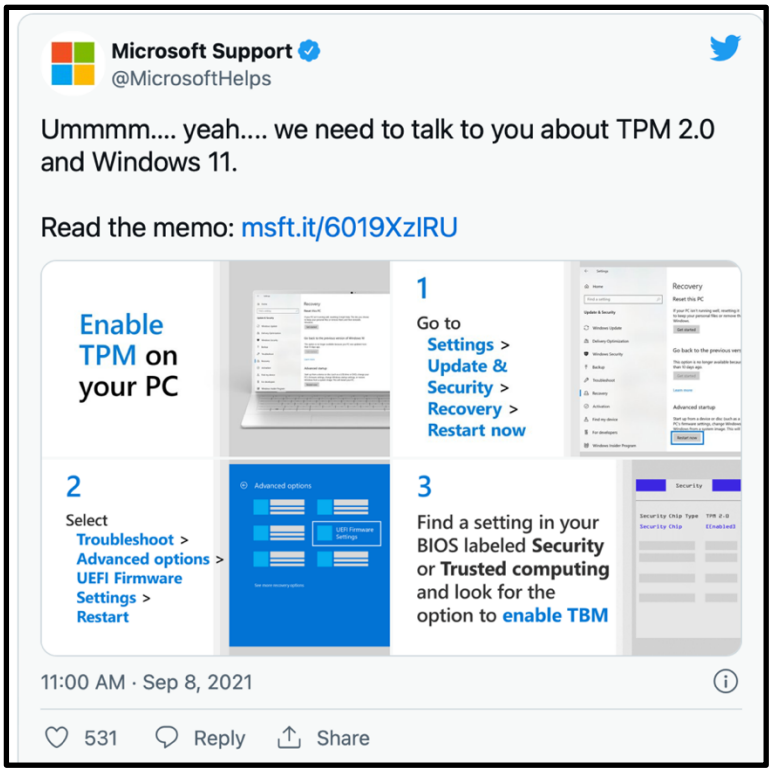
109. The newly published Windows 11 system requirements led to an immediate run on hardware TPMs. Reports were widespread of TPM modules being "scalped" at inflated prices.



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:



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 Acer, 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

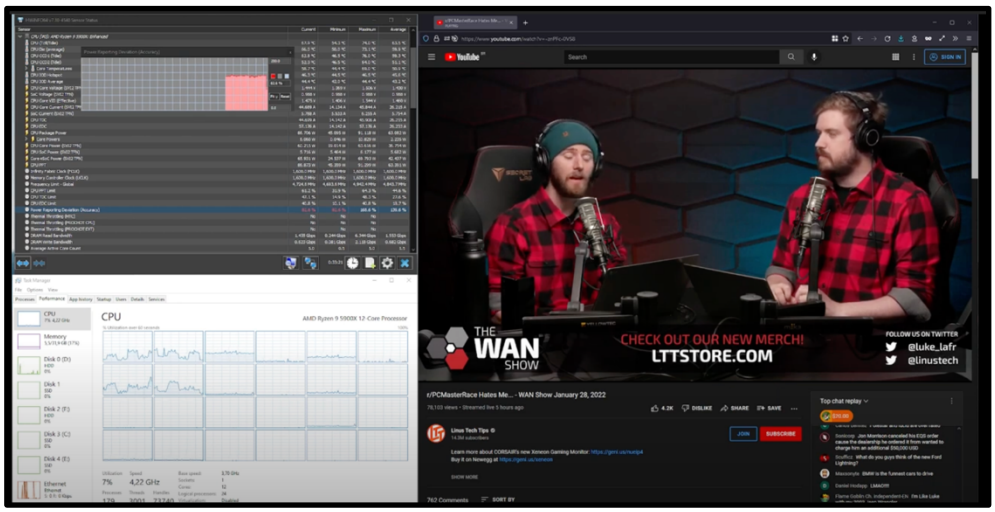
150. AMD's implementation of fTPM as part of the PSP had serious implications for the performance of AMD-based systems, particular Ryzen processors touted by OEMs, including Acer, for their speed and security.

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.



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.

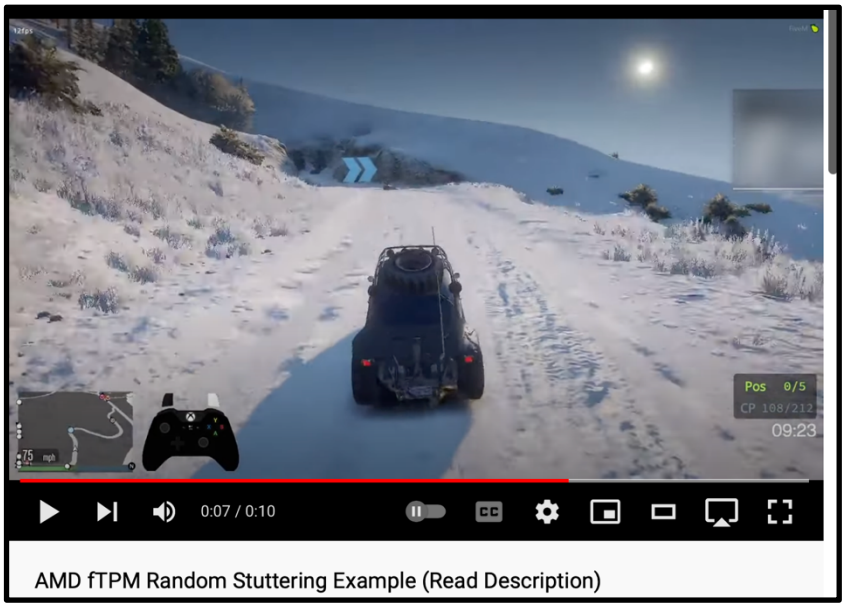
157. User comments confirmed the same behavior—user after user. As one user recounted:

> 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.



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. Acer's Forums Receive Complaints of Stuttering and Other Performance Issues

165. OEM forums were deluged with requests for help. For example, the Acer support forum included pleas for help with AMD-based systems that stuttered due to AMD's fTPM flaw. As one Acer gaming laptop user posted on the Acer support forum in July 2022:

> Basically the dreaded issue which is caused by the fTPM module installed in the chipset itself (can't be disabled in BIOS) of the laptop.
>
> Symptoms: Every now and then you get a robotic sounds and everything gets laggy (1-2 fps) for a couple of seconds.
>
> AMD started rolling out updates for the BIOS. Will Acer follow?

166. Such posts have been met with silence by Acer.

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

167. 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.

168. 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.

169. 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.

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

171. 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 Acer, 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)."

172. Acer 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

173. 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.

174. 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.

175. 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.

176. 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.

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

178. 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."

179. 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.

180. 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.

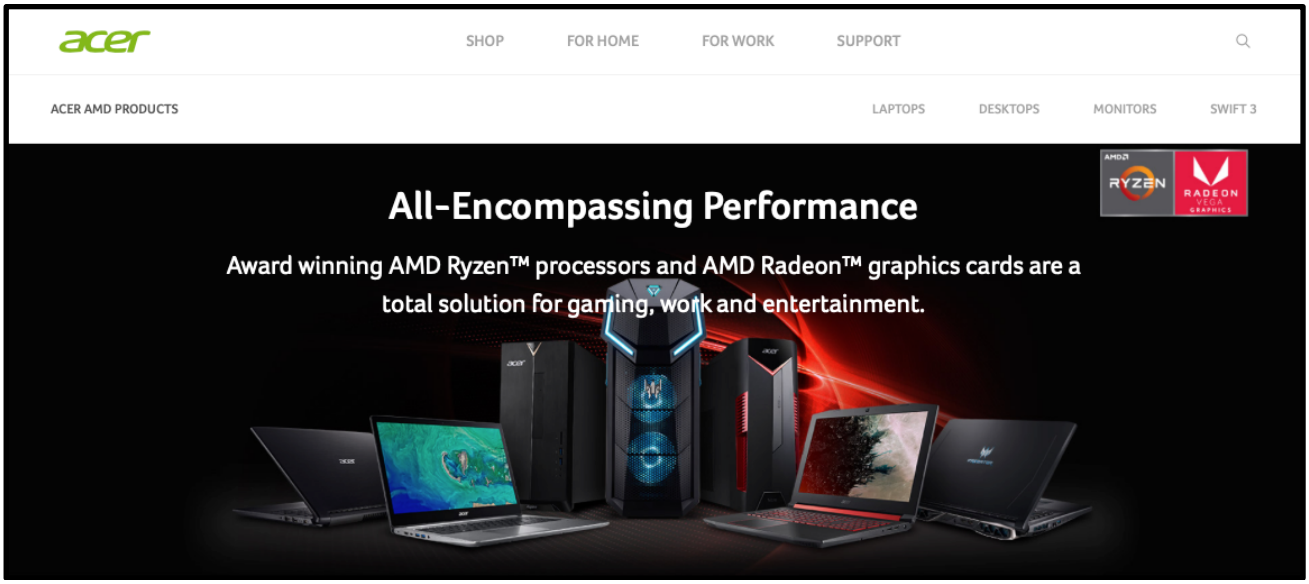
181. AMD's fTPM was not (and is not) a TPM. It was designed as a defeat device to placate the Windows operating system, which requires that a TPM be present and enabled. And AMD's defeat device not only woefully fails to provide the security provided by the TPM 2.0 standard, it causes the system itself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

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

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

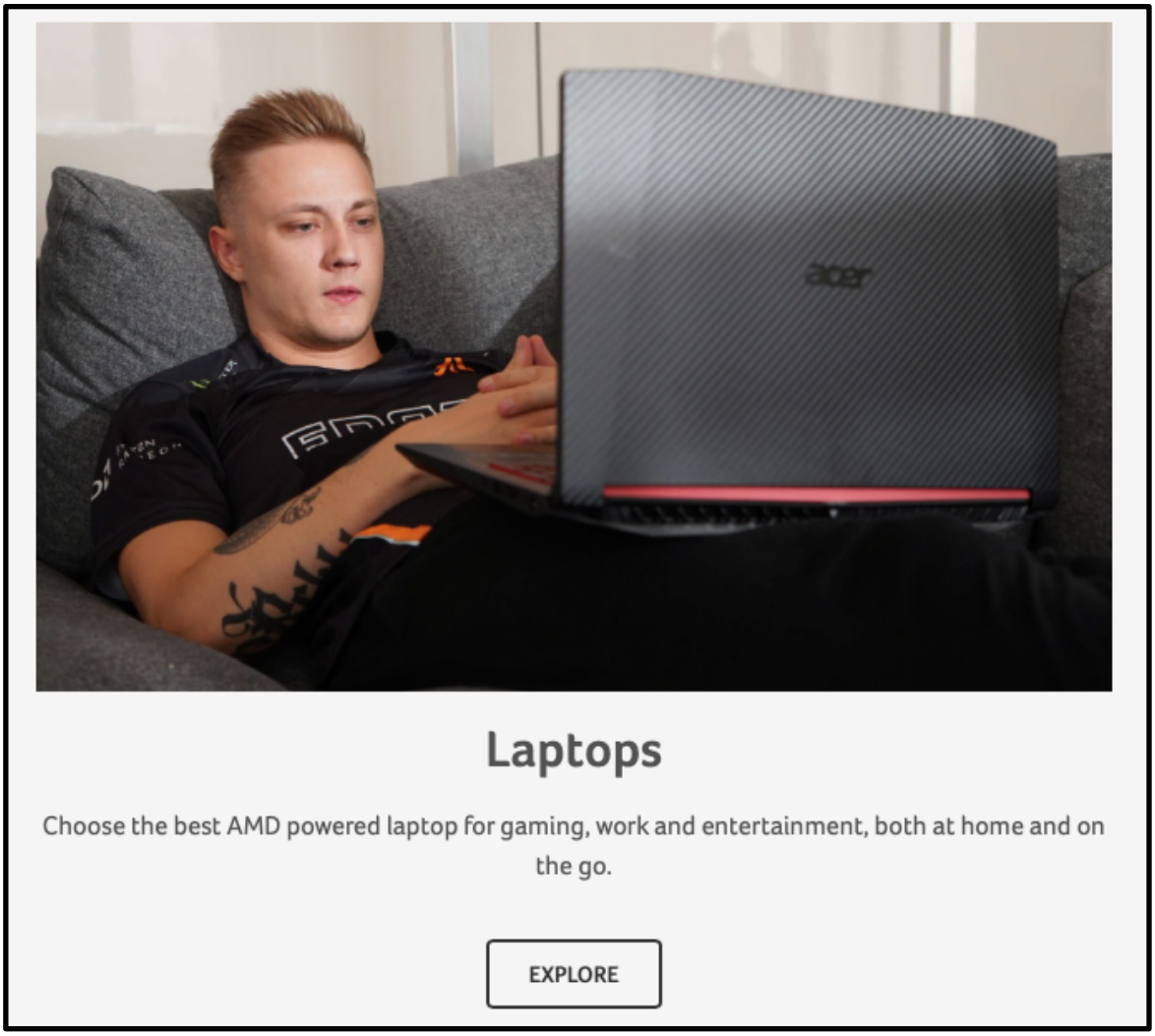
182. Acer has long jointly marketed its PCs with AMD, touting AMD's processors. For example, the Acer.com website dedicates entire pages to joint marketing in connection with Acer's AMD computers, including Acer's Nitro AMD, Aspire AMD, TravelMate AMD, and Swift AMD laptops.

183. Thus, for example, Acer has an "Acer AMD Products" portion of its website that markets the "All-Encompassing Performance" of its AMD-based computers, stating that "Award winning AMD Ryzen™ processors and AMD Radeon™ graphics cards are a total solution for gaming, work and entertainment."



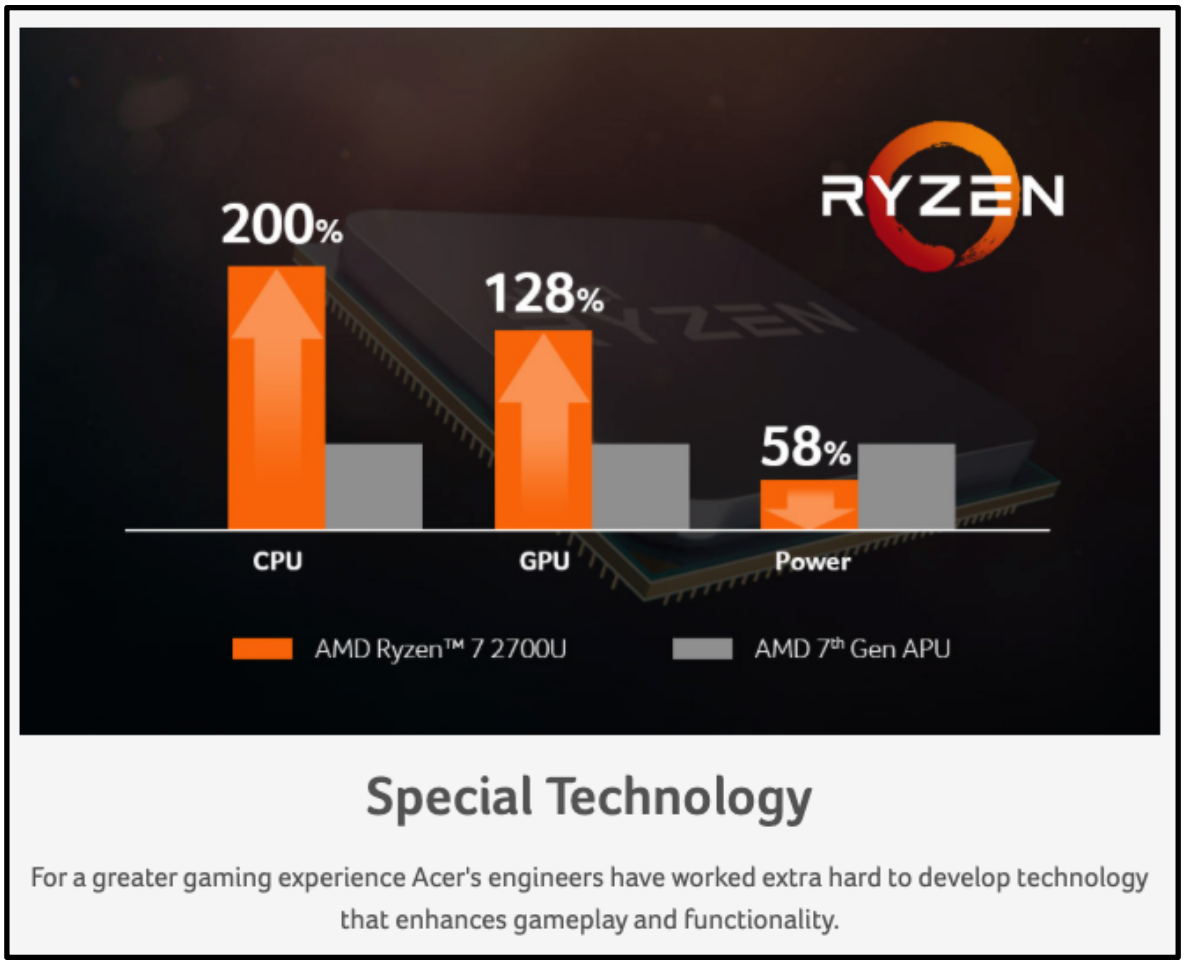
184. Acer directs users toward its AMD-powered laptops (including Acer Nitro AMD, Acer Aspire AMD, Acer TravelMate AMD, and Acer Swift AMD laptops) with a picture of a "gamer" using

an Acer AMD laptop and the statement "Choose the best AMD powered laptop for gaming, work and entertainment, both at home and on the go."



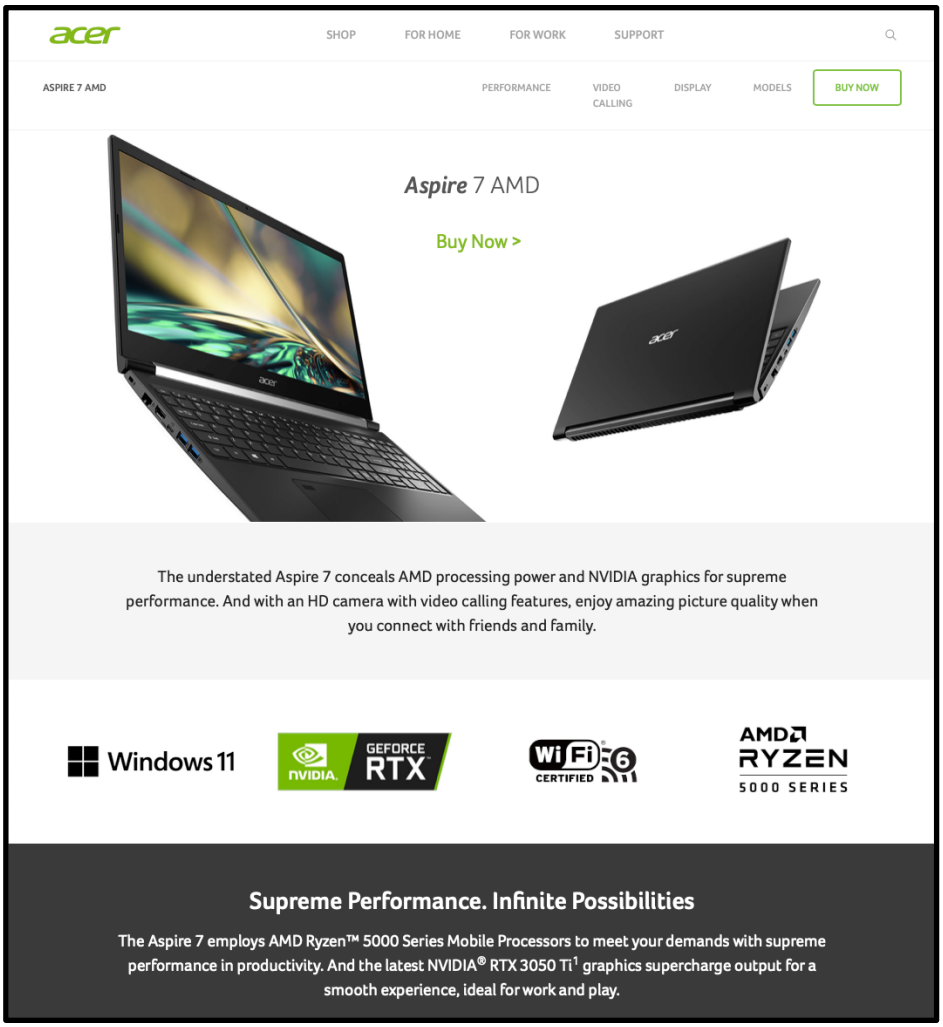
185. Indeed, Acer touts the performance of AMD Ryzen CPUs in connection with its Nitro AMD, Aspire AMD, TravelMate AMD, Swift AMD laptops throughout its website, including in its online store.

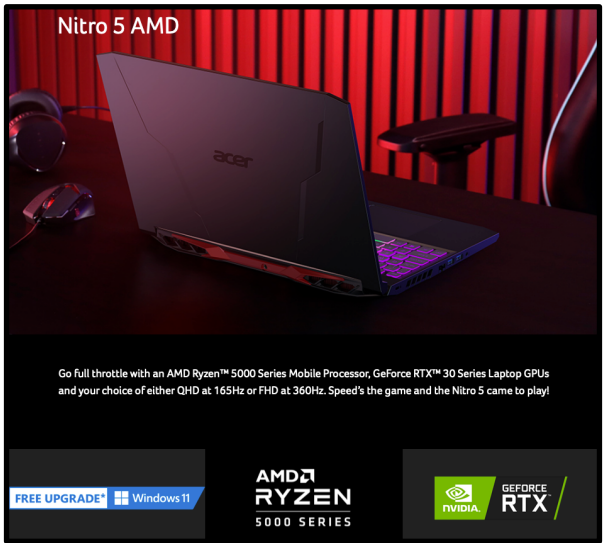
186. Acer represents on its website that AMD processors offer "Special Technology" that "enhances gameplay and functionality," which "***Acer's engineers have worked extra hard to develop***" "[f]or a greater gaming experience":



187. Acer's representations regarding the benefits of its AMD-based laptops are, indeed, very specific, and target precisely the applications and uses affected by the flawed AMD fTPM design.

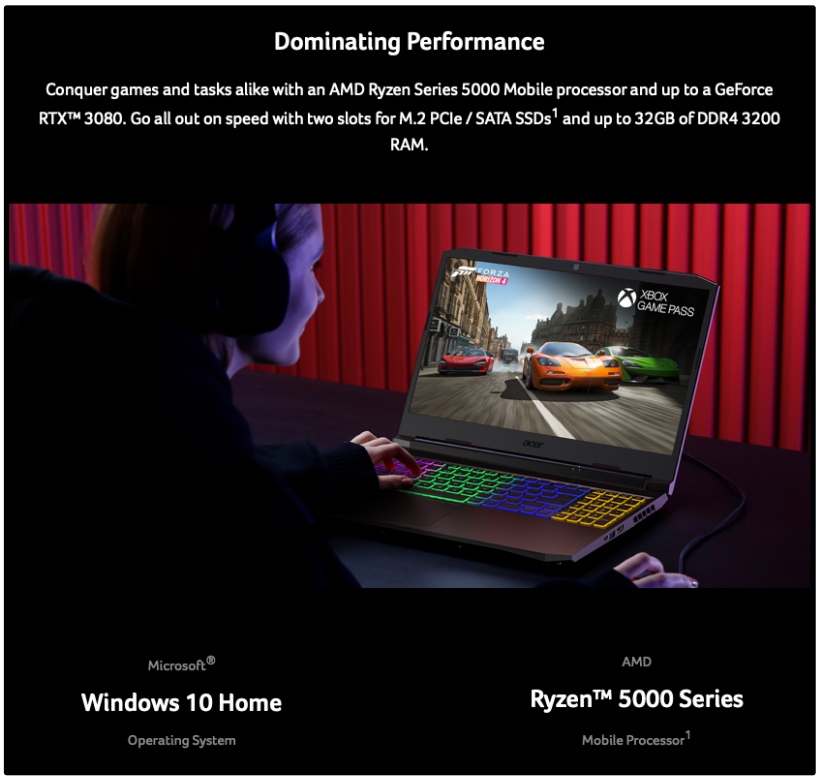
188. Thus, for example, Acer touts the AMD CPUs in its laptops as having "supreme performance in productivity," providing "a smooth experience, ideal for work and play," and touts "video calling features" and "full throttle" gaming superiority in connection with its AMD laptops.



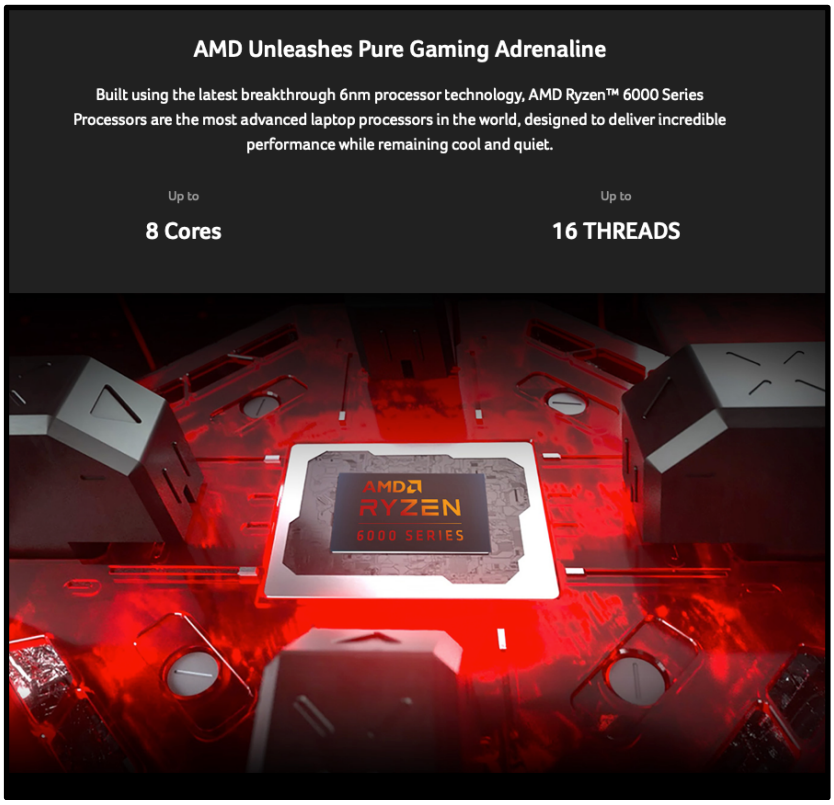


189. Acer markets the AMD Ryzen processors in its Aspire laptops as "power[ing]" these laptops "for multitasking and productivity," including "accelerated photo and video editing."

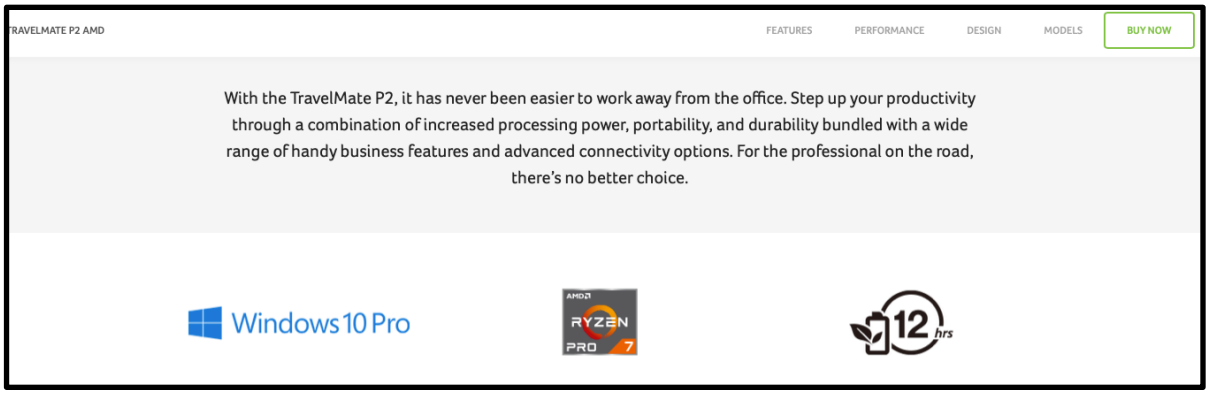
190. On an Acer.com page touting Acer's AMD Ryzen "gaming laptops," Acer touts the benefits of AMD Ryzen processors, which Acer calls "Dominating," "Made to Game," and describes as "the most advanced laptop processors in the world to deliver bleeding edge efficiency":



191. On its Acer.com website and in its online store, Acer asserts that its laptops with AMD Ryzen processors have "Dominating Specs" and "Unleash[] Pure Gaming Adrenaline," using "the most advanced laptop processors in the world."



192. On its website, Acer touts the supposed "office . . . productivity" benefits of its AMD-powered laptops, including AMD Ryzen-powered Acer TravelMate laptops. Indeed, Acer specifically asserts that consumers can "[s]ay goodbye to clunky video conferencing" in its TravelMate AMD laptops, and promises that users will "[a]ccelerate your multitasking" with the AMD Ryzen processor.



193. Across its website and elsewhere, Acer specifically represents that its AMD-based systems are suited for video chats, video playback, and gaming. Indeed, Acer represents that its AMD-powered laptops use "Picture-Perfect," "Furiously Fast" technology that "guarantee[s] your game sessions with be fluid, unbroken, and unmatched."

194. However, despite Acer's specific representations to the contrary, the AMD PSP/fTPM flaw in its AMD computers, including in its Acer Aspire AMD, Acer Nitro AMD, and Acer Travelmate AMD laptops, causes media playback/conferencing and game sessions to be anything but "fluid, unbroken, and unmatched." Acer's statement to the contrary is false and misleading.

195. So, too, are Acer's statements—found all over its website and online store in connection with Acer AMD laptops—that these laptops with AMD Ryzen processors are "Made to Game" with "Dominating Performance" to "[c]onquer games and tasks alike" with "the most advanced laptop processors in the world" false and misleading. In reality, Acer laptops with AMD Ryzen processors—

e.g., Acer Aspire AMD, Acer Nitro AMD, and Acer TravelMate AMD laptops—offer subpar (and indeed, commercially unacceptable) performance in gaming and other common laptop tasks like media playback because of the AMD fTPM flaw in their CPUs, which causes, among other things, intrusive stuttering in gaming, in media playback, and in video- and audioconferencing.

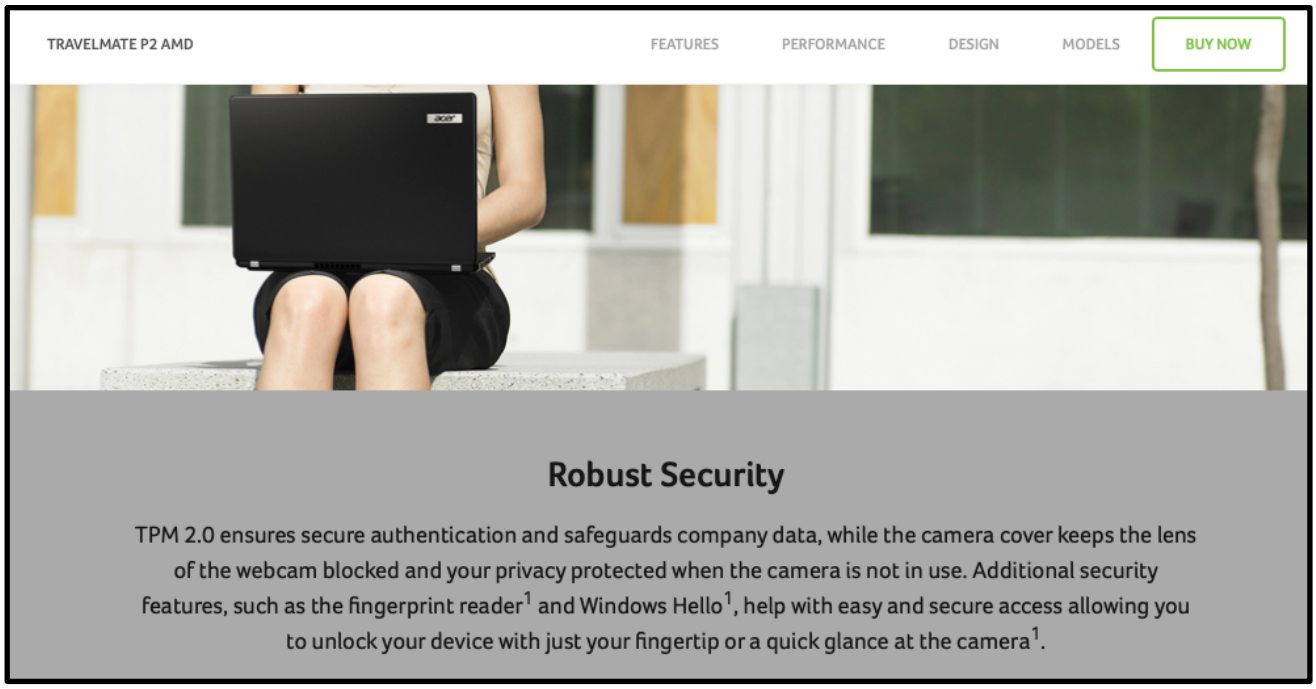
196. Again and again on its website—for example, in the screenshots provided above—Acer represents that its AMD-powered laptops offer smooth media playback, videoconferencing, and gameplay.

197. 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.

198. 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. Acer's AMD laptops are not "powered . . . for multitasking and productivity," with "accelerated photo and video editing"—these are tasks that are specifically and intrusively hampered by the AMD fTPM flaw and its stuttering manifestation.

199. Acer also markets its Aspire and Nitro laptops 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.

200. Acer also touts the security and enterprise features of its AMD-based laptops, including the supposed security benefits of "TPM 2.0" in these laptops:



201. Acer's representations on security and enterprise features make 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.

202. 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.

203. Put simply, the security features touted on Acer's marketing pages 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.

204. Acer 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 Acer 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.

205. 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.

206. Acer made—and continues to make—specific claims, including on its Acer.com website, about its AMD-based PCs, including about its Acer Aspire AMD, Acer Nitro AMD, and Acer TravelMate AMD laptops.

207. With respect to its TravelMate AMD laptops, Acer represents on its website that its Ryzen Pro CPU will "accelerate your multitasking," that "[y]ou'll work fast and accomplish even more," that the user can "[s]ay goodbye to clunky video conferencing," and that "TPM 2.0 ensures secure authentication and safeguards company data."

208. Likewise, Acer represents that "picture-perfect" media and game playback are a distinct strength of its AMD-based laptops, including Acer Nitro AMD and Acer Aspire AMD laptops.

209. These specific representations about Acer AMD-based laptops 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 Acer AMD-based computers. The reality is that AMD's flawed PSP and fTPM designs made (and continue to make) Acer AMD computers less secure, and render multimedia playback and gaming on those PCs prone to intrusive stuttering.

210. Acer and AMD also jointly market, including on Acer.com and on YouTube (among other places), Acer's 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 marketing materials like a webpage touting Acer's "Remote Work & Study Solutions," which explains that "[w]hether you're working from home or studying remotely, Acer has you covered," which then links to Acer's Aspire, Nitro, TravelMate, and

Swift laptops—focus on AMD computers' (supposed) prowess in videoconferencing and their (supposed) ability to maintain enterprise-level security while away from the physical office.

211. Thus, Acer's website advertises the TravelMate P2 AMD laptop with the statement:

> With the TravelMate P2, it has never been easier to work away from the office. Step up your productivity through a combination of increased processing power, portability, and durability bundled with a wide range of handy business features and advanced connectivity options. For the professional on the road, there's no better choice.

212. And an Acer marketing video (titled a "training video" by Acer) posted to Acer's YouTube channel and linked and embedded on Acer.com alongside Acer's AMD laptops describes the Acer TravelMate AMD as follows:

> Boasting the latest AMD Ryzen PRO platform and certified for military grade durability, the Acer TravelMate P2 Series enables professionals to work between the office, home and on the go. These laptops are built around the idea of prompting collaboration, productivity, security, organizational efficiency and added protections. Helping you adapt to and excel in today's new hybrid work styles.

213. Acer's marketing video continues:

> With up to an AMD Ryzen 7 PRO 4750U processor and Radeon Graphics, you'll accelerate your multitasking as you work quicker throughout the day. AMD processors also offer modern solutions for manageability and security, providing seamless deployment and simplified management at

> scale. This, combined with a multi-layered approach to security, allows the AMD and Windows Secured-Core PC ecosystem to help protect your sensitive data from sophisticated attacks, avoid downtime, and reduce resource drain for your business. Say goodbye to clunky video conferencing.

214. In addition to linking to Acer TravelMate laptops, Acer's "Work Anywhere" and "Learn Anywhere" subsections of its "Remote Work" page on its website link to Acer's Aspire, Swift, and Nitro laptops.

215. Neither Acer's website nor its marketing videos mentions the flawed design of the AMD PSP and fTPM subsystems, which leave AMD-based Acer computers vulnerable to devastating firmware attacks (among other low-level vulnerabilities not present in enterprise-class "multi-layered . . . security" systems). Indeed, Acer's website and marketing videos specifically tout the supposed "TPM 2.0" security features of its TravelMate AMD laptops, without mentioning the flaws in the AMD PSP and fTPM subsystems. However, 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.

216. Acer's representation that its AMD-based systems are secure based on a Multi-layered approach to security . . . to help protect your sensitive data from sophisticated attacks"—belied by the flawed PSP/fTPM design Acer incorporates into its systems in collaboration with AMD.

217. Acer 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 Acer.com) for Acer's business-oriented laptop offerings.

218. Moreover, Acer has expressly acknowledged the importance of BIOS-level security in, among other things, gaming PCs. Thus, for example, a February 2, 2022, Acer Corner blog post titled "How to Set Up Your Gaming PC for Optimal Performance," explains:

> It's a tale as old as time: you could be running the most powerful gaming PC on the market, but if it's riddled with malware, you'll find its performance sluggish and your experience of actually using it less than ideal. . . .

> ***Also be sure to invest in gaming PCs that come with must-have security features like Trusted Platform Module (TPM) security and BIOS protection***.

(emphasis added).

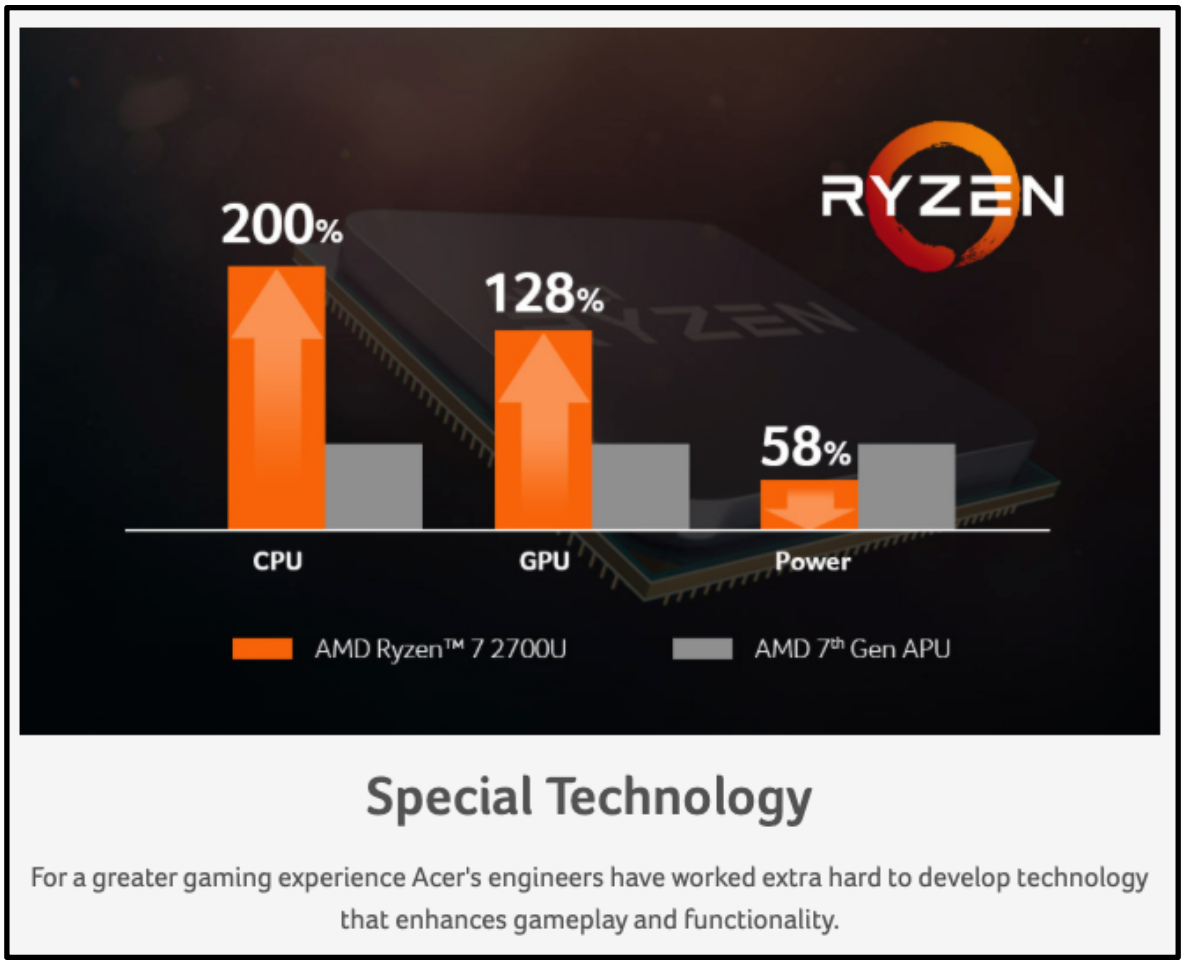
219. In short, an Acer blog post—like many other representations and statements across the company's website and social media platforms (among other places)—explains precisely why TPM security and BIOS protection are "must-have security features" for modern PCs, especially those purchased for gaming. Yet this blog post—and the many Acer representations that its AMD PCs are "Made to Game"—says nothing about the flawed AMD PSP/fTPM design included in Acer's products, which leaves Acer's AMD-based PCs open to firmware attacks.

220. Far from the hardware-based "security features like Trusted Platform Module (TPM) security and BIOS protection" that Acer itself acknowledges as "must-have[s]" for modern gaming PCs, Acer's AMD-based PCs, 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. Acer Knew and Knows About the AMD PSP/fTPM Design Flaw, Including Its Stuttering Manifestation

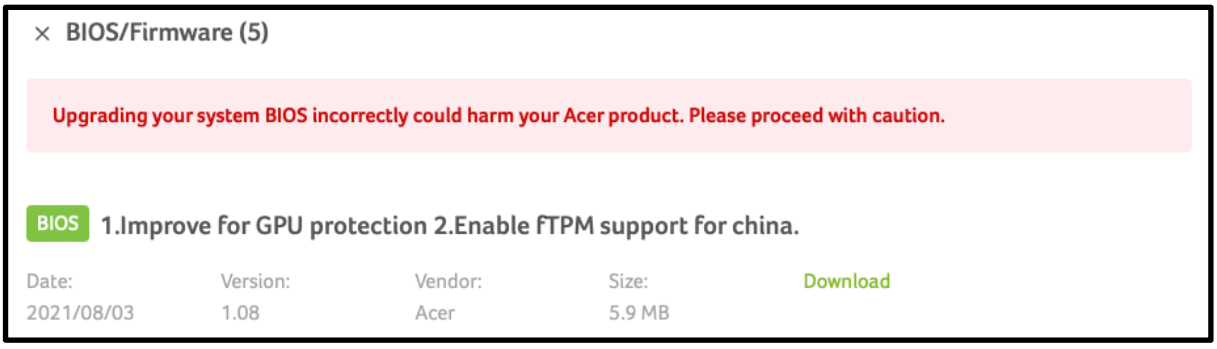
221. Acer represents that it collaborates with AMD on security and design. Indeed, Acer tests AMD-based configurations and motherboards before packaging them into its computers and computer systems.

222. Acer also states on its website that "Acer's engineers" work with AMD to "develop technology that enhances gameplay and functionality" for "a greater gaming experience."



223. Acer 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. Acer 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.

224. Indeed, Acer has released firmware updates for the AMD fTPM system, including an August 3, 2021, BIOS/Firmware update that to "[e]nable fTPM support for china" *[sic]*.



225. The "Vendor" on this fTPM firmware update in 2021 was "Acer."

226. Even after AMD announced the stuttering issues related to the fTPM and its SPIROM access time, Acer 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.

227. To the contrary, to this day Acer continues to affirmatively tout the supposed media playback, videoconferencing, and immersive gaming prowess of its AMD-based computers, including through the specific representations shown and referenced earlier in this Complaint.

228. Even though Acer 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.

229. Put simply, Acer 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. ACER OVERCHARGED CONSUMERS FOR PCS WITH AMD CPUS AS A RESULT OF ITS FALSE AND MISLEADING STATEMENTS AND OMISSIONS

230. 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.

231. 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.

232. 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.

233. Both effects (collectively referred to as the "Effects") result in direct harm to Plaintiff and the Classes. Because of these Effects, the economic value of the PCs purchased from Acer by Plaintiff and Class Members was lower at the time of purchase than the price Plaintiff 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 Plaintiff and Class Members purchased from Acer is and remains lower than it otherwise would have been, including upon resale, resulting in additional injury because of the diminution of value of Plaintiff's and Class Members' Acer PCs.

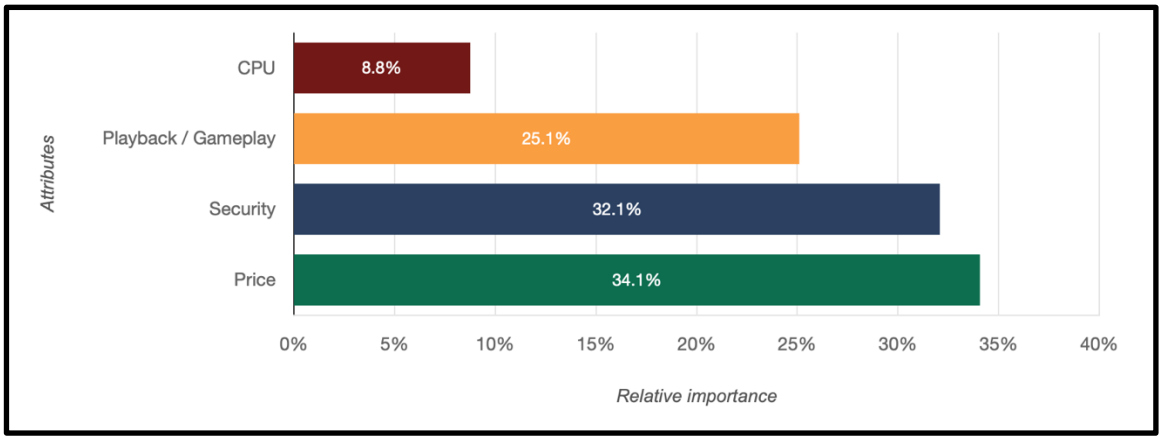
234. Plaintiff and Class Members were able to identify and quantify these injuries with a pre-complaint survey-based statistical analysis, called a conjoint analysis. This analysis allows Plaintiff and Class Members to pinpoint relative values of the Effects as well as price and brand features of PCs.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

235. 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

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

237. 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:



238. 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.

239. 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.

240. 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.

241. 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.

242. Finally, the conjoint analysis shows that Acer 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. Acer 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.

243. 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%.

244. 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%.

245. Acer 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. Plaintiff and the Class Members conferred that benefit on Acer by paying an inflated price for AMD-based Acer PCs at purchase.

CLASS ACTION ALLEGATIONS

246. Plaintiff brings this action and seeks 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 himself and on behalf of the proposed classes of persons (collectively, the "Classes") defined below.

247. Each class's claims derive directly from a course of conduct by Acer.

248. Acer has engaged in uniform and standardized conduct toward each class. Acer 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.

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

250. 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.

251. 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. Plaintiff may sue for the benefit of all as representative parties pursuant to Federal Rule of Civil Procedure 23.

The Nationwide Class

252. Plaintiff Stewart brings this action and seeks to certify and maintain it as a class action on behalf of himself and a Nationwide Class. The Nationwide Class comprises:

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

253. Excluded from the Nationwide Class are Acer, 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 Florida Subclass

254. Plaintiff Stewart brings this action and seeks to certify and maintain it as a class action on behalf of himself and a Florida Subclass. The Florida Subclass comprises:

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

255. Excluded from the Florida Subclass are Acer, 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

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

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

Ascertainability

258. The Classes are ascertainable.

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

260. 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

261. Plaintiff's claims are typical of the members of the Classes.

262. Plaintiff's claims are the same as those asserted by members of the Classes. Plaintiff, like the members of the Classes, has purchased a defective computer with an affected AMD processor, and has been harmed by overpaying for such computer in a manner typical of each of the Classes.

263. Plaintiff alleges injury that is not unique to him, 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.

264. Plaintiff alleges that his injury flows from the common course of conduct alleged as to Acer.

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

Adequate Representation

266. Plaintiff will fairly and adequately protect the interests of the class members.

267. Plaintiff is committed to putting the interest of the Classes ahead of his own and to act in the best interest of members of the Classes.

268. Plaintiff understands his obligations to the Classes and is committed to monitoring/supervising developments in the case and class counsel.

269. Plaintiff has retained competent counsel experienced in computer science, computer architecture, cryptography, and computer security, as well as in consumer class actions.

270. Plaintiff has retained counsel with the resources and capital to litigate the case on behalf of the Classes.

271. Plaintiff and his 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 media playback, audio/videoconferencing, and gameplay).

Superiority

272. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(2) because Acer 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.

273. 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 Acer has engaged.

274. 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.

275. 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.

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

277. 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.

278. 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 Acer's sale of defective PCs will go unaddressed.

Commonality and Predominance

279. 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.

280. These questions of fact and law concern Acer'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.

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

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

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

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

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

d. Whether Acer'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 Acer's alleged conduct;

f. Whether Acer was unjustly enriched by its conduct;

g. Whether Acer employed unlawful, unfair, and/or deceptive practices that harmed Plaintiff 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 Acer and to vindicate statutory and public policy;

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

k. Whether Acer violated the consumer protection statutes of each State, including Florida;

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

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

Grounds Generally Applicable to the Classes

283. Plaintiff intends to seek injunctive relief ending Acer's sale of defective computers with AMD processors.

284. Plaintiff is properly situated to seek such an injunction because Acer has acted and/or refused to act on grounds generally applicable to Plaintiff and the members of the Classes.

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

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

CLAIMS FOR RELIEF

REALLEGATION AND INCORPORATION BY REFERENCE

287. Plaintiff realleges 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

COUNT ONE
Fraud
(On behalf of the Nationwide Class)

288. Plaintiff incorporates by reference all preceding and succeeding allegations as though fully set forth in this Count.

289. Plaintiff Stewart brings this cause of action on his own behalf and on behalf of Nationwide Class Members against Acer under the common law of fraud, which is materially uniform in all states. In the alternative, Plaintiff brings this claim on behalf of the Florida Subclass.

290. As described above, Acer defrauded Plaintiff and the Class Members by knowingly and intentionally misrepresenting to them and to the public at large that its AMD computers 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.

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

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

293. Acer's actions constitute actual fraud and deceit because Acer did the following with the intent to deceive Plaintiff 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.

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

295. Acer's intentionally deceptive conduct induced Plaintiff and the Class Members to purchase the Affected PCs and resulted in harm and damage to Plaintiff and the Class Members.

296. Plaintiff believed and relied to his detriment upon Acer's affirmative misrepresentations. Class Members may be presumed to have believed and relied upon Acer'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.

297. Acer also fraudulently concealed and suppressed material facts regarding the Affected PCs. Acer knew when it marketed and sold its PCs that they were not superior in quality, performance, and security as represented. Acer failed to disclose these facts to consumers at the time it marketed and

sold the Affected PCs. Acer 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.

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

299. Acer 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. Acer 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 Acer;

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

d. Acer 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 Acer's PCs were defectively designed.

300. 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 Plaintiff and the Class Members purchased. Whether the Affected PCs were defective would have been an important factor in Plaintiff's and the Class Members' decisions to purchase or obtain the Affected PCs.

301. Plaintiff and the Class Members trusted Acer not to sell them products that were defective.

302. Acer 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 Acer and as reasonably expected by consumers.

303. Plaintiff 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.

304. Plaintiff and the Class Members relied to their detriment upon Acer's reputation, fraudulent misrepresentations, and material omissions in deciding to purchase the Affected PCs.

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

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

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

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

308. Plaintiff incorporates by reference all preceding and succeeding allegations as though fully set forth in this Count.

309. Plaintiff Stewart brings this cause of action on his own behalf and on behalf of the Nationwide Class Members against Acer under the common law of fraudulent concealment, which is materially uniform in all states. In the alternative, Plaintiff brings this claim on behalf of the Florida Subclass.

310. As alleged in this Complaint, Acer 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.

311. Acer also misrepresented the performance, quality, and security of the Affected PCs. These representations were false because, unbeknownst to Plaintiff and the 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.

312. Acer's misrepresentations and omissions about the Affected PCs were material because the misrepresentations and omissions alleged in this Complaint induced Plaintiff 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.

313. Acer 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 Acer.

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

315. Acer concealed the truth about the defective PCs, including as to the defective AMD processors and on-board fTPM modules, intending for Plaintiff and the Class Members to rely on their

misrepresentations and omissions. Plaintiff and the Class Members relied on Acer'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. Plaintiff and Class Members were reasonable and justified in their reliance on Acer's representations about the PCs and its omissions about their defective nature because Acer is a multinational PC designer and manufacturer well-versed in the design, manufacture, and service of devices like the PCs purchased by Plaintiff and Class Members.

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

317. Acer's omissions were made with knowledge of their falsity, and with the intent that Plaintiff and the Class Members rely on them.

318. Plaintiff and the Class Members were entitled to rely on Acer's misrepresentations and omissions because they are purchasers of Acer's PCs, and Acer has been enriched by the sales of these PCs.

319. Plaintiff and the Class Members reasonably relied on Acer's misrepresentations and omissions, and suffered injury and monetary damages as a direct and proximate result. Had Acer not concealed material facts regarding the Affected PCs, including as to the defective AMD computers and on-board fTPM modules incorporated within them, Plaintiff and the Class Members would not have purchased the Affected PCs or would have paid less for them. Plaintiff 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 Acer's fraud and the growing public awareness about the Affected PCs'

defect, including the incorporated AMD processors and on-board fTPM modules. Accordingly, Acer is liable to Plaintiff and the Class Members for damages in an amount to be proven at trial.

320. Acer's acts were committed wantonly, maliciously, oppressively, deliberately, with intent to defraud; in reckless disregard of the rights of Plaintiff and the Class Members; and in order for Acer to enrich itself. Acer'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 THREE
Unjust Enrichment/Quasi-Contract
(On behalf of the Nationwide Class)

321. Plaintiff incorporates by reference all preceding and succeeding allegations as though fully set forth in this Count.

322. Plaintiff Stewart brings this cause of action on his own behalf and on behalf of the Nationwide Class Members against Acer under the common law of unjust enrichment/quasi-contract, which is materially uniform in all states. In the alternative, Plaintiff brings this claim on behalf of the Florida Subclass.

323. Plaintiff brings this claim as an alternative to the contractual warranty claims asserted in this Complaint and/or due to Acer's intentional and deceptive efforts to conceal the defects in the Affected PCs and avoid its warranty obligations.

324. Acer received millions of dollars in revenue from the sale of Affected PCs.

325. This revenue was a benefit conferred upon Acer by Plaintiff and the Class Members.

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

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

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

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

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

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

331. Plaintiff incorporates by reference all preceding and succeeding allegations as though fully set forth in this Count.

332. Plaintiff Stewart brings this cause of action on his own behalf and on behalf of the Nationwide Class under the law of warranties, which is materially uniform in all states. In the alternative, Plaintiff brings this claim on behalf of the Florida Subclass.

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

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

335. Acer 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. Acer's representations formed the basis of the bargain in Plaintiff's and Class Members' decisions to purchase the Affected PCs.

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

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

338. 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.

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

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

341. Plaintiff 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 Acer's conduct described in this Complaint. Affording Acer a reasonable opportunity to cure the breach of written warranties would be unnecessary and futile.

342. Accordingly, Acer is liable to Plaintiff and the Class Members for damages in an amount to be proven at trial.

B. Claims Brought on Behalf of the Florida Subclass

COUNT FIVE
Violation of Florida's Unfair & Deceptive Trade Practices Act
Fla. Stat. § 501.201 et seq.
(On behalf of the Florida Subclass)

343. Plaintiff incorporates by reference all preceding and succeeding allegations as though fully set forth in this Count.

344. Plaintiff Stewart brings this Count on his own behalf and on behalf of the Florida Subclass against Acer.

345. The Florida Unfair and Deceptive Trade Practices Act ("FUDTPA") prohibits "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or conduct." Fla. Stat. § 501.204(1).

346. Plaintiff Stewart and the Florida Subclass Members are "consumers" within the meaning of Fla. Stat. § 501.203(7).

347. Acer is engaged in "trade or commerce" within the meaning of Fla. Stat. § 501.203(8).

348. In the course of Acer's business, Acer 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 Acer'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, Acer 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.

349. In purchasing the Affected PCs, Plaintiff Stewart and the Florida Subclass Members were deceived by Acer'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.

350. Plaintiff Stewart and the Florida Subclass Members reasonably relied upon Acer's false representations. They had no way of knowing that Acer's representations were false and gravely

misleading. As alleged in this Complaint, Acer engaged in technically sophisticated methods of deception. Plaintiff Stewart and the Florida Subclass Members did not, and could not, unravel Acer's deception on their own, and were not aware of the defective condition of the Affected PCs.

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

352. Acer's deception, fraud, misrepresentation, concealment, suppression, and/or omission of material facts was likely to—and did in fact—deceive reasonable consumers, including Plaintiff Stewart and the Florida Subclass Members.

353. Acer intentionally and knowingly misrepresented material facts regarding the Affected PCs, with intent to mislead Plaintiff Stewart and the Florida Subclass Members.

354. Acer knew or should have known that its conduct violated the FUDTPA.

355. Acer owed Plaintiff Stewart and the Florida Subclass Members a duty to disclose the truth about the defective PCs because Acer:

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 Stewart and the Florida 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 Stewart and the Florida Subclass Members that contradicted these representations.

356. Due to Acer'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) Acer's false representations regarding the performance, durability, security, and functionality of the Affected PCs; and (c) Plaintiff Stewart and the Florida Subclass Members' reliance on these material representations, Acer had a duty to disclose to Plaintiff Stewart and the Florida Subclass Members that the Affected PCs were defective. Having volunteered to provide information to Plaintiff Stewart and the Florida Subclass Members, Acer had the duty to disclose not just the partial truth, but the

entire truth. The facts that Acer omitted and concealed were material because they directly impact the value of the Affected PCs purchased by Plaintiff Stewart and the Florida 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 Stewart and the Florida Subclass Members. Acer represented that the Affected PCs were free from defect, when in fact they included defective AMD-based processors and fTPM subsystems.

357. By misleading and failing to disclose to Plaintiff Stewart and the Florida Subclass as recited above, Acer engaged in deceptive business practices in violation of the FUDTPA.

358. Because Acer fraudulently concealed the facts recited above, including that 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, Plaintiff Stewart and the Florida Subclass Members were deprived of the benefit of their bargain and the value of their Acer computers has greatly diminished.

359. Acer's omissions and/or representations about the Affected PCs were and are material to Plaintiff Stewart and the Florida Subclass Members.

360. Plaintiff Stewart and the Florida Subclass Members suffered ascertainable loss caused by Acer's misrepresentations and its concealment of and failure to disclose material information. Plaintiff Stewart and the Florida Subclass Members who purchased Affected PCs either would have paid less for their Affected PCs or would not have purchased them at all but for Acer's violations of the FUDTPA.

361. Acer had an ongoing duty to all Acer customers to refrain from unfair and deceptive practices under the FUDTPA. Plaintiff Stewart and the Florida Subclass Members each suffered ascertainable loss in the form of loss of the benefit of their bargain and the diminished value of their Affected PCs as a result of Acer's deceptive and unfair acts and practices made in the course of Acer's business.

362. Acer's violations present a continuing risk to Plaintiff Stewart and the Florida Subclass Members as well as to the general public. Acer's unlawful acts and practices complained of here affect the public interest.

363. As a direct and proximate cause of Acer's violations of the FUDTPA, Plaintiff Stewart and the Florida Subclass Members have suffered injury-in-fact and/or actual damage.

364. Plaintiff Stewart and the Florida Subclass Members are entitled to recover their actual damages under Fla. Stat. § 501.211(2) and attorneys' fees under Fla. Stat. § 501.2105(1).

365. Plaintiff Stewart and the Florida Subclass Members seek an order enjoining Acer's unfair and/or deceptive acts or practices, punitive damages, and attorneys' fees, and any other just and proper relief available under FUDTPA.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of members of the Proposed Classes, respectfully requests that the Court enter judgment in his favor and against Acer, as follows:

A. Certification of the proposed Nationwide Class and State Subclass, including appointment of Plaintiff's 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 Acer 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 Acer 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

Plaintiff demands a trial by jury on all claims so triable as a matter of right.

Dated: August 16, 2022

Respectfully submitted,

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
Barton Oaks Plaza I, Suite 300
Austin, TX 78746
Tel.: (213) 462-2772

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 Plaintiff and the Proposed Class