UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

ERIC H. BERNSTEIN and STEPHEN C. BEVILACQUA, Individually and On Behalf of All Others Similarly Situated,

Plaintiffs,

vs.

INTEL CORPORATION,

Defendant.

Civil Action No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

Plaintiffs Eric H. Bernstein and Stephen C. Bevilacqua, individually and on behalf of all other similarly situated, by their undersigned attorneys, bring this class action complaint against Defendant Intel Corporation ("Intel" or the "Company") based on personal knowledge as to themselves and upon information and belief as to all other matters, based on the investigation of counsel.

I. NATURE OF THE ACTION

1. Intel is the world's most prolific and well-known manufacturer of computer chips. More than 90 percent of all computers in the world include Intel chips.

2. Intel's success is driven in large party by its ability to regularly improve the speed and performance of its computer chips. Intel's co-founder, Gordon Moore, accurately predicted that Intel would decrease the size of its computer chips every two years—a rate now known as Moore's Law—and Moore's contemporaries further predicted that overall performance of a chip would double every 18 months. This dramatic improvement of performance is reflected in the price of Intel's computer chips: the faster the speed, the higher the price.

3. To increase the speed and performance of its computer chips, Intel designed them to rely heavily on a process known as "speculative execution." Speculative execution improves a chip's efficiency because the process enables a computer to perform a number of different tasks out of order and ahead of time in anticipation that the results of one of those tasks will be needed in the future.

4. Although speculative execution increases speed and performance, it also compromises the security of a computer. Indeed, since as early as 1995, unbeknownst to the public, Intel has been selling computer chips that suffer from two significant security flaws, both of which take advantage of Intel's aggressive reliance on speculative execution to improve the performance of its chips.

5. Details of the security vulnerabilities became public on January 2, 2018, when it was revealed that Google researchers identified two security flaws—known as Meltdown and Spectre—that affect all computers containing Intel chips—***i.e., nearly every computer in the world***.

6. Meltdown and Spectre allow a non-privileged user (i.e., a hacker) to access information on a computer that the hacker should not be able to access, such as secret keys, usernames, passwords, and any other sensitive information a user enters into a computer. The flaws are so significant that one of the researchers who discovered them referred to Meltdown specifically as "probably one of the worst CPU bugs ever found."[1]

7. Although the details of Meltdown and Spectre first became public on January 2, 2018, Intel reportedly first learned about the defects by as early as June 2017, and yet Intel continued to manufacture, market, and sell defective chips in the interim.

8. Only a complete redesign of Intel chips can completely resolve the Meltdown and Spectre security flaws. Installing a software "patch" or update can potentially resolve the Meltdown flaw (Spectre can only be completely fixed by replacing the hardware), but these software patches dramatically slow down computer performance. One such patch has been shown to slow down a computer by up to 30 percent,[2] and Microsoft has reported that a patch for Windows operating systems results in significant slowdowns.[3] Intel itself has acknowledged that computers that are patched have shown a decrease in performance of between 2 and 25 percent

---

[1] Samuel Gibbs, *Spectre and Meltdown processor security flaws – explained*, The Guardian (Jan. 4, 2018).

[2] Rob Thubron, *Massive security flaw found in Intel CPUs, patch could hit performance by up to 30%*, Techspot (Jan. 3, 2018).

[3] Terry Myerson, *Understanding the performance impact of Spectre and Metldown mitigations on Windows Systems*, Microsoft Secure, https://cloudblogs.microsoft.com/microsoftsecure/2018/01/09/understanding-the-performance-impact-of-spectre-and-meltdown-mitigations-on-windows-systems/.

and are rebooting more than usual.[4] The reboot problem became so significant that on January 22, 2018, Intel announced that the patches it had released were faulty and advised customers ***not*** to install them until a new patch it is developing becomes available.[5]

9. Plaintiffs retained an expert in microprocessor chips who worked at Intel from 1992 to 2004 as a director of CPU and chip development and has over 25 years of industry experience working on CPU and memory chip development ("Expert A"). Expert A estimated that a 10% decrease in performance of a chip corresponds to a 10% decrease in price. Thus, a $200 chip that experiences a 10% performance decrease (when a patch is added) diminishes the value of that chip by approximately $20.

10. The decrease in performance of Intel's chips is especially damaging to Plaintiffs and Class members because Intel's products are sold specifically on performance and are priced accordingly. Intel's chips would have been sold at a much lower price had they been priced to reflect the speed at which they perform when patched.

11. Now, Plaintiffs and Class members are forced to either use a chip that is vulnerable to a dangerous security flaw or install a patch that significantly reduces performance (and yet still remains vulnerable to future attacks).

12. Plaintiffs and the Class, who paid a premium for Intel-designed chips, have suffered ascertainable injuries and loss of money or property as a result of Defendant's wrongful conduct. Indeed, had Plaintiffs and the Class known about the security flaws and the need for a

---

[4] *Intel Fix Causes Reboots and Slowdowns*, BBC News (Jan. 18, 2018), *http://www.bbc.com/news/technology-42733032*.

[5] Intel Newsroom, *Root Cause of Reboot Issue Identified; Updated Guidance for Customers and Partners* (Jan. 22, 2018), https://newsroom.intel.com/news/root-cause-of-reboot-issue-identified-updated-guidance-for-customers-and-partners/.

security patch that would slow performance, they would not have purchased Intel chips (or devices containing them) or would have paid substantially less for them.

II. PARTIES

13. Plaintiff Eric H. Bernstein is an individual who is a citizen and resident of New York. Mr. Bernstein purchased two MacBook computers, each containing an Intel CPU. Mr. Bernstein uses his computers primarily for personal purposes. Plaintiff was unware of the Meltdown and Spectre security flaws described herein when he purchased his computers. Had Mr. Bernstein known of the security flaws, and the need to install a performance-reducing patch on his computers to resolve them that would decrease the value of the chips (as described herein), Plaintiff would not have purchased the computers with Intel chips or would have paid substantially less for them.

14. Plaintiff Stephen C. Bevilacqua is an individual who is a citizen and resident of New York. Mr. Bevilacqua purchased two Lenovo Thinkpads, each containing two different Intel CPUs. Mr. Bevilacqua uses his computers primarily for personal purposes. Plaintiff was unware of the Meltdown and Spectre security flaws described herein when he purchased his computers. Had Mr. Bevilacqua known of the security flaws, and the need to install a performance-reducing patch on his computers to resolve them that would decrease the value of the chips (as described herein), Plaintiff would not have purchased the computers with Intel chips or would have paid substantially less for them.

15. Defendant Intel is a Delaware corporation headquartered at 2200 Mission College Boulevard, Santa Clara, California. Intel is licensed to and does business throughout the State of New York and the United States. Intel designs, manufactures, distributes, and sells computer products worldwide.

III. JURISDICTION AND VENUE

16. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) ("CAFA"), because (i) the proposed Class consists of well over 100 members; (ii) the parties are minimally diverse, as members of the proposed Class are citizens of a state different from Defendant's home state; and (iii) the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs.

17. This Court has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367.

18. This Court has personal jurisdiction over Plaintiffs because Plaintiffs submit to the Court's jurisdiction. This Court has personal jurisdiction over Defendant Intel because Intel has sufficient minimum contacts with New York, either directly or through its subsidiaries, and has otherwise purposefully availed itself of the markets in New York through the marketing and sale of its products in New York.

19. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant Intel is registered to do business in this District, maintains an office in this District, and regularly conducts business in this District.

IV. FACTUAL ALLEGATIONS

A. Intel and Central Processing Units

20. Intel is a technology company that designs and manufactures the world's most widely used microprocessor chips. ***More than 90 percent of all computers in the world use Intel chips***.[6]

[6] Cade Metz and Nicole Perlroth, *Researchers Discover Two Major Flaws in the World's Computers*, N.Y. Times (Jan. 3, 2018).

21. A microprocessor chip is the main component of all desktop and laptop computers and is often referred to as the "brain" of a computer. The key functional block of a microprocessor chip is a central processing unit ("CPU"), which functions as a calculator that can quickly execute operations (add, subtract, multiply, divide, etc.) at billions of times per second. When a user commands a computer program to perform a function, the CPU carries out that command, working with the other parts of the system to perform the desired task.

22. Microprocessor chips (and, therefore, CPUs) are also key components of other consumer electronics, including tablet computers, smart phones, and flat-screen televisions. Intel sells its chips as stand-alone component parts, as well as to third-party manufacturers, such as Dell Inc., HP Inc., and Apple Inc., who incorporate Intel's chips into a wide range of computer products and devices.

23. The performance of computer chips has improved dramatically over the last four decades due to constant improvements to the underlying technology. This improvement is set at a rate forecasted by Moore's Law. Named after Intel's co-founder, Gordon Moore, Moore's Law predicts that "the number of transistors incorporated into a chip will approximately double every 24 months." Put differently, Moore observed that a doubling of the number of transistors over a given area on a computer chip had been occurring approximately every two years, and projected that this trend would continue into the future.

24. David House, a colleague of Moore's at Intel, later factored in increased performance of individual transistors to conclude that overall performance of circuits would double every 18 months.[7] This means that every two years the size of a computer chip would

[7] Michael (Siyang) Li, *Keeping Up With Moore's Law*, Dartmouth Undergraduate J. of Sci. (May 29, 2013).

decrease and its speed and performance would more than double, which also has an effect on price: the faster the speed of a chip, the higher its price.

25. Intel produces some of the fastest computer chips in the world and prices them accordingly. Intel also touts the speed of its chips when marketing them and sells them on this basis.

B. Researchers Identify Vulnerabilities Affecting Intel Computer Chips

26. On January 3, 2018, a team of researchers at Google's Project Zero announced that they had discovered two major security flaws in the microprocessor chips found in nearly every computer in the world, including Intel chips. The release stated, in part:

> We have discovered that CPU data cache timing can be abused to efficiently leak information out of mis-speculated execution, leading to (at worst) arbitrary virtual memory read vulnerabilities across local security boundaries in various contexts.
>
> Variants of this issue are known to affect many modern processors, including certain processors by Intel, AMD and ARM. For a few Intel and AMD CPU models, we have exploits that work against real software. We reported this issue to Intel, AMD and ARM on 2017-06-01.[8]

27. Numerous articles discussing the significance of the two security flaws, known as Meltdown and Spectre, immediately followed. *The New York Times*, for instance, published an article that same day titled "Researchers Discover Two Major Flaws in the World's Computers," which stated:

> Computer security experts have discovered two major security flaws in the microprocessors inside nearly all of the world's computers.
>
> The two problems, called Meltdown and Spectre, could allow hackers to steal the entire memory contents of computers,

[8] Jann Horn, *Reading privileged memory with a side-channel*, Google Project Zero (Jan. 3, 2018).

including mobile devices, personal computers and servers running in so-called cloud computer networks.[9]

28. Although the researchers who discovered the flaws publicized their findings in January 2018, they first notified Intel of the issue in June 2017. In late November 2017, while aware of the issue but before it became public, Intel's CEO, Brian Krzanich, sold $24 million of Intel stock, leaving Krzanich with merely 250,000 shares of Intel stock—the minimum amount of shares his employment agreement allows him to hold.[10]

C. Meltdown and Spectre Exploit Intel's Efforts to Improve Computer Performance

29. Meltdown and Spectre present different security risks (and require different mitigating fixes) but both have one thing in common: the two vulnerabilities allow a non-privileged user (i.e., a hacker) to access information on a computer that the hacker should not be able to access—information including secret keys, passwords, or any other information sensitive information stored on a computer.[11]

30. Both flaws allow attackers to gain unauthorized access to computer memory and Meltdown can even attack a crucial feature of a computer's operating system known as the "kernel." The kernel performs a wide range of important functions, but one of its most significant responsibilities is to prevent data in one program (or application) from being read by another. As detailed in *Figure 1* below, the kernel connects the application software to the basic hardware of a computer, such as the CPU, the computer's main memory, and the device itself.

---

[9] Cade Metz and Nicole Perlroth, *Researchers Discover Two Major Flaws in the World's Computers*, N.Y. Times (Jan. 3, 2018).

[10] Troy Wolverton, *Intel sas Aware of the chip vulnerability when its CEO sold off $24 million in company stock*, Business Insider (Jan. 3, 2018).

[11] Ben Thompson, *Meltdown, Spectre, and the State of Technology*, Stratechery (Jan. 8, 2018).

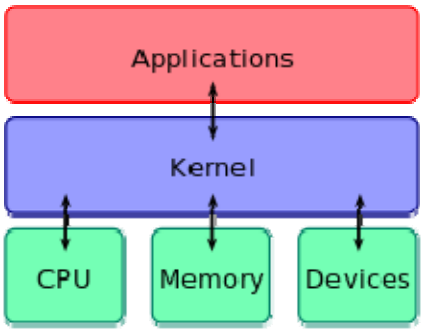

Figure 1

31. To maintain security, the kernel also acts as a barrier between the computer's main memory and other parts of a computer. The computer's main memory includes the computer's dynamic random-access memory ("DRAM"), as well as what is known as "kernel memory." Kernel memory is a protected area of memory used by the operating system and contains a computer's most confidential information, such as passwords and encryption keys.

32. Intel's success at creating faster and faster computer chips ultimately exposed those chips to Meltdown and Spectre. This is because both exploits take advantage of a foundational feature of computer processing known as "speculative execution"—a performance-enhancing process that Intel pursued aggressively at the expense of computer security.

33. Speculative execution means that a computer will perform a number of different tasks out of order (i.e., speculatively) and ahead of time in anticipation that the results of one of those tasks will be needed in the future. Although speculative execution of instructions increases efficiency, the process can also introduce security flaws if not performed correctly, because speculative execution moves sensitive data from a computer's main memory to its less secure "cache" memory, where it can be processed more efficiently. This increases speed, but it also leaves data more exposed because data in the "cache" memory is more vulnerable to unauthorized access than when it is stored in the main memory.

34. Intel was particularly aggressive in allowing its chips to perform tasks speculatively, which ultimately made its chips more vulnerable to security flaws that exploit this process. Indeed, both Meltdown and Spectre enable a hacker to use speculative execution to "trick" a computer into moving sensitive information into cache memory, where it can be more easily viewed.

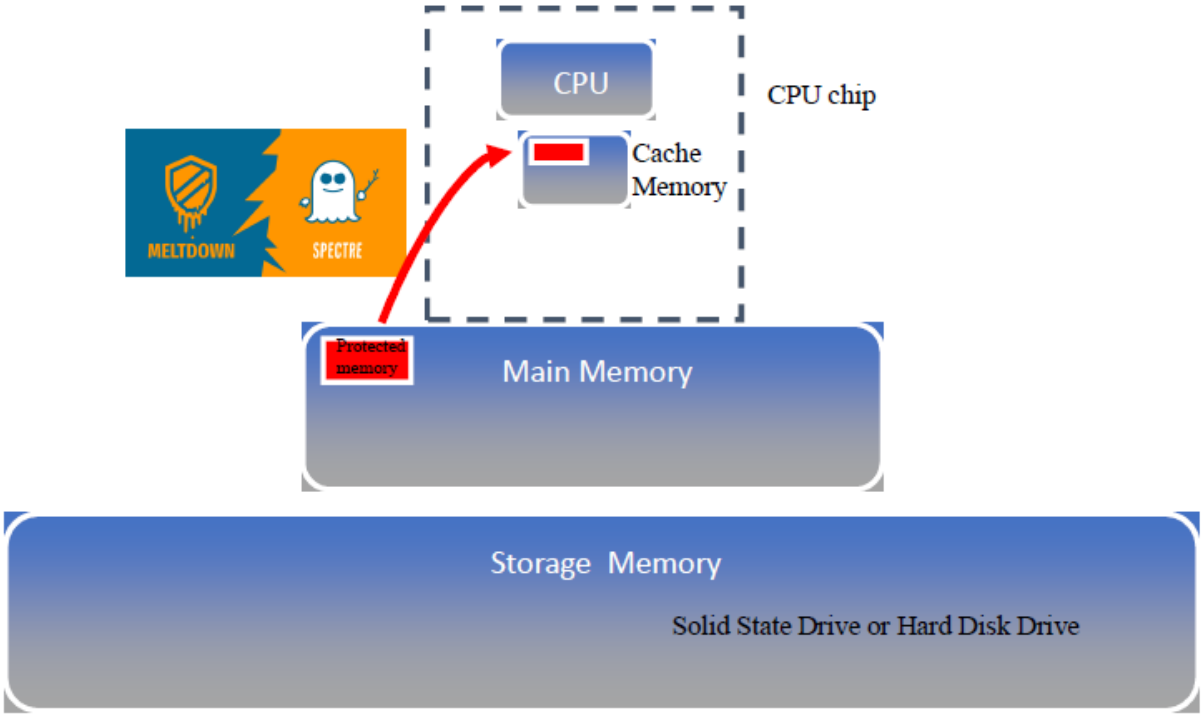

Figure 2

35. Although both Meltdown and Spectre exploit speculative execution, they do so in slightly different ways.

36. Meltdown allows a hacker to move the highly-sensitive data stored in kernel memory to the cache memory. The hacker can then use any program on the computer to access information moved to the cache memory (if the sensitive data were still in kernel memory, the

hacker would not be able to access it). Meltdown has been described by one of the researchers who discovered the flaw as "probably one of the worst CPU bugs ever found."[12]

37. Spectre does not involve kernel memory, but instead allows hackers to trick otherwise error-free applications into providing sensitive information to the cache memory. There are two variants of the Spectre flaw—the branch-prediction variant and the array-bounds variant—both of which allow a hacker to train or trick a computer to perform a speculative execution task that makes sensitive data more accessible.

38. Meltdown is a flaw that predominately affects Intel-designed chips, and impacts nearly every Intel chip since 1995—i.e., ***approximately 90 percent of all devices***. Spectre affects ***virtually every microprocessor on the market***, including those designed by Intel.

D. Fixing the Meltdown Flaw Dramatically Decreases Processing Speed

39. The only way Intel can completely eliminate the Meltdown and Spectre flaws is to entirely redesign its chips. Replacing a computer chip will not resolve the issue either because, according to some indications, ***there are no chips currently being made that are not defective***.[13]

40. The Meltdown flaw can be fixed, however, by installing a "patch" of software code on a computer's operating system.

41. Updates for the three main computer operating systems—Microsoft's Windows, Apple's Mac OS, and Linux—that would purportedly fix the Meltdown flaw have either been released or are currently in development. Additional security updates will likely be needed to further resolve the problem.

---

[12] Samuel Gibbs, *Spectre and Meltdown processor security flaws – explained*, The Guardian (Jan. 4, 2018).

[13] Chris O'Brien, *CERT: Only Way To Fix Meltdown and Spectre Vulnerabilities Is To Replace CPU*, Venture Beat (Jan. 4, 2018).

42. Although a security patch purportedly resolves the Meltdown flaw, it has been reported that a patch significantly impacts and slows down computer performance.[14] One such fix, known as the Kernel Page Table Isolation, is said to cause the computer program to slow down by ***up to 30 percent***.[15]

43. Microsoft issued a release on its website that details how security patches may impact computer performance, revealing that for many devices Microsoft "expect[s] that some users will notice a decrease in system performance."[16] The performance impact will be particularly pronounced computers running on an older Intel chip and older Windows 7 or 8 operating systems.[17]

44. Despite reports that the software patches slow down computer performance, Intel has largely downplayed the significance of the performance impact. On January 3, 2018, an Intel spokesperson stated: "Any performance impacts are workload-dependent, and, for the average computer user, should not be significant and will be mitigated over time."[18]

45. On January 9, 2018, Intel issued a press release in which it again suggested that performance impact would be workload dependent, but acknowledged that computers that are patched have shown a decrease in performance of between 2 and 14 percent:

---

[14] Tom Warren, *Intel's Processors Have a Security Bug and the Fix Could Slow Down PCs*, The Verge (Jan. 3, 2018).

[15] Rob Thubron, *Massive Security Flaw Found in Intel CPUs, Patch Could Hit Performance By Up to 30%*, Techspot (Jan. 3, 2018).

[16] Terry Myerson, Understanding the Performance Impact of Spectre and Metldown Mitigations on Windows Systems, Microsoft Secure, https://cloudblogs.microsoft.com/microsoftsecure/2018/01/09/understanding-the-performance-impact-of-spectre-and-meltdown-mitigations-on-windows-systems/

[17] *Id.*

[18] Tom Warren, *Intel says processor bug isn't unique to its chips and performance issues are 'workload-dependent*, The Verge (Jan. 3, 2018).

> Based on our tests on SYSmark 2014 SE, a leading benchmark of PC performance, 8th Generation Core platforms with solid state storage will see a performance impact of 6 percent or less. (SYSmark is a collection of benchmark tests; individual test results ranged from 2 percent to 14 percent.)[19]

46. Then, on January 17, 2018, Intel revealed that its test showed a reduction in performance ranging from 2 to 25 percent and that devices are rebooting more than usual after being patched.[20]

47. Intel continued to give customers mixed messages on January 22, 2018, when the Company announced that it was working on a new patch that would stop the rebooting problem and advised customers ***not*** to install the previously released patch until the new patch is available.[21]

48. Intel's unwillingness to fully admit the extent of the performance impact is not surprising: Intel's products are sold specifically on performance speed and are priced accordingly.

49. If Intel's computer chips were priced to reflect the speed at which they perform when patched, they would have been sold at a significantly lower price. Thus, had Plaintiffs and the Class known about the security flaws and the need for a security patch that would slow performance, they would have paid substantially less for Intel's chips.

50. Unlike Meltdown, Spectre cannot be mitigated with a patch because it is a problem with the fundamental way the processor is designed, and therefore requires the hardware

---

[19] Intel Newsroom, Intel Offers Security Update (Jan. 9, 2018), https://newsroom.intel.com/news/intel-offers-security-issue-update/.

[20] *Intel Fix Causes Reboots and Slowdowns*, BBC News (Jan. 18, 2018), *http://www.bbc.com/news/technology-42733032*.

[21] Intel Newsroom, *Root Cause of Reboot Issue Identified; Updated Guidance for Customers and Partners* (Jan. 22, 2018), https://newsroom.intel.com/news/root-cause-of-reboot-issue-identified-updated-guidance-for-customers-and-partners/.

(i.e., the computer chip) to be replaced entirely.[22] According to Expert A, however, there currently is no CPU replacement that can completely fix the Spectre flaw because a complete fix requires changes in the chip architecture that are only currently in the development phase.

51. Intel knew or should have known of the Meltdown and Spectre flaws many years ago given that Intel was best positioned to discover the defects—which ultimately were discovered by third-party researchers without access to Intel's proprietary information. To the extent Intel was not aware of the flaws, the Company's failure to discover them was either negligent or reckless.

52. When Intel ultimately learned about the flaws—as early as June 2017—Intel continued to sell its defective chips to unknowing consumers at prices that were significantly higher than what consumers would have paid had they known the truth about Intel's chips.

E. According to Expert A, the Reported Performance Issues Would Significantly Impact the Price of Intel Products

53. Plaintiffs consulted an expert on CPU chips and cache memory. Expert A has a Ph.D in Electrical Engineering and worked at Intel from 1992 to 2004 as a director of CPU and chip development and has over 25 years of industry experience on CPU and cache memory. Expert A has also been a consultant to a semiconductor company for 14 years working on CPU and memory chips. Specifically, Expert A has industry experience working on many aspects of CPU and cache memory: computer chip transitor development, CPU and memory testing, timing, reliability and yield, and standard cell and memory design. Expert A was also the technology group member for Intel's CPU strategic long-range planning group and ran Intel's task forces to push CPU performance. While at Intel, Expert A was the program manager for the

[22] Cade Metz and Nicole Perlroth, *Researchers Discover Two Major Flaws in the World's Computers*, N.Y. Times (Jan. 3, 2018).

technology that is used in all of Intel's advanced logic chips as well as other modern computer chips, such as those found in not just computers, but also Apple and Samsung mobile phones.

54. After leaving Intel, Expert A has been a tenured professor of Electrical and Computer Engineering at one of the country's largest public universities, where he teaches, among other things, undergraduate and graduate level courses on CPU and memory design and manufacturing. Expert A has over 70 granted patents and 60 publications all in the field of chip development.

55. Expert A confirmed that Intel's aggressive use of speculative execution ultimately caused the Meltdown and Spectre flaws. According to Expert A, these flaws trick a "victim" CPU into speculatively performing operations that would not occur during correct program execution. An attack program can move a victim's confidential information to cache memory, which is stored on the CPU chip. As Expert A explained, cache memory is local in time and space to the CPU and is physically located on the same chip as the CPU, whereas the computer's main memory is located off the chip. Once confidential information is moved to cache memory, it is then susceptible to unauthorized access by a hacker.

56. Expert A explained that the underpinnings of these attacks is that the CPU executes software (and moves data to cache memory) before a computer's safety checks are performed. Even if a security check fails, the confidential data, which is now located in cache memory, will remain in cache memory and not be "flushed" (i.e., removed) from the cache.

57. With respect to the performance impact of patched Intel chips, Expert A explained that a decrease in performance (after a patch is added) corresponds to a decrease in a chip's value, which can be quantified in dollar figures. According to Expert A, a 10% decrease in performance corresponds to a 10% decrease in price. Thus, a $200 chip that experiences a 10%

performance decrease (when a patch is added) diminishes the value of that chip by approximately $20.

58. Expert A also explained that no chip exists that does not suffer from the Spectre flaw because it can only be completely fixed with a complete redesign of a chip's architecture—a fix that is still only in development. As a result, Expert A explained, any chip that suffers from the Spectre flaw (even after a performance-diminishing patch is added to address Meltdown) has further decreased value.

V. CLASS ACTION ALLEGATIONS

59. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 ("Rule 23") on behalf of themselves and a class of other similarly situated individuals (the "Class"), as defined specifically below:

> All persons and entities within the United States who purchased one or more Intel CPUs from Intel or its authorized retailers or sellers, or one or more devices containing Intel CPUs.

60. Plaintiffs also bring this action pursuant to Rule 23 on behalf of themselves and the following subclass for Class members in New York (the "New York Subclass"):

> All persons and entities within the State of New York who purchased one or more Intel CPUs from Intel or its authorized retailers or sellers, or one or more devices containing Intel CPUs.

61. The Class and New York Subclass shall be referred to collectively throughout the Complaint as the Class.

62. Excluded from the Class is Defendant; any person who is an officer, director, partner or controlling person of Defendant, including any of its subsidiaries or affiliates; any entity in which Defendant has a controlling interest; and the legal representatives, heirs, successors and assigns of any such excluded person or entity.

63. Plaintiffs satisfy the numerosity, commonality, typicality, and adequacy prerequisites for suing as a representative party pursuant to Rule 23.

64. **Numerosity**. More than 90 percent of all computers sold in the United States contain Intel CPUs that are affected by the Meltdown and Spectre security flaws. Over 84% of all U.S. households own a computer, i.e., over 272 million people. Joinder is therefore impracticable and the numerosity requirement of Rule 23 is easily satisfied here.

65. **Commonality**. Plaintiffs' and Class members' claims raise predominately common factual and legal questions that can be answered for all Class members through a single class-wide proceeding. For example, to resolve any Class member's claims, it will be necessary to answer the following questions, and the answer to each of these questions will necessarily be the same for each Class member.

(a) whether Intel's chips or CPUs are affected by the Meltdown and Spectre flaws;

(b) whether Intel made any implied warranties in connection with its sale of its defective chips or CPUs;

(c) whether Intel breached any implied warranties relating to its sale of defective chips or CPUs by failing to resolve the Meltdown and Spectre security flaw in a manner required by law;

(d) whether Intel violated New York consumer protection law; and

(e) whether Plaintiffs and Class members are entitled to damages or other relief.

66. **Typicality.** Plaintiffs' claims are typical of the claims of the members of the Class. Among other things, Plaintiffs and Class members all purchased products containing defective Intel CPUs and all sustained injuries based on the same improper conduct.

67. **Adequacy**. Plaintiffs will adequately represent the proposed Class members. They have retained counsel competent and experienced in class action litigation and intend to pursue this action vigorously. Plaintiffs have no interests contrary to or in conflict with the interests of Class members.

68. In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual members and a class action is superior to individual litigation. Plaintiffs know of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action.

VI. CAUSES OF ACTION

COUNT I
BREACH OF IMPLIED WARRANTY

69. Plaintiffs repeat and re-allege every allegation set forth above as if fully set forth herein.

70. Defendant Intel and its authorized agents are resellers who sold Intel computer chips and CPUs to Plaintiffs and Class members in the regular course of business.

71. Defendant impliedly warranted to members of the general public, including Plaintiffs and Class members, that these computer chips and CPUs were of merchantable quality—i.e., that they were of high enough quality to make fit for sale, usuable for the purpose for which they were made, of average worth in the marketplace, or not broken, unworkable, damaged, contaminated, or flawed—were of the same quality as those generally acceptable in

the trade or that would pass without objection in the trade, were free from material defects, and were reasonably fit for the ordinary purposes for which they were intended or used.

72. Defendant Intel either was or should have been aware of the particular purposes for which such chips and CPUs are used, and that Plaintiffs and the Class members were relying on the skill and judgment of Intel to furnish suitable goods for such purpose.

73. Pursuant to agreements between Defendant Intel and its authorized agents and resellers, the stores Plaintiffs and Class members purchased their defective Intel chips and CPUs from are authorized retailers and authorized CPU service facilities. Plaintiffs and Class members are therefore third-party beneficiaries of, and substantially benefited from, such contracts.

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

75. The defect in the Intel chips and CPUs existed when the chips and CPUs left Intel's and their authorized agents' and retail sellers' possession and thus is inherent in those products.

76. As a direct and proximate result of Intel's breach of its implied warranties, Plaintiffs and Class members have suffered damages and continue to suffer damages, including economic damages at the point of sale in terms of the difference between the value of the chips and CPUs as warranted and the value of the chips and CPUs as delivered. Additionally, Plaintiffs and Class members either have or will incur economic, incidental, and consequential damages in the cost of repair or replacement and costs of complying with continued contractual obligations

as well as the cost of buying an additional chips and CPU they would not have purchased had the chips and CPUs in question not contained the non-repairable defect.

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

COUNT II
VIOLATIONS OF THE MAGNUSON-MOSS WARRANTY ACT, 15 U.S.C.§2301, *et seq.*

78. Plaintiffs repeat and re-allege every allegation set forth above as if fully set forth herein.

79. The Magnuson-Moss Warranty Act ("MMWA") defines "implied warranty" as any implied warranty arising "under State law . . . in connection with the sale by a supplier of a consumer product." MMWA 15 U.S.C. § 2301.

80. As defined by the MMWA, Plaintiffs and Class members are "consumers," Defendant is a "supplier" and the defective chips or CPUs are "consumer products." MMWA 15 U.S.C. § 2301.

81. Defendant Intel impliedly warranted that Intel's chips or CPUs were merchantable and fit for the ordinary and particular purpose for which they were used.

82. Defendant Intel breached the implied warranty by delivering chips or CPUs that were neither merchantable nor fit for the ordinary and particular purpose for which the chips or CPUs were used.

83. As a direct and proximate result of Defendant's breach of the implied warranty or merchantability, Plaintiffs and Class members have been damaged.

COUNT III
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349

84. Plaintiffs repeat and re-allege every allegation set forth above as if fully set forth herein.

85. New York General Business Law § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce.

86. Defendant Intel conducts business and trade within the meaning of New York General Business Law § 349.

87. Defendant Intel's conduct, as alleged herein, was consumer oriented because it sold its defective chips and CPUs, either directly or to authorized agents or resellers, to Plaintiffs and the Class, who purchased Intel's products for their personal use.

88. Defendant Intel's unlawful and deceptive consumer-oriented conduct is misleading in a material way because Defendant Intel induced Plaintiffs and the Class to pay a premium for chips and CPUs that purportedly performed at a certain speed but were not actually capable of performing at that speed when those products were operating safely. Plaintiffs and the Class, acting reasonably under the circumstances, therefore paid a price for Intel chips and CPUs that they would not have had they known the truth. Defendant Intel made its untrue and misleading statements and representations willfully, wantonly, and with reckless disregard for the truth.

89. Plaintiffs and the Class suffered injury as a result of Defendant Intel's deceptive acts because they paid a premium for Intel chips and CPUs that were vulnerable to hacking and not capable of performing as Intel represented when accounting for the need to resolve the security flaws. Accordingly, Plaintiffs and the Class received less than what they bargained and/or paid for.

90. Defendant Intel's deceptive and misleading practices constitute a deceptive act and practice in the conduct of business in violation of New York General Business Law § 349(a) and Plaintiffs and the Class have been damaged thereby.

91. As a result of Defendant's recurring unlawful deceptive acts and practices, Plaintiffs and the Class are entitled to monetary, compensatory, treble, and punitive damages, injunctive relief, restitution and disgorgement of all moneys obtained by means of Defendant Intel's unlawful conduct, interest, and attorneys' fees and costs.

COUNT IV
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 350

92. Plaintiffs repeat and re-allege every allegation set forth above as if fully set forth herein.

93. New York General Business Law § 350 prohibits false advertising in the conduct of any business, trade, or commerce. False advertising constitutes advertising, including labeling, of a commodity in a manner that is misleading in a material respect.

94. Defendant Intel falsely advertised its chips and CPUs because Defendant Intel failed to disclose the security flaws those products suffered from and that resolving those flaws would require fixing Intel's chips and CPUs in a manner that would significantly slow down performance.

95. Plaintiffs and Class members have been injured as a result of Defendant Intel's conduct inasmuch as they purchased Intel's chips and CPUs in reliance on Defendant's representations.

96. Defendant Intel's advertising induced Plaintiffs and the Class to purchase Defendant's products.

97. As described herein, Defendant's advertising included untrue and misleading statements and omissions, which Defendant Intel made willfully, wantonly, and with reckless disregard for the truth.

98. Defendant Intel's conduct, as described herein, constitutes false advertising in the conduct of business, trade, or commerce in violation of New York General Business Law § 350 and Plaintiffs and the Class have been damaged thereby. Specifically, as a result of Defendants' conduct, Plaintiffs and the Class paid a premium for Intel chips and CPUs that were vulnerable to hacking and not capable of performing as Intel represented when accounting for the need to resolve the security flaws. Accordingly, Plaintiffs and the Class received less than what they bargained and/or paid for.

99. Defendant Intel's material misrepresentations and omissions were substantially uniform in content, presentation, and impact on consumers at large, including Plaintiffs and the Class.

100. As a result of Defendant's recurring unlawful deceptive acts and practices, Plaintiffs and the Class are entitled to monetary, compensatory, treble, and punitive damages, injunctive relief, restitution and disgorgement of all moneys obtained by means of Defendant Intel's unlawful conduct, interest, and attorneys' fees and costs.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the other members of the Class, prays for judgment as follows:

(a) Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs as representatives of the Class, and appointing its counsel as Class Counsel;

(b) Awarding damages, including, but not limited to, compensatory, statutory, and punitive damages, to Plaintiffs and Class members in an amount to be determined at trial;

(c) Awarding Plaintiffs and the Class their reasonable litigation expenses and attorneys' fees;

(d) Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and

(e) Awarding such other and further relief as equity and justice may require.

VIII. JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury of all issues so triable.

DATED: January 25, 2018

LABATON SUCHAROW LLP

By: /s/ Michael P. Canty
Michael P. Canty
Ross M. Kamhi
140 Broadway
New York, NY 10005
Telephone: 212.907.0700
Facsimile: 212.818.0477
Email: mcanty@labaton.com
rkamhi@labaton.com

Attorneys for Plaintiffs Eric H. Bernstein and Stephen C. Bevilacqua

GOLDMAN SCARLATO & PENNY, P.C.
Mark S. Goldman
8 Tower Bridge, Suite 1025
161 Washington Street
Conshohocken, PA 19428
Telephone: 484.342.0700
Facsimile: 484.580.8747
Email: goldman@lawgsp.com

CARELLA, BYRNE, CECCHI, OLSTEIN,
BRODY & ANGELLO, P.C.
James E. Cecchi
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: 973.994.1700
Facsimile: 973.994.1744
Email: JCecchi@carellabyrne.com

SEEGER WEISS LLP
Christopher A. Seeger
55 Challenger Road, 6th Fl.
Ridgefield Park, NJ 07660
Telephone: 973.639.9100
Email: cseeger@seegerweiss.com

Additional Counsel for Plaintiffs

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

ERIC H. BERNSTEIN and STEPHEN C. BEVILACQUA

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Michael P. Canty
Labaton Sucharow LLP, 140 Broadway, New York, NY 10005
(212) 907-0700

DEFENDANTS

INTEL CORPORATION

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

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

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

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

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

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

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	☐ 625 Drug Related Seizure of Property 21 USC 881	☐ 422 Appeal 28 USC 158	☐ 375 False Claims Act
☐ 120 Marine	☐ 310 Airplane	☐ 365 Personal Injury - Product Liability	☐ 690 Other	☐ 423 Withdrawal 28 USC 157	☐ 376 Qui Tam (31 USC 3729(a))
☐ 130 Miller Act	☐ 315 Airplane Product Liability	☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	☐ 400 State Reapportionment
☐ 140 Negotiable Instrument	☐ 320 Assault, Libel & Slander	☐ 368 Asbestos Personal Injury Product Liability		☐ 820 Copyrights	☐ 410 Antitrust
☐ 150 Recovery of Overpayment & Enforcement of Judgment	☐ 330 Federal Employers' Liability	PERSONAL PROPERTY		☐ 830 Patent	☐ 430 Banks and Banking
☐ 151 Medicare Act	☐ 340 Marine	☒ 370 Other Fraud	LABOR	☐ 835 Patent - Abbreviated New Drug Application	☐ 450 Commerce
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	☐ 345 Marine Product Liability	☐ 371 Truth in Lending	☐ 710 Fair Labor Standards Act	☐ 840 Trademark	☐ 460 Deportation
☐ 153 Recovery of Overpayment of Veteran's Benefits	☐ 350 Motor Vehicle	☐ 380 Other Personal Property Damage	☐ 720 Labor/Management Relations	SOCIAL SECURITY	☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 160 Stockholders' Suits	☐ 355 Motor Vehicle Product Liability	☐ 385 Property Damage Product Liability	☐ 740 Railway Labor Act	☐ 861 HIA (1395ff)	☐ 480 Consumer Credit
☐ 190 Other Contract	☐ 360 Other Personal Injury		☐ 751 Family and Medical Leave Act	☐ 862 Black Lung (923)	☐ 490 Cable/Sat TV
☐ 195 Contract Product Liability	☐ 362 Personal Injury - Medical Malpractice		☐ 790 Other Labor Litigation	☐ 863 DIWC/DIWW (405(g))	☐ 850 Securities/Commodities/ Exchange
☐ 196 Franchise			☐ 791 Employee Retirement Income Security Act	☐ 864 SSID Title XVI	☐ 890 Other Statutory Actions
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS		☐ 865 RSI (405(g))	☐ 891 Agricultural Acts
☐ 210 Land Condemnation	☐ 440 Other Civil Rights	Habeas Corpus:	IMMIGRATION	FEDERAL TAX SUITS	☐ 893 Environmental Matters
☐ 220 Foreclosure	☐ 441 Voting	☐ 463 Alien Detainee	☐ 462 Naturalization Application	☐ 870 Taxes (U.S. Plaintiff or Defendant)	☐ 895 Freedom of Information Act
☐ 230 Rent Lease & Ejectment	☐ 442 Employment	☐ 510 Motions to Vacate Sentence	☐ 465 Other Immigration Actions	☐ 871 IRS—Third Party 26 USC 7609	☐ 896 Arbitration
☐ 240 Torts to Land	☐ 443 Housing/ Accommodations	☐ 530 General			☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 245 Tort Product Liability	☐ 445 Amer. w/Disabilities - Employment	☐ 535 Death Penalty			☐ 950 Constitutionality of State Statutes
☐ 290 All Other Real Property	☐ 446 Amer. w/Disabilities - Other	Other:			
	☐ 448 Education	☐ 540 Mandamus & Other			
		☐ 550 Civil Rights			
		☐ 555 Prison Condition			
		☐ 560 Civil Detainee - Conditions of Confinement			

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Breach of Warranty; Magnuson-Moss; NY GBL §§ 349, 350

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Nicholas G. Garaufis DOCKET NUMBER 1:18-cv-00065

DATE SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

CERTIFICATION OF ARBITRATION ELIGIBILITY

Local Arbitration Rule 83.10 provides that with certain exceptions, actions seeking money damages only in an amount not in excess of $150,000, exclusive of interest and costs, are eligible for compulsory arbitration. The amount of damages is presumed to be below the threshold amount unless a certification to the contrary is filed.

I, Michael P. Canty, counsel for Plaintiff, do hereby certify that the above captioned civil action is ineligible for compulsory arbitration for the following reason(s):

- [X] monetary damages sought are in excess of $150,000, exclusive of interest and costs,
- [ ] the complaint seeks injunctive relief,
- [ ] the matter is otherwise ineligible for the following reason

DISCLOSURE STATEMENT - FEDERAL RULES CIVIL PROCEDURE 7.1

Identify any parent corporation and any publicly held corporation that owns 10% or more or its stocks:

RELATED CASE STATEMENT (Section VIII on the Front of this Form)

Please list all cases that are arguably related pursuant to Division of Business Rule 50.3.1 in Section VIII on the front of this form. Rule 50.3.1 (a) provides that "A civil case is "related" to another civil case for purposes of this guideline when, because of the similarity of facts and legal issues or because the cases arise from the same transactions or events, a substantial saving of judicial resources is likely to result from assigning both cases to the same judge and magistrate judge." Rule 50.3.1 (b) provides that " A civil case shall not be deemed "related" to another civil case merely because the civil case: (A) involves identical legal issues, or (B) involves the same parties." Rule 50.3.1 (c) further provides that "Presumptively, and subject to the power of a judge to determine otherwise pursuant to paragraph (d), civil cases shall not be deemed to be "related" unless both cases are still pending before the court."

NY-E DIVISION OF BUSINESS RULE 50.1(d)(2)

1.) Is the civil action being filed in the Eastern District removed from a New York State Court located in Nassau or Suffolk County? [ ] Yes [X] No

2.) If you answered "no" above:

a) Did the events or omissions giving rise to the claim or claims, or a substantial part thereof, occur in Nassau or Suffolk County? [ ] Yes [X] No

b) Did the events or omissions giving rise to the claim or claims, or a substantial part thereof, occur in the Eastern District? [X] Yes [ ] No

c) If this is a Fair Debt Collection Practice Act case, specify the County in which the offending communication was received:

If your answer to question 2 (b) is "No," does the defendant (or a majority of the defendants, if there is more than one) reside in Nassau or Suffolk County, or, in an interpleader action, does the claimant (or a majority of the claimants, if there is more than one) reside in Nassau or Suffolk County? [ ] Yes [X] No

(Note: A corporation shall be considered a resident of the County in which it has the most significant contacts).

BAR ADMISSION

I am currently admitted in the Eastern District of New York and currently a member in good standing of the bar of this court.

[X] Yes [ ] No

Are you currently the subject of any disciplinary action (s) in this or any other state or federal court?

[ ] Yes (If yes, please explain [X] No

I certify the accuracy of all information provided above.

Signature: s/ Michael P. Canty

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

ERIC H. BERNSTEIN and STEPHEN C. BEVILACQUA, Individually and On Behalf of All Others Similarly Situated, *Plaintiff(s)* v. INTEL CORPORATION, *Defendant(s)*	)	Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* INTEL CORPORATION
2200 Mission College Blvd.
Santa Clara, CA 95054-1549

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Michael P. Canty
Labaton Sucharow LLP
140 Broadway
New York, NY 10005

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

DOUGLAS C. PALMER
CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)*

was received by me on *(date)* .

❒ I personally served the summons on the individual at *(place)*

on *(date)* ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)*

, a person of suitable age and discretion who resides there,

on *(date)* , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* , who is

designated by law to accept service of process on behalf of *(name of organization)*

on *(date)* ; or

❒ I returned the summons unexecuted because ; or

❒ Other *(specify):*

My fees are $ for travel and $ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date:

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc: