CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

NO: 500-06-000898-185

(Class Action)
SUPERIOR COURT

9085-4886 QUÉBEC INC.

Petitioner

-vs.-

INTEL OF CANADA, LTD., legal person duly constituted, having its head office at 5300-199 Bay Street, Commerce Court West, City of Toronto, Province of Ontario, M5L 1B9

and

INTEL INTERNATIONAL, INC., legal person duly constituted, having its head office at 2200 Mission College Boulevard, City of Santa Clara, State of California, 95054, USA

and

INTEL CORPORATION, legal person duly constituted, having its head office at 2200 Mission College Boulevard, City of Santa Clara, State of California, 95054, USA

Respondents

APPLICATION TO AUTHORIZE THE BRINGING OF A CLASS ACTION & TO APPOINT THE PETITIONER AS REPRESENTATIVE PLAINTIFF
(Art. 574 C.C.P and following)

TO ONE OF THE HONOURABLE JUSTICES OF THE SUPERIOR COURT, SITTING IN AND FOR THE DISTRICT OF MONTREAL, YOUR PETITIONER STATES AS FOLLOWS:

I. GENERAL PRESENTATION

A) The Action

1. The Petitioner wishes to institute a class action on behalf of the following class, of which it is a member, namely:

    - All persons residing in Quebec who purchased and/or leased, either alone or as part of an electronic device, an Intel processor with x86-64 architecture (the "Intel Processors"), or any other group to be determined by the Court;

2. Intel Processors are a line of mid to high-end consumer, workstation, and enthusiast central processing units ("CPUs") that are designed, developed, manufactured, licensed, marketed, distributed, promoted, sold and/or warranted by the Respondents;

3. "Intel Processors" include, but are not limited to: Intel Celeron, Intel Pentium, Intel Core i3, Intel Core i5, Intel Core i7, Intel Core i9, Intel Xeon, Intel Xeon Phi, Intel Atom, and Intel Itanium processors. Intel Processors can be found in desktop, laptop, and cloud-based computers, as well as in servers, tablets and smartphones;

4. "Intel Processor Products" means electronic devices containing Intel Processors, which are manufactured by major technology companies such as Lenovo, Hewlett Packard, Dell, Apple, Asus, and Acer, in accordance with design specifications prepared by the Intel Respondents;

5. It is alleged that the Respondents designed, developed, manufactured, licensed, marketed, distributed, promoted, sold and/or warranted Intel Processors which contain security flaws that may be exploited by hackers to access Class Members' personal and/or private information, such as passwords, usernames, security keys, credentials, cryptographic keys, social security/insurance numbers, personal photos, credit card and banking information, emails and other data (the "Design Defect");

6. It is further alleged that the Respondents have effectively known about the Design Defect since at least June 1, 2017 and should have known about the Design Defect significantly earlier than that, yet they intentionally made the business decision to not disclose its existence to consumers;

7. The Respondents have not offered to compensate consumers to remedy their damages, instead Class Members are asked to download a "patch", which will

dramatically degrade the CPUs' performance and slow the electronic device down by between 5% to 30%;

8. By reason of the Respondents' conduct, the Petitioner and the members of the Class have suffered damages upon which they wish to claim;

B) The Respondents

9. Respondent Intel of Canada, Ltd. ("Intel Canada") is a Canadian corporation with its head office in Markham, Ontario. It is a wholly-owned subsidiary of Respondent Intel International, Inc. that does business throughout Canada, including within the province of Quebec, the whole as appears more fully from a copy of an extract from the *Registraire des enterprise*, produced herein as **Exhibit R-1**;

10. Respondent Intel International, Inc. ("Intel International") is a wholly-owned subsidiary of Respondent Intel Corp. and it is the sole shareholder of Respondent Intel Corp.'s Canadian operations;

11. Respondent Intel Corporation ("Intel Corp.") is an American technology company and is the world's second largest and second highest valued semiconductor chip maker, and is the inventor of the x86 series of microprocessors, the processors found in most personal computers. Intel Corp. supplies processors for computer system manufacturers such as Apple, Lenovo, HP, and Dell and in most of the large, cloud-based servers, such as those of Google, Microsoft, and Amazon;

12. Intel Corp. is the parent company under which all of the other Respondents operate. It is the current registrant of 71 Canadian trade-marks going as far back as 1972 and 450 Canadian patents, the whole as appears more fully from a copy of said trade-marks from the Canadian Intellectual Property Office (CIPO), produced herein *en liasse* as **Exhibit R-2**;

13. The Respondents designed, developed, manufactured, licensed, marketed, distributed, promoted, sold and/or warranted Intel Processors throughout Canada, including within the province of Quebec;

14. Given the close ties between the Respondents and considering the preceding, all Respondents are solidarily liable for the acts and omissions of the other. Unless the context indicates otherwise, all Respondents will be referred to as "Intel" for the purposes hereof;

C) The Situation

a) The Central Processing Unit ("CPU") a.k.a. the Processor

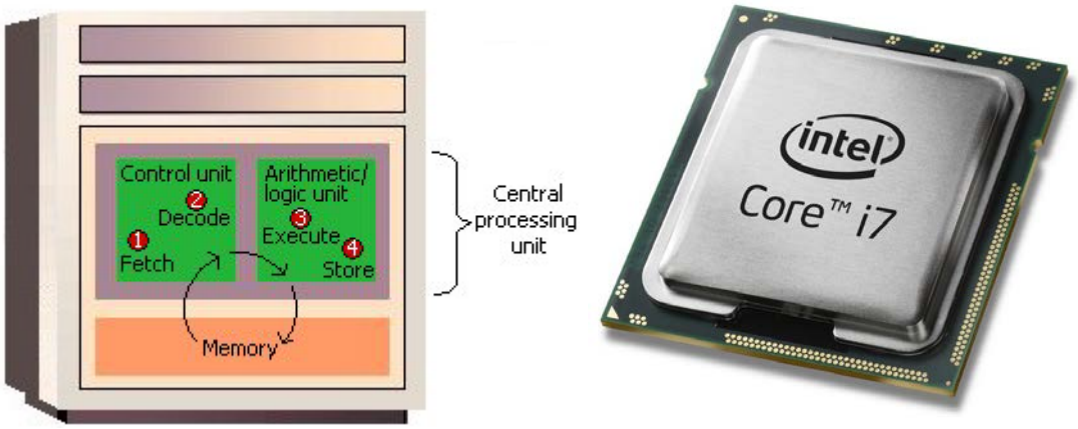
15. All modern-day desktop computers, laptop computers, tablets, smartphones, and televisions contain a central processing unit (a "CPU");

16. The CPU, also known as the processor or microprocessor, is the main chip in an electronic device that is responsible for carrying out all tasks. The CPU is the “brains” of a computer, and is responsible for executing a sequence of stored instructions called a program, the whole as appears more fully from a copy of the Trusted Reviews article entitled “What is a CPU? A beginner’s guide to processors” dated April 19, 2017, produced herein as **Exhibit R-3**;

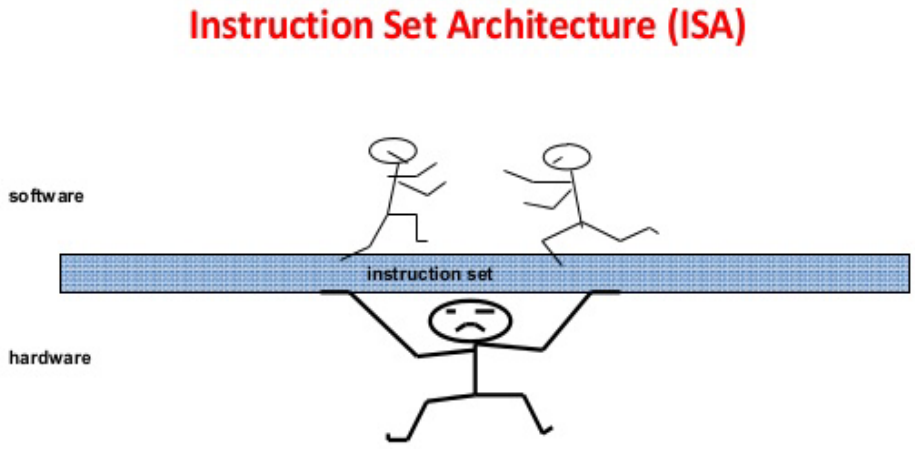
17. The CPU carries out the instructions of a computer program by performing the basic arithmetic, logical, control and input/output operations specified by the instructions;

18. The fundamental operation of most CPUs, regardless of the physical form they take, is to execute a sequence of stored instructions that is called a program. The instructions to be executed are kept in some kind of computer memory;

19. Hardwired into a CPU’s circuitry is a set of basic operations it can perform, called an instruction set. Such operations may involve, for example, adding or subtracting two numbers, comparing two numbers, or jumping to a different part of a program;



b) <u>Instruction Set Architecture and the x86-64 Processor</u>



20. Instruction Set Architecture ("ISA"), also referred to as the instruction set or simply as architecture, is the set of basic instructions that a computer processor understands. The ISA serves as the interface between software and hardware;

21. Computer programmers utilize the ISA to provide commands to a computer processor to tell it how to operate;

22. Software that has been written for an ISA can run on different implementations of the same ISA and thus, different computer processors can use almost the same ISA while still having very different internal designs. An example of an ISA is the x86-64 instruction set;

23. The term "x86" came into being because the names of several successors to Intel's 8086 processor end in "86", including the 80186, 80286, 80386 and 80486 processors;

24. In 1978, Intel introduced the first variation of the x86 instruction set and in May of 2017, it introduced the Intel Core i9 and the new Core X platform;

25. As of 2017, the majority of personal computers and laptops are based on the x86 architecture, x86 continues to dominate compute-intensive workstation and cloud computing segments;

c) <u>The Operating System, the Kernel, and Speculative Execution</u>

26. An operating system ("OS") is the name of a group of computer programs that allow an individual to operate a computer. Examples of operating systems are Microsoft Windows, Linux and MacOS;

27. An operating system has many functions. It is responsible for making sure that all the programs can use the CPU, system memory, displays, input devices, and other hardware;

28. The kernel is the central part of an operating system. It manages the operations of the computer and the hardware, most notably, memory and CPU time. The kernel is responsible for assigning and unassigning memory space to allow software to run;

29. There are thus two different types of "modes" a computer can be in: the "user" mode, and the "kernel" mode. The user mode is when the user of the computer is inputting commands and the kernel mode being when the computer is carrying out the task that the user inputted;

30. Kernel memory is used for tasks such as writing to a file, or opening a network connection. When a software program needs to execute an action, it temporarily hands control of the CPU to the kernel memory to carry out the task.

31. Back in the early 1990s, in an effort to speed up computer processing, computer chip engineers developed the idea of enabling computers guess at what data would be needed next. It was called "speculative execution";

32. Speculative execution is one way that rivals differentiate themselves is to perform faster than their competitors - in order to keep their internal pipelines primed with computer code to obey, they do their best to guess which instructions will be executed next, fetch those from memory, and carry them out. If the CPU guesses wrong, it has to undo the speculatively executed code, and run the actual stuff required, the whole as appears more fully from a copy of the Register article entitled "Meltdown, Spectre: The password theft bugs at the heart of Intel CPUs" dated January 4, 2018, produced herein as **Exhibit R-4**;

33. Unfortunately, the chips in electronic devices do not completely retract every step taken when they realize they have gone down the wrong path of code. That means remnants of data they should not have been allowed to fetch remain in their temporary caches, and may be accessed later (Exhibit R-4);

d) <u>The Security Flaws in the Intel Processors – "Meltdown" and "Spectre"</u>

34. On January 2 to 3, 2018, it was revealed that the Respondents' x86-64 processors contained three closely-related security flaws involving an abuse of speculative execution, namely:

- Variant 1 – CVE-2017-5753: a bounds check bypass – Spectre
- Variant 2 – CVE-2017-5715: a branch target injection – Spectre
- Variant 3 – CVE-2017-5754: a rogue data cache load – Meltdown

The whole as appears more fully from a copy of an extract from the website detailing the attacks entitled "Meltdown and Spectre" at both

www.spectreattack.com and www.meltdownattack.com, produced herein as **Exhibit R-5**;

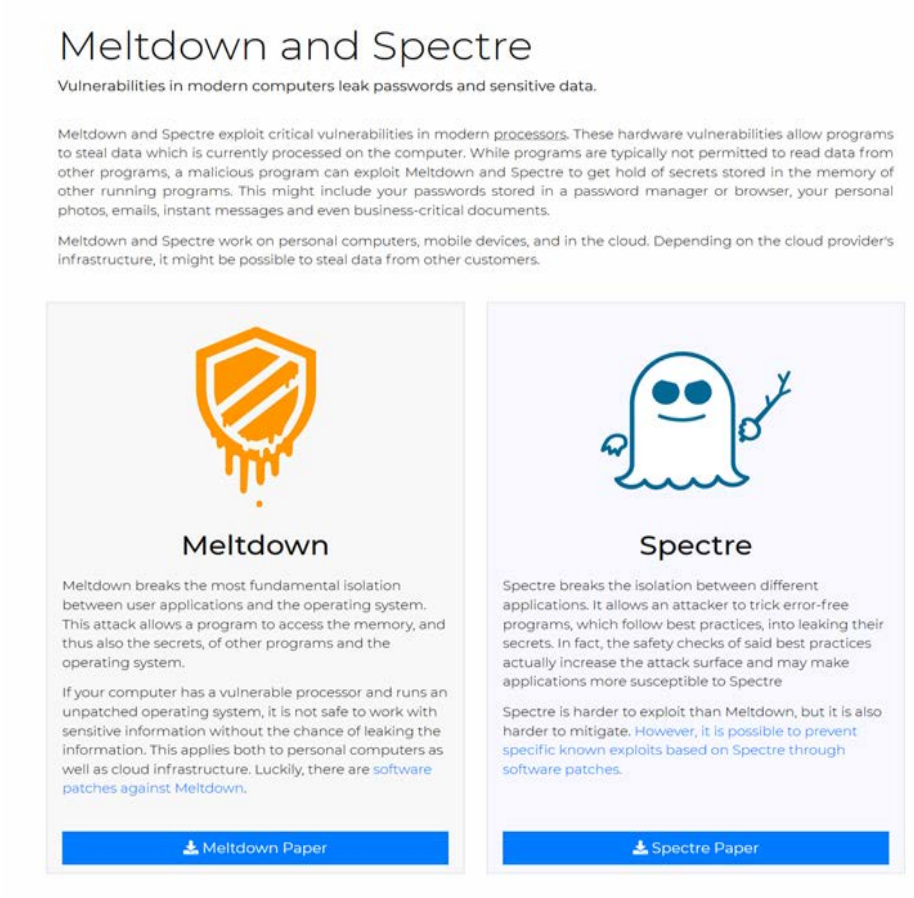
35. Hackers can exploit these vulnerabilities to steal the entire memory contents of electronic devices as well as servers running in so-called cloud computer networks. This means that the security flaws enable hackers to gain access to the contents of the kernel's memory, including personal and/or private information, such as passwords, usernames, security keys, credentials, cryptographic keys, social security/insurance numbers, personal photos, credit card and banking information, emails and other data;

36. It was revealed that these security flaws were found in "virtually all Intel processors [made in the past two decades] that will require fixes within Windows, macOS and Linux", the whole as appears more fully from a copy of the Guardian article entitled "Major security flaw found in Intel processors" dated January 3, 2018 and from a copy of the Verge article entitled "How to protect your PC against the major 'Meltdown' CPU security flaw" dated January 4, 2018, produced herein *en liasse* as **Exhibit R-6**;

37. Significantly, unlike ordinary malware, which runs like applications, hackers exploiting these kernel defects cannot be seen by antivirus software;

38. According to the website detailing the attacks (Exhibit R-5):

> Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.
>
> Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. Depending on the cloud provider's infrastructure, it might be possible to steal data from other customers.



(i) Meltdown (Variant 3)

39. Meltdown is a particular problem for cloud computing services (which are run by Intel, Google, and Microsoft, for example);

40. Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory and thus, also the secrets, of other programs and the operating system, the whole as appears more fully from a copy of the paper entitled “Meltdown” produced herein as **Exhibit R-7**;

41. All that a hacker needs to do in order to gain access to a person’s personal and/or private information is rent space on a cloud service, just like any other business customer. Once they were on the service, the flaw would allow them to grab any information they desire from other customers;

42. On a shared system, such as a public cloud server, it is possible, depending on the configuration, for software in a guest virtual machine to drill down into the host machine’s physical memory and steal data from other customers' virtual machines;

43. Meltdown is a major threat to the way cloud-computing systems operate. Cloud services often share machines among many customers – and it is quite uncommon for a single server to be dedicated to a single customer. Though security tools and protocols are intended to separate customers' data, the recently discovered chip flaws would allow hackers to circumvent these protections for their own purposes, the whole as appears more fully from a copy of The New York Times article entitled "Researchers Discover Two Major Flaws in the World's Computers" dated January 3, 2018, produced herein as **Exhibit R-8**;

44. The personal computers used by consumers are also vulnerable, but hackers would have to first find a way to run software on a personal computer before they could gain access to information elsewhere on the machine. There are various ways that could happen: Attackers could fool consumers into downloading software in an email, from an app store or visiting an infected website (Exhibit R-8);

45. According to the researchers, the Meltdown flaw affects virtually every microprocessor made by Intel, which makes chips used in more than 90 percent of the computer servers that underpin the internet and private business operations (Exhibit R-8);

46. Microsoft customers, the maker of the Windows operating system, will need to install an update from the company to fix the problem. The worldwide community of coders that oversees the open-source Linux operating system, which runs about 30% of computer servers worldwide, has already posted a patch for that operating system. Apple had a partial fix for the problem and is expected to have an additional update (Exhibit R-8);

47. To safeguard a computer from the Meltdown security flaw, the operating system must be updated or "patched" with software code. The patch will result in computers with Intel CPUs ignoring the kernel memory inside of Intel microprocessors. This process is known as kernel page-table isolation or "KPTI", the whole as appears more fully from a copy of the Bleeping Computer article entitled "OS Makers Preparing Patches for Secret Intel CPU Security Bug" dated January 3, 2018, produced herein as **Exhibit R-9**;

48. It has been estimated that the software patches could slow the performance of affected machines by up to 30%, the whole as appears more fully from a copy of the Verge article entitled "Intel's processors have a security bug and the fix could slow down PCs" dated January 3, 2018 and from a copy of the Register article entitled "Kernel-memory-leaking Intel processor design flaw forces Linux, Windows redesign" dated January 2, 2018, produced herein *en liasse* as **Exhibit R-10**;

49. While it is unclear whether this vulnerability has yet been exploited, once a security problem becomes public (such as the present), it becomes necessary to fix the issue as the likelihood of a breach becomes greatly increased;

(ii) Spectre (Variants 1 and 2)

50. Spectre affects most processors in use today and, unfortunately, there is no known fix or patch for it – it is unclear what the Respondents will do to address it;

51. Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre, the whole as appears more fully from a copy of the paper entitled "Spectre" produced herein as **Exhibit R-11**;

52. According to The New York Times, "[t]here is no easy fix for Spectre ... as for Meltdown, the software patch needed to fix the issue could slow down computers by as much as 30 percent" (Exhibit R-8);

53. Spectre is a problem in the fundamental way processors are designed, and the threat from Spectre is "going to live with us for decades," said Mr. Kocher, the president and chief scientist at Cryptography Research, a division of Rambus. "Whereas Meltdown is an urgent crisis, Spectre affects virtually all fast microprocessors," Mr. Kocher said. An emphasis on speed while designing new chips has left them vulnerable to security issues, he said. "We've really screwed up," Mr. Kocher said. "There's been this desire from the industry to be as fast as possible and secure at the same time. Spectre shows that you cannot have both" (Exhibit R-8);

54. A fix may not be available for Spectre until a new generation of chips hit the market (Exhibit R-8);

e) Intel's Prior Knowledge of the Design Defect – At Least as Early as June 1, 2017

55. It has been reported that Intel was informed of the Design Defect on June 1, 2017 when the Meltdown flaw was discovered by Jann Horn, a security analyst at a Google-run security research group called Google Project Zero. Mr. Horn was the first to alert Intel. The chip giant then heard from other researchers who had also discovered the flaw, including Werner Haas and Thomas Prescher, at Cyberus Technology; and Daniel Gruss, Moritz Lipp, Stefan Mangard and Michael Schwarz at the Graz University of Technology (Exhibit R-8), the whole as appears more fully from a copy of the article entitled "Negative Result: Reading Kernel Memory From User Mode" undated and from a copy of the Project Zero report entitled "Reading privileged memory with a side-channel" dated January 2018, produced herein *en liasse* as **Exhibit R-12**;

56. The second flaw, Spectre, was also discovered by Mr. Horn at Google and separately by Mr. Kocher, in coordination with Mike Hamburg at Rambus, Mr. Lipp at Graz University and Yuval Yarom at the University of Adelaide in Australia (Exhibit R-8);

57. On October 30, 2017, Intel's CEO Brian Krzanich put into place a plan to sell nearly half of his own shares by November 29, 2017. The sale yielded him $50 million and left him with only 250,000 shares – the fewest he was allowed to hold under his contract, the whole as appears more fully from a copy of the CNN article entitled "Intel CEO's massive stock dump raises eyebrows" dated January 4, 2018, produced herein as **Exhibit R-13**;

58. On January 2, 2018, it was revealed in the media that the Intel Processors suffer from the Design Defect. The next day, Intel's shares dropped by 3% and another 5% the day after that;

59. Yet, Intel only announced the Design Defect to the public on January 3, 2018;

f) Intel's Response

60. On January 3, 2018, Intel released a press release, which attempted to downplay the issue:

> "Intel and other technology companies have been made aware of new security research describing software analysis methods that, when used for malicious purposes, have the potential to improperly gather sensitive data from computing devices that are operating as designed. Intel believes these exploits do not have the potential to corrupt, modify or delete data.
> …
> Intel is committed to the industry best practice of responsible disclosure of potential security issues, which is why Intel and other vendors had planned to disclose this issue next week…
> …
> Intel believes its products are the most secure in the world and that, with the support of its partners, the current solutions to this issue provide the best possible security for its customers."

The whole as appears more fully from a copy of Intel's Press Release entitled "Intel Respond to Security Research Findings" dated January 3, 2018 and from a copy of the Register article entitled "We translated Intel's crap attempt to spin its way out of CPU security bug PR nightmare" dated January 4, 2018, produced herein *en liasse* as **Exhibit R-14**;

II. FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY THE PETITIONER

61. On March 11, 2013, the Petitioner purchased a Dell OptiPlex 960 desktop computer with an Intel Core 2 Duo processor from XDS Electronics for $455.06

including taxes and shipping, the whole as appears more fully from a copy of the invoice from said purchase dated March 11, 2013, produced herein as **Exhibit R-15**;

62. On December 12, 2013, Petitioner purchased a Dell Latitude E6410 laptop computer with an Intel Core i5 processor for $581.76 including taxes and shipping, the whole as appears more fully from a copy of the invoice from said purchase dated December 12, 2013, produced herein as **Exhibit R-16**;

63. These computers contain the Intel Processors which suffer from security flaws that put the Petitioner's personal and/or private information at risk of exposure;

64. At no time did the Respondents advise the Petitioner that its x86-64 computer processors contained the Design Defect;

65. Even with notice and knowledge, the Respondents have not offered to compensate the Petitioner to remedy its damages;

66. Had the Petitioner known of the Intel Processor's Design Defect or that Intel's microchip would require a patch that would reduce its performance rate, it would not have purchased the computers which contained the x86-64 computer processor, and certainly would not have agreed to pay the price that it did;

67. The Petitioner is aware, through his online research, that several class actions have been filed in the United States against Intel for the same issues as outlined herein, the whole as appears more fully from a copy of said Class Action Complaints, produced herein *en liasse* **as Exhibit R-17**;

68. The Petitioner's damages are a direct and proximate result of the Respondents' conduct;

69. In consequence of the foregoing, the Petitioner is justified in claiming damages;

III. FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY EACH OF THE MEMBERS OF THE GROUP

70. Every member of the Class has purchased and/or leased the Respondents' Intel Processors with the Design Defect;

71. Class Members were thus sold products that do not perform or possess the capabilities, uses and/or benefits reasonably expected, and contained a latent design or manufacturing defect that prevents electronic devices containing these CPUs from performing as reasonably expected, or remain subject to a significant security flaw;

72. Thus, Class Members have sustained economic injury by paying for processors or electronic devices that they would not have otherwise purchased and by being deprived of the full intended use of their purchased products;

73. In consequence of the foregoing, each member of the Class is justified in claiming at least one or more of the following as damages:

    i. An amount equal to the full value/purchase price of the Intel Processors;

    ii. Reduced value of the Intel Processors and the electronic devices in which they are contained;

    iii. Damages due to the reduced functionality of the Intel Processors and the electronic devices in which they are contained;

    iv. Punitive damages;

74. All of these damages to the Class Members are a direct and proximate result of the Respondents' conduct;

IV. CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

A) The composition of the Class makes it difficult or impracticable to apply the rules for mandates to sue on behalf of others or for consolidation of proceedings

75. The Petitioner does not know the exact size of the class; however, given how prevalent the Intel Processors are and how widespread their use is in various electronic devices, it is safe to estimate that it is encompasses hundreds of thousands of individuals. Further, Intel's sales figures could establish the approximate number of Class Members;

76. Class Members are numerous and are scattered across the entire province;

77. In addition, given the costs and risks inherent in an action before the courts, many people will hesitate to institute an individual action against the Respondents. Even if the Class Members themselves could afford such individual litigation, it would place an unjustifiable burden on the courts and, at the very least, is not in the interests of judicial economy. Furthermore, individual litigation of the factual and legal issues raised by the conduct of the Respondents would increase delay and expense to all parties and to the court system;

78. While certain Class Members may have suffered a substantial loss, it is expected that the majority have suffered small losses making it economically unfeasible to finance the litigation expenses inherent in any legal proceeding;

79. This class action overcomes the dilemma inherent in an individual action whereby the legal fees alone would deter recovery and thereby in empowering

the consumer, it realizes both individual and social justice as well as rectifies the imbalance and restore the parties to parity;

80. Also, a multitude of actions instituted in either the same or different judicial districts, risks having contradictory judgments on questions of fact and law that are similar or related to all members of the Class;

81. These facts demonstrate that it would be impractical, if not impossible, to contact each and every member of the Class to obtain mandates and to join them together into one action;

82. In these circumstances, a class action is the only appropriate procedure and the only viable means for all of the members of the Class to effectively pursue their respective legal rights and have access to justice;

B) <u>The claims of the members of the Class raise identical, similar or related issues of law or fact</u>

83. Individual issues, if any, pale by comparison to the numerous common issues that are significant to the outcome of the litigation;

84. The damages sustained by the Class Members flow, in each instance, from a common nucleus of operative facts, namely, Respondents' misconduct;

85. The claims of the members raise identical, similar or related issues of fact or law, namely:

a) Are the Intel processors with x86-64 architecture (the "Intel Processors") defective?

b) Do Intel Processors contain security flaws that expose users' personal and/or private information?

c) Are the Intel Processors fit to be used as intended?

d) Did the Respondents know, or should they have known that their Intel Processors were defective?

e) Did the Respondents fail to adequately disclose to users that their Intel Processors were defective or did they do so in a timely manner?

f) Does the remedy of the defects reduce the performance of the electronic devices which contain the Intel Processors?

g) Have Class Members been damaged by the Respondents' conduct and, if so, what is the proper measure of such damages?

h) Should an injunctive remedy be ordered to force the Respondents to recall, repair, and/or replace Class Members' Intel Processors free of charge?

i) In the affirmative to any of the above issues, did the Respondents' conduct engage their solidary liability toward the members of the Class?

j) Are members of the Class entitled to punitive (exemplary) damages?

86. The interests of justice favour that this application be granted in accordance with its conclusions;

V. NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

87. The action that the Petitioner wishes to institute on behalf of the members of the Class is an action in damages and injunctive relief;

88. The conclusions that the Petitioner wishes to introduce by way of an application to institute proceedings are:

GRANT the class action of the Petitioner and each of the members of the Class;

ORDER the Defendants to recall, repair, and/or replace the Intel Processors free of charge;

DECLARE the Defendants solidarily liable for the damages suffered by the Petitioner and each of the Class Members;

CONDEMN the Defendants to pay to each member of the Class a sum to be determined in compensation of the damages suffered, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay to each of the members of the Class, punitive damages, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay interest and additional indemnity on the above sums according to law from the date of service of the application to authorize a class action;

ORDER the Defendants to deposit in the office of this Court the totality of the sums which forms part of the collective recovery, with interest and costs;

ORDER that the claims of individual Class Members be the object of collective liquidation if the proof permits and alternately, by individual liquidation;

CONDEMN the Defendants to bear the costs of the present action including expert and notice fees;

RENDER any other order that this Honourable Court shall determine and that is in the interest of the members of the Class;

A) <u>The Petitioner requests that it be attributed the status of representative of the Class</u>

89. The Petitioner is a member of the Class;

90. The Petitioner is ready and available to manage and direct the present action in the interest of the members of the Class that it wishes to represent and is determined to lead the present dossier until a final resolution of the matter, the whole for the benefit of the Class, as well as, to dedicate the time necessary for the present action before the Courts and the *Fonds d'aide aux actions collectives*, as the case may be, and to collaborate with its attorneys;

91. Petitioner has the capacity and interest to fairly, properly, and adequately protect and represent the interest of the members of the Class;

92. Petitioner has given the mandate to its attorneys to obtain all relevant information with respect to the present action and intends to keep informed of all developments;

93. Petitioner, with the assistance of its attorneys, is ready and available to dedicate the time necessary for this action and to collaborate with other members of the Class and to keep them informed;

94. Petitioner has given instructions to its attorneys to put information about this class action on its website and to collect the coordinates of those Class Members that wish to be kept informed and participate in any resolution of the present matter, the whole as will be shown at the hearing;

95. Petitioner is in good faith and has instituted this action for the sole goal of having its rights, as well as the rights of other Class Members, recognized and protected so that they may be compensated for the damages that they have suffered as a consequence of the Respondents' conduct;

96. Petitioner understands the nature of the action;

97. Petitioner's interests do not conflict with the interests of other Class Members and further Petitioner has no interest that is antagonistic to those of other members of the Class;

98. Petitioner is prepared to be examined out-of-court on its allegations (as may be authorized by the Court) and to be present for Court hearings, as may be required and necessary;

99. Petitioner has spent time researching this issue on the internet and meeting with its attorneys to prepare this file. In so doing, it is convinced that the problem is widespread;

B) <u>The Petitioner suggests that this class action be exercised before the Superior Court of Justice in the district of Montreal</u>

100. A great number of the members of the Class reside in the judicial district of Montreal and in the appeal district of Montreal;

101. The Petitioner's attorneys practice their profession in the judicial district of Montreal;

102. The present application is well founded in fact and in law.

FOR THESE REASONS, MAY IT PLEASE THE COURT:

GRANT the present application;

AUTHORIZE the bringing of a class action in the form of an application to institute proceedings in damages and injunctive relief;

DESIGNATE the Petitioner as representative of the persons included in the Class herein described as:

- All persons residing in Quebec who purchased and/or leased, either alone or as part of an electronic device, an Intel processor with x86-64 architecture (the "Intel Processors"), or any other group to be determined by the Court;

IDENTIFY the principle issues of fact and law to be treated collectively as the following:

a) Are the Intel processors with x86-64 architecture (the "Intel Processors") defective?

b) Do Intel Processors contain security flaws that expose users' personal and/or private information?

c) Are the Intel Processors fit to be used as intended?

d) Did the Respondents know, or should they have known that their Intel Processors were defective?

e) Did the Respondents fail to adequately disclose to users that their Intel Processors were defective or did they do so in a timely manner?

f) Does the remedy of the defects reduce the performance of the electronic devices which contain the Intel Processors?

g) Have Class Members been damaged by the Respondents' conduct and, if so, what is the proper measure of such damages?

h) Should an injunctive remedy be ordered to force the Respondents to recall, repair, and/or replace Class Members' Intel Processors free of charge?

i) In the affirmative to any of the above issues, did the Respondents' conduct engage their solidary liability toward the members of the Class?

j) Are members of the Class entitled to punitive (exemplary) damages?

103. The interests of justice favour that this application be granted in accordance with its conclusions;

IDENTIFY the conclusions sought by the class action to be instituted as being the following:

GRANT the class action of the Petitioner and each of the members of the Class;

ORDER the Defendants to recall, repair, and/or replace the Intel Processors free of charge;

DECLARE the Defendants solidarily liable for the damages suffered by the Petitioner and each of the Class Members;

CONDEMN the Defendants to pay to each member of the Class a sum to be determined in compensation of the damages suffered, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay to each of the members of the Class, punitive damages, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay interest and additional indemnity on the above sums according to law from the date of service of the application to authorize a class action;

ORDER the Defendants to deposit in the office of this Court the totality of the sums which forms part of the collective recovery, with interest and costs;

ORDER that the claims of individual Class Members be the object of collective liquidation if the proof permits and alternately, by individual liquidation;

CONDEMN the Defendants to bear the costs of the present action including expert and notice fees;

RENDER any other order that this Honourable Court shall determine and that is in the interest of the members of the Class;

DECLARE that all members of the Class that have not requested their exclusion, be bound by any judgment to be rendered on the class action to be instituted in the manner provided for by the law;

FIX the delay of exclusion at thirty (30) days from the date of the publication of the notice to the Class Members, date upon which the members of the Class that have not exercised their means of exclusion will be bound by any judgment to be rendered herein;

ORDER the publication of a notice to the members of the group in accordance with article 579 C.C.P. within sixty (60) days from the judgment to be rendered herein in the La Presse, The Montreal Gazette, and Le Soleil;

ORDER that said notice be posting the on the Respondents' website at www.intel.ca, Facebook page(s), and twitter accounts with a link stating "Notice to Quebec residents with Intel processors";

RENDER any other order that this Honourable Court shall determine and that is in the interest of the members of the Class;

THE WHOLE with costs, including all publication fees.

Montreal, January 8, 2018

(s) Andrea Grass

_____

CONSUMER LAW GROUP INC.
Per: Me Andrea Grass
Attorneys for the Petitioner

CONSUMER LAW GROUP INC.
1030 rue Berri, Suite 102
Montréal, Québec, H2L 4C3
Telephone: (514) 266-7863
Telecopier: (514) 868-9690
Email: agrass@clg.org