UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KASPERSKY LAB, INC. 500 Unicorn Park, 3rd Floor Woburn, Massachusetts 01801; and KASPERSKY LABS LIMITED New Bridge Street House 30-34 New Bridge Street London, EC4V 6BJ United Kingdom Plaintiffs, v. UNITED STATES OF AMERICA 950 Pennsylvania Ave., NW Washington, DC 20530 Defendant	Civil Action No. _____

COMPLAINT

Those who wrote our Constitution well knew the danger inherent in special legislative acts which take away the life, liberty, or property of particular named persons because the legislature thinks them guilty of conduct which deserves punishment. They intended to safeguard the people of this country from punishment without trial by duly constituted courts…When our Constitution and Bill of Rights were written, our ancestors had ample reason to know that legislative trials and punishments were too dangerous to liberty to exist in the nation of free men they envisioned. And so they proscribed bills of attainder… Much as we regret to declare that an Act of Congress violates the Constitution, we have no alternative here.

--United States v. Lovett, 328 U.S. 303 (1946)

1. Kaspersky Lab, Inc., a Massachusetts corporation, together with its U.K. parent company Kaspersky Labs Limited ("Plaintiffs" or "Kaspersky Lab"), bring this action to invalidate Sections 1634 (a) and (b) of the National Defense Authorization Act for Fiscal Year 2018, Pub. Law No. 115-91 (the "NDAA") as an unconstitutional bill of attainder.

2. President Trump signed the NDAA into law on December 12, 2017. Sections 1634(a) and (b) state that effective October 1, 2018, "[n]o department, agency, organization, or other element of the Federal Government may use... any hardware, software, or services developed or provided, in whole or in part, by… Kaspersky Lab…"

3. Those sections were introduced and adopted hastily by Congress in the context of mounting animosity towards Russia and substantial political pressure on all branches of Government to be seen as reacting to the apparent Russian interference in the 2016 presidential elections. However, Congress's action against Plaintiffs through the NDAA is based solely on vague and inflammatory allegations directed at Plaintiffs unsubstantiated by any legislative fact-finding. These sections of the NDAA singularly and unfairly name and punish Kaspersky Lab, one of the world's leading antivirus software companies, by prohibiting the federal government from using any Kaspersky Lab products or services and permanently depriving Kaspersky Lab of any direct or indirect federal government business.

4. Congress violated the foundational principle of separations of powers by circumventing the judicial process and enacting an unconstitutional bill of attainder in direct contravention of Article I, Section 9 of the U.S. Constitution (the "Bill of Attainder Clause" or "Clause"). The Bill of Attainder Clause forbids Congress from enacting laws which impose individualized deprivations of life, liberty, and property and inflict punishment on individuals and corporations without a judicial trial. The Clause ensures that Congress accomplishes

legitimate and non-punitive objectives by establishing rules of general applicability which do not specify persons to be sanctioned. The Clause is intended to prevent Congress from assuming the power of the executive and judiciary branches and then determining for itself conduct it regards as blameworthy and deserving of punishment, what evidence will suffice as proof, whether to pronounce a disfavored person guilty, and what manner and degree of punishment to impose.

5. The NDAA violates this prohibition because, rather than enacting objective rules of general applicability, Sections 1634(a) and (b) specifically, individually, and exclusively name Kaspersky Lab as a target for legislative punishment.

6. At the same time that it legislated with the maximum specificity possible, Congress also enacted the broadest ban possible, covering not only Kaspersky Lab's antivirus software—the company's principal product—and not only "software" generally, as proposed in the version of the NDAA that was approved by the Senate Armed Services Committee, but anything and everything bearing Kaspersky Lab's name.

7. To achieve legitimate national security objectives within the bounds of its Constitutional authority, Congress could, and should, have enacted a rule of general applicability. In fact they did. Section 1634(c) of the NDAA, which contains a series of requirements upon the Secretary of Defense to review and report on the procedures for removing suspect products and services from federal government information technology networks, is such a rule.

8. The absence of any legitimate legislative purpose on the face of the law itself and the thread-bare legislative record make it difficult to discern any non-punitive Congressional

intent. The ready availability of less burdensome alternatives to the expansive ban actually imposed is also strongly suggestive of an intent to inflict punishment on Kaspersky Lab.

9. Kaspersky Lab has never been convicted of any crime or subject to any adverse judicial finding. Nor is there any compelling reason to even suspect the company of a crime. In fact, Department of Homeland Security ("DHS") officials testifying before Congress have expressly stated that there is no conclusive evidence that Kaspersky Lab has ever facilitated a breach of government information systems.

10. The NDAA is therefore a bill of attainder. The law "attaints"—or "stains"—Kaspersky Lab and as a result the company suffers profound reputational injury by design.

11. For these reasons, Plaintiffs bring this suit seeking a declaratory judgment that the ban—as set forth in Sections 1634(a) and (b)—is unconstitutional, and seek injunctive relief enjoining its enforcement.

PARTIES

12. Plaintiff Kaspersky Lab, Inc. is a Massachusetts corporation with its principal place of business in Woburn, Massachusetts. Kaspersky Lab, Inc. is a directly wholly-owned subsidiary of Plaintiff Kaspersky Labs Limited, a U.K. holding company.

13. Defendant United States of America is a defendant through the action of the U.S. Congress in enacting the NDAA.

JURISDICTION AND VENUE

14. This action arises under the Bill of Attainder Clause, Article I, § 9, c1.3 of the U.S. Constitution. This Court has jurisdiction pursuant to 28 U.S.C. § 1331.

15. This Court also has jurisdiction under the Declaratory Judgment Act, 28 U.S.C. § 2201 et seq., in order to settle an actual controversy between plaintiffs and defendant United States of America involving the constitutionality of a federal law.

16. The Court has the authority to grant declaratory and injunctive relief pursuant to 28 U.S.C. §§ 2201 and 2202, and its inherent equitable powers.

17. Venue is proper in this district pursuant to 28 U.S.C. § 1391(e)(1).

FACTUAL ALLEGATIONS

I. Kaspersky Lab, Its Reputation in the Industry, and Its Principles of Fighting Cyberthreats

18. Kaspersky Lab is a multinational cybersecurity company exclusively focused on protecting against cyberthreats, no matter their origin. It is one of the world's largest privately owned cybersecurity companies. It operates in 200 countries and territories and maintains 35 offices in 31 countries. Among its offices are research and development centers employing anti-malware experts in the U.S., Europe, Japan, Israel, China, Russia, and Latin America.

19. Kaspersky Lab was founded in 1997 by Eugene Kaspersky and a small group of his associates. Mr. Kaspersky has been CEO of Kaspersky Lab since 2007.

20. Although the corporate group's global headquarters are in Moscow, approximately 80% of Kaspersky Lab's sales are generated outside of Russia. Kaspersky Lab has successfully investigated and disrupted Arabic-, Chinese-, English-, French-, Korean-, Russian-, and Spanish-speaking threat actors and hacker groups. Kaspersky Lab's presence in Russia and its deployment in areas of the world in which many sophisticated cyberthreats originate, makes it a unique and essential partner in the fight against such threats which, in its absence, may not otherwise be met. Kaspersky Lab researchers have also investigated and

publicly reported on hacker groups alleged to be connected with, or directed by, Russian intelligence services.

21. Kaspersky Lab products have received top ratings for malware detection (among other performance factors). For example, in 2017, Kaspersky Lab products participated in 86 independent tests & reviews—and the company was awarded 72 first places and top-three finishes in 91% of all product tests in 2017. Kaspersky Lab consistently ranks among the world's top four vendors of security solutions for endpoint users.

22. The U.S. has been, and remains, one of the most significant geographic markets in Kaspersky Lab's global business.

23. Plaintiffs have a substantial interest in its ability to conduct federal government business, and for its business partners to do so using Kaspersky Lab code.

II. The NDAA Amendment

24. The NDAA is the U.S. law authorizing appropriations and setting forth policies for the U.S. Department of Defense ("DoD") programs and activities. The law is roughly seven hundred and fifty pages long. No provisions relative to Kaspersky Lab were part of the legislation when introduced in either chamber of Congress.

25. On June 7, 2017, H.R. 2810, the NDAA was first introduced in the U.S. House of Representatives ("House") by Representatives Mac Thornberry and Adam Smith. 163 Cong. Rec. H4700 (2017). The bill was marked up by the House Committee on Armed Services on June 28, 2017, and voted out of committee on that same day. That bill, which was passed by the House on July 14, 2017, also did not contain any provision regarding Kaspersky Lab. 163 Cong. Rec. H5836-68 (2017).

26. On July 10, 2017, Senator John McCain introduced a Senate version of the NDAA for Fiscal Year 2018, S. 1519, which was then considered by the Senate Committee on Armed Services. During the committee markup of the bill, Senator Jeanne Shaheen first introduced an amendment singling out Kaspersky Lab. Her amendment prohibited the DoD from directly or indirectly using Kaspersky Lab "software platforms" and required that any network connection between DoD and such a software platform be "immediately severed." The amendment established an effective date for the section on October 1, 2018. The full text is attached as **Exhibit A**.

27. Upon the approval of H.R. 2810 by the House, the bill was sent to the U.S. Senate for consideration and on July 27, 2017, Senator Shaheen submitted for consideration an amendment to H.R. 2810 consisting of a broader provision related to Kaspersky Lab, Senate Amendment 663, banning the entire federal government from using any product – "hardware," "software," or "services" – from Kaspersky Lab. 163 Cong. Rec. S4053 (2017). The full text is attached as **Exhibit B**.

28. On September 4, 2017, Senator Shaheen authored an editorial for the New York Times, entitled "The Russian Company that is a Danger to Our Security." Her Opinion, attached as **Exhibit C**, stated in part:

> The Kremlin hacked our presidential election, is waging a cyberwar against our NATO allies and is probing opportunities to use similar tactics against democracies worldwide. Why then are federal agencies, local and state governments and millions of Americans unwittingly inviting this threat into their cyber networks and secure spaces?
>
> That threat is posed by antivirus and security software products created by Kaspersky Lab, a Moscow-based company with extensive ties to Russian intelligence. To close this alarming national security vulnerability, I am advancing bipartisan legislation to prohibit the federal government from using Kaspersky Lab software.

Senator Shaheen also stated in her New York Times Opinion that she is seeking a broader, government-wide ban on Kaspersky Lab software:

> The Senate Armed Services Committee in June adopted my measure to prohibit the Department of Defense from using Kaspersky Lab software, to limit fallout from what I fear is already a huge breach of national security data. When broad defense legislation comes before the Senate in the weeks ahead, I hope to amend it to ban Kaspersky software from all of the federal government.

29. On September 13, 2017, a substitute amendment to the House version of the NDAA was offered, Senate Amendment 1003, that included language identical to Senator Shaheen's original Senate amendment. The full text is attached as **Exhibit D**.

30. This substitute amendment was itself later amended to include broader language (banning the entire federal government from using any product – "hardware," "software," or "services" – from Kaspersky Lab) and approved as the engrossed Senate amendment to the House version of the NDAA on September 18, 2017.

31. That same day, September 18, 2017, Senator Shaheen issued a press release which began, "The case against Kaspersky Lab is overwhelming." Her press release, attached as **Exhibit E**, includes the following language:

> The strong ties between Kaspersky Lab and the Kremlin are alarming and well-documented. I'm very pleased that the Senate has acted in a bipartisan way on my amendment that removes a real vulnerability to our national security. I applaud the Trump administration for heeding my call to remove Kaspersky Lab software from all federal computers. It's important that this prohibition also be a part of statute and be expanded to the entire federal government, as my amendment would do. Considering the strong bipartisan, bicameral support for this proposal, I'm optimistic this will soon be signed into law.

32. Then, on October 5, 2017, Senator Shaheen issued a press release that repeated allegations contained in a Wall Street Journal news report that Russian hackers used Kaspersky Lab software installed on a National Security Agency (NSA) contractor's home computer to identify and exfiltrate sensitive malware that was apparently and unlawfully retained there.

33. On October 25, 2017, the House and Senate conference committee began negotiations on the NDAA, and on November 9, 2017, the Conference Report was issued. The November 9, 2017, Conference Report included "an amendment that would add a review and report for removing suspect products or services from the information technology of the Federal Government." More specifically, Section 1634(c) of the NDAA contained a series of review and reporting requirements not specifically targeting Kaspersky Lab. 163 Cong. Rec. H9019 (2017).

34. The November 9, 2017, Conference Report also explained that the provision amending the substitute Senate amendment that was adopted "represented a broader substitute," compared to prior versions that applied to the Department of Defense and to software alone. 163 Cong. Rec. H9027 (2017).

35. On November 14, 2017, the Conference Report, which contained this "broader substitute" was passed by the House, and on November 16, 2017, the Conference Report was passed by the Senate. On December 12, 2017, President Trump signed the NDAA into law.

36. As now enacted as law, Sections 1634(a) and (b) of the NDAA provide:

> SEC. 1634. PROHIBITION ON USE OF PRODUCTS AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB.
>
> (a) PROHIBITION.—No department, agency, organization, or other element of the Federal Government may use, whether directly or through work with or on behalf of another department, agency, organization, or element of the Federal Government, any hardware, software, or services developed or provided, in whole or in part, by—
>
> (1) Kaspersky Lab (or any successor entity);
>
> (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
>
> (3) any entity of which Kaspersky Lab has majority ownership.

> (b) EFFECTIVE DATE.—The prohibition in subsection (a) shall take effect on October 1, 2018.

37. Section 1634(c) of the NDAA, added at the end of the legislative process as explained in the November 9, 2017, Conference Report, in contrast to Sections 1634(a) and (b), is a rule of general applicability. Section 1634(c) provides that the Secretary of Defense shall lead a review of the procedures for removing "suspect" products and services from federal information technology networks, and submit a report to Congress on the authorities that may be used to exclude such products and services from federal networks and the adequacy of the government's relevant monitoring, information sharing, and removal mechanisms. The full text is attached as **Exhibit F**.

III. The NDAA's Ban on Kaspersky Lab is Legislative Punishment

38. Kaspersky Lab has not been convicted of any crimes, subject to any related adverse judicial finding, nor are there any meaningful legislative or other findings indicative of any articulable threat to federal government information systems. In fact, at a November 14, 2017, hearing by the House Science, Space, and Technology Committee's Subcommittee on Oversight, Jeanette Manfra, Assistant Secretary for Cybersecurity and Communications at DHS, testified that *there was no conclusive evidence that Kaspersky Lab had facilitated any breaches* of federal government information systems. When she was asked whether there is concrete evidence that Kaspersky Lab has ties to the Russian government, Manfra testified that she could not make a judgment based off of press reporting. Further, while Senator Shaheen's statements refer to allegations of improper relationships between Kaspersky Lab and the Russian government also contained in uncorroborated media reports, which Plaintiffs have consistently refuted, Congress engaged in no legislative fact-finding to investigate or test the veracity of these claims.

39. Yet Congress nevertheless enacted a legislative and punitive debarment to deprive Kaspersky Lab of its entire direct and indirect federal government business.

40. Congress could have enacted a rule of general applicability concerning cyber-security consistent with legitimate national security policy objectives contemplated by Congress. Indeed, that is exactly what Congress did in Section 1634(c).

41. Notwithstanding the general applicability and effect of Section 1634(c) of the NDAA, however, Congress singled out Kaspersky Lab by name in the preceding two sections and, without having undertaken any legislative fact-finding or analysis, imposed a legislative punishment.

42. The absence from the legislative record of any fact-finding or floor debate, combined with the extra-legislative statements of Senator Shaheen and others, are clearly indicative of the underlying intent to punish Plaintiffs rather than to engage in a constitutionally permissible and legitimate legislative purpose. The NDAA imposes this punishment permanently. In contrast to other provisions within the NDAA, Sections 1634 (a) and (b), as noted above, contain no "sunset" provision.

43. Congress imposed the broadest possible ban against Kaspersky Lab. Although Senator Shaheen stated in her September 4, 2017, New York Times Op-Ed that she was advancing "legislation to prohibit the federal government from using Kaspersky Lab software"—and the September 18, 2017, press release was to the same effect—the NDAA, as enacted, bans "hardware, software, [and] services." In other words, it bans every Kaspersky Lab product and service, whether offered directly by the company or embedded into third-party products, whether now existing or developed at any time in the future, and whether or not doing

so would advance any legitimate national security purpose with respect to that product or service.

44. The sheer breadth of the ban and the availability of less burdensome alternatives are also indicative of a legislative intent to punish Kaspersky Lab.

INJURY AND STANDING

45. Plaintiff Kaspersky Lab, Inc. has standing to bring this suit. The company and its customers and business partners have sold its products to the U.S. government, and the NDAA now bans them all from doing so. The consequences involve profound reputational injuries, a substantial loss of sales, and great financial harm. This harm has been immediate and is ongoing.

46. Plaintiff Kaspersky Labs Limited also has standing. As the U.K. parent, Kaspersky Labs Limited suffers financial harm due to its wholly-owned subsidiary's loss of sales, and direct reputational injury, resulting from the NDAA. Kaspersky Labs Limited is also injured by the NDAA's preclusive effect.

CAUSE OF ACTION

(Bill of Attainder)

47. Plaintiffs incorporate by reference, as if fully restated herein, paragraphs 1-45 above.

48. Article I, § 9, c1.3 of the Constitution states: "No bill of attainder or ex post facto law shall be passed."

49. Sections 1634 (a) and (b) of the NDAA have a sole target, Kaspersky Lab, identified by name, rather than by objective or generalized criteria. The NDAA deprives Kaspersky Lab of its entire direct and indirect federal government business, yet provides no

mechanism for the company to ever extricate itself from the ban. The ban is permanent. Kaspersky Lab has never been convicted of any crime, nor subjected to any related adverse judicial finding.

50. This legislative act is an unconstitutional Bill of Attainder.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that a judgment be granted:

(a) Declaring Sections 1634 (a) and (b) of the NDAA unconstitutional;

(b) Preliminarily and permanently invalidating Sections 1634 (a) and (b) of the NDAA; and

(c) Granting such other relief as the Court deems just and proper.

Dated: February 12, 2018

Respectfully submitted,

/s/ Ryan P. Fayhee
Ryan P. Fayhee (Bar No. 1033852)
Steven Chasin (Bar No. 495853)
Baker & McKenzie LLP
815 Connecticut Avenue NW
Washington D.C. 20006
Tel: (202) 452 7024
Fax: (202) 416 7024
Ryan.Fayhee@bakermckenzie.com
Steven.Chasin@bakermckenzie.com

Attorneys for Kaspersky Lab, Inc. and Kaspersky Labs Limited