RUSS, AUGUST & KABAT
Marc A. Fenster, SBN 181067
mfenster@raklaw.com
Ben Wang, SBN 228712
bwang@raklaw.com
12424 Wilshire Boulevard
Twelfth Floor
Los Angeles, California 90025
Telephone: (310) 826-7474
Facsimile: (310) 826-6991

Attorneys for Plaintiff
SPEX TECHNOLOGIES, INC.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

SPEX TECHNOLOGIES, INC.,

Plaintiff,

v.

APRICORN,

Defendant.

Case No. 8:16-cv-01803

COMPLAINT FOR PATENT INFRINGEMENT

JURY TRIAL DEMANDED

1. Plaintiff SPEX Technologies, Inc. ("SPEX" or "Plaintiff"), for its Complaint against Defendant Apricorn ("Defendant"), hereby alleges as follows:

PARTIES

2. SPEX is a California corporation with its headquarters at 1860 Hartog Dr., San Jose, CA 95131.

3. On information and belief, Apricorn is a California corporation with its headquarters at 12191 Kirkham Rd., Poway, CA 92064.

NATURE OF THE ACTION

4. This is a civil action for the infringement of United States Patent No. 6,088,802 (the "'802 patent") (attached as Exhibit A) and United States Patent No. 6,003,135 (the "'135 patent") (attached as Exhibit B) (collectively, the "Patents-in-Suit") under the patent laws of the United States, 35 U.S.C. § 1, et seq.

5. This action involves Defendant's manufacture, use, sale, offer for sale, and/or importation into the United States of infringing products, methods, processes, services and systems that are hardware encrypting memory products that infringe one or more of the claims of the Patents-in-Suit.

JURISDICTION AND VENUE

6. This Court has original jurisdiction over the subject matter of this Complaint under 28 U.S.C. §§ 1331 and 1338(a) because this action arises under the patent laws of the United States, including 35 U.S.C. §§ 271, et seq.

7. Defendant is subject to personal jurisdiction in this judicial district because Defendant regularly transacts business in this judicial district by, among other things, offering Defendant's products and services to customers, business affiliates and/or partners located in this judicial district. In addition, Defendant has committed acts of direct infringement of one or more of the claims of one or more of the Patents-in-Suit in this judicial district.

8. Venue in this district is proper under 28 U.S.C. §§ 1400(b) and 1391(b) and (c), because Defendant is subject to personal jurisdiction in this district and has committed acts of infringement in this district.

FACTUAL BACKGROUND

9. The Patents-in-Suit were originally assigned to Spyrus, Inc. ("Spyrus"). SPEX acquired full rights to the Patents-in-Suit from Spyrus.

SPYRUS IS A PIONEERING ENCRYPTION COMPANY THAT HAS DEVELOPED CRYPTOGRAPHIC PRODUCTS RELIED ON TO SECURE SENSITIVE INFORMATION

10. Spyrus was founded around October 1992 by two pioneering women. The founding concept of Spyrus was to make cryptography more affordable and usable for distributing and accessing electronic content.

11. Instead of building up the company with venture capital money, Spyrus initially built itself up using small capital investments from friends and family. Spyrus' first major achievement was to propose and win a contract with the Department of Defense ("DoD") to design a specification for a hardware security module ("HSM") to be used for encrypting sensitive communications. In 1993, Spyrus released the LYNKS HSM based on an ARM processor.

12. In approximately 1993 or 1994, in partnership with Mykotronx, Spyrus released the successor to the LYNKS HSM, the Fortezza Crypto Card, originally named the Tessera Crypto Card. *See, e.g.*, https://en.wikipedia.org/wiki/Fortezza. The Fortezza Crypto Card and its successor versions were capable of protecting sensitive data, including classified data. The Fortezza Crypto Card was used in a number of government and military applications.

13. Around 1996 or 1997, Spyrus began expanding on the cryptographic technology embodied in the LYNKS HSM and Fortezza Crypto Card technologies. In particular, Spyrus developed its Hydra series of products, which added capabilities such as flash memory or modem functionalities to the family of LYNKS

HSM and Fortezza Crypto Card technologies. Spyrus' initial Hydra products were released around 1997. Spyrus' Hydra-based products are still sold today. Spyrus' Hydra-based products include the PocketVault P-3X, PocketVault P-384, PocketVault P-384E, Worksafe, Worksafe Pro and Secure Portable Workplace.

14. Spyrus' Hydra-based products have won awards and have been consistently praised. *See, e.g.*, http://www.pcmag.com/article2/0,2817,2478715,00.asp (editor rating of "Excellent" for the Worksafe Pro); http://www.pcmag.com/article2/0,2817,2478716,00.asp (editor rating of "excellent" for the Worksafe); http://www.thessdreview.com/our-reviews/spyrus-worksafe-pro-wtg-secure-flash-drive-review-worlds-secure-flash-drive/3/ (Worksafe Pro was given an "Editor's Choice" award; called the "worlds most secure flash drive"); http://www.spyrus.com/spyrus-named-winner-in-2011-golden-bridge-awards-for-virtual-office-technology/ (Secure Pocket Drive named the winner in the Virtual Office Technology category of the 3rd Annual 2011 Golden Bridge Awards as well as the Security Products Guide's Tomorrow's Technology Today award and the GSN Homeland Security award); http://www.darkreading.com/risk/nsa-approves-spyrus-hyrda-pc-for-protection-of-classified-government-data/d/d-id/1132286?print=yes (Hydra Privacy Card Series II was first commercial-off-the-shelf device approved by the DoD to protect confidential information at SECRET level and below); http://www.businesswire.com/news/home/20060612005367/en/Info-Security-Products-Guide-Names-SPYRUS-Hydra (Hydra Privacy Card Series II won 2006 Global Excellence in Secure and Removable Mass Storage Device Award from Info Security Products Guide); http://www.scmagazine.com/spyrus-hydra-privacy-card-series-ii/review/1087/ (very positive review of Hydra Privacy Card Series II; "If you deal with sensitive data, especially on laptops, you need the Hydra").

15. The Patents-in-Suit, and Spyrus' technology, have been licensed in the past by Kingston Digital, Inc. and PNY Technologies, Inc.

16. SPEX was formed to facilitate licensing of the technology developed and practiced by Spyrus in both domestic and foreign markets.

THE PATENTS-IN-SUIT

17. SPEX is the owner by assignment of the Patents-in-Suit. SPEX owns all rights to the Patents-in-Suit, including the right to enforce the Patents-in-Suit.

18. United States Patent No. 6,088,802, entitled "Peripheral Device With Integrated Security Functionality," issued on July 11, 2000 from United States Patent Application No. 08/869,305 filed on June 4, 1997. A true and correct copy of the '802 patent is attached as Exhibit A.

19. United States Patent No. 6,003,135, entitled "Modular Security Device," issued on December 14, 1999 from United States Patent Application No. 08/869,120 filed on June 4, 1997. A true and correct copy of the '135 patent is attached as Exhibit B.

20. All maintenance fees for the Patents-in-Suit have been timely paid, and there are no fees currently due.

COUNT I

(DEFENDANT'S INFRINGEMENT OF THE '802 PATENT)

21. Paragraphs 1 through 20 are incorporated by reference as if fully restated herein.

22. United States Patent No. 6,088,802, entitled "Peripheral Device With Integrated Security Functionality," issued on July 11, 2000 from United States Patent Application No. 08/869,305 filed on June 4, 1997. A true and correct copy of the '802 patent is attached as Exhibit A.

23. On information and belief, Defendant has made, used, offered for sale, sold and/or imported into the United States products that infringe various claims of the '802 patent, and continues to do so. By way of illustrative example, these infringing products include, without limitation, Defendant's hardware encrypting storage solutions, including but not limited to Defendant's Aegis Secure Key, Aegis

Secure Key 3.0, Aegis Padlock SSD USB 3.0 SSD, Aegis Padlock USB 3.0, Aegis Padlock USB 3 SSD, Aegis Padlock Fortress USB 3.0 SSD, Aegis Padlock DT FIPS USB 3.0 Desktop Drive, Aegis Padlock DT USB 3.0 Desktop Drive, Aegis Bio USB 3.0 and Aegis Bio 3.0 SSD.

24. Defendant has been and now is directly infringing one or more claims of the '802 patent under 35 U.S.C. §271(a), in this judicial District and elsewhere in the United States, by, among other things, making, using, selling, offering to sell and/or importing into the United States for subsequent sale or use hardware encrypting storage solutions that include, for example, (a) a cryptographic processor for performing security operations on data; (b) mass storage memory, such as flash or magnetic storage; (c) an interface between the cryptographic processor and the mass storage memory; (d) an interface with the host computer (*e.g.*, a USB or SATA interface); and (e) a mediating interface that ensures that data communicated between the host computer and mass storage memory passes through the cryptographic processor. An exemplary chart showing how Defendant infringes the '802 patent is attached as Exhibit C.[1] Exhibit C is based on the public information available to Plaintiff, and Plaintiff reserves the right to amend Exhibit C based on information obtained through discovery. Accordingly, the aforementioned products infringe the '802 patent literally and/or under the doctrine of equivalents.

25. Defendant actively, knowingly, and intentionally induces, and continues to actively, knowingly, and intentionally induce, infringement of the '802 patent under 35 U.S.C. §271(b) by its customers and end users.

26. Defendant has had knowledge of and notice of the '802 patent and its infringement since at least the filing of this complaint.

[1] Plaintiff reserves the right to assert additional claims of the '802 patent against Defendant as the litigation proceeds. For example, Plaintiff expressly reserves the right to assert additional claims in its infringement contentions to be served during the discovery process.

27. Defendant has induced its customers and end users to infringe the '802 patent by using hardware encrypting storage solutions to (a) communicate with a host computer to exchange data with the hardware encrypting storage solution; (b) perform security operations on the data; (c) store or retrieve the data; and (d) mediate communications so that data must first pass through the hardware encrypting processor. *See, e.g.*, Ex. C. For example, Defendant encourages its customers and end users to perform infringing methods by the very nature of the products. When using the infringing products, security operations are performed on all data passed between Defendant's infringing products and the customer's or end user's computer.

28. Defendant specifically intends its customers and/or end users infringe the '802 patent, either literally or by the doctrine of equivalents, because Defendant has known about the '802 patent and how Defendant's products infringe the claims of the '802 patent but Defendant has not taken steps to prevent infringement by its customers and/or end users. Accordingly, Defendant has acted with the specific intent to induce infringement of the '802 patent.

29. Accordingly, Defendant has induced, and continues to induce, infringement of the '802 patent under 35 U.S.C. §271(b).

30. Defendant has been and continues to infringe one or more of the claims of the '802 patent through the aforesaid acts.

31. Defendant has committed these acts of infringement without license or authorization.

32. Plaintiff is entitled to recover damages adequate to compensate for the infringement.

COUNT II

(DEFENDANT'S INFRINGEMENT OF THE '135 PATENT)

33. Paragraphs 1 through 20 are incorporated by reference as if fully restated herein.

34. United States Patent No. 6,003,135, entitled "Modular Security Device," issued on December 14, 1999 from United States Patent Application No. 08/869,120 filed on June 4, 1997. A true and correct copy of the '135 patent is attached as Exhibit B.

35. On information and belief, Defendant has made, used, offered for sale, sold and/or imported into the United States products that infringe various claims of the '135 patent, and continues to do so. By way of illustrative example, these infringing products include, without limitation, Defendant's hardware encrypting storage solutions, including but not limited to Defendant's hardware encrypting storage solutions, including but not limited to Defendant's Aegis Secure Key, Aegis Secure Key 3.0, Aegis Padlock SSD USB 3.0 SSD, Aegis Padlock USB 3.0, Aegis Padlock USB 3 SSD, Aegis Padlock Fortress USB 3.0 SSD, Aegis Padlock DT FIPS USB 3.0 Desktop Drive, Aegis Padlock DT USB 3.0 Desktop Drive, Aegis Bio USB 3.0 and Aegis Bio 3.0 SSD.

36. Defendant has been and now is directly infringing one or more claims of the '135 patent under 35 U.S.C. §271(a), in this judicial District and elsewhere in the United States, by, among other things, making, using, selling, offering to sell and/or importing into the United States for subsequent sale or use hardware encrypting storage solutions that include, for example, (a) a security portion including (i) a cryptographic processor for performing security operations on data; and (ii) an interface to the memory portion; (b) a memory portion including (i) mass storage memory, such as flash or magnetic storage; and (ii) an interface to the security portion; (c) an interface with the host computer (*e.g.*, a USB or SATA interface); and (d) a means for operably connecting the security module and/or the target module to the host computing device in response to an instruction from the host computing device. An exemplary chart showing how Defendant infringes the

'135 patent is attached as Exhibit D.[2] Exhibit D are based on the public information available to Plaintiff, and Plaintiff reserves the right to amend Exhibit D based on information obtained through discovery. Accordingly, the aforementioned products infringe the '135 patent literally and/or under the doctrine of equivalents.

37. Defendant actively, knowingly, and intentionally induces, and continues to actively, knowingly, and intentionally induce, infringement of the '135 patent under 35 U.S.C. §271(b) by its customers and end users.

38. Defendant has had knowledge of and notice of the '135 patent and its infringement since at least the filing of this complaint.

39. Defendant has induced its customers and end users to infringe the '135 patent by using hardware encrypting storage solutions to (a) communicate with a host computer to exchange data with the hardware encrypting storage solution; (b) perform security operations on the data; (c) mediate communications so that data must first pass through the hardware encrypting processor; and (d) operably connect the hardware encrypting storage solution in to the host computer in response to an instruction from the host computer. *See, e.g.*, Ex. D. For example, Defendant encourages its customers and end users to perform infringing methods by the very nature of the products. When using the infringing products, security operations are performed on all data passed between Defendant's infringing products and the customer's or end user's computer.

40. Defendant specifically intends its customers and/or end users infringe the '135 patent, either literally or by the doctrine of equivalents, because Defendant has known about the '135 patent and how Defendant's products infringe the claims of the '135 patent but Defendant has not taken steps to prevent infringement by its

[2] Plaintiff reserves the right to assert additional claims of the '135 patent against Defendant as the litigation proceeds. For example, Plaintiff expressly reserves the right to assert additional claims in its infringement contentions to be served during the discovery process.

customers and/or end users. Accordingly, Defendant has acted with the specific intent to induce infringement of the '135 patent.

41. Accordingly, Defendant has induced, and continues to induce, infringement of the '135 patent under 35 U.S.C. §271(b).

42. Defendant has been and continue to infringe one or more of the claims of the '135 patent through the aforesaid acts.

43. Defendant has committed these acts of infringement without license or authorization.

44. Plaintiff is entitled to recover damages adequate to compensate for the infringement.

PRAYER FOR RELIEF

Wherefore, SPEX Technologies, Inc., respectfully requests the following relief:

a) A judgment that Defendant has infringed the '802 patent;

b) A judgment that Defendant has infringed the '135 patent;

c) A judgment that awards Plaintiff all appropriate damages under 35 U.S.C. § 284 for Defendant's past infringement, and any continuing or future infringement of the Patents-in-Suit, up until the date such judgment is entered, including interest, costs, and disbursements as justified under 35 U.S.C. § 284 and, if necessary, to adequately compensate Plaintiff for Defendant's infringement;

d) An adjudication that this case is exceptional within the meaning of 35 U.S.C. § 285;

e) An adjudication that Plaintiff be awarded the attorneys' fees, costs, and expenses it incurs in prosecuting this action; and

f) An adjudication that Plaintiff be awarded such further relief at law or in equity as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury of all issues so triable.

Respectfully submitted,

DATED: September 28, 2016

RUSS, AUGUST & KABAT

/s/ Marc A. Fenster

Marc A. Fenster, SBN 181067
Ben Wang, SBN 228712
12424 Wilshire Boulevard
Twelfth Floor
Los Angeles, California 90025
Telephone: (310) 826-7474
Facsimile: (310) 826-6991

Attorneys for Plaintiff
SPEX Technologies, Inc.