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.

KINGSTON TECHNOLOGY CORPORATION, KINGSTON DIGITAL, INC., KINGSTON TECHNOLOGY COMPANY, INC., IMATION CORPORATION, DATALOCKER INC., DATA LOCKER INTERNATIONAL, LLC

Defendants.

Case No. 8:16-cv-01790

COMPLAINT FOR PATENT INFRINGEMENT

JURY TRIAL DEMANDED

1. Plaintiff SPEX Technologies, Inc. ("SPEX" or "Plaintiff"), for its Complaint against Defendants Kingston Technology Corporation, Kingston Digital, Inc., Kingston Technology Company, Inc., Imation Corporation, DataLocker Inc. and Data Locker International, LLC (collectively, "Defendants"), 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, Kingston Technology Corporation is a California corporation with its headquarters at 17600 Newhope St., Fountain Valley, California 92708.

4. On information and belief, Kingston Digital, Inc. ("Kingston Digital") is a Delaware corporation with its headquarters at 17600 Newhope St., Fountain Valley, California 92708.

5. On information and belief, Kingston Technology Company, Inc. is a Delaware corporation with its headquarters at 17600 Newhope St., Fountain Valley, California 92708.

6. Kingston Technology Corporation, Kingston Digital, Inc. and Kingston Technology Company, Inc. are referred to together as "Kingston."

7. On information and belief, Imation Corporation ("Imation") is a Delaware corporation with its headquarters at 1 Imation way, Oakdale, Minnesota 55128.

8. On information and belief, DataLocker Inc. is a Kansas corporation with its headquarters at 7007 College Blvd., Suite 240, Overland Park, Kansas 66211.

9. On information and belief, Data Locker International, LLC is a Delaware corporation with its headquarters at 7007 College Blvd., Suite 240, Overland Park, Kansas 66211.

10. DataLocker Inc. and Data Locker International, LLC are referred to together as "DataLocker."

NATURE OF THE ACTION

11. 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.

12. This action involves Defendants' 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

13. 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.

14. Defendants are subject to personal jurisdiction in this judicial district because Defendants regularly transact business in this judicial district by, among other things, offering Defendants' products and services to customers, business affiliates and partners located in this judicial district. In addition, Defendants have 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.

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

16. On information and belief, joinder is appropriate because a portion of Plaintiff's right to relief is based on the making, using, importing, offering for sale and selling of IronKey-branded products. The IronKey brand was owned by Imation until February 2016, when it was acquired by Kingston and DataLocker. *See, e.g.*,

https://www.kingston.com/us/company/press/article/40465 (Imation sold the USB IronKey assets to Kingston Digital and the IronKey hard drive assets to DataLocker). The parties were therefore involved in the same transaction upon which at least a portion of Plaintiff's claims are based.

FACTUAL BACKGROUND

17. 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 ALL TYPES OF SENSITIVE INFORMATION

18. 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.

19. 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.

20. 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 and applications.

21. 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' current Hydra-based products include the PocketVault P-3X, PocketVault P-384, PocketVault P-384E, Worksafe, Worksafe Pro and Secure Portable Workplace.

22. 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").

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

IMATION DISCUSSED A RELATIONSHIP WITH SPYRUS PRIOR TO ACQUIRING IRONKEY

24. In approximately September 2011, Imation purchased the hardware assets of IronKey, Inc. ("IronKey"). http://www.computerworld.com/article/2511295/data-center/imation-buys-ironkey-s-hardware-assets.html.

25. Prior to acquiring the assets from IronKey, Imation was in discussions with Spyrus regarding Spyrus and its technology.

26. On March 9, 2010, Spyrus and Imation entered into a Confidential Disclosure Agreement.

27. Spyrus and Imation had multiple meetings during 2010 and 2011 to discuss a potential business relationship between Spyrus and Imation. Topics discussed included synergies between Spyrus' technology and patents, and Imation's products.

28. In April 2010, high-level executives of Spyrus and Imation met for an in-person meeting at Imation's headquarters in Minneapolis, Minnesota to discuss Imation's possible acquisition of Spyrus. The executives from Imation that attended the meeting included Dr. Subodh Kukarni (Chief Technology Officer and Vice President Global Commercial Business), Mark LeClair (Executive Directory Manufacturing Operations, Research, Development & Engineering) and Stephen Bradley (Director Strategic Growth Programs). During this meeting, among other things, Spyrus discussed its intellectual property, including the Patents-in-Suit, its other patents and its core technologies.

29. On August 30th, 2010, Spyrus met again with Imation to continue the discussion of Imation's possible acquisition of Spyrus. Attendees included Mr.

Bradley and Jim Ellis (Vice President M&A and Strategy). The topics discussed were similar to those discussed in the April 2010 meeting.

30. The discussions came to a permanent halt after Imation acquired IronKey and MXI Security (http://www.storagenewsletter.com/rubriques/security/imation-acquires-assets-mxi-security/).

KINGSTON ENTERED INTO A PARTNERSHIP WITH SPYRUS AND THEN IMPROPERLY USED SPYRUS' CONFIDENTIAL INFORMATION BY DISCLOSING IT TO A THIRD PARTY IN ORDER TO COMPETE WITH SPYRUS

DataTraveler 5000 and DataTraveler 6000

31. On March 14, 2008, Spyrus and Kingston entered into a mutual Non-Disclosure Agreement ("NDA"). A copy of the NDA is attached as Exhibit C to this complaint. The NDA prohibited unauthorized disclosure of confidential information and limited the use of confidential information to "discuss opportunities for joint business partnerships including integration of SPYRUS components and Kingston components into products…and joint development of products and strategies." Ex. C at ¶¶ 1, 2.

32. The purpose of the NDA was to allow Spyrus and Kingston to explore a potential partnership to develop a next generation version of Kingston's DataTraveler Black Box product. Among the topics discussed after the NDA was executed were synergies between Spyrus' technology and Kingston's business needs as well as Spyrus' patent portfolio, including the Patents-in-Suit.

33. The discussions were successful and, on April 14, 2009, Spyrus and Kingston entered into a Technology License and executed the first Licensed Product Appendix. Paragraph 11 of the Technology License extended the terms of the NDA to cover the disclosure of the confidential information during the new joint development relationship: "The obligations regarding confidentiality shall be

governed by the Mutual Confidentiality Agreement between the parties effective May 14, 2008."[1]

34. Paragraph 20.1 of the Technology License included a choice of law and venue clause agreeing to "personal and exclusive jurisdiction of and venue in the federal and state courts located in Orange County, California."

35. The first Licensed Product Appendix was for the development of the Kingston DataTraveler Black Box Gen. 2. The Licensed Product Appendix licensed certain Spyrus patents, including the '802 patent, for the manufacture and sale of the DataTraveler Black Box Gen. 2.

36. The DataTraveler Black Box Gen. 2 was to be the same size and form factor of the DataTraveler Black Box. To accomplish this goal, Spyrus shrank its existing Hydra technology to fit inside the Black Box case. The new technology was awarded FIPS 140-2 Level 2 certification.

37. The Black Box Gen. 2 was renamed the DataTraveler 5000 and was released by Kingston in January 2010. The DataTraveler 5000 was a Kingston case and memory card combined with Spyrus' new smaller Hydra cryptographic technology. The DataTraveler 5000 was awarded FIPS 140-2 Level 2 certification by reusing Spyrus' FIPS 140-2 certification for the Hydra technology. The DataTraveler 5000 became Kingston's first FIPS 140-2-certified product offering in the market.

38. Federal Information Process Standards ("FIPS") are standards and guidelines developed by the National Institute of Standards and Technology ("NIST") for use in federal computer systems. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. FIPS 140-2 details the security requirements for cryptographic modules to be used in federal computer

[1] The Technology License is marked confidential information and therefore cannot be attached to the Complaint.

systems. *Id.* There are four levels of FIPS 140-2, with level 4 including the most stringent security. *Id.*

39. Spyrus also developed the DataTraveler 6000, which was released by Kingston in September 2011. Like the DataTraveler 5000, the DataTraveler 6000 was a Kingston case and memory card combined with Spyrus' new smaller Hydra cryptographic technology that had been certified to FIPS 140-2 Level 3. The DataTraveler 6000 was awarded FIPS 140-2 Level 3 certification by reusing the Spyrus FIPS 140-2 certification and became Kingston's first FIPS 140-2 Level 3-certified product offering.

40. On January 21, 2015, Kingston simultaneously informed Spyrus of its intent to release the DataTraveler 4000 G2, which had recently achieved FIPS 140-2 Level 3 certification, as well as its intent to cease supporting the DataTraveler 6000.

41. As a result of Kingston ceasing its support of the DataTraveler 6000, Spyrus sent a letter terminating the Technology License on January 21, 2015. The Technology License with Kingston terminated on April 21, 2015.

Kingston Used Its Partnership With Spyrus As A Pretext To Improperly Receive And Use Spyrus' Confidential Information

42. While Spyrus was fully dedicated to the partnership, Kingston was not. On information and belief, Kingston used the partnership with Spyrus to learn Spyrus' confidential information in order to develop its own competing technology in partnership with a Taiwanese company, Phison Electronics Corp. ("Phison").

43. Between about November 2008 and April 2010, at Kingston's request, Spyrus shared highly confidential and proprietary technical information with Kingston. While some of the less detailed confidential information was needed for marketing purposes, Kingston did not need the detailed information it requested to perform its obligations under the Technology License. Rather, Kingston claimed it

needed Spyrus' highly confidential and proprietary technical information to confirm that Spyrus' cryptographic protections were as strong as Spyrus claimed.

44. The highly confidential and proprietary information requested by Kingston comprised Spyrus' competitive advantage in the marketplace, such as Spyrus' proprietary method for encryption key unwrapping and asymmetric cryptography techniques. Spyrus did not share its information lightly. Spyrus, however, shared its information in an effort to solidify its partnership with Kingston.

45. In or around September 15, 2009, for example, Spyrus engineers and Jason Chen of Kingston had technical discussions regarding Spyrus' proprietary password implementation. On the same day, Burt Tregub, Spyrus' Vice President Corporate Development, emailed and spoke with Jason Chen to confirm the confidentiality of the shared information. Jason Chen confirmed this understanding.

46. At Kingston's request, confidential information in greater detail was discussed during a meeting on December 11, 2009 with Kingston's Technical Resource Group ("TRG"), including Jason Chen, at Kingston's headquarters in Fountain Valley, California. Kingston specifically requested, and received, the written materials used in the December 11 presentation. The written materials were marked with confidentiality designations.

47. On January 11, 2010, Jason Chen called Spyrus' Duane Linsenbardt seeking further detailed, highly confidential information about Spyrus' technology. When Mr. Linsenbardt informed Jason Chen that he was in the car and asked Jason Chen to follow-up via email, Jason Chen responded that an email was not possible because Ben Chen (of Kingston) was in Taiwan and needed the information that night.

48. Spyrus was not aware that Ben Chen, Director of Flash Engineering at Kingston, had a need to receive, let alone received, Spyrus' highly confidential and proprietary information while working in Taiwan. Until the January 11 call, Spyrus was only aware of Ben Chen's receipt of high-level information about Spyrus

technology. Learning that Ben Chen had received Spyrus' confidential information was particularly concerning because Spyrus was aware that Ben Chen was working on a project with Phison, who was and continues to be one of Spyrus' competitors. Further, Spyrus did not have an export license for its Technical Data or the Spyrus manufacturing tools.

49. The January 11, 2010 call was also the first time that Spyrus learned that its confidential information was being shared and discussed outside of the United States. As cryptographic information, the information is export controlled and Spyrus did not have a license to export the Technical Data outside of the United States, including to Taiwan.

50. Until Jason Chen's call, Spyrus believed that Kingston was complying with Spyrus' requirement that its proprietary, confidential information only be shared with necessary engineers in Kingston's Fountain Valley, California headquarters.

51. On the day after Jason Chen's call, on January 12, 2010, Burt Tregub wrote a letter to John Terpening, Manager of Flash Engineering at Kingston, expressing Spyrus' concerns. The letter set out the relevant facts, including those above, and asked for confirmation that Spyrus' proprietary and confidential information had not been shared with third parties or people outside of the United States.

52. More than a month later, on February 18, 2010, Calvin Leong, Director Legal Department at Kingston, responded to the January 12, 2010 letter. Mr. Leong indicated that Spyrus' confidential information had not been shared with any third party, including Phison, without Spyrus' knowledge. Mr. Leong further indicated that, as Jason Chen's boss, Ben Chen had the authority to access information about projects under development, including the DataTraveler 5000.

53. Spyrus believed Kingston's assurances and continued working with Kingston.

54. In October 2010, Kingston and Phison announced the formation of a joint venture focusing on embedded memory system product development. http://www.phison.com/English/NewsView.asp?ID=199&SortID=35.

55. On February 22, 2011, Kingston announced the release of the DataTraveler 4000, which was an encrypting flash drive, like the DataTraveler 5000. Kingston did not have permission to use Spyrus' patented technology in the DataTraveler 4000. On information and belief, the DataTraveler 4000 was developed as part of the joint venture between Kingston and Phison.

56. While Spyrus was not pleased by Kingston's release of the DataTraveler 4000, in light of Kingston's February 2010 representation, the weaker security protections on the DataTraveler 4000 and Kingston's intent to focus on sales of the DataTraveler 6000 with FIPS 140-2 Level 3 certification for higher security requirements, Spyrus had no reason to believe at the time that the DataTraveler 4000 was developed by Kingston and Phison using Spyrus' highly confidential and proprietary information.

57. In January 2015, Spyrus' belief changed. On January 21, 2015, Andrew Ewing, Kingston's manager of encrypted drives, informed Burt Tregub of the impending release of the DataTraveler 4000 G2 and that Kingston would no longer support the DataTraveler 6000. Unlike the original DataTraveler 4000, the DataTraveler 4000 G2 contained significantly upgraded security features consistent with Spyrus' proprietary and confidential information shared with Kingston and had been certified to FIPS 140-2 Level 3. Like the DataTraveler 4000, the DataTraveler 4000 G2 uses Phison technology.

58. On information and belief, despite Kingston's February 2010 representation to the contrary, Kingston disclosed Spyrus' highly confidential and proprietary information to Phison to assist in the development of the hardware encrypting chips by Phison. The cryptographic feature set of the DataTraveler 4000

G2 makes it clear that the technology was developed using Spyrus' highly confidential and proprietary information.

THE PATENTS-IN-SUIT

59. 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.

60. 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.

61. 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.

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

COUNT I

(KINGSTON'S INFRINGEMENT OF THE '802 PATENT)

63. Paragraphs 1 through 62 are incorporated by reference as if fully restated herein.

64. On information and belief, Kingston 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, Kingston's hardware encrypting storage solutions, including but not limited to the DataTraveler 4000, DataTraveler 4000 G2, DataTraveler Vault Privacy 3.0, DataTraveler 2000, IronKey D80, IronKey Enterprise S1000, IronKey Enterprise S250, IronKey Enterprise D250, IronKey F150, IronKey F100, IronKey Basic S1000, IronKey Basic S250, IronKey Basic D250, IronKey F200, IronKey Personal S250, IronKey D250, IronKey

Workspace W700, IronKey Workspace W500, IronKey Workspace W300, IronKey Workspace W200, IronKey Workspace W700SC, MXI M200, MXI M500, MXI M500 and MXP Bio.

65. Kingston 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. Exemplary charts showing how Kingston infringes the '802 patent are attached as Exhibits D and E.[2] Exhibits D and E are based on the public information available to Plaintiff, and Plaintiff reserves the right to amend Exhibits D and E based on information obtained through discovery. Accordingly, the aforementioned products infringe the '802 patent literally and/or under the doctrine of equivalents.

66. Kingston 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.

67. Kingston has had knowledge of and notice of the '802 patent and its infringement. For example, Kingston licensed the '802 patent from 2009 to 2015 to

[2] Plaintiff reserves the right to assert additional claims of the '802 patent against Kingston 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.

produce and sell the DataTraveler 5000 and 6000. Kingston is aware of the scope of the '802 patent and its application to Kingston's products.

68. Kingston 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.*, Exs. D, E. For example, Kingston 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 Kingston's infringing products and the customer's or end user's computer.

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

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

71. As discussed above, Kingston has had knowledge of and notice of the '802 patent since at least April 2009, when it entered into the Technology License with Spyrus. Kingston was well aware of the scope of the '802 patent and agreed to mark the DataTraveler 5000 and 6000 with the '802 patent. Kingston is aware of the scope of the '802 patent and its application to Kingston's products. Furthermore, on information and belief, Kingston knowingly and intentionally used Spyrus' highly confidential and proprietary information to develop at least the DataTraveler 4000 and 4000 G2. Kingston, at the very least, should be aware of its infringing actions.

Despite this knowledge, Kingston continues to commit tortious conduct by way of patent infringement.

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

73. Kingston has committed these acts of infringement without license or authorization.

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

75. Kingston has and continues to infringe the '802 patent, acting with an objectively high likelihood that its actions constitute infringement of the '802 patent. Kingston has known or should have known of this risk at least as early as 2009. Accordingly, Kingston's infringement of the '802 patent has been and continues to be willful.

COUNT II

(KINGSTON'S INFRINGEMENT OF THE '135 PATENT)

76. Paragraphs 1 through 62 are incorporated by reference as if fully restated herein.

77. On information and belief, Kingston 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, Kingston's hardware encrypting storage solutions, including but not limited to the DataTraveler 4000, DataTraveler 4000 G2, DataTraveler Vault Privacy 3.0, DataTraveler Vault Privacy, DataTraveler 2000, IronKey D80, IronKey Enterprise S1000, IronKey Enterprise S250, IronKey Enterprise D250, IronKey F150, IronKey F100, IronKey Basic S1000, IronKey Basic S250, IronKey Basic D250, IronKey F200, IronKey Personal S250, IronKey D250, IronKey Workspace W700, IronKey Workspace W500, IronKey Workspace

W300, IronKey Workspace W200, IronKey Workspace W700SC, MXI M200, MXI M500, MXI M500 and MXP Bio.

78. Kingston 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. Exemplary charts showing how Kingston infringes the '135 patent are attached as Exhibits F and G.[3] Exhibits F and G are based on the public information available to Plaintiff, and Plaintiff reserves the right to amend Exhibits F and G based on information obtained through discovery. Accordingly, the aforementioned products infringe the '135 patent literally and/or under the doctrine of equivalents.

79. Kingston 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.

80. Kingston has had knowledge of and notice of the '135 patent and its infringement since at least 2009, when Kingston entered into the Technology License with Spyrus. As a result of the Technology License and discussions leading

[3] Plaintiff reserves the right to assert additional claims of the '135 patent against Kingston 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.

to the technology license, Kingston was familiar with the '135 patent and its scope. Kingston is aware of the scope of the '135 patent and its application to Kingston's products.

81. Kingston 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.*, Exs. F, G. For example, Kingston 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 Kingston's infringing products and the customer's or end user's computer.

82. Kingston specifically intends its customers and/or end users infringe the '135 patent, either literally or by the doctrine of equivalents, because Kingston has known about the '135 patent and how Kingston's products infringe the claims of the '135 patent but Kingston has not taken steps to prevent infringement by its customers and/or end users. Accordingly, Kingston has acted with the specific intent to induce infringement of the '135 patent.

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

84. As discussed above, Kingston has had knowledge of and notice of the '135 patent since at least April 2009, when it entered into the Technology License with Spyrus. Kingston is aware of the scope of the '135 patent and its application to Kingston's products. Furthermore, on information and belief, Kingston knowingly and intentionally used Spyrus' highly confidential and proprietary information to develop at least the DataTraveler 4000 and 4000 G2. Kingston, at the very least,

should be aware of its infringing actions. Despite this knowledge, Kingston continues to commit tortious conduct by way of patent infringement.

85. Kingston has been and continues to infringe one or more of the claims of the '135 patent through the aforesaid acts.

86. Kingston has committed these acts of infringement without license or authorization.

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

88. Kingston has and continues to infringe the '135 patent, acting with an objectively high likelihood that its actions constitute infringement of the '135 patent. Kingston has known or should have known of this risk at least as early as 2009. Accordingly, Kingston's infringement of the '135 patent has been and continues to be willful.

COUNT III

(IMATION'S INFRINGEMENT OF THE '802 PATENT)

89. Paragraphs 1 through 62 are incorporated by reference as if fully restated herein.

90. On information and belief, Imation 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, Imation's hardware encrypting storage solutions, including but not limited to the IronKey D80, IronKey Enterprise S1000, IronKey Enterprise S250, IronKey Enterprise D250, IronKey F150, IronKey F100, IronKey Basic S1000, IronKey Basic S250, IronKey Basic D250, IronKey F200, IronKey Personal S250, IronKey D250, IronKey Workspace W700, IronKey Workspace W500, IronKey Workspace W300, IronKey Workspace W200, IronKey Workspace W700SC, IronKey Enterprise H350, IronKey Enterprise H300, IronKey

H200 Biometric, IronKey H100, IronKey Basic H350, IronKey Basic H300, MXI M200, MXI M500, MXI M500 and MXP Bio.

91. Imation has infringed 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 Imation infringes and/or infringed the '802 patent is attached as Exhibit E.[4] Exhibit E is based on the public information available to Plaintiff, and Plaintiff reserves the right to amend Exhibit E based on information obtained through discovery. Accordingly, the aforementioned products infringe the '802 patent literally and/or under the doctrine of equivalents.

92. Imation actively, knowingly, and intentionally induced infringement of the '802 patent under 35 U.S.C. §271(b) by its customers and end users.

93. Imation has had knowledge of and notice of the '802 patent and its infringement. For example, in April 2010, Imation discussed the possible acquisition of Spyrus and, during the course such discussions, discussed the Patents-in-Suit. Imation has been and continues to be aware of the scope of the '802 patent and its application to Imation's products.

[4] Plaintiff reserves the right to assert additional claims of the '802 patent against Imation 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.

94. Imation 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. E. For example, Imation encouraged 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 Imation's infringing products and the customer's or end user's computer.

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

96. Accordingly, Imation has induced infringement of the '802 patent under 35 U.S.C. §271(b).

97. As discussed above, Imation has had knowledge of and notice of the '802 patent since at least April 2010, when it discussed acquiring Spyrus. Imation was well aware of the scope of the '802 patent. Imation, at the very least, should have been aware of its infringing actions. Despite this knowledge, Imation committed tortious conduct by way of patent infringement.

98. Imation infringed one or more of the claims of the '802 patent through the aforesaid acts.

99. Imation committed these acts of infringement without license or authorization.

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

101. Imation has infringed the '802 patent, acting with an objectively high likelihood that its actions constitute infringement of the '802 patent. Imation has known or should have known of this risk at least as early as September 2011, when it acquired IronKey. Accordingly, Imation's infringement of the '802 patent was willful.

COUNT IV

(IMATION'S INFRINGEMENT OF THE '135 PATENT)

102. Paragraphs 1 through 62 are incorporated by reference as if fully restated herein.

103. On information and belief, Imation 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, Imation's hardware encrypting storage solutions, including but not limited to the Imation's hardware encrypting storage solutions, including but not limited to the IronKey D80, IronKey Enterprise S1000, IronKey Enterprise S250, IronKey Enterprise D250, IronKey F150, IronKey F100, IronKey Basic S1000, IronKey Basic S250, IronKey Basic D250, IronKey F200, IronKey Personal S250, IronKey D250, IronKey Workspace W700, IronKey Workspace W500, IronKey Workspace W300, IronKey Workspace W200, IronKey Workspace W700SC, IronKey Enterprise H350, IronKey Enterprise H300, IronKey H200 Biometric, IronKey H100, IronKey Basic H350, IronKey Basic H300, MXI M200, MXI M500, MXI M500 and MXP Bio.

104. Imation has directly infringed 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 Imation infringes the '135 patent is attached as Exhibit G.[5] Exhibit G is based on the public information available to Plaintiff, and Plaintiff reserves the right to amend Exhibit G based on information obtained through discovery. Accordingly, the aforementioned products infringe the '135 patent literally and/or under the doctrine of equivalents.

105. Imation actively, knowingly, and intentionally induced infringement of the '135 patent under 35 U.S.C. §271(b) by its customers and end users.

106. Imation has had knowledge of and notice of the '135 patent and its infringement. For example, in April 2010, Imation discussed the possible acquisition of Spyrus and, during the course such discussions, discussed the Patents-in-Suit. Imation has been aware of the scope of the '135 patent and its application to Imation's products.

107. Imation 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. G. For example, Imation encouraged its customers and end users to perform infringing methods by the very

[5] Plaintiff reserves the right to assert additional claims of the '135 patent against Imation 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.

nature of the products. When using the infringing products, security operations are performed on all data passed between Imation's infringing products and the customer's or end user's computer.

108. Imation specifically intended its customers and/or end users infringe the '135 patent, either literally or by the doctrine of equivalents, because Imation knew about the '135 patent and how Imation's products infringed the claims of the '135 patent but Imation did not taken steps to prevent infringement by its customers and/or end users. Accordingly, Imation acted with the specific intent to induce infringement of the '135 patent.

109. Accordingly, Imation has induced infringement of the '135 patent under 35 U.S.C. §271(b).

110. As discussed above, Imation has had knowledge of and notice of the '135 patent since at least April 2010, when it discussed acquiring Spyrus. Imation was well aware of the scope of the '135 patent. Imation, at the very least, should have been aware of its infringing actions. Despite this knowledge, Imation commited tortious conduct by way of patent infringement.

111. Imation has infringed one or more of the claims of the '135 patent through the aforesaid acts.

112. Imation committed these acts of infringement without license or authorization.

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

114. Imation has infringed the '135 patent, acting with an objectively high likelihood that its actions constitute infringement of the '135 patent. Imation has known or should have known of this risk at least as early as April 2010. Accordingly, Imation's infringement of the '135 patent was been willful.

COUNT V

(DATALOCKER'S INFRINGEMENT OF THE '802 PATENT)

115. Paragraphs 1 through 62 are incorporated by reference as if fully restated herein.

116. On information and belief, DataLocker 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, DataLocker's hardware encrypting storage solutions, including but not limited to the DL3 FE, DL3, DL2, IronKey H350, IronKey H300, IronKey H200, IronKey H100, IronKey Enterprise H350, IronKey Enterprise H300, IronKey H200 Biometric, IronKey Basic H350, IronKey Basic H300, Sentry 3.0, Sentry 3 FIPS, Sentry 2, Sentry FIPS and Sentry.

117. DataLocker 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 DataLocker infringes the '802 patent is attached as Exhibit H.[6] Exhibit H is based on the public information available to Plaintiff, and Plaintiff reserves the right to amend Exhibit

[6] Plaintiff reserves the right to assert additional claims of the '802 patent against DataLocker 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.

H based on information obtained through discovery. Accordingly, the aforementioned products infringe the '802 patent literally and/or under the doctrine of equivalents.

118. DataLocker 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.

119. DataLocker has had knowledge of and notice of the '802 patent and its infringement since at least the filing of this complaint. DataLocker may also have learned of the '802 patent and its infringement as a result of its acquisition of a portion of Imation's IronKey brand in in February 2016.

120. DataLocker 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. H. For example, DataLocker 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 DataLocker's infringing products and the customer's or end user's computer.

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

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

123. As discussed above, DataLocker has had knowledge of and notice of the '802 patent since at least the filing of this complaint. DataLocker, at the very least, should be aware of its infringing actions. Despite this knowledge, DataLocker continues to commit tortious conduct by way of patent infringement.

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

125. DataLocker has committed these acts of infringement without license or authorization.

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

COUNT VI

(DATALOCKER'S INFRINGEMENT OF THE '135 PATENT)

127. Paragraphs 1 through 62 are incorporated by reference as if fully restated herein.

128. On information and belief, DataLocker 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, DataLocker's hardware encrypting storage solutions, including but not limited to the DL3 FE, DL3, DL2, IronKey H350, IronKey H300, IronKey H200, IronKey H100, IronKey Enterprise H350, IronKey Enterprise H300, IronKey H200 Biometric, IronKey Basic H350, IronKey Basic H300, Sentry 3.0, Sentry 3 FIPS, Sentry 2, Sentry FIPS and Sentry.

129. DataLocker 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 DataLocker infringes the '135 patent is attached as Exhibit I.[7] Exhibit I is based on the public information available to Plaintiff, and Plaintiff reserves the right to amend Exhibit I based on information obtained through discovery. Accordingly, the aforementioned products infringe the '135 patent literally and/or under the doctrine of equivalents.

130. DataLocker 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.

131. DataLocker has had knowledge of and notice of the '802 patent and its infringement since at least the filing of this complaint. DataLocker may also have learned of the '802 patent and its infringement as a result of its acquisition of a portion of Imation's IronKey brand in in February 2016.

132. DataLocker 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. I. For example, DataLocker encourages its customers and end users to perform infringing methods by the very

[7] Plaintiff reserves the right to assert additional claims of the '135 patent against DataLocker 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.

nature of the products. When using the infringing products, security operations are performed on all data passed between DataLocker's infringing products and the customer's or end user's computer.

133. DataLocker specifically intends its customers and/or end users infringe the '135 patent, either literally or by the doctrine of equivalents, because DataLocker has known about the '135 patent and how DataLocker's products infringe the claims of the '135 patent but DataLocker has not taken steps to prevent infringement by its customers and/or end users. Accordingly, DataLocker has acted with the specific intent to induce infringement of the '135 patent.

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

135. As discussed above, DataLocker has had knowledge of and notice of the '135 patent since at least the filing of this complaint. DataLocker, at the very least, should be aware of its infringing actions. Despite this knowledge, DataLocker continues to commit tortious conduct by way of patent infringement.

136. DataLocker has been and continues to infringe one or more of the claims of the '135 patent through the aforesaid acts.

137. DataLocker has committed these acts of infringement without license or authorization.

138. 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 Defendants have infringed the '802 patent;

b) A judgment that Defendants have infringed the '135 patent;

c) A judgment that awards Plaintiff all appropriate damages under 35 U.S.C. § 284 for Defendants' 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 Defendants' infringement;

d) An adjudication that Kingston's and Imation's infringement of the Patents-in-Suit has been willful and deliberate;

e) An adjudication that Plaintiff be awarded treble damages and pre-judgment interest under 35 U.S.C. § 284 as a result of, *inter alia*, Kingston's and Imation's willful and deliberate infringement of the Patents-in-Suit;

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

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

h) 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 27, 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.