IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

BLUE SPIKE LLC; BLUE SPIKE INTERNATIONAL LTD.; WISTARIA TRADING LTD., Plaintiffs, v. DISH NETWORK CORPORATION, DISH NETWORK L.L.C., AND DISH NETWORK SERVICE L.L.C., Defendants.	**Civil Action No. 1:19-cv-00160-LPS-CJB** **JURY TRIAL DEMANDED**

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Blue Spike LLC ("Blue Spike LLC"), Plaintiff Blue Spike International Ltd. ("Blue Spike Int."), and Plaintiff Wistaria Trading Ltd. ("Wistaria") (collectively, "Plaintiffs"), for their First Amended Complaint against Defendants Dish Network Corporation, Dish Network L.L.C., and Dish Network Service L.L.C, (referred to collectively herein as "Dish" or "Defendant"), allege the following:

NATURE OF THE ACTION

1. This is an action for patent infringement arising under the Patent Laws of the United States, 35 U.S.C. § 1 *et seq*.

THE PARTIES

2. Plaintiff Blue Spike LLC is a limited liability company organized under the laws of the State of Texas with a place of business at 1820 Shiloh Road, Suite 1201-C, Tyler, Texas 75703.

3. Plaintiff Blue Spike Int. is a limited liability company established in Ireland with a place of business at Unit 6, Bond House, Bridge Street, Dublin 8, Ireland. Blue Spike Int. was recently acquired by Blue Spike Inc., a Florida corporation. Blue Spike Inc. has no right, title, or interest in the patents in suit, nor any licensing rights to the patents in suit, nor any enforcement rights in the patents in suit.

4. Plaintiff Wistaria Trading Ltd. is a Bermuda corporation with a place of business at Clarendon House, 2 Church St., Hamilton HM 11, Bermuda.

5. Upon information and belief, Defendant Dish Network Corporation is a corporation established under the laws of the State of Nevada, with a principal place of business at 9601 S. Meridian Boulevard, Englewood, Colorado 80112. Defendant can be served through its registered agent, CSC Services of Nevada, Inc., located at 2215-B Renaissance Drive, Las Vegas, Nevada 89119.

6. Upon information and belief Defendant Dish Network L.L.C. is established under the laws of the State of Colorado, with a principal place of business at 9601 S. Meridian Boulevard, Englewood, Colorado 80112. Defendant can be served through its registered agent, Corporation Service Company d/b/a CSC – Lawyers Incorporating Service Company, located at 211 E. 7th Street, Suite 620, Austin, Texas 78701.

7. Upon information and belief Defendant Dish Network Service L.L.C. established under the laws of the State of Colorado, with a principal place of business at 9601 S. Meridian Boulevard, Englewood, Colorado 80112. Defendant can be served through its registered agent, Corporation Service Company d/b/a CSC – Lawyers Incorporating Service Company, located at 211 E. 7th Street, Suite 620, Austin, Texas 78701.

8. Upon information and belief, Dish sells, offers to sell, and/or uses products and services throughout the United States, including in this judicial district, and introduces infringing products and services into the stream of commerce knowing that they would be sold and/or used in this judicial district and elsewhere in the United States.

JURISDICTION AND VENUE

9. This is an action for patent infringement arising under the Patent Laws of the United States, Title 35 of the United States Code.

10. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

11. Venue is proper in this judicial district under 28 U.S.C. § 1400(b). Defendants previously agreed to accept the propriety of venue in this district.

12. This Court has personal jurisdiction over Dish under the laws of the State of Delaware, due at least to their substantial business in Delaware and in this judicial district, directly or through intermediaries, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct and/or deriving substantial revenue from goods and services provided to individuals in the State of Delaware.

BACKGROUND

The Inventions

13. Scott A. Moskowitz and Michael Berry are the inventors of U.S. Patent Nos. 7,475,246 ("the '246 patent"). A true and correct copy of the '246 patent is attached as Exhibit A.

14. Scott A. Moskowitz and Michael Berry are the inventors of U.S. Patent Nos. 8,739,295 ("the '295 patent"). A true and correct copy of the '295 patent is attached as Exhibit B.

15. Scott A. Moskowitz and Michael Berry are the inventors of U.S. Patent No. 9,934,408 (the '408 patent"). A true and correct copy of the '408 patent is attached to Exhibit C.

16. Scott A. Moskowitz and Marc Cooperman are the inventors of U.S. Patent No. 9,021,602 ("the '602 patent"). A true and correct copy of the '602 patent is attached as Exhibit F.

17. Scott A. Moskowitz is the inventor of U.S. Patent No. 9,104,842 ("the '842 patent"). A true and correct copy of the '842 patent is attached as Exhibit G.

18. The '246 patent, the '295 patent, the '408 patent, the '602 patent, and the '842 patent (collectively, "the patents in suit") all cover pioneering technologies for rights management and content security.

19. The patents in suit are all assigned to and owned by Wistaria. Blue Spike LLC is the exclusive licensee of the patents in suit. Blue Spike LLC's exclusive license to the patents in suit includes the right to assert infringement under 35 U.S.C. §271 and grant sub-licenses to the patents in suit.

20. Blue Spike Int. is a prior exclusive licensee of the patents in suit, which license was revoked upon the grant of the exclusive license to Blue Spike LLC; however, Blue Spike Int. retains the right to receive all revenues from Blue Spike LLC's licensing of the patents in suit.

21. Blue Spike LLC, Blue Spike Int., and Wistaria are each exclusively and entirely owned and controlled by Scott Moskowitz.

22. The '246, '295, and '408 patents (collectively, "the Secure Server patents") all resulted from the pioneering efforts of the named inventors in the area of secure distribution of digitized value-added information, or media content, while preserving the ability of publishers to make available unsecured versions of the same value-added information, or media content,

without adverse effect to the systems security. These efforts resulted in the secure personal content server memorialized in mid-2000. At the time of these pioneering efforts, the most widely implemented technology used to address unauthorized copying and distribution of digital content was focused solely on cryptography. Content could be encrypted, but there was no association between the encryption and the actual content. This meant that there could be no efficient and openly accessible market for tradable information. The Inventors conceived of the inventions claimed in the Secure Server patents as a way to separate transactions from authentication in the sale of digitized data.

23. For example, the Inventors developed methods and systems which enable secure, paid exchange of value-added information, while separating transaction protocols. The methods and systems improve on existing means for distribution control by relying on authentication, verification and authorization that may be flexibly determined by both buyers and sellers. These determinations may not need to be predetermined, although pricing matrix and variable access to the information opens additional advantages over the prior art. The present invention offers methods and protocols for ensuring value-added information distribution can be used to facilitate trust in a large or relatively anonymous marketplace (such as the Internet's World Wide Web).

24. The ‘602 patent and the ‘842 patent (collectively, the “Watermarking patents”) resulted from the pioneering efforts of the Inventor and Marc Cooperman (“Cooperman”) in the area of protection of digital information. These efforts resulted in the development of systems, methods, and devices for data protection memorialized in the mid-2000s. At the time of these pioneering efforts, the most widely implemented technology used to address the difficulty of protecting intellectual property was copy protection. However, in that type of system the cost of developing such protection was not justified considering the level of piracy that occurred despite

the copy protection. The Inventor and Cooperman conceived of the inventions claimed in the Watermarking patents as a way to combine transfer functions with predetermined key creation.

25. For example, the Inventor and Cooperman developed systems and methods that protect digital information by identifying and encoding a portion of the format information. Encoded digital information, including the digital sample and the encoded format information, is generated to protect the original digital information.

Advantage Over the Prior Art

26. The patented inventions disclosed in the Secure Server patents provide many advantages over the prior art, and in particular improved the operations of secure personal content servers. *E.g.*, Exhibit A, '246 patent at 2:24–64; Exhibit B, '295 patent at 2:39–65; Exhibit C, '408 patent at 2:55–3:15. One advantage of the patented invention is the handling of authentication, verification, and authorization with a combination of cryptographic and steganographic protocols to achieve efficient, trusted, secure exchange of digital information. *E.g.*, Exhibit A, '246 patent at 1:53–56; Exhibit B, '295 patent at 1:27–30; Exhibit C, '408 patent at 1:42–45.

27. Another advantage of the patented invention is leveraging the benefits of digital information (such as media content) to consumers and publishers, while ensuring the development and persistence of trust between all parties. *E.g.*, Exhibit A, '246 patent at 3:16–30; Exhibit B, '295 patent at 3:32–47; Exhibit C, '408 patent at 3:49–64.

28. Another advantage of the patented invention is the separation and independent quantification of interests and requirements of different parties to a transaction by market participants in shorter periods of time. *E.g.*, Exhibit A, '246 patent at 3:32–51; Exhibit B, '295 patent at 3:47–67; Exhibit C, '408 patent at 3:65–4:18.

29. Because of these significant advantages that can be achieved through the use of the patented invention, Plaintiffs believe the Secure Server patents present significant commercial value for companies like Dish. Indeed, the technology described and claimed in the Secure Server patents read on the core functionality of Dish's Hopper and satellite TV products and services.

30. The patented inventions disclosed in the Watermarking patents provide many advantages over the prior art, and in particular improved the operations of digital content generation and/or display devices. *E.g.*, Exhibit F, '602 patent at 7:22–40; Exhibit G, '842 patent at 7:20–38. One advantage of the patented invention is the provision of a level of security for executable code on similar grounds as that which can be provided for digitized samples. *E.g.*, Exhibit F, '602 patent at 7:22–29; Exhibit G, '842 patent at 7:20–27.

31. Another advantage of the patented invention is that it does not attempt to stop copying, but rather, determines responsibility for a copy by ensuring that licensing information must be preserved in descendant copies from an original. Without the correct license information, the copy cannot function. *E.g.*, Exhibit F, '602 patent at 7:22–29; Exhibit G, '842 patent at 7:20–27.

32. Because of these significant advantages that can be achieved through the use of the patented invention, Blue Spike believes the Watermarking patents present significant commercial value for companies like Dish. Indeed, the technology described and claimed in the Watermarking patents reads on the core security functionality of Dish's digital security in its Hopper and satellite TV products and services.

Technological Innovation

33. The patented invention disclosed in the Secure Server patents resolve technical problems related to the secure distribution of digitized value-added information, or media content, while preserving the ability of publishers to make available unsecured versions of the same value-added information, or media content, without adverse effect to the systems security. As the Secure Server patents explain, one of the limitations of the prior art as regards the secure distribution of digitized value-add information or media content was that content could be encrypted, but there was no association between the encryption and the actual content. This meant that there could be no efficient and openly accessible market for tradable information that was securely distributable. (*See* Exhibit A, '246 patent at 1:48–56; Exhibit B, '295 patent at 1:22–26; '408 patent at 1:24-31.)

34. The claims of the Secure Server patents do not merely recite the performance of some well-known business practice from the pre-Internet world along with the requirement to perform it on the Internet. Instead, the claims of the Secure Server patents recite inventive concepts that are deeply rooted in engineering technology, and overcome problems specifically arising out of how to secure distribution of digitized value-added information, or media content, while preserving the ability of publishers to make available unsecured versions of the same value-added information, or media content, without adverse effect to the systems security.

35. In addition, the claims of the Secure Server patents recite inventive concepts that improve the functioning of secure personal content servers, particularly varying quality levels in a manner designed to improve security.

36. Moreover, the claims of the Secure Server patents recite inventive concepts that are not merely routine or conventional use of computer components. Instead, the patented

invention disclosed in the Secure Server patents provide a new and novel solution to specific problems related to improving secure distribution of digitized value-added information, or media content, while preserving the ability of publishers to make available unsecured versions of the same value-added information, or media content, without adverse effect to the systems security.

37. And finally, the patented invention disclosed in the Secure Server patents does not preempt all the ways that secure distribution of digitized value-added information, or media content, while preserving the ability of publishers to make available unsecured versions of the same value-added information, or media content, without adverse effect to the systems security may be used to improve the personal content servers, nor do the Secure Server patents preempt any other well-known or prior art technology.

38. Accordingly, the claims in the Secure Server patents recite a combination of elements sufficient to ensure that the claim in substance and in practice amounts to significantly more than a patent-ineligible abstract idea.

39. The patented invention disclosed in the Watermarking patents resolves technical problems related to protection of digital information particularly problems related to a method and device for data protection. As the Watermarking patents explain, one of the limitations of the prior art as regards the protection of digital information was that existing methods of copy protection were too expensive and/or required outside determination and verification of the license. (*See* Exhibit F, '602 patent at 2:47–4:48; Exhibit G, '842 patent at 1:29–60.)

40. The claims of the Watermarking patents do not merely recite the performance of some well-known business practice from the pre-Internet world along with the requirement to perform it on the Internet. Instead, the claims of the Watermarking patents recite inventive

concepts that are deeply rooted in engineering technology, and overcome problems specifically arising out of protecting digital information in a highly distributed computing environment.

41. In addition, the claims of the Watermarking patents recite inventive concepts that improve the functioning of devices for protecting digital information, particularly by combining transfer functions with predetermined key creation.

42. Moreover, the claims of the Watermarking patents recite inventive concepts that are not merely routine or conventional use of computer components. Instead, the patented invention disclosed in the Watermarking patents provides a new and novel solution to specific problems related to protecting digital information.

43. And finally, the patented inventions disclosed in the Watermarking patents do not preempt all the ways that protecting digital information may be used to improve devices for data protection, nor do the Watermarking patents preempt any other well-known or prior art technology.

44. Accordingly, the claims in the Watermarking patents recite a combination of elements sufficient to ensure that the claim in substance and in practice amounts to significantly more than a patent-ineligible abstract idea.

COUNT I – INFRINGEMENT OF U.S. PATENT NO. 7,475,246

45. The allegations set forth in the foregoing paragraphs are incorporated into this First Claim for Relief.

46. On January 6, 2009, the ‘246 Patent was duly and legally issued by the United States Patent and Trademark Office under the title “Secure Personal Content Server.”

47. Upon information and belief, Dish has and continues to directly infringe one or more claims of the ‘246 Patent by selling, offering to sell, using, and/or providing and causing to be used products, specifically one or more Hopper, Hopper Duo, Hopper with Sling, Hopper 3,

Wally, and/or Joey Receivers (the "Accused Instrumentalities"). (*See* Exhibit. 1, Dish, *The Hopper Family*, Dish website, https://www.mydish.com/upgrades/products/ receivers/the-hoppers (last accessed October 10, 2018).)

48. Upon information and belief, the Accused Instrumentalities infringe at least claim 1 of the '246 patent. The Accused Instrumentalities include a local content server system ("LCS") for creating a secure environment for digital content. Said LCS is found within the Accused Instrumentalities. For example, Dish offers for sale multiple "Hopper" Receivers, which contain an LCS. (*See* Exhibit 1.) Dish also offers for sale the Dish TV service for use with the Hopper Receivers, which is a secure environment for digital content. (*See* Exhibit 2, Dish, *Satellite TV Packages*, https://www.dish.com/programming/packages/ (last accessed October 10, 2018).)

49. Upon information and belief, the Accused Instrumentalities include a communications port for connecting the system via a network to at least one Secure Electronic Content Distributor ("SECD"). Said SECD is found within the Accused Instrumentalities. For example, as part of its satellite TV service, Dish allows only authorized users to view encrypted digital content. On information and belief, Dish controls at least one server that regulates authorized access to this encrypted digital content and at least one SECD. (*See* Exhibit 3, *Dish, Satellite TV Pirate Sentenced to 14 Months in Federal Prison After Pleading Guilty to Illegally Rebroadcasting DISH Network's Programming*, http://about.dish.com/news-releases?item=123167 (last accessed October 10, 2018).) The Accused Instrumentalities include a MoCa cable in port – a communications port – for connecting the system via a network to Dish's authorization server. (*See* Exhibit 4 at 6, *Dish, Hopper System Components*,

https://www.dish.com/cedia/downloads/ hopperjoeysystem_jobaid_v3.pdf (last accessed October 10, 2018).)

50. Upon information and belief, the Accused Instrumentalities include a SECD which stores a plurality of data sets. Said SECD is found in the Accused Instrumentalities. For example, Dish controls at least one server that regulates authorized access to this encrypted digital content, which includes at least one SECD. On information and belief, the Dish server stores a plurality of digital video content (a plurality of data sets), including video on demand, for transmission to the Accused Instrumentalities. (*See* Exhibits 2 and 3.)

51. Upon information and belief, the Accused Instrumentalities include a SECD storing a plurality of data sets, which receives a request to transfer at least one content data set, and transmits at least one content data set in a secured transmission. Said SECD is found in the Accused Instrumentalities. For example, in order to view on-demand video, the Dish SECD must receive a request to transfer the video and transmit the video in a secured transmission. (*See* Exhibit 5 at 22, *Dish, Hopper Whole-Home HD DVR System User Guide*, Dish website, https://www.dish.com/downloads/user_guides_and_manuals/hopperuserguide_user.pdf (last accessed October 10, 2018).)

52. Upon information and belief, the Accused Instrumentalities include a rewritable storage medium whereby content received from outside the LCS is stored and received. Said rewritable storage medium is found in the Accused Instrumentalities. For example, the Accused Instrumentalities include a hard drive (a rewritable storage medium). On information and belief, in order to play video content received from Dish's SECD, the various Hopper Receivers must receive the content from the SECD and store the content. (*See* Exhibit 1 at 1.)

53. Upon information and belief, the Accused Instrumentalities include a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS. Said domain processor is found within the Accused Instrumentalities. For example, the Accused Instrumentalities include a central processing unit (a domain processor). (*See* Exhibit 6 at 2, Dish, *Introducing the Hopper 3: More Capabilities, Fewer Conflicts*, Dish Insider's Guide, https://www.dish.com/dig/technology/hopper-3-more-capabilities-fewer-conflicts/ (last accessed October 10, 2018).) On information and belief, the processor within the Hopper Receivers imposes rules and procedures for content being transferred between the Hopper Receivers and Dish servers. (*See* Exhibit 5 at 22.)

54. Upon information and belief, the Accused Instrumentalities include a programmable address module programmed with an identification code uniquely associated with the LCS. Said programmable address module is found within the Accused Instrumentalities. For example, the various Hopper Receivers include a MAC address (an identification code) that is unique to the Hopper Receiver. (*See* Exhibit 7, Dish, *Hopper 3 Wifi Issue*, Dish Communities Forum (March 14, 2017), https://communities.dish.com/t5/At-Home/Hopper-3-wifi-issue/td-p/8359 (last accessed October 10, 2018).)

55. Upon information and belief, the Accused Instrumentalities include a domain processor permitting the LCS to receive digital content from outside the LCS provided the LCS first determines that the digital content being delivered to the LCS is authorized for use by the LCS. Said domain processor is found within the Accused Instrumentalities. For example, the various Hopper Receivers allow a user to receive ultra-high definition ("UHD" or "4k") video content (digital content) only if the user has subscribed to UHD service (authorized for use by

the LCS). (*See* Exhibit 8 at 2, Dish, 4K Joey, Dish website, https://www.dish.com/equipment/joey-receivers/4k-joey/ (last accessed October 10, 2018).)

56. Upon information and belief, the Accused Instrumentalities include a domain processor wherein if the digital content is not authorized by the LCS, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content. Said domain processor is found within the Accused Instrumentalities. For example, the various Hopper Receivers provide a user with standard definition ("SD") or high definition ("HD") video content (digital content at a predetermined quality level, said predetermined quality level having been set for legacy content) if the user has not subscribed to UHD service (not authorized for use by the LCS). (*See* Exhibit 8 at 2.)

57. Since at least the time of receiving the Complaint filed on July 6, 2018 in 6:18-cv-333 (E.D. Tex.), Dish has induced and continues to induce others to infringe at least claim 1 of the '246 Patent under 35 U.S.C. § 271(b) by, among other things, and with specific intent or willful blindness, actively aiding and abetting others to infringe, including but not limited to Dish's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 1 of the '246 Patent.

58. In particular, Dish's actions that aid and abet others such as their partners and customers to infringe include distributing the Accused Instrumentalities and providing materials and/or services related to the Accused Instrumentalities. On information and belief, Dish has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Dish has had actual knowledge of the '246 Patent and that its acts were inducing infringement of the '246 Patent since at least the time of receiving the Complaint filed on July 6, 2018 in 6:18-cv-333 (E.D. Tex.).

59. On information and belief, Dish's infringement has been and continues to be willful.

60. Plaintiffs have been harmed by Dish's infringing activities.

COUNT II – INFRINGEMENT OF U.S. PATENT NO. 8,739,295

61. The allegations set forth in the foregoing paragraphs are incorporated into this Second Claim for Relief.

62. On May 27, 2014, the '295 Patent was duly and legally issued by the United States Patent and Trademark Office under the title "Secure Personal Content Server."

63. Upon information and belief, Dish has and continues to directly infringe one or more claims of the '295 Patent by selling, offering to sell, using, and/or providing and causing to be used products, specifically one or more Hopper, Hopper Duo, Hopper with Sling, Hopper 3, Wally, and/or Joey Receivers (the "Accused Instrumentalities"). (*See* Exhibit 1.)

64. Upon information and belief, the Accused Instrumentalities infringe at least claim 1 of the '295 patent. The Accused Instrumentalities include a local content server system ("LCS"). Said LCS is found within the Accused Instrumentalities. For example, Dish offers for sale multiple "Hopper" Receivers (a LCS). (*See* Exhibit 1.) Dish offers for sale the Dish TV service for use with the Hopper Receivers. (*See* Exhibit 2.)

65. Upon information and belief, the Accused Instrumentalities include an LCS communications port. Said communications port is found within the Accused Instrumentalities. For example, as part of its satellite TV service, Dish allows only authorized users to view encrypted digital content. On information and belief, Dish controls at least one server that regulates authorized access to this encrypted digital content. (*See* Exhibit 3.) The Accused Instrumentalities include a MoCa cable in port – an LCS communications port – for connecting the system via a network to Dish's authorization server. (*See* Exhibit 4 at 6.)

66. Upon information and belief, the Accused Instrumentalities include an LCS storage unit for storing digital data. Said LCS storage unit is found within the Accused Instrumentalities. For example, the various Hopper Receivers include a hard drive. On information and belief, in order to play video content received from Dish's Secure Electronic Content Distributor ("SECD") the various Hopper Receivers must receive the content from the SECD and store the content. (*See* Exhibit 1 at 1.)

67. Upon information and belief, the Accused Instrumentalities include an LCS domain processor that imposes a plurality of rules and procedures for content being transferred between said LCS and devices outside said LCS, thereby defining a first LCS domain. Said domain processor is found within the Accused Instrumentalities. For example, the various Hopper Receivers include a central processing unit (a domain processor). (*See* Exhibit 6 at 2.) On information and belief, the processor within the Hopper Receivers imposes rules and procedures for content being transferred between the Hopper Receivers and the Dish servers. (*See* Exhibit 5 at 22.)

68. Upon information and belief, the Accused Instrumentalities include a programmable address module which can be programmed with an LCS identification code uniquely associated with said LCS domain processor. Said programmable address module is found within the Accused Instrumentalities. For example, the various Hopper Receivers include a MAC address (an identification code) that is unique to the Hopper Receiver. (*See* Exhibit 7.)

69. Upon information and belief, the Accused Instrumentalities include an LCS where said LCS stores in said LCS storage unit a plurality of rules for processing a data set. Said LCS is found within the Accused Instrumentalities. For example, in order to play video content

received from Dish, the various Receivers must store a plurality of rules for processing data. (*See* Exhibit 1 at 1.)

70. Upon information and belief, the Accused Instrumentalities include an LCS wherein said LCS is configured to receive via the LCS communications port, a first data set that includes data defining first content. Said LCS is found within the Accused Instrumentalities. For example, the various Hopper Receivers allow a user to receive, via the communications port, data associated with a channel available from Dish (a first data set). Further, the Hopper Receivers allow a user to receive a "channel lineup" listing the channels available (data defining first content). (*See* Exhibit 5 at 22.)

71. Upon information and belief, the Accused Instrumentalities include an LCS wherein said LCS is configured to determine whether said first content belongs to a different LCS domain than said first LCS domain. Said LCS is found within the Accused Instrumentalities. For example, the Hopper Receivers are configured to determine whether a given channel is part of the user's subscription package, and thus whether the available channels are available to the user of the Hopper Receiver (determine whether said first content belongs to a different LCS domain than said first LCS domain). (*See* Exhibit 8 at 2.)

72. Upon information and belief, the Accused Instrumentalities include an LCS wherein said LCS is configured to exclude from the first LCS domain the first content the said LCS determines that the first content belongs to a different LCS domain. Said LCS is found within the Accused Instrumentalities. For example, the Hopper Receivers are configured to exclude from the available channels those channels for which a user does not have access through their current subscription (exclude from said first LCS domain said first content when

said LCS determines that said first content belongs to said different LCS domain). (*See* Exhibit 8 at 2.)

73. Upon information and belief, the Accused Instrumentalities include an LCS wherein the LCS is configured to use the LCS domain processor to determine, upon receipt by the LCS of the first data set via the LCS communications port, from inspection of the first data set, a first data set status value of the first data set to be at least one of unsecure, secure, and legacy. Said LCS is found within the Accused Instrumentalities. For example, the Hopper Receivers are configured to determine whether data identifying a specific channel (first data set) can be recorded or not. For example, the Hopper Receiver is configured such that it will only allow viewing of certain on demand programming for a limited amount of time. On information and belief, in order to make this determination, the Hopper Receiver must determine a data value (first data set status value) indicating whether a channel may be recorded. This data value would indicate whether the channel is not recordable (secure) or recordable (unsecure). (*See* Exhibit 5 at 40.) Alternatively, the Hopper Receivers are configured to determine whether data identifying a specific HD channel (first data set) is available for a user to view using the Hopper Receiver. On information and belief, in order to make this determination, the Hopper Receiver must determine a data value (first data set status value) indicating whether the channel is in standard definition (legacy) or high definition. (*See* Exhibit 8 at 2.)

74. Upon information and belief, the Accused Instrumentalities include an LCS wherein the LCS is configured to use the first data set status value to determine which of a set of rules to apply to process the first data set. Said LCS is found within the Accused Instrumentalities. For example, the Hopper Receivers are configured to use the indication of whether a channel is recordable to determine whether the Box can record the channel in response

to a user request to do so (determine which of a set of rules to apply to process said first data set). (*See* Exhibit 5 at 40.) Alternatively, the Hopper Receivers are configured to use the indication of whether a channel is in standard definition or high definition to determine whether the Box can display the channel in response to a user request to do so (determine which of a set of rules to apply to process said first data set). (*See* Exhibit 8 at 2.)

75. Upon information and belief, the Accused Instrumentalities include an LCS wherein the LCS is configured to determine, at least in part from rights associated with a user identification associated with a prompt received by the LCS for the first content, a quality level at which to transmit the first content. Said LCS is found within the Accused Instrumentalities. For example, the Hopper Receivers are configured to determine whether to transmit the requested secure content (a quality level at which to transmit said first content, wherein the quality level is secure) at least in part from a user's authentication from requesting the Dish On Demand Programming (first content). Dish asks for a user's PIN number in ordering On Demand Programming. (*See* Exhibit 5 at 40.) Alternatively, the Hopper Receivers are configured to determine whether to transmit the requested standard definition content (a quality level at which to transmit said first content, wherein the quality level is legacy (see next element)) at least in part from a user's current subscription. (*See* Exhibit 8 at 2.)

76. Upon information and belief, the Accused Instrumentalities include an LCS wherein the quality level is one of at least unsecure, secure, and legacy. Said LCS is found within the Accused Instrumentalities. For example, the Hopper Receivers are configured to transmit on demand programming (quality level is secure). (*See* Exhibit 5 at 40.) Alternatively, the Hopper Receivers are configured to transmit standard definition channels (quality level is legacy). (*See* Exhibit 8 at 2.)

77. Upon information and belief, the Accused Instrumentalities include an LCS wherein the LCS is configured to transmit the first content at the determined quality level in response to a prompt. Said LCS is found within the Accused Instrumentalities. For example, the Hopper Receivers are configured to transmit on demand programming in response to a user's selection of the programming, and/or in response to a user entering a Purchase PIN (prompt). (*See* Exhibit 5 at 40.) Alternatively, the Hopper Receivers are configured to transmit standard definition channels in response to a user's selection of the unavailable high definition channel from the channel guide (prompt). (*See* Exhibit 8 at 2.)

78. Upon information and belief, since at least the time of receiving the Complaint filed on July 6, 2018 in 6:18-cv-333 (E.D. Tex.), Dish has induced and continues to induce others to infringe at least claim 1 of the '295 Patent under 35 U.S.C. § 271(b) by, among other things, and with specific intent or willful blindness, actively aiding and abetting others to infringe, including but not limited to Dish's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 1 of the '295 Patent.

79. In particular, Dish's actions that aid and abet others such as their partners and customers to infringe include distributing the Accused Instrumentalities and providing materials and/or services related to the Accused Instrumentalities. On information and belief, the Dish has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Dish has had actual knowledge of the '295 Patent and that its acts were inducing infringement of the '295 Patent since at least the time of receiving the Complaint filed on July 6, 2018 in 6:18-cv-333 (E.D. Tex.).

80. On information and belief, Dish's infringement has been and continues to be willful.

81. Plaintiffs have been harmed by Dish's infringing activities.

COUNT III – INFRINGEMENT OF U.S. PATENT NO. 9,934,408

82. The allegations set forth in the foregoing paragraphs are incorporated into this Third Claim for Relief.

83. On April 3, 2018, the '408 Patent was duly and legally issued by the United States Patent and Trademark Office under the title "Secure Personal Content Server."

84. Upon information and belief, Dish has and continues to directly infringe one or more claims of the '408 Patent by selling, offering to sell, using, and/or providing and causing to be used products, specifically one or more Hopper, Hopper Duo, Hopper with Sling, Hopper 3, Wally, and/or Joey Receivers (the "Accused Instrumentalities"). (*See* Exhibit 1.)

85. Upon information and belief, the Accused Instrumentalities infringe at least claim 1 of the '408 patent. The Accused Instrumentalities include a local content server system (LCS) for providing conditional access to content. Said LCS is found within the Accused Instrumentalities. For example, Dish offers for sale multiple "Hopper" Receivers (LCS). (*See* Exhibit 1). Further, Dish offers for sale the Dish TV service for use with the Hopper Receivers. (*See* Exhibit 2.)

86. Upon information and belief, the Accused Instrumentalities include an LCS address module storing an LCS identification code. Said LCS address module is found within the Accused Instrumentalities. For example, the various Hopper Receivers include a MAC address (identification code) that is unique to the Hopper Receiver. (*See* Exhibit 7.)

87. Upon information and belief, the Accused Instrumentalities include an LCS storage unit for storing content in encrypted or scrambled digital form in non-transient memory. Said LCS storage unit is found within the Accused Instrumentalities. For example, the various Hopper Receivers include a hard drive (LCS storage unit) for storing date. (*See* Exhibit 1 at 1.)

On information and belief, Dish encrypts all of its channels for delivery to the Hopper Receivers. (*See* Exhibit 3.)

88. Upon information and belief, the Accused Instrumentalities include an LCS communications port designed to receive content in the form of digital date. Said LCS communications port is found within the Accused Instrumentalities. For example, the various Hopper Receivers include a MoCa cable in port for connecting the system via a network to Dish's authorization server. (*See* Exhibit 4 at 6.)

89. Upon information and belief, the Accused Instrumentalities include an LCS domain processor for processing digital data, wherein the LCS domain processor is configured to: (1) determine if encrypted or scrambled first content received by the LCS communications port contains indicia indicating authenticity. Said LCS domain processor is found within the Accused Instrumentalities. For example, the various Hopper Receivers include a central processing unit (LCS domain processor). (*See* Exhibit 6 at 2.) On information and belief, the processor within the Hopper Receiver determines if a channel (first content) that a user wishes to view is authorized by the user's current subscriptions (contains indicia indicating authenticity). (*See* Exhibit 5 at 22.)

90. Upon information and belief, the Accused Instrumentalities include an LCS domain processor that stores the first content in the LCS storage unit in encrypted or scrambled digital form when the LCS domain processor determines that the encrypted or scrambled first content received by the LCS communications port contains indicia indicating authenticity. Said LCS domain processor is found within the Accused Instrumentalities. Dish encrypts all of its channels. Video on those channels (first content) is stored on the Hopper Receiver in encrypted

form when the Receiver determines that the user's subscription authorizes viewing the channel. (*See* Exhibit 5 at 22.)

91. Upon information and belief, the Accused Instrumentalities include an LCS domain processor for processing digital data, wherein the LCS domain processor is configured to: (2) determine if encrypted or scrambled first content received by the LCS communications port contains indicia indicating lack of authenticity. Said LCS domain processor is found within the Accused Instrumentalities. Dish encrypts all of its channels. Video on those channels (first content) may either be authorized (contains indicia indicating authenticity) or unauthorized (contains indicia indicating lack of authenticity), according to the user's subscription. (*See* Exhibit 5 at 22; Exhibit 8 at 2.)

92. Upon information and belief, the Accused Instrumentalities include an LCS domain processor for processing digital data, wherein the LCS domain processor is configured to not store the first content in the LCS storage unit when the LCS domain processor determines that the encrypted or scrambled first content received by the LCS communications port contains indicia indicating lack of authenticity. Said LCS domain processor is found within the Accused Instrumentalities. Dish encrypts all of its channels. Video on those channels (first content) is not stored on the Hopper Receiver in encrypted form when the Box determines that the user's subscription does not authorize viewing the channel. (*See* Exhibit 8 at 2.)

93. Upon information and belief, the Accused Instrumentalities include an LCS domain processor for processing digital data, wherein the LCS domain processor is configured to: (3) determine if encrypted or scrambled first content received by the LCS communications port contains neither one of indicia indicating authenticity and indicia indicating lack of authenticity and degrade the first content and store the degraded first content in said LCS storage

unit when said LCS domain processor determines that said first content contains neither one of indicia indicating authenticity and indicia indicating lack of authenticity. Said LCS domain processor is found within the Accused Instrumentalities. Dish encrypts all of its channels. This includes standard-definition video on those channels for which a user is not authorized to view the high-definition version and/or non-UHD video on those channels for which a user is not authorized to view the UHD video (neither one of indicia indicating authenticity and indicia indicating lack of authenticity). When the user is not authorized to view the high-definition version, the Box still displays the standard-definition version (degrade said first content). (*See* Exhibit 8 at 2.) On information and belief, in order to display the allowed content (whether SD or non-UHD), the Hopper Receivers must store the standard-definition content in local storage. (*See* Exhibit 8 at 2.)

94. Upon information and belief, since at least the time of receiving the Complaint filed on July 6, 2018 in 6:18-cv-333 (E.D. Tex.), Dish has induced and continues to induce others to infringe at least claim 1 of the '408 Patent under 35 U.S.C. § 271(b) by, among other things, and with specific intent or willful blindness, actively aiding and abetting others to infringe, including but not limited to Dish's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 1 of the '408 Patent.

95. In particular, Dish's actions that aid and abet others such as their partners and customers to infringe include distributing the Accused Instrumentalities and providing materials and/or services related to the Accused Instrumentalities. On information and belief, the Dish has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Dish has had actual knowledge of the '408 Patent and that its acts

were inducing infringement of the '408 Patent since at least the time of receiving the Complaint filed on July 6, 2018 in 6:18-cv-333 (E.D. Tex.).

96. On information and belief, Dish's infringement has been and continues to be willful.

97. Plaintiffs have been harmed by Dish's infringing activities.

COUNT IV – INFRINGEMENT OF U.S. PATENT NO. 9,021,602

98. The allegations set forth in the foregoing paragraphs are incorporated into this Fourth Claim for Relief.

99. On April 28, 2015, the '602 Patent was duly and legally issued by the United States Patent and Trademark Office under the title "Data Protection Method and Device."

100. Upon information and belief, Dish has and continues to directly infringe one or more claims of the '602 Patent by selling, offering for sale, using, and/or providing and causing to be used products and/or services, specifically one or more Hopper, Hopper Duo, Hopper with Sling, Hopper 3, Wally, and/or Joey Receivers (the "Accused Instrumentalities"). (*See* Exhibit 1.)

101. Upon information and belief, the Accused Instrumentalities infringe at least claim 1 of the '602 patent. The Accused Instrumentalities include a computer-based method for accessing functionality provided by an application software. Said computer-based method is found in the Accused Instrumentalities. For example, Dish requires its Wally TV Boxes to be authenticated when connected to a TV for the first time (a computer-based method for accessing functionality). The method is performed at least by authentication software (provided by an application software). On information and belief, Dish performs this method at least in its testing and development of the Wally TV Boxes and the software stored thereon. Additionally, Dish induces the users of the Wally TV Boxes to perform the method by instructing them how to

authenticate the Box when connected to a TV for the first time. The authentication process requires at least the user's zip code and a DISH Account Number. (*See* Exhibit 9 at 13, Dish, *Set Up Your Wally*, Dish Website, https://www.mydish.com/filestream.ashx?id=16232 (last visited Oct. 9, 2018).)

102. Upon information and belief, the Accused Instrumentalities include a computer-based method for accessing functionality provided by storing said application software in non-transient memory of a computer. Said computer-based method is found in the Accused Instrumentalities. For example, on information and belief, the authentication software is stored in non-transient memory of the Wally TV Boxes. (*See* Exhibit 9 at 16.)

103. Upon information and belief, the Accused Instrumentalities include a computer-based method for accessing functionality provided by said application software in said computer prompting a user to enter into said computer personalization information. Said computer-based method is found in the Accused Instrumentalities. For example, the authentication process requires at least the user's zip code and a Dish Account Number. (*See* Exhibit 9 at 13.)

104. Upon information and belief, the Accused Instrumentalities include a computer-based method for accessing functionality provided by said application software storing, in said non-transient memory, in a personalization data resource, both computer configuration information of said computer, and a license code entered in response to said prompting. Said computer-based method is found in the Accused Instrumentalities. For example, on information and belief, the Wally TV Boxes store, in non-transient memory, firmware necessary for the proper functioning of the TV Box (computer configuration information) and an authentication of the user's account (license code) stored in response to the user entering personalized information. (*See* Exhibit 9 at 15.)

105. Upon information and belief, the Accused Instrumentalities include a computer-based method for accessing functionality provided by said application software in said computer generating a proper decoding key, said generating comprising using said license code. Said application software is found in the Accused Instrumentalities. For example, on information and belief, in order to maintain data security, Dish encrypts the authentication of the user's account (said license code). Typically, encryption requires the use of a key. On information and belief, therefore, in order to maintain data security, the Dish authentication software generates a decoding key for use in authorization.

106. Upon information and belief, the Accused Instrumentalities include a computer-based method for accessing functionality provided by said application wherein said application software, in said computer, cannot access at least one encoded code resource of said application software, unless said license code is stored in said personalization data resource. Said application is found within the Accused Instrumentalities. For example, the Wally TV boxes cannot access any digital TV content (at least one encoded code resource of said application software) unless the user's account (license code) has been verified (stored in said personalization data resource). (*See* Exhibit 9 at 8.)

107. Upon information and belief, since at least the time of receiving the Complaint filed on July 6, 2018 in 6:18-cv-333 (E.D. Tex.), Dish has induced and continues to induce others to infringe at least claim 1 of the '602 Patent under 35 U.S.C. § 271(b) by, among other things, and with specific intent or willful blindness, actively aiding and abetting others to infringe, including but not limited to Dish's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 1 of the '602 Patent. Additionally, Dish induces the users of the Accused Instrumentalities to perform the method

described above in the claims by instructing them how to authenticate the Receiver when connected to a TV for the first time.

108. In particular, Dish's actions that aid and abet others such as their partners and customers to infringe include distributing the Accused Instrumentalities and providing materials and/or services related to the Accused Instrumentalities. On information and belief, the Dish has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Dish has had actual knowledge of the '602 Patent and that its acts were inducing infringement of the '602 Patent since at least the time of receiving the Complaint filed on July 6, 2018 in 6:18-cv-333 (E.D. Tex.).

109. On information and belief, Dish's infringement has been and continues to be willful.

110. Plaintiffs have been harmed by Dish's infringing activities.

COUNT V – INFRINGEMENT OF U.S. PATENT NO. 9,104,842

111. The allegations set forth in the foregoing paragraphs are incorporated into this Fifth Claim for Relief.

112. On August 11, 2015, the '842 Patent was duly and legally issued by the United States Patent and Trademark Office under the title "Data Protection Method and Device."

113. Upon information and belief, Dish has and continues to directly infringe one or more claims of the '842 Patent by selling, offering for sale, using, and/or providing and causing to be used products and/or services, specifically one or more Hopper, Hopper Duo, Hopper with Sling, Hopper 3, Wally, and/or Joey Receivers (the "Accused Instrumentalities"). (*See* Exhibit 1.)

114. Upon information and belief, the Accused Instrumentalities infringe at least claim 1 of the '842 patent. The Accused Instrumentalities include a method for licensed software use.

Said method is found in the Accused Instrumentalities. For example, Dish requires its Wally TV Boxes to be authenticated when connected to a TV for the first time (a method for licensed software use). The method is performed at least by the activation application. On information and belief, Dish performs this method at least in its testing and development of the Wally TV Boxes and the software stored thereon. Additionally, Dish induces the users of the Wally TV Boxes to perform the method by instructing them how to authenticate the Box when connected to a TV for the first time. The authentication process requires at least the user's zip code and a DISH Account Number. (*See* Exhibit 9 at 13.)

115. Upon information and belief, the Accused Instrumentalities include a method for licensed software use, comprising loading a software product on a computer, said computer comprising a processor, memory, an input, an output, so that said computer is programmed to execute said software product. Said method is found in the Accused Instrumentalities. For example, when setting up a Wally TV Box for the first time, the activation application (software product) is loaded onto the TV Box (computer) so that the TV Box executes the activation application. (*See* Exhibit 9 at 13.) The Wally TV Box includes a processor, memory, an input, and an output. (*See* Exhibit 1 at 1; Exhibit 6 at 2; Exhibit 4 at 5.)

116. Upon information and belief, the Accused Instrumentalities include a method for licensed software use, said software product outputting a prompt for input of license information. Said method is found within the Accused Instrumentalities. For example, as part of the activation process, the activation application prompts a user for the user's zip code and a Dish Network Account (input of license information). (*See* Exhibit 9 at 13.)

117. Upon information and belief, the Accused Instrumentalities include a method for licensed software use, said software product using license information entered via said input in

response to said prompt in a routine designed to decode a first license code encoded in said software product. Said method and software product are included in the Accused Instrumentalities. For example, on information and belief, the activation application uses the user's zip code and Dish Account Number to decode license information associated with the user's account (a first license code) encoded in the activation application. (*See* Exhibit 9 at 13.) Further, on information and belief, in order to maintain data security, Dish encrypts the authentication of the user's account (said license code). Typically, encryption requires the use of a key. On information and belief, therefore, in order to maintain data security, the Dish authentication software generates a decoding key for use in authorization.

118. Upon information and belief, since at least the time of receiving the Complaint filed on July 6, 2018 in 6:18-cv-333 (E.D. Tex.), Dish has induced and continues to induce others to infringe at least claim 1 of the '842 Patent under 35 U.S.C. § 271(b) by, among other things, and with specific intent or willful blindness, actively aiding and abetting others to infringe, including but not limited to Dish's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 1 of the '842 Patent. Additionally, Dish induces the users of the Accused Instrumentalities to perform the method by instructing them how to authenticate the Receiver when connected to a TV for the first time.

119. In particular, Dish's actions that aid and abet others such as their partners and customers to infringe include distributing the Accused Instrumentalities and providing materials and/or services related to the Accused Instrumentalities. On information and belief, the Dish has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Dish has had actual knowledge of the '842 Patent and that its acts

were inducing infringement of the '842 Patent since at least the time of receiving the Complaint filed on July 6, 2018 in 6:18-cv-333 (E.D. Tex.).

120. On information and belief, Dish's infringement has been and continues to be willful.

121. Plaintiffs have been harmed by Dish's infringing activities.

JURY DEMAND

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiffs Blue Spike LLC, Blue Spike Int., and Wistaria demand a trial by jury on all issues triable as such.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Blue Spike LLC, Blue Spike Int., and Wistaria demand judgment for themselves and against Dish as follows:

A. An adjudication that Dish has infringed the patents in suit;

B. An award of damages to be paid by Dish adequate to compensate Plaintiffs for Dish's past infringement of the patents in suit, and any continuing or future infringement through the date such judgment is entered, including interest, costs, expenses and an accounting of all infringing acts including, but not limited to, those acts not presented at trial;

C. A declaration that this case is exceptional under 35 U.S.C. § 285, and an award of Plaintiffs' reasonable attorneys' fees; and

D. An award to Plaintiffs of such further relief at law or in equity as the Court deems just and proper.

Dated: March 29, 2019

DEVLIN LAW FIRM LLC

/s/ Timothy Devlin

Timothy Devlin (No. 4241)
James Lennon (No. 4570)
1306 N. Broom St., 1st Floor
Wilmington, Delaware 19806
Telephone: (302) 449-9010
Facsimile: (302) 353-4251

Attorneys for Plaintiffs
Blue Spike LLC
Blue Spike International Ltd.
Wistaria Trading Ltd.