IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

BLUE SPIKE LLC; BLUE SPIKE INTERNATIONAL LTD.; WISTARIA TRADING LTD. Plaintiffs,	**Civil Action No. ______________**
v.	**JURY TRIAL DEMANDED**
COMCAST CABLE COMMUNICATIONS, LLC Defendant.	

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 Complaint against Defendant Comcast Cable Communications, LLC ("Comcast" 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. 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 Comcast Cable Communications, LLC is a limited liability company organized under the laws of the State of Delaware with a place of business at 1701 John F Kennedy Boulevard, Philadelphia, Pennsylvania, 19103.

6. Upon information and belief, Comcast 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

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

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

9. Venue is proper in this judicial district under 28 U.S.C. § 1400(b).

10. This Court has personal jurisdiction over Comcast under the laws of the District of Delaware due at least to its 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. Further, this Court has personal jurisdiction and proper authority to exercise venue over Comcast because defendant is incorporated in Delaware and by doing so has purposely availed itself of the privileges and benefits of the laws of the State of Delaware

BACKGROUND

The Inventions

11. 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.

12. 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.

13. 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.

14. Scott A. Moskowitz is the inventor of U.S. Patent Nos. 7,159,116 ("the '116 patent"). A true and correct copy of the '116 patent is attached as Exhibit D.

15. Scott A. Moskowitz is the inventor of U.S. Patent Nos. 8,538,011 ("the '011 patent"). A true and correct copy of the '011 patent is attached as Exhibit E.

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. Scott A. Moskowitz is the inventor of U.S. Patent No. 8,224,705 ("the '705 patent"). A true and correct copy of the '705 patent is attached as Exhibit H.

19. Scott A. Moskowitz is the inventor of U.S. Patent No. 7,287,275 ("the '275 patent"). A true and correct copy of the '275 patent is attached as Exhibit I.

20. Scott A. Moskowitz is the inventor of U.S. Patent No. 8,473,746 ("the '746 patent"). A true and correct copy of the '746 patent is attached as Exhibit J.

21. Scott A. Moskowitz is the inventor of U.S. Patent Reissue No. RE 44,222 ("the '222 patent"). A true and correct copy of the '222 patent is attached as Exhibit K.

22. Scott A Moskowitz is the inventor of U.S. Patent Reissue No. RE 44,307 ("the '307 Patent"). A true and correct copy of the '307 Patent is attached as Exhibit L.

23. The '246 patent, the '295 patent, the '408 patent, the '116 patent, the '011 patent, '602 patent, the '842 patent, the '705 patent, the '275 patent, the '746 patent, the '222 patent, and the '307 patent (collectively, "the patents in suit") all cover pioneering technologies for rights management and content security.

24. 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.

25. 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.

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

27. 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.

28. 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).

29. The ‘116 patent and the ‘011 patent (collectively, the “Trusted Transaction patents”) resulted from the pioneering efforts of Mr. Moskowitz (hereinafter “the Inventor”) in the area of transferring information between parties. These efforts resulted in the development of systems, methods, and devices for trusted transactions memorialized in mid-2000. At the time of these pioneering efforts, the most widely implemented technology used to address the difficulty of providing to a prospective acquirer of good or services full, accurate, and verifiable information regarding the nature, value, authenticity, and other suitability-related characteristics

of the product in question. In that type of system, reciprocal and non-reciprocal systems could use non-secret algorithms to provide encryption and decryption. The Inventor conceived of the inventions claimed in the '116 and '011 patents as a way to enhance trust on the part of participants in the transaction.

30. For example, the Inventor developed methods and systems which enhance trust in transactions in connection with sophisticated security, scrambling, and encryption technology by, for example, steganographic encryption, authentication, and security means.

31. 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.

32. 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.

33. The '705, '275, '746, '222, and '307 patents (collectively, the "Packet Transfer patents") resulted from the pioneering efforts of the Inventor in the area of optimizing and provisioning the allocation of bandwidth. These efforts resulted in the development of systems,

methods, and devices for packet watermarking and efficient provisioning of bandwidth memorialized in the early- to mid-2000s. At the time of these pioneering efforts, the most widely implemented technology used to optimize and provision the allocation of bandwidth

34. Focused on priority of transmission paths for data in an attempt to alleviate bottlenecks within a given network. The Inventor conceived of the inventions claimed in the Packet Transfer patents as a way to transmit a stream of data by receiving a stream, organizing the stream into a plurality of packets, generating a packet watermark with each of the plurality of packets to form watermarked packets, and transmitting at least one of the watermarked packets across a network. *E.g.*, Exhibit I, '275 patent at 5:35–67; Exhibit H, '705 patent at 4:34–65; Exhibit J, '746 patent at 4:66–3:51; Exhibit K, '222 patent at 5:11–6:9; Exhibit L, '307 patent at 4:47–5:11.

35. For example, the Inventor developed systems and methods that generate, monitor, and authenticate packet watermarking data.

Advantage Over the Prior Art

36. 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.

37. 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.

38. 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.

39. 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 Comcast. Indeed, the technology described and claimed in the Secure Server patents read on the core functionality of Comcast's Xfinity product and services.

40. The patented inventions disclosed in the Trusted Transaction patents provide many advantages over the prior art, and in particular improved the operations of transaction devices. *E.g.*, Exhibit D, '116 patent at 3:38–7:67; Exhibit E, '011 patent at 3:42–7:60. 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. *See* Exhibit D, '116 patent at 3:46–51; Exhibit E, '011 patent at 3:50–57.

41. 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 D, '116 patent at 3:16–30.

42. Another advantage of the patented invention is the integration of system components, optimally requiring comparatively little processing resources so as to maximize its usefulness and minimize its cost. *E.g.*, Exhibit D, '116 patent at 3:52–55; Exhibit E, '011 patent at 3:53–57.

43. Because of these significant advantages that can be achieved through the use of the patented invention, Plaintiffs believe the Trusted Transaction patents present significant commercial value for companies like Comcast. Indeed, the technology described and claimed in the Trusted Transaction patents read on the core security functionality of Comcast's downloadable apps.

44. 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.

45. 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.

46. Because of these significant advantages that can be achieved through the use of the patented invention, Plaintiffs believe the Watermarking patents present significant commercial value for companies like Comcast. Indeed, the technology described and claimed in

the Watermarking patents reads on the core security functionality of Comcast's digital security in its Xfinity digital TV devices and products.

47. The Packet Transfer patents resulted from the pioneering efforts of the Inventor in the area of optimizing and provisioning the allocation of bandwidth. These efforts resulted in the development of systems, methods, and devices for packet watermarking and efficient provisioning of bandwidth memorialized in the early- to mid-2000s. At the time of these pioneering efforts, the most widely implemented technology used to optimize and provision the allocation of bandwidth

48. Focused on priority of transmission paths for data in an attempt to alleviate bottlenecks within a given network. The Inventor conceived of the inventions claimed in the Packet Transfer patents as a way to transmit a stream of data by receiving a stream, organizing the stream into a plurality of packets, generating a packet watermark with each of the plurality of packets to form watermarked packets, and transmitting at least one of the watermarked packets across a network. *E.g.*, Exhibit I, '275 patent at 5:35–67; Exhibit H, '705 patent at 4:34–65; Exhibit J, '746 patent at 4:66–3:51; Exhibit K, '222 patent at 5:11–6:9; Exhibit L, '307 patent at 4:47–5:11.

49. For example, the Inventor developed systems and methods that generate, monitor, and authenticate packet watermarking data.

Technological Innovation

50. 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.)

51. 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.

52. 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.

53. 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.

54. 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.

55. 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.

56. The patented invention disclosed in the Trusted Transaction patents resolves technical problems related to transferring information between parties, particularly problems related to the utilization of sophisticated security, scrambling, and encryption technology by, for example, steganographic encryption, authentication, and security means. As the Trusted Transaction patents explain, one of the limitations of the prior art as regards the technical problems related to transferring information between parties was the difficulty of providing to a prospective acquirer of good or services full, accurate, and verifiable information regarding the nature, value, authenticity, and other suitability-related characteristics of the product in question. In that type of system, reciprocal and non-reciprocal systems could use non-secret algorithms to provide encryption and decryption. (*See* Exhibit D, ‘116 patent at 2:53–3:35; Exhibit E, ‘011 patent at 2:57–3:38.)

57. The claims of the Trusted Transaction 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 Trusted Transaction patents

recite inventive concepts that are deeply rooted in engineering technology, and overcome problems specifically arising out of how to enhance trust on the part of participants in the transaction.

58. In addition, the claims of the Trusted Transaction patents recite inventive concepts that improve the functioning of devices for conducting trusted transactions, particularly by creating a bridge between mathematically determinable security and analog or human measure of trust.

59. Moreover, the claims of the Trusted Transaction patents recite inventive concepts that are not merely routine or conventional use of computer components. Instead, the patented invention disclosed in the Trusted Transaction patents provides a new and novel solution to specific problems related to enhancing trust on the part of participants in a transaction.

60. And finally, the patented inventions disclosed in the Trusted Transaction patents do not preempt all the ways that enhancing trust on the part of participants in a transaction may be used to improve devices for trusted transactions, nor do the Trusted Transaction patents preempt any other well-known or prior art technology.

61. Accordingly, the claims in the Trusted Transaction 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.

62. 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.)

63. 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.

64. 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.

65. 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.

66. 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.

67. 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.

68. The patented invention disclosed in the Packet Transfer patents resolves technical problems related to optimizing and provisioning the allocation of bandwidth, particularly

problems related to better handling of the competitive needs between networks and the concept of Quality of Service. As the Packet Transfer patents explain, one of the limitations of the prior art as regards the protection of digital information was that users seek data objects which by their very structure or format may occupy large amounts of bandwidth, thereby creating bandwidth demand that has little or no relationship to how the data is valued by third parties, including owners of rights related to the objects. (*See* Exhibit H, '705 patent at 2:48–59; Exhibit I, '275 patent at 2:43–55; Exhibit J, '746 patent at 2:56–63; Exhibit K, '222 patent at 2:60–67; Exhibit L, '307 patent at 2:47–3:1).

69. The claims of the Packet Transfer 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 Packet Transfer patents recite inventive concepts that are deeply rooted in engineering technology, and overcome problems specifically arising out of optimizing and provisioning the allocation of bandwidth.

70. In addition, the claims of the Packet Transfer patents recite inventive concepts that improve the functioning of devices for packet watermarking and efficient provisioning of bandwidth.

71. Moreover, the claims of the Packet Transfer patents recite inventive concepts that are not merely routine or conventional use of computer components. Instead, the patented invention disclosed in the Packet Transfer patents provide a new and novel solution to specific problems related to optimizing and provisioning the allocation of bandwidth.

72. And finally, the patented inventions disclosed in the Packet Transfer patents do not preempt all the ways that bandwidth may be optimized and/or allocation, nor do the Packet Transfer patents preempt any other well-known or prior art technology.

73. Accordingly, the claims in the Packet Transfer 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

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

75. 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."

76. Upon information and belief, Comcast 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 Xfinity X1 TV Boxes, which by way of example include Arris XG1v3, Arris XG1v4, Arris Xi6, Pace XG1v1, Pace RNG150nP2, and Pace Xi5 (for the purposes of this section, the "Accused Instrumentalities"). (See Ex. 1 at 1–3.)

77. Upon information and belief, the Accused Instrumentalities infringe 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, Comcast offers for sale multiple "Xfinity XI TV Boxes," which contain a LCS. *See* Comcast's Xfinity website page entitled "X1 TV Box Comparison- DVR vs. Non-DVR*"* (available online at https://www.xfinity.com/support/articles/x1-hub-vs-companion-box (last visited Dec. 17, 2018), a copy of which is available as Exhibit 1.) Comcast also offers for sale Xfinity XI TV service for use with the Xfinity X1 television boxes, which also contain a secure environment for digital content. *See* Comcast's Xfinity website page entitled "X1 Cloud DVR (available online at https://www.xfinity.com/learn/digital-cable-tv/x1 (last visited Dec. 17, 2018), a copy of which is available as Exhibit 2.)

78. 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 Comcast's Xfinity X1 TV service only authorized users are allowed to view encrypted digital content. Comcast controls at least one server that regulates the authorized access to this encrypted digital content, and at least one SECD. *See* Comcast's Xfinity website page entitled "What is Digital Encryption of a Channel" (available at https://www.xfinity.com/support/articles/what-is-digital-encryption (last visited Dec. 6, 2018), a copy of which is available as Exhibit 3.)

79. 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, Comcast controls at least one server that regulates authorized access to the encrypted digital content, which utilizes at least one SECD. *See* Ex. 3 at 1; Comcast's Xfinity website page entitled "Watch Xfinity On Demand Shows and Movies on XI" (available at https://www.xfinity.com/support/articles/x1-on-demand-menu-watch-tv-programs-and-movies (last visited Dec. 17, 2018), a copy of which is available as Exhibit 5.)

80. 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, to view a video on-demand a Comcast SECD must receive a request to transfer a video (i.e. at least one content data set) in order to transmit the video in a secured transmission. *See* Ex. 5 at 2-4.

81. 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, in various Comcast XI TV Boxes a hard drive (a rewritable storage medium) is included, which must receive and store the content from the SECD in order to play video content from Comcast's SECD. *See* Comcast's Xfinity website page entitled "XI DVR Services Overview" (available at https://www.xfinity.com/support/articles/x1-dvr-overview (last visited Dec. 6, 2018), a copy of which is available as Exhibit 6); Comcast's Xfinity website page entitled "Xfinity X1 Equipment" (available at https://www.xfinity.com/learn/digital-cable-tv/x1/equipment# (last visited Dec. 6, 2018), a copy of which is available as Exhibit 7.)

82. 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, various Comcast XFinity XI TV Boxes include a central processing unit. *See* Warren Bowman's review entitled "Comcast Xfinity XI Box Review" (available at https://www.bwone.com/xfinity-x1-review/ (last visited Dec. 6, 2018), a copy of which is available as Exhibit 8.)

83. 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, various Comcast XFinity X1 TV Boxes include a machine address code ("MAC") address. This MAC address is an identification code, and is unique to the Xfinity X1 TV Box. *See* Comcast's Xfinity website page entitled "View XI TV Box Information Online" (available at

https://www.xfinity.com/support/articles/x1-view-set-top-box-information-online (last visited Dec. 6, 2018), a copy of which is available as Exhibit 9.)

84. 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, Comcast's various XFinity X1 TV Boxes allow a user to receive high definition ("HD") video content (i.e. digital content). A user is only able to receive HD video content if they have subscribed to HD service, which is authorized for use by the LCS. *See* Comcast's Xfinity website page entitled "New Channel Lineup Frequently Asked Questions" (available at https://www.xfinity.com/support/articles/new-channel-lineup (last visited Dec. 6, 2018), a copy of which is available as Exhibit 10.)

85. Upon information and belief, the Accused Instrumentalities include a domain processor permitting the LCS to receive digital content from outside the LCS, and if the digital content is not authorized for use 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, Comcast's various Xfinity X1 TV Boxes provide to a user standard definition ("SD") 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 HD service [not authorized for use by the LCS]. *See* Ex. 10 at 2.

86. The Accused Instrumentalities infringed and continues to infringe at least claim 1 of the '246 Patent during the pendency of the '246 Patent.

87. Since at least the time of the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.), Comcast 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 Comcast’s partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 1 of the ‘246 Patent.

88. In particular, Comcast’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, Comcast has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Comcast 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 August 27, 2018 in 6:18-CV-181 (E.D. Tex.).

89. On information and belief, Comcast’s infringement has been and continues to be willful.

90. Plaintiffs have been harmed by Comcast’s infringing activities.

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

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

92. 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.”

93. Upon information and belief, Comcast 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 Xfinity X1 TV Boxes, which by way of example

include Arris XG1v3, Arris XG1v4, Arris Xi6, Pace XG1v1, Pace RNG150nP2, and Pace Xi5 (for the purposes of this section, the "Accused Instrumentalities"). (See Ex. 1 at 1–3.)

94. Upon information and belief, the Accused Instrumentalities infringe at least claim 13 of the '295 patent. The Accused Instrumentalities include a method for using a local content server system ("LCS"). Said method is found within the Accused Instrumentalities. For example, Comcast offers for sale multiple Xfinity XI TV Boxes, which contain a LCS. *See* Ex. 1 at 1-3; Ex. 2 at 1.

95. Upon information and belief, the Accused Instrumentalities include a method comprising a LCS communications port. Said method is found within the Accused Instrumentalities. For example, Comcast offers for sale various Xfinity XI TV Boxes, which include a "Cable In/FR In" port (i.e. an LCS communications port). This Cable In/RF In port connects the system via a network to Comcast's authorization server. *See* Comcast's Xfinity website page entitled "X1 Self-Installation Quick Start Guide*"* (available online at https://secure.xfinity.com/anon.comcastonline2/support/help/faqs/ (last visited Oct. 1, 2018), a copy of which is available as Exhibit 4.)

96. Upon information and belief, the Accused Instrumentalities include a method comprising a LCS storage unit for storing digital data. Said method is found within the Accused Instrumentalities. For example, various Comcast X1 TV Boxes include a hard drive (i.e. an LCS storage unit) for storing data. *See* Ex. 6 at 4; Ex. 7 at 2.

97. Upon information and belief, the Accused Instrumentalities include a method comprising a 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 method is found within the Accused Instrumentalities. For example, various

Comcast X1 TV Boxes include a central processing unit (i.e. an LCS domain processor). *See* Ex. 8 at 2; Ex. 5 at 4.

98. Upon information and belief, the Accused Instrumentalities include a method comprising a programmable address module which can be programmed with an LCS identification code uniquely associated with said LCS domain processor. Said method is found within the Accused Instrumentalities. For example, various Xfinity X1 TV Boxes include a MAC address (i.e. an LCS identification code) that is unique to the Xfinity XI TV Box. *See* Ex. 9 at 2.

99. Upon information and belief, the Accused Instrumentalities include a method comprising a LCS which stores in said LCS storage unit a plurality of rules for processing a data set. Said method is found within the Accused Instrumentalities. For example, various Comcast X1 TV Boxes must store a plurality of rules for processing data in order to play video content received from Comcast. *See* Ex. 6 at 4; Ex. 7 at 2.

100. Upon information and belief, the Accused Instrumentalities include a method for receiving, via said LCS communications port, a first data set that includes data defining first content. Said method is found in various Xfinity X1 TV Boxes, which allow a user to receive, via the communication port, data associated with a channel available from Comcast (i.e. a first data set). Additionally, the Xfinity X1 TV Boxes allow a user to receive a "channel lineup" listing the channels available (i.e. data defining first content). *See* Ex. 10 at 1.

101. Upon information and belief, the Accused Instrumentalities include a method comprising a LCS wherein said LCS determines whether said first content belongs to a different LCS domain. Said method is found within the Accused Instrumentalities. For example, Comcast's Xfinity X1 TV Boxes are configured to determine whether a given channel is part of

the subscription package, and thus whether the available channels are available to the user of the Xfinity X1 TV Box (i.e. determine whether said first content belongs to a different LCS domain than said first LCS domain). *See* Ex. 10 at 2.

102. Upon information and belief, the Accused Instrumentalities include a method comprising a LCS wherein said LCS excludes from said first LCS domain said first content when said LCS determines that said first content belongs to said different LCS domain. Said method is found within the Accused Instrumentalities. For example, Comcast's Xfinity X1 TV Boxes, which are configured to exclude from available channels those channels for which a user does not have access through their current subscription (i.e. exclude from said first LCS domain said first content when said LCS determines that said first content belongs to said different LCS domain). *See* Ex. 10 at 2.

103. Upon information and belief, the Accused Instrumentalities include a method comprising a LCS wherein said LCS determines, from said first data set, a first data set status value of said first data set to be at least one of unsecure, secure, and legacy. Said method comprising is found within the Accused Instrumentalities. For example, the Xfinity X1 TV Boxes are configured to determine whether data identifying a specific HD channel (i.e. a first data set) can be recorded. The X1 DVR is configured such that it will not record Xfinity "On Demand Programming." In order to make this determination, the Xfinity X1 TV Box must determine a data value (i.e. a first data set status value) indicating whether a channel may be recorded. This data value would indicate whether the channel is not recordable (i.e. secure) or recordable (i.e. unsecure). *See* Comcast's Xfinity website page entitled "New Channel Lineup Frequently Asked Questions*"* (available online at https://www.xfinity.com/support/articles/new-channel-lineup (last visited Oct. 1, 2018), a copy of which is available as Exhibit 12.)

104. Upon information and belief, the Accused Instrumentalities include a method comprising a LCS wherein said LCS determines, using said first data set status value, which set of rules to apply to process said first data set. Said method is found within the Accused Instrumentalities. For example, the Xfinity TV Boxes 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 (i.e. determining which of a set of rules to apply to process said first data set). Ex. 12 at 4; Ex. 10 at 2.

105. Upon information and belief, the Accused Instrumentalities include a method comprising a LCS wherein said LCS determines, at least in part from rights associated with an identification associated with a prompt received by said LCS for said first content, a quality level at which to transmit said first content. Said method found within the Accused Instrumentalities. For example, the Xfinity XI TV Boxes ask for a user's PIN number in ordering On Demand Programming, and the Xfinity X1 TV Boxes are configured to determine whether to transmit the requested secure content (i.e. 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 Xfinity On Demand Programming (i.e. first content). *See* Comcast's Xfinity website page entitled "Block Pay-Per-View and Xfinity On Demand Purchases PIN*"* (available online at https://www.xfinity.com/support/articles/how-to-block-purchase-of-pay-per-view (last visited Dec. 6, 2018), a copy of which is available as Exhibit 13); Ex. 12 at 4.

106. Alternatively, upon information and belief, the above described Accused Instrumentalities in the Xfinity X1 TV Boxes are configured to determine whether to transmit the requested standard definition content (i.e. a quality level at which to transmit said first content, wherein the quality level is legacy), at least in part from a user's current subscription. *See* Ex. 10

at 2. The Xfinity X1 TV Boxes are configured to transmit on demand programming (i.e. a secure quality level). *See* Ex. 12 at 4; Ex. 10 at 2.

107. Upon information and belief, the Accused Instrumentalities include a method comprising a LCS transmitting said first content at the determined quality level wherein said quality level is one of at least unsecure, secure, and legacy. Said method is found within the Accused Instrumentalities. For example, the Xfinity X1 TV Boxes are configured to transmit on demand programming (i.e. where quality level is secure). *See* Ex. 12 at 4. Alternatively, the Xfinity X1 TV Boxes are configured to transmit standard definition channels (i.e. wherein said quality level is legacy). *See* Ex. 10 at 2.

108. Upon information and belief, since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.), Comcast has induced and continues to induce others to infringe at least claim 13 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 Comcast's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 13 of the '295 patent. For example, Comcast uses the Xfinity X1 TV Boxes for its own testing and use, as well as inducing its customers to use the Xfinity TV Boxes in a method for using an LCS. *See* Ex. 1 at 1-3; Ex. 2 at 1.

109. In particular, Comcast'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 Comcast has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Comcast 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 August 27, 2018 in 6:18-CV-181 (E.D. Tex.).

110. On information and belief, Comcast's infringement has been and continues to be willful.

111. Plaintiffs have been harmed by Comcast's infringing activities.

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

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

113. 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."

114. Upon information and belief, Comcast 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 Xfinity X1 TV Boxes, which by way of example include Arris XG1v3, Arris XG1v4, Arris Xi6, Pace XG1v1, Pace RNG150nP2, and Pace Xi5 (for the purposes of this section, the "Accused Instrumentalities"). (See Ex. 1 at 1–3.)

115. Upon information and belief, the Accused Instrumentalities infringe at least claim 8 of the '408 patent. The Accused Instrumentalities include a method for using a LCS for providing conditional access to content. Said LCS is found within the Accused Instrumentalities, for example, the Xfinity X1 TV Boxes (i.e. a LCS). *See* Ex. 1 at 1-3. Additionally, Comcast offers for sale the Xfinity X1 TV service for use with the Xfinity X1 TV Boxes (i.e. a secure environment for digital content). *See* Ex. 2 at 1.

116. Upon information and belief, the Accused Instrumentalities include a method comprising a LCS comprising a LCS address module storing an LCS identification code. Said method is found within the Accused Instrumentalities. For example, the Xfinity X1 TV Boxes,

which include a MAC address (i.e. an LCS identification code) that is unique to the Xfinity X1 TV Box. *See* Ex. 9 at 2.

117. Upon information and belief, the Accused Instrumentalities include a method comprising an LCS storage unit for storing content in encrypted or scrambled digital form in non-transient memory. Said method is found within the Accused Instrumentalities. For example, Comcast encrypts all of its channels for delivery to the Xfinity X1 TV Boxes. *See* Comcast's Xfinity website page entitled "Block Pay-Per-View and Xfinity On Demand Purchases PIN" (available online at https://www.digitaltrends.com/home-theater/comcast-encrypting-all-cable-channels/ (last visited Dec. 6, 2018), a copy of which is available as Exhibit 14.) These Xfinity X1 TV Boxes and other various Comcast X1 TV Boxes include a hard drive (i.e. an LCS storage unit) for storing data. *See* Ex. 6 at 4; Ex. 7 at 2.

118. Upon information and belief, the Accused Instrumentalities include a method comprising an LCS communications port designed to receive content in the form of digital data. Said method is found within the Accused Instrumentalities. For example, the various Xfinity X1 TV Boxes include a "Cable In/RF In" port (i.e. an LCS communications port) for receiving content in the form of digital data. *See* Ex. 4 at 2.

119. Upon information and belief, the Accused Instrumentalities include a method comprising an LCS domain processor for processing digital data, wherein said LCS domain processor is configured to determine if encrypted or scrambled first content received by said LCS communications port contains indicia indicating authenticity, and storing said first content in said LCS storage unit in encrypted or scrambled digital form when said LCS domain processor determines that said encrypted or scrambled first content contains indicia indicating authenticity. Said method is found within the Accused Instrumentalities. For example, various Xfinity X1 TV

Boxes include a central processing unit (i.e. an LCS domain processor). *See* Ex. 8 at 2. The processor within the Xfinity X1 TV Box determines if a channel (i.e. first content) that a user wishes to view is authorized by the user's current subscriptions (i.e. contains indicia indicating authenticity). *See* Ex. 10 at 2. Furthermore, Comcast encrypts all of its channels, and the videos on those channels (i.e. the first content) are stored on the Xfinity X1 TV Box in encrypted form when the Box determines that the user's subscription authorizes viewing the channel. *See* Ex. 10 at 2.

120. Upon information and belief, the Accused Instrumentalities include a method comprising a LCS domain processor for processing digital data, wherein said LCS domain processor is configured to determine if encrypted or scrambled first content received by said LCS communications port contains indicia indicating lack of authenticity, and to not store said first content in said LCS storage unit when said LCS domain processor determines that said encrypted or scrambled first content received by said LCS communications port contains indicia indicating lack of authenticity. Said method is found within the Accused Instrumentalities. For example, Comcast encrypts all of its channels, and the video on those channels (i.e. first content) may either be authorized (i.e. contain indicia indicating authenticity) or unauthorized (i.e. contain indicia indicating lack of authenticity) depending on the user's subscription. *See* Ex. 10 at 2. Furthermore, video on Comcast's channels are not stored on the Xfinity X1 TV Box in encrypted form when the Box determines that the user's subscription does not authorize viewing the channel. *See* Ex. 10 at 2.

121. Upon information and belief, the Accused Instrumentalities include a method comprising an LCS domain processor for processing digital data, wherein said LCS domain processor is configured to determine if encrypted or scrambled first content received by said LCS

communications port contains neither one of indicia indicating authenticity and indicia indicating lack of authenticity and degrade said 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 method is found within the Accused Instrumentalities. For example, Comcast encrypts all of its channels, including standard-definition video for which a user is not authorized to view the HD version (i.e. neither one of indicia indicating authenticity and indicia indicating lack of authenticity). When the user is not authorized to view the HD version, the Box still displays the standard-version (i.e. degrades said first content). *See* Ex. 10 at 2. Furthermore, in order to display the standard-definition content, the Xfinity X1 TV Boxes must store the standard-definition content in local storage. *See* Ex. 10 at 2.

122. Upon information and belief, since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.), Comcast has induced and continues to induce others to infringe at least claim 8 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 Comcast's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 8 of the '408 patent.

123. In particular, Comcast'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 Comcast has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Comcast 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 August 27, 2018 in 6:18-CV-181 (E.D. Tex.). Additionally, Comcast uses the Xfinity X1 TV Boxes for its own testing and use, as well as inducing its customers to use the Xfinity X1 TV Boxes in a method for using an LCS for providing conditional access to content.

124. On information and belief, Comcast's infringement has been and continues to be willful.

125. Plaintiffs have been harmed by Comcast's infringing activities.

COUNT IV – INFRINGEMENT OF U.S. PATENT NO. 7,159,116

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

127. On January 2, 2007, the '116 patent was duly and legally issued by the United States Patent and Trademark Office under the title "Systems, Methods, and Devices for Trusted Transactions."

128. Upon information and belief, Comcast has and continues to directly infringe one or more claims of the '116 patent by using, and/or providing and causing to be used products, specifically one or more apps, which by way of example include the Xfinity Stream app (the "Accused Instrumentalities" for the purposes of this section). (See Ex. 1 at 1–3.)

129. Upon information and belief, the Accused Instrumentalities infringe at least claim 14 of the '116 patent. The Accused Instrumentalities include a device for conducting a trusted transaction between at least two parties who have agree to transact. Said device is found within the Accused Instrumentalities. For example, the multiple apps Comcast provides for its Xfinity users (i.e. at least two parties who have agreed to transact), including the "Xfinity Stream" app. These apps are available from the Google Play store (amongst other places). Comcast maintains at least one server (i.e. a device for conducting trusted transactions between at least two parties) on which Comcast's app downloading and app authentication services ("App Server") (i.e. a

device) are hosted. *See* Comcast's Xfinity website page entitled "Xfinity Mobile Apps*"* (available online https://www.xfinity.com/apps (last visited Oct. 1, 2018), a copy of which is available as Exhibit 16.)

130. Upon information and belief, Comcast desires the above-referenced apps (available via the Google Play store or other sources) to be as secure as possible. *See* Ex. 16 at 4. The best practices for securing apps available via the Google Play store are outlined in Google's Android developer's guidelines. Therefore, Comcast's App Server makes its apps, including the Xfinity Stream app, available via the Google Play store in a similar manner to the practice described in Google's Android developer's guidelines. *See* Google's Android website page entitled "Adding Licensing to Your App*"* (available at https://developer.android.com/google/play/licensing/adding-licensing (last accessed Dec. 7, 2018) attached hereto as Exhibit 17.)

131. Upon information and belief, the Accused Instrumentalities contain a device comprising a means for uniquely identifying information selected from the group consisting of a unique identification of one of the parties, a unique identification of the transaction, a unique identification of value added information to be transacted, a unique identification of value adding component. Said device is found within the Accused Instrumentalities. For example, Comcast's App Server includes one or more components configured to identify at least "the most recent successful license response in local persistent storage (i.e. a unique identification of a value adding component). *See* Ex. 17 at 4.

132. Upon information and belief, the above-mentioned Google's Android developer's guidelines used by Google's License Verification Library ("LVL") in its Xfinity Stream app, which is available through the Google Play store. *See* Ex. 17 at 1-2. As noted

above, Comcast desires its above-referenced apps (available via the Google Play store or other sources) to be as secure as possible. *See* Ex. 16 at 4. The best practices for securing apps available via the Google Play store are outlined in Google's Android developer's guidelines. Therefore, Comcast's App Server makes its apps, including the Xfinity Stream app, available via the Google Play store in a similar manner to the practice described in Google's Android developer's guidelines.

133. Upon information and belief, the above referenced Google's Android developer's guidelines details how Google's LVL allows Google Play to send a license check to Comcast's App Server ("Google Play licensing service does not itself determine whether a given user with a given license should be granted access to your application.") *See* Ex. 17 at 1-2. Furthermore, one of Google's recommended design points for a custom policy is obfuscation of license responses (i.e. a unique identification of a value adding component). *See* Ex. 17 at 4. As noted above, Comcast implements a license verification and custom license policy in order to best protect its available apps. *See* Ex. 17 at 4.

134. Upon information and belief, the Accused Instrumentalities contain a device comprising a steganographic cipher for generating said unique identification information. Said device is found within the Accused Instrumentalities. For example, Comcast's App Server employs a steganographic cipher for generating the most recent successful license report (i.e. unique identification information). Comcast incorporates into its Xfinity Stream app (available through the Google Play store, amongst other places) an obfuscation program similar to the AESObfuscator found in Google's LVL. *See* Ex. 17 at 4. As noted above, Google's LVL allows Google Play to send a license check to Comcast's App Server ("Google Play licensing service does not itself determine whether a given user with a given license should be granted access to

your application.") *See* Ex. 17 at 1-2. One of Google's recommended design points for a custom policy is obfuscation of license response (i.e. a unique identification of a value adding component). *See* Ex. 17 at 4. Comcast implements the license verification and a custom license policy in order to best protect its available apps.

135. Upon information and belief, the Accused Instrumentalities contain a device comprising a steganographic cipher wherein the steganographic cipher is governed by at least the following elements: a predetermined key, a predetermined message, and a predetermined carrier signal. Said device is found within the Accused Instrumentalities. For example, and as noted above, Comcast's App Server employs a steganographic cipher for generating the most recent successful license report (i.e. unique identification information). Comcast incorporates in its Xfinity Stream app (available through the Google Play store, amongst other places) an obfuscation program similar to the AESObfuscator found in Google's LVL. *See* Ex. 17 at 4. The obfuscation provided by Google is an interface called "AESObfuscator" (i.e. a steganographic cipher). *See* Ex. 17 at 7. The AESObfuscator "seed[s] the encryption using three data fields provided by the application," a "salt" (an array of random bytes) (i.e. a predetermined key), an "application identifier string, typically the package name of the application" (i.e. a predetermined carrier signal), and "a device identifier string, derived from as many device-specific sources as possible, so as to make it unique" (i.e. a predetermined message). *See* Ex. 17 at 7.

136. Upon information and belief, the Accused Instrumentalities contain a device comprising a steganographic cipher wherein the steganographic cipher is governed by at least a means for verifying an agreement to transact between the parties. Said device is found within the Accused Instrumentalities. For example, said device is found within Comcast's App Server.

As noted previously, Comcast desires its above-referenced available apps (via the Google Play store or other sources) to be as secure as possible. *See* Ex. 16 at 4. The best practices for securing apps available via the Google Play store are outlined in Google's Android developer's guidelines. Therefore, Comcast's App Server makes its apps, including the Xfinity Stream app, available via the Google Play store in a similar manner to the practice described in Google's Android developer's guidelines. *See* Ex. 17 at 1-2. In line with Google's Android developer's guidelines, Comcast's App Server includes one or more components to verify the license information (an agreement to transact between the parties) in order to authorize the download and/or installation of Comcast's apps, including the Xfinity Stream app. *See* 17 at 9-10.

137. Upon information and belief, since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.), Comcast has induced and continues to induce others to infringe at least claim 14 of the '116 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 Comcast's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 14 of the '116 patent.

138. In particular, Comcast'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 Comcast has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Comcast has had actual knowledge of the '116 patent and that its acts were inducing infringement of the '116 patent since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.).

139. On information and belief, Comcast's infringement has been and continues to be willful.

140. Plaintiffs have been harmed by Comcast's infringing activities.

COUNT V – INFRINGEMENT OF U.S. PATENT NO. 8,538,011

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

142. On September 17, 2013, the '011 patent was duly and legally issued by the United States Patent and Trademark Office under the title "Systems, Methods, and Devices for Trusted Transactions."

143. Upon information and belief, Comcast has and continues to directly infringe one or more claims of the '011 patent by using, and/or providing and causing to be used products, specifically one or more apps, which by way of example include the Xfinity Stream app (the "Accused Instrumentalities" for the purposes of this section). (See Ex. 1 at 1–3.)

144. Upon information and belief, the Accused Instrumentalities infringe at least claim 35 of the '011 patent. The Accused Instrumentalities includes a device for conducting trusted transactions between at least two parties. For example, and as noted above, the device is found within the Accused Instrumentalities within the multiple apps Comcast provides for its Xfinity users, including the Xfinity Stream app. The Xfinity Stream app and others are available from the Google Play store (and other places). *See* Ex. 16 at 4. As noted above, Comcast desires to utilize best practices for securing apps. The best practices for securing apps available via the Google Play store are outlined in Google's Android developer's guidelines. Therefore, Comcast's App Server makes its apps, including the Xfinity Stream app, available via the Google Play store in a similar manner to the practice described in Google's Android developer's guidelines. *See* Ex. 17 at 4. Comcast maintains at least one server (i.e. a device for conducting

trusted transactions between at least two parties) on which App Server (i.e. devices) are hosted. *See* Ex. 16 at 2.

145. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties, comprising a steganographic cipher. Said device is found within the Accused Instrumentalities. For example, and as noted above, Comcast's App Server employs a steganographic cipher. Furthermore, Comcast incorporates Google's LVL in its Xfinity Stream app, which is available through the Google Play store. As noted above, Google's LVL allows Google Play to send a license check to Comcast's App Server. *See* Ex. 17 at 1-2. One of Google's recommended design points for a custom policy is obfuscation of a license response. Comcast implements a license verification and custom license policy to best protect its available apps. *See* Ex. 17 at 4. The obfuscation for Comcast's available apps provided by Google, including the Xfinity Stream app, is an AESObfuscator (a steganographic cipher). The AESObfuscator "seed[s] the encryption using three data fields provided by the application," a "salt" (an array of random bytes) (i.e. a predetermined key), an "application identifier string, typically the package name of the application" (i.e. a predetermined carrier signal), and "a device identifier string, derived from as many device-specific sources as possible, so as to make it unique" (i.e. a predetermined message). *See* Ex. 17 at 7.

146. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties, comprising a controller for receiving input data or outputting output data and at least one input/output connection. Said device is found within the Accused Instrumentalities. For example, the Comcast App Server includes a controller for receiving input data or outputting output data. *See* Ex. 16 at 4.

147. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties, wherein the device has a device identification code stored in the device. Said device is found within the Accused Instrumentalities. For example, the Comcast App Server has an IP address, MAC address, or other device identification code stored in the device.

148. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties, wherein the device has an analog to digital converter. Said device is found within the Accused Instrumentalities. For example, the Comcast App Server has input/output and communications capabilities (i.e. an analog-to-digital converter).

149. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties, wherein the device has a steganographically ciphered software application, wherein said steganographically ciphered software application has been subject to a steganographic cipher for serialization. Said device is found within the Accused Instrumentalities. For example, the Comcast App Server provides multiple apps (including the Xfinity Stream app) whose code has been obfuscated in order to hinder reverse engineering (i.e. a steganographically ciphered software application). Comcast obfuscates its apps' source code in a manner similar to that described by Google in its guidelines for app developers, stating: "To ensure the security of your application, particularly for a paid application that uses licensing and/or custom constraints and protections, it's very important to obfuscate your application code. Properly obfuscating your code makes it more difficult for a malicious user to decompile the application's bytecode, modifying it- such as by removing the licensing check- and then recompile." *See* Ex. 17 at 20.

150. Furthermore, upon information and belief, the code obfuscation provided by ProGuard and/or the license data obfuscation provided by Google's AESObfuscator (a steganographic cipher) allows the code to be ciphered for serialization. For example, the AESObfuscator obfuscates the most recent successful license response in local persistent storage. *See* Ex. 17 at 4. This obfuscation allows for serialized license responses.

151. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties wherein said steganographic cipher receives said output data, steganographically ciphering said output data using a key to define stenganographically ciphered output data. Said steganographic cipher is found in the Accused Instrumentality. For example, Comcast's App Server makes use of steganographic ciphers similar to Google's AESObfuscator and/or ProGuard. *See* Ex. 17 at 7. Therefore, Comcast's App server makes use of a steganographic cipher that receives output data. *See* Ex. 17 at 7. As another example, ProGuard receives the actual code of the apps output from the App Server. *See* Trevor Johns article, entitled "Securing Android LVL Applications" (available online at https://android-developers.googleblog.com/2010/09/securing-android-lvl-applications.html (last accessed Dec. 7, 2018) a copy of which is available as Exhibit 18.)

152. Furthermore, upon information and belief, as detailed above Comcast's App Server makes use of steganographic ciphers similar to Google's AESObfuscator and/or ProGuard. Therefore, Comcast's App server steganographically ciphers output data using a key. For example, Google's AESObfuscator and ProGuard steganographically cipher code using either a public or private key. *See* Ex. 18 at 2. As detailed above, Comcast's App Server makes use of steganographic ciphers similar to Google's AESObfuscator and/or ProGuard. Therefore, Comcast's App server defines steganographically ciphered output data. This is demonstrated by

Google's AESObfuscator and ProGuard, which define steganographically ciphered license responses and steganographically ciphered code, respectively. *See* Ex. 17 at 7; Ex. 18 at 2.

153. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties wherein said steganographic cipher transmits said steganographically ciphered output data to said at least one input/output connection. Said device is found within the Accused Instrumentalities. For example, and as noted above, the Comcast App Server provides multiple apps (including the Xfinity Stream app), available from the Google Play store (amongst other places). The Comcast App Server transmits the steganographically ciphered output data (i.e. the steganographically ciphered code and/or code containing the steganographically ciphered license response) via at least one output/input connection. *See* Ex. 16 at 4.

154. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties wherein the device is configured to steganographically cipher both value-added information and at least one value-added component associated with the value-added information. Said device is found within the Accused Instrumentalities. For example, and as detailed above, Comcast's App Server makes use of steganographic ciphers similar to Google's AESObfuscator and/or ProGuard. Therefore, Comcast's App server is configured to steganographically cipher license information and/or proprietary source code. This is demonstrated by Google's AESObfuscator and ProGuard, which define steganographically ciphered license responses as well as an application identifier string, and steganographically ciphered code including various proprietary code portions, respectively. *See* Ex. 17 at 7; Ex. 18 at 2.

155. Upon information and belief, since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.), Comcast has induced and continues to induce others to infringe at least claim 35 of the '011 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 Comcast's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 35 of the '011 patent.

156. In particular, Comcast'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 Comcast has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Comcast has had actual knowledge of the '011 patent and that its acts were inducing infringement of the '011 patent since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.).

157. On information and belief, Comcast's infringement has been and continues to be willful.

158. Plaintiffs have been harmed by Comcast's infringing activities.

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

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

160. 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."

161. Upon information and belief, Comcast 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 Xfinity X1 TV Boxes,

which by way of example include Arris XG1v3, Arris XG1v4, Arris Xi6, Pace XG1v1, Pace RNG150nP2, and Pace Xi5 (for the purposes of this section, the "Accused Instrumentalities"). (See Ex. 1 at 1–3.)

162. 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, in Comcast Xfinity X1 TV Boxes, Comcast requires its Xfinity X1 TV Boxes to be authenticated when connected to a TV for the first time (i.e. a computer-based method for accessing functionality). The method is performed at least by authentication software (i.e. provided by an application software). Comcast performs this method at least in its testing and development of the Xfinity X1 TV Boxes and the software stored therein.

163. 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, the authentication software is stored in the non-transient memory of the Xfinity X1 TV Boxes. *See* Comcast's Xfinity website page entitled "X1 Activation Process Overview*"* (available online at https://www.xfinity.com/support/articles/x1-stb-activation (last visited Dec. 7, 2018), a copy of which is available as Exhibit 15); Ex. 7 at 2.

164. 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 for

Comcast's Xfinity X1 TV Boxes requires at least the user's last four digits of a phone number and/or verification code. *See* Ex. 15 at 3-4.

165. 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, in Comcast Xfinity X1 TV Boxes, firmware necessary for the proper functioning of the TV Box (i.e. computer configuration information) is stored in non-transient memory, and authentication of the user's account (i.e. a license code) is stored in response to the user entering personalization information. *See* 15 at 3.

166. 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, in order to maintain data security Comcast encrypts the authentication of the user's account (i.e. said license code). Typically, encryption requires the use of a key. Therefore, in order to maintain data security, Comcast authentication software generates a decoding key for use in authorization. *See* Ex. 15 at 6.

167. Furthermore, upon information and belief, Comcast's activation application may work similarly to the way Comcast provides Xfinity service through a CableCARD. CabelCARD authenticates a user via an encrypted "Entitlement Control Message." Comcast's authentication through the Xfinity X1 TV Boxes' authentication software also generates a key

using the license code. *See* Nate Anderson's article entitled "CableCARD: A Primer" (available online at https://arstechnica.com/gadgets/2006/02/cablecard/2/ (last visited Dec. 7, 2018), a copy of which is available as Exhibit 23.) Alternatively, Comcast's authentication software generates a key for comparison with other encrypted authentication information stored on another Xfinity X1 device installed in a user's home. Therefore, in order to tie the devices together, generating the key must include the user's account information. *See* Ex. 15 at 8.

168. 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, Xfinity TV Boxes cannot access any digital TV content (i.e. at least at least one encoded code resource of said application software) unless the user's account (i.e. license code) has been verified (i.e. stored in said personalization data resource). *See* Ex. 15 at 1.

169. Upon information and belief, since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.), Comcast 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 Comcast's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 1 of the '602 patent Additionally, Comcast induces the users of the Xfinity X1 TV Boxes to perform the method described above in the claims by instructing them how to authenticate the Box when connected to a TV for the first time. *See* Ex. 15 at 3-4.

170. In particular, Comcast'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 Comcast has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Comcast 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 August 27, 2018 in 6:18-CV-181 (E.D. Tex.).

171. On information and belief, Comcast's infringement has been and continues to be willful.

172. Plaintiffs have been harmed by Comcast's infringing activities.

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

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

174. 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."

175. Upon information and belief, Comcast 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 Xfinity X1 TV Boxes, which by way of example include Arris XG1v3, Arris XG1v4, Arris Xi6, Pace XG1v1, Pace RNG150nP2, and Pace Xi5 (for the purposes of this section, the "Accused Instrumentalities"). (See Ex. 1 at 1–3.)

176. 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, Comcast requires its

Xfinity X1 TV Boxes to be authenticated when connected to a TV for the first time (i.e. a method for licensed software use). The method is performed at least by the activation application. As noted above, Comcast performs this method at least in its testing and development of the Xfinity X1 TV Boxes and the software stored therein.

177. 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 an Xfinity X1 TV Box for the first time the activation application (i.e. software produce) is loaded onto the TV Box (computer) so that the TV Box executes the activation application. *See* Ex. 15 at 1. Furthermore, the Xfinity X1 TV Box includes a processor, memory, an input, and an output. *See* Ex. 8 at 2; Ex. 6 at 4; Ex. 4 at 2.

178. 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 noted above, part of the activation process, the activation application prompts a user for the user's last four digits of the phone number and/or a verification code (i.e. input of license information). *See* Ex. 15 at 3-4.

179. 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, and as noted above, as part of the activation process the

activation application prompts a user for the user's last four digits of the phone number and/or a verification code to decode license information associated with the user's account (i.e. a first license code) encoded in the activation application. *See* Ex. 15 at 6.

180. Upon information and belief, since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.), Comcast 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 Comcast's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 1 of the '842 patent. Additionally, Comcast induces the users of the Xfinity X1 TV Boxes to perform the method by instructing them how to authenticate the Box when connected to a TV for the first time. *See* Ex. 15 at 3-4.

181. In particular, Comcast'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 Comcast has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Comcast 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 August 27, 2018 in 6:18-CV-181 (E.D. Tex.).

182. On information and belief, Comcast's infringement has been and continues to be willful.

183. Plaintiffs have been harmed by Comcast's infringing activities.

COUNT VIII – INFRINGEMENT OF U.S. PATENT NO. 8,224,705

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

185. On July 17, 2012, the '705 patent was duly and legally issued by the United States Patent and Trademark Office under the title "Methods, Systems and Devices for Packet Watermarking and Efficient Provisioning of Bandwidth."

186. Upon information and belief, Comcast has and continues to directly infringe one or more claims of the '705 patent by selling, offering for sale, using, and/or providing and causing to be used products and/or services, specifically one or more Xfinity X1 TV Boxes, which by way of example include Arris XG1v3, Arris XG1v4, Arris Xi6, Pace XG1v1, Pace RNG150nP2, and Pace Xi5 (for the purposes of this section, the "Accused Instrumentalities"). (See Ex. 1 at 1–3.)

187. Upon information and belief, the Accused Instrumentalities infringe at least claim 8 of the '705 patent. The Accused Instrumentalities include an electronic method for selling at least one item and/or service said method. Said electronic method is found within the Accused Instrumentalities. For example, Comcast sells live television and video on demand services, including individual pay-per-view ("PPV") content items. Thus, Comcast performs an electronic method for selling at least one item and/or service. *See* Ex. 5 at 1; Comcast's Xfinity website page entitled "Order a Pay Per View Event on X1*"* (available online at https://www.xfinity.com/support/articles/ (last visited Oct. 1, 2018), a copy of which is available as Exhibit 11.)

188. Upon information and belief, the Accused Instrumentalities include an electronic method for selling at least one item and/or service said method, establishing a communication link between a vending system and a purchasing system; and transmitting a stream of data

comprising a plurality of packets using a packet watermark protocol. Said electronic method is found in the Accused Instrumentalities. For example, when a Comcast subscriber watches a live TV channel or a PPV item, a communication link is established between a Comcast network element (i.e. vending system), such as a server, and the subscriber's cable modem ("CM") (i.e. purchasing system) to deliver a selected live TV channel or PPV item. The lice TV channel or PPV item is delivered in a stream of data, and communication between the Comcast server and the cable modem is performed in accordance with the DOCSIS 3.1 standard (i.e. packet watermark protocol). The subscriber's DOCSIS 3.1-compatible cable modem is model Comcast XB6. *See* Jorge Salinger's presentation entitled "Comcast's Network Architecture*"* (available online at https://slideplayer.com/slide/11325893/ (last visited Dec. 7, 2018), a copy of which is available as Exhibit 19); DOCSIS 3.1 Security Specification, CM-SP-SECV3.1-I07-170111, §1.25 at 13 (attached hereto as Exhibit 22 at 13); "Comcast Broadens DOCSIS 3.1 Rollout," March 29, 2018, available at https://www.multichannel.com/news/comcast-broadens-docsis-3-1-rollout (last accessed October 4, 2018) (attached hereto as Exhibit 20); Jeff Baumgartner article entitled "Comcast Taps Arris, Technicolor for 'XB6' Gateways: Sources" (available online at https://www.multichannel.com/news/comcast-taps-arris-technicolor-xb6-gateways-sources-409944 (last visited Dec. 7, 2018), a copy of which is available as Exhibit 21.)

189. Upon information and belief, the Accused Instrumentalities include an electronic method for selling at least one item and/or service said method, generating a packet watermark associated with the stream of data wherein the packet watermark enables identification of at least one of the plurality of packets; and combining the packet watermark with each of the plurality of packets to form watermarked packets. Said electronic method is found within the Accused Instrumentalities. For example, the DOCSIS 3.1 defines a Base Line Privacy Plus ("BPI+")

architecture that applies to various communication between a CM and upstream network nodes, such as a cable modem termination system ("CMTS"). A DOCSIS 3.1 CM must support a primary security association ("SA") and fifteen additional SAs that can be used as dynamic SAs or static SAs. A CMTS must support a primary SA for each CM and at least one dynamic SA per CMTS. A SA's shared information includes the cryptographic suite in use, traffic encryption keys, and lifetime (i.e., expiration period) of associated keying information. Each SA is identified with a 14-bit handle called a security association identifier ("SAID"). *See* Ex. 22 at 22-24, 28-34.

190. Furthermore, upon information and belief, the above detailed CM encrypts upstream traffic using its primary SA. Downstream traffic can be encrypted using a SA, which varies depending on whether a packet is intended for a single or multiple CMs (e.g., unicast vs. multicast). Upstream and downstream packets either include a SAID or a quality of service ("QoS") service identifier ("SID") that can be used to deduce the relevant SAID. Once the SAID is identified, the receiving device knows how to decrypt the payload of the packet, because the SAID can be used to identify the relevant cryptographic keying information. The generation of the SAID or QoS SID is a generation of a packet watermark that enables identification of packets that correspond to a particular stream/flow, as different streams/flows will be tagged with different SAIDs or QoS SIDs. Each packet of the stream/flow includes the SAID or SID (i.e., the packet watermark is combined with each packet to form watermarked packets), and DOCSIS 3.1 defines several packet formats to choose from. These packet formats include a variable-length PDU MAC frame format, a fragmentation MAC frame format, and a registration request (REG-REQ-MP) MAC management message format. *See* Ex. 22 at 22-24, 28-34.

191. Upon information and belief, the Accused Instrumentalities include an electronic method for selling at least one item and/or service said method, wherein the transmitting is for at least one of the following: receiving a request to purchase a selected item; determining a purchase value for the selected item; causing a debit to the purchaser's account in an amount of bandwidth usage which corresponds to the agreed upon value for the selected item; and sending an instruction to deliver the selected item. Said electronic method is found in the Accused Instrumentalities. For example, in the context of a live TV channel, the DOCSIS 3.1 communication identified in the previous paragraphs is, *inter alia*, for sending an instruction to deliver the selected TV channel. Furthermore, in the context of a PPV item, the DOCSIS 3.1 communication identified in the previous paragraphs is, *inter alia*, for receiving a request to purchase the selected PPV item and/or sending an instruction to deliver the selected PPV item. *See* Ex. 5 at 1; Ex 11 at 1.

192. Upon information and belief, since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.), Comcast has induced and continues to induce others to infringe at least claim 8 of the '705 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 Comcast's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 8 of the '705 patent. Additionally, Comcast uses the Xfinity X1 TV Boxes for its own testing and use, as well as inducing its customers to use the Xfinity X1 TV Boxes in an electronic method for selling at least one item and/or service.

193. In particular, Comcast'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, Comcast has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Comcast has had actual knowledge of the '705 patent and that its acts were inducing infringement of the '705 patent since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.).

194. On information and belief, Comcast's infringement has been and continues to be willful.

195. Plaintiffs have been harmed by Comcast's infringing activities.

COUNT IX – INFRINGEMENT OF U.S. PATENT NO. 7,287,275

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

197. On October 23, 2007, the '275 patent was duly and legally issued by the United States Patent and Trademark Office under the title "Methods, Systems and Devices for Packet Watermarking and Efficient Provisioning of Bandwidth."

198. Upon information and belief, Comcast has and continues to directly infringe one or more claims of the '275 patent by using, and/or providing and causing to be used products and/or services, specifically one or more Comcast servers used to transmit a stream of data, including, for example, when Xfinity television or Internet access services are provided (for the purposes of this section, the "Accused Instrumentalities"). (See Ex. 1 at 1–3.)

199. Upon information and belief, the Accused Instrumentalities infringe at least claim 1 of the '275 patent. The Accused Instrumentalities include a method for transmitting a stream of data. Said method is found within the Accused Instrumentalities. For example, Comcast performs a method for transmitting a stream of data, including when Xfinity TV or data (e.g. Internet access) services are provided.

200. Upon information and belief, the Accused Instrumentalities include a method for transmitting a stream of data, receiving a stream of data; organizing the stream of data into a plurality of packets. Said method is found within the Accused Instrumentalities, as illustrated by internal Comcast documents regarding Comcast's network architecture label subscriber devices as Internet Protocol ("IP") hosts. Therefore, communication between a network element (e.g. a server or CMTS) and the subscriber devices is in the form of packets. Accordingly, when a subscriber watches a live TV channel or a PPV item, a Comcast network element receives a stream of data corresponding to the live TV channel or PPV item and organizes the stream of data into packets for transmission. *See* Ex. 5 at 1; Ex. 11 at 1; Ex. 19 at 29; Ex. 22 at 13.

201. Upon information and belief, the Accused Instrumentalities include a method for transmitting a stream of data, generating a packet watermark associated with the stream of data wherein the packet watermark enables identification of at least one of the plurality of packets; combining the packet watermark with each of the plurality of packets to form watermarked patents. Said method is found within the Accused Instrumentalities. For example, and as noted above, communication with the subscriber's CM is performed in accordance with the DOCSIS 3.1 standard. The subscriber's DOCSIS 3.1-compatible cable modem is model Comcast XB6. DOCSIS 3.1 defines a BPI+ architecture that applies to various communication between a CM and upstream network nodes, such as a CMTS. A DOCSIS 3.1 CM must support a primary SA and 15 additional SAs that can be used as dynamic SAs or static SAs. A CMTS must support a primary SA for each CM and at least one dynamic SA (per CMTS). A SA's shared information includes the cryptographic suite in use, traffic encryption keys, and lifetime (i.e., expiration period) of associated keying information. Each SA is identified with a 14-bit handle called a SAID. *See* Jeff Baumgartner article entitled "Comcast Broadens DOCSIS 3.1 Rollout"

(available online at https://www.multichannel.com/news/comcast-broadens-docsis-3-1-rollout (last visited Dec. 7, 2018), a copy of which is available as Exhibit 20); Ex. 21 at 1; Ex. 22 at 22-24, 28-33.

202. Furthermore, upon information and belief, the CM encrypts upstream traffic using its primary SA. Downstream traffic can be encrypted using a SA that varies depending on whether a packet is intended for a single or multiple CMs (e.g., unicast vs. multicast). As noted above, upstream and downstream packets either include a SAID or a QoS SID that can be used to deduce the relevant SAID. Once the SAID is identified, the receiving device knows how to decrypt the payload of the packet, because the SAID can be used to identify the relevant cryptographic keying information. The generation of the SAID or QoS SID is generation of a packet watermark that enables identification of packets that correspond to a particular stream/flow, as different streams/flows will be tagged with different SAIDs or QoS SIDs. Each packet of a stream/flow includes the SAID or SID (i.e., the packet watermark is combined with each packet to form watermarked packets), and DOCSIS 3.1 defines several packet formats to choose from. These packet formats include a variable-length PDU MAC frame format, a fragmentation MAC frame format, and a registration request (REG-REQ-MP) MAC management message format. *See* Ex. 20 at 2; Ex. 21 at 1; Ex. 22 at 22-24, 28-33. The watermarked packets are transmitted across Comcast's distribution network, as indicated by the fact that the subscriber is able to successfully watch a live TV channel or a PPV item, access a website on the internet, etc.

203. Upon information and belief, since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.), Comcast has induced and continues to induce others to infringe at least claim 1 of the '275 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 Comcast's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 1 of the '275 patent.

204. In particular, Comcast'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 Comcast has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Comcast has had actual knowledge of the '275 patent and that its acts were inducing infringement of the '275 patent since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.). Additionally, Comcast uses Xfinity television or Internet access services for its own testing and use, as well as inducing its customers to use Xfinity television or Internet access services in a method for securely transmitting a stream of data.

205. On information and belief, Comcast's infringement has been and continues to be willful.

206. Plaintiffs have been harmed by Comcast's infringing activities.

COUNT X – INFRINGEMENT OF U.S. PATENT NO. 8,473,746

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

208. On June 25, 2013, the '746 patent was duly and legally issued by the United States Patent and Trademark Office under the title "Methods, Systems and Devices for Packet Watermarking and Efficient Provisioning of Bandwidth."

209. Upon information and belief, Comcast has and continues to directly infringe one or more claims of the '746 patent by using, and/or providing and causing to be used products

and/or services, specifically one or more Comcast servers used to transmit a stream of data, including, for example, when Xfinity television or Internet access services are provided (for the purposes of this section, the "Accused Instrumentalities"). (See Ex. 1 at 1–3.)

210. Upon information and belief, the Accused Instrumentalities infringe at least claim 9 of the '746 patent. The Accused Instrumentalities include a method for generating a watermarked packet. Said method is found within the Accused Instrumentalities. For example, and as noted above, Comcast performs a method for generating a watermarked packet including, as noted above, when Xfinity TV or data (e.g. Internet access) services are provided.

211. Upon information and belief, the Accused Instrumentalities include a method for generating a watermarked packet comprising a processor applying an algorithm to at least (1) a packet watermark and (2) packet content, thereby generating a watermark identification ("WID"). Said method is found within the Accused Instrumentalities. For example, and as noted above, internal Comcast documents regarding Comcast's network architecture label subscriber devices as Internet Protocol ("IP") hosts. Therefore, upstream communication from a subscriber's cable modem (CM) and a network element (e.g., server or CMTS) and a subscriber device is in the form of packets. Comcast's DOCSIS 3.1 compatible CM is the XB6, which upon information and belief includes a processor. *See* Ex. 5 at 1; Ex. 11 at 1; Ex. 19 at 29; Ex. 22 at 13; Ex. 20 at 2; Ex. 21 at 1; Ex. 22 at 22-24, 28.

212. Furthermore, upon information and belief, as noted above the DOCSIS 3.1 defines a BPI+ architecture that applies to various communication between a CM and upstream network nodes, such as a CMTS. A DOCSIS 3.1 CM must support a primary SA and 15 additional SAs that can be used as dynamic SAs or static SAs. A CMTS must support a primary SA for each CM and at least one dynamic SA (per CMTS). A SA's shared information includes

the cryptographic suite in use, traffic encryption keys, and lifetime (i.e., expiration period) of associated keying information. Each SA is identified with a 14-bit SAID. *See* Ex. 5 at 1; Ex. 19 at 29; Ex. 22 at 13; Ex. 20 at 2; Ex. 21 at 1; Ex. 22 at 22-24, 28.

213. Additionally, upon information and belief, as noted above the CM encrypts upstream traffic using its primary SA. Downstream traffic can be encrypted using a SA that varies depending on whether a packet is intended for a single or multiple CMs (e.g., unicast vs. multicast). Upstream and downstream packets either include a SAID or a QoS SID that can be used to deduce the relevant SAID. Once the SAID is identified, the receiving device knows how to decrypt the payload of the packet, because the SAID can be used to identify the relevant cryptographic keying information. The SAID or QoS SID is a packet watermark and the encrypted payload of the packet is the packet content, and the processor of the XB6 generates a watermark identification based on the combination of the two. *See* Ex. 5 at 1; Ex. 19 at 29; Ex. 22 at 13; Ex. 20 at 2; Ex. 21 at 1; Ex. 22 at 22-24, 28.

214. Upon information and belief, the Accused Instrumentalities include a method for generating a watermarked packet wherein said packet content is less than all data of a data object. Said method is found within the Accused Instrumentalities. For example, DOCSIS 3.1 defines several packet formats to choose from, including a fragmentation MAC frame format. The fragmentation MAC fram format is used when the packets are fragments of a larger upstream MAC frame (i.e. the packet content is less than all of a data object). *See* Ex. 22 at 31-32.

215. Upon information and belief, the Accused Instrumentalities include a processor generating a watermarked packet comprising said packet watermark and at least some of said packet content. Said processor is found within the Accused Instrumentalities. For example, as

noted above watermarked packets are transmitted across Comcast's distribution network, as indicated by the fact that the subscriber is able to successfully watch a live TV channel or a PPV item, access a website on the Internet, etc. Each of the packets transmitted in accordance with the fragmentation MAC frame format includes the packet watermark (SID) and an encrypted payload (packet content). A processor in the CM generates the packets.

216. Upon information and belief, since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.), Comcast has induced and continues to induce others to infringe at least claim 9 of the '746 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 Comcast's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 9 of the '746 patent. Additionally, Comcast uses Xfinity television or Internet access services for its own testing and use, as well as inducing its customers to use Xfinity television or Internet access services in a method for securely transmitting a stream of data.

217. In particular, Comcast'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 Comcast has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Comcast has had actual knowledge of the '746 patent and that its acts were inducing infringement of the '746 patent since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.).

218. On information and belief, Comcast's infringement has been and continues to be willful.

219. Plaintiffs have been harmed by Comcast's infringing activities.

COUNT XI – INFRINGEMENT OF U.S. PATENT REISSUE NO. RE 44,222

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

221. On May 14, 2013, the '222 patent was duly and legally reissued by the United States Patent and Trademark Office under the title "Methods, Systems and Devices for Packet Watermarking and Efficient Provisioning of Bandwidth."

222. Upon information and belief, Comcast has and continues to directly infringe one or more claims of the '222 patent by using, and/or providing and causing to be used products and/or services, specifically one or more Comcast servers used to transmit a stream of data, including, for example, when Xfinity television or Internet access services are provided (for the purposes of this section, the "Accused Instrumentalities"). (See Ex. 1 at 1–3.)

223. Upon information and belief, the Accused Instrumentalities infringe at least claim 1 of the '222 patent. The Accused Instrumentalities include a process for transmitting a stream of data. Said process is found within the Accused Instrumentalities. For example, and as noted above, when Comcast performs a method for transmitting a stream of data, including when Xfinity TV or data (e.g. Internet access) services are provided.

224. Upon information and belief, the Accused Instrumentalities include a process for transmitting a stream of data, receiving a stream of data; organizing the stream of data into a plurality of packets. Said process is found within the Accused Instrumentalities. As noted above, said process is illustrated by internal Comcast documents regarding Comcast's network architecture label subscriber devices as IP hosts. This demonstrates communication between a network element (e.g. a server or CMTS) and the subscriber devices is in the form of packets. Accordingly, when a subscriber watches a live TV channel or a pay per view (PPV) item, a

Comcast network element receives a stream of data corresponding to the live TV channel or PPV item and organizes the stream of data into packets for transmission. *See* Ex. 5 at 1; Ex. 11 at 1; Ex. 19 at 29; Ex. 22 at 13.

225. Upon information and belief, the Accused Instrumentalities include a process for transmitting a stream of data, generating a packet watermark associated with the stream of data wherein the packet watermark enables identification of at least one of the plurality of packets; combining the packet watermark with each of the plurality of packets to form watermarked patents. For example, and as noted above, said process is found within the Accused Instrumentalities when communication with the subscriber's CM is performed in accordance with the DOCSIS 3.1 standard. The subscriber's DOCSIS 3.1-compatible cable modem is model Comcast XB6. DOCSIS 3.1 defines a BPI+ architecture that applies to various communication between a CM and upstream network nodes, such as a CMTS. A DOCSIS 3.1 CM must support a primary SA and 15 additional SAs that can be used as dynamic SAs or static SAs. A CMTS must support a primary SA for each CM and at least one dynamic SA (per CMTS). A SA's shared information includes the cryptographic suite in use, traffic encryption keys, and lifetime (i.e., expiration period) of associated keying information. Each SA is identified with a 14-bit SAID. *See* Ex. 20 at 2; Ex. 21 at 1; Ex. 22 at 22-24, 28-33.

226. Furthermore, upon information and belief, the CM encrypts upstream traffic using its primary SA. Downstream traffic can be encrypted using a SA that varies depending on whether a packet is intended for a single or multiple CMs (e.g., unicast vs. multicast). Upstream and downstream packets either include a SAID or a QoS SID, which can be used to deduce the relevant SAID. Once the SAID is identified, the receiving device knows how to decrypt the payload of the packet because the SAID can be used to identify the relevant cryptographic

keying information. The generation of the SAID or QoS SID is generation of a packet watermark that indicates packet integrity, as unauthorized devices would not be in possession of the necessary keying information to decrypt packet payloads. Each packet of a stream/flow includes the SAID or SID (i.e., the packet watermark is combined with each packet to form watermarked packets), and DOCSIS 3.1 defines several packet formats to choose from. These packet formats include a variable-length PDU MAC frame format, a fragmentation MAC frame format, and a registration request (REG-REQ-MP) MAC management message format. *See* Ex. 20 at 2; Ex. 21 at 1; Ex. 22 at 22-24, 28-33.

227. Upon information and belief, the Accused Instrumentalities include a process for transmitting a stream of data, transmitting at least one of the watermarked packets across a network. Said process is found within the Accused Instrumentalities. For example, the watermarked packets are transmitted across Comcast's distribution network. As noted above, this is indicated by the fact that the subscriber is able to successfully watch a live TV channel or a PPV item, access a website on the Internet, etc.

228. Upon information and belief, since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.), Comcast has induced and continues to induce others to infringe at least claim 1 of the '222 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 Comcast's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 1 of the '222 patent.

229. In particular, Comcast'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 Comcast

has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Comcast has had actual knowledge of the ‘222 patent and that its acts were inducing infringement of the ‘222 patent since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.).

230. On information and belief, Comcast’s infringement has been and continues to be willful.

231. Plaintiffs have been harmed by Comcast’s infringing activities.

COUNT XII – INFRINGEMENT OF U.S. PATENT REISSUE NO. RE 44,307

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

233. On June 18, 2013, the ‘307 Patent was duly and legally reissued by the United States Patent and Trademark Office under the title “Methods, Systems and Devices for Packet Watermarking and Efficient Provisioning of Bandwidth.”

234. Upon information and belief, Comcast has and continues to directly infringe one or more claims of the ‘307 Patent by using, and/or providing and causing to be used products and/or services, specifically one or more Comcast servers used to transmit a stream of data, including, for example, when Xfinity television or Internet access services are provided (for the purposes of this section the “Accused Instrumentalities”). (See Ex. 1 at 1–3.)

235. Upon information and belief, the Accused Instrumentalities infringe at least claim 19 of the ‘307 patent. The Accused Instrumentalities include a method of authenticating a packet flow. Said method is found within the Accused Instrumentalities. For example, and as noted above, Comcast performs a method of authenticating a packet flow, including when Xfinity TV or data (e.g. Internet access) services are provided.

236. Upon information and belief, the Accused Instrumentalities include a method of authenticating a packet flow, receiving digital content, organizing the digital content into a packet flow comprising at least two packets. Said method is found within the Accused Instrumentalities. For example, and as noted above, said method is illustrated by internal Comcast documents regarding Comcast's network architecture label subscriber devices as IP hosts. This demonstrates communication between a network element (e.g., server or CMTS) and the subscriber devices is in the form of packets. Accordingly, when a subscriber watches a live TV channel or a PPV item, a Comcast network element receives a stream of data corresponding to the live TV channel or PPV item and organizes the stream of data into packets for transmission. *See* Ex. 5 at 1; Ex. 11 at 1; Ex. 19 at 29; Ex. 22 at 13.

237. Upon information and belief, the Accused Instrumentalities include a method of authenticating a packet flow, generating at least a portion of a packet watermark associated with at least one of the packets, the packet watermark being associated with authentication data, combining at least one portion of a packet watermark, and at least one packet, for transmission across a network. Said method is found within the Accused Instrumentalities. For example, and as noted above, communication with the subscriber's CM is performed in accordance with the DOCSIS 3.1 standard. The subscriber's DOCSIS 3.1-compatible CM is model Comcast XB6. The DOCSIS 3.1 defines a BPI+ architecture that applies to various communication between a CM and upstream network nodes, such as a CMTS. A DOCSIS 3.1 CM must support a SA and fifteen additional SAs that can be used as dynamic SAs or static SAs. A CMTS must support a primary SA for each CM and at least one dynamic SA per CMTS. A SA's shared information includes the cryptographic suite in use, traffic encryption keys, and lifetime (i.e., expiration

period) of associated keying information. Each SA is identified with a 14-bit SAID. *See* Ex. 20 at 2; Ex. 21 at 1; Ex. 22 at 22-24, 28-34.

238. Furthermore, upon information and belief, as previously noted the above detailed CM encrypts upstream traffic using its primary SA. Downstream traffic can be encrypted using a SA that varies depending on whether a packet is intended for a single or multiple CMs (e.g., unicast vs. multicast). Upstream and downstream packets either include a SAID or a QoS SID that can be used to deduce the relevant SAID. Once the SAID is identified, the receiving device knows how to decrypt the payload of the packet, because the SAID can be used to identify the relevant cryptographic keying information. The generation of the SAID or QoS SID is generation of a packet watermark that is associated with authentication data, as unauthorized devices would not be in possession of the necessary keying information to decrypt packet payloads. Each packet of the stream/flow includes the SAID or SID (i.e., the packet watermark is combined with each packet to form watermarked packets), and DOCSIS 3.1 defines several packet formats to choose from. These packet formats include a variable-length PDU MAC frame format, a fragmentation MAC frame format, and a registration request (REG-REQ-MP) MAC management message format. *See* Ex. 20 at 2; Ex. 21 at 1; Ex. 22 at 22-24, 28-34.

239. Upon information and belief, the Accused Instrumentalities include a method of authenticating a packet flow, receiving the combined at least one portion of a packet watermark, and at least one packet that has been transmitted across the network; analyzing the combined at least one portion of a packet watermark, and at least one packet using at least a portion of the packet watermark; and in the event the analysis indicates authentication of at least one packet, permitting the authentication of the packet, permitting the authentication of the packet flow, and in the event that the analysis indicates tampering of the at least one packet, indicating a signal of

non-authentication. Said method is found within the Accused Instrumentalities. For example, when the watermarked packets are received at the subscriber's CM (e.g., the DOCSIS 3.1 compatible Comcast XB6). The subscriber's CM analyzes the watermarked packets by determining the SAID/SID and checking if the corresponding keying information is available. If the keying information is available, the watermarked packet's payload is decrypted (i.e. permitting the authentication of the packet flow), as indicated by the subscriber being able to watch the selected live TV channel or PPV item, or access the requested Internet website. If the CM is not authorized, one or more Reject messages are communicated based on operation of state machines that control authorization and keying. *See* Ex. 22 at 42-43, 49.

240. Upon information and belief, since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.), Comcast has induced and continues to induce others to infringe at least claim 19 of the '307 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 Comcast's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 19 of the '307 Patent. Additionally, Comcast uses Xfinity television or Internet access services for its own testing and use, as well as inducing its customers to use Xfinity television or Internet access services in a method for securely transmitting a stream of data.

241. In particular, Comcast'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 Comcast has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Comcast has had actual knowledge of the '307 Patent and

that its acts were inducing infringement of the '307 Patent since at least the time of receiving the Complaint filed on August 27, 2018 in 6:18-CV-181 (E.D. Tex.).

242. On information and belief, Comcast's infringement has been and continues to be willful.

243. Plaintiffs have been harmed by Comcast'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 Comcast as follows:

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

B. An award of damages to be paid by Comcast adequate to compensate Plaintiffs Blue Spike LLC, Blue Spike Int., and Wistaria for Comcast's past infringement of the patents in suit.

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 Blue Spike LLC, Blue Spike Int., and Wistaria of such further relief at law or in equity as the Court deems just and proper.

Dated: January 28, 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.