IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TEXARKANA DIVISION

SIPCO, LLC,

Plaintiff,

v.

COMMSCOPE HOLDING COMPANY, INC.,
COMMSCOPE INC.,
RUCKUS WIRELESS, INC.,
ARRIS US HOLDINGS, INC.,
ARRIS ENTERPRISES LLC, and
ARRIS SOLUTIONS, INC.

Defendants.

Civil Action No. 5:20-cv-00168-RWS-CMC

COMPLAINT AND
DEMAND FOR JURY TRIAL

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff SIPCO, LLC ("SIPCO"), by and through its undersigned counsel, files this complaint under 35 U.S.C. § 271 for Patent Infringement against Defendants Ruckus Wireless Inc. ("Ruckus"); ARRIS US Holdings, Inc., ARRIS Enterprises LLC, and ARRIS Solutions, Inc., (collectively "ARRIS"); and CommScope Holding Company, Inc., and CommScope Inc. (collectively "CommScope") (all, collectively, "Defendants"), and further alleges as follows, upon actual knowledge with respect to itself and its own acts, and upon information and belief as to all other matters.

OVERVIEW

1. Plaintiff SIPCO is a small research, development and technology company now based in Virginia. T. David Petite is a founding member of the company.

2. In the 1990s, through his own individual research and development efforts, Mr. Petite invented a large number of wireless control and distribution technology applications. The inventions resulting from Mr. Petite's efforts include, but are not limited to, various ways of moving data as economically and seamlessly as possible over both wired and wireless networks.

3. Through the 1990s and early 2000s investors contributed tens of millions of dollars for technology development and implementation of networks. Clients included Georgia Power, Alabama Power, Newnan Utilities GA, Johnson Controls, Synovus Bank and Grand Court Lifestyles residential living facilities.

4. After proving that the technology worked in the field, several companies competed to purchase an exclusive license to Mr. Petite's technology for the market known as "smart grid." Landis+Gyr (http://www.landisgyr.com/) (previously Siemens Metering) took an exclusive license to the smart grid technology in 2002 and in 2005 purchased rights to the technology for utility applications for $30,000,000. Mr. Petite's technology has been deployed in millions of meters deployed across North America and throughout the world.

5. SIPCO retained the rights to the mesh network patents, and for use of the technology outside of the utility space. It still maintains ownership of the software, firmware, hardware and patent portfolio that resulted from Mr. Petite's research and development efforts, and SIPCO continues to develop and deploy wireless technology applications and wireless technology systems throughout the United States.

6. SIPCO's patent portfolio (of which the patents-in-suit are a part) include inventions that are widely recognized as pioneering in various fields of use. As a result, more than 100 companies have taken licenses to them. Licensees include companies operating in the vertical markets of Industrial Controls, Lighting, Smart Grid, Building Automation, Network Backhaul,

Home Appliance, Home Automation and Entertainment, Sensor Monitoring, and Internet Service Provisioning. Licensed products include products using standard wireless mesh protocols such as WirelessHART, ZigBee, IEEE 802.15.4, and Z-Wave, as well as proprietary wireless protocols such as that marketed by EnOcean.

7. SIPCO is the exclusive owner of all rights, title, and interest in the patents-in-suit, including the right to exclude others and to enforce, sue and recover damages for past and future infringement thereof.

8. This is an action for patent infringement by SIPCO.

PARTIES

9. SIPCO is a limited liability company organized and existing under the laws of the State of Georgia, having its principal office at 13921 Park Center Road, Suite 380, Herndon, Virginia 20171.

10. Upon information and belief, Defendant Ruckus Wireless, Inc. is a corporation organized and existing under the laws of the State of Delaware, with a place of business at 350 West Java Dr., Sunnyvale, CA 94089, and can be served through its counsel of record or registered agent, United Agent Group Inc., 3411 Silverside Road, Tatnall Building, #104, Wilmington, DE 19810. Upon information and belief, Ruckus Wireless, Inc. sells and offers to sell products and services throughout the United States, including in this judicial district, and introduces products and services into the stream of commerce that incorporate infringing technology, knowing that they would be sold in this judicial district and elsewhere in the United States.

11. Upon information and belief, Defendant ARRIS US Holdings, Inc. is a corporation organized and existing under the laws of the State of Delaware, with a place of business at 350 West Java Dr., Sunnyvale, CA 94089, and can be served through its counsel of record or registered

agent, United Agent Group Inc., 3411 Silverside Road, Tatnall Building, #104, Wilmington, DE 19810. Upon information and belief, ARRIS US Holdings, Inc. sells and offers to sell products and services throughout the United States, including in this judicial district, and introduces products and services into the stream of commerce that incorporate infringing technology, knowing that they would be sold in this judicial district and elsewhere in the United States.

12. Upon information and belief, Defendant ARRIS Enterprises LLC is a corporation organized and existing under the laws of the State of Delaware, with a place of business at 350 West Java Dr., Sunnyvale, CA 94089, and can be served through its counsel of record or registered agent, United Agent Group Inc., 3411 Silverside Road, Tatnall Building, #104, Wilmington, DE 19810. Upon information and belief, ARRIS Enterprises LLC sells and offers to sell products and services throughout the United States, including in this judicial district, and introduces products and services into the stream of commerce that incorporate infringing technology, knowing that they would be sold in this judicial district and elsewhere in the United States.

13. Upon information and belief, Defendant ARRIS Solutions, Inc. is a corporation organized and existing under the laws of the State of Delaware, with a place of business at 350 West Java Dr., Sunnyvale, CA 94089, and can be served through its counsel of record or registered agent, United Agent Group Inc., 3411 Silverside Road, Tatnall Building, #104, Wilmington, DE 19810. Upon information and belief, ARRIS Solutions, Inc. sells and offers to sell products and services throughout the United States, including in this judicial district, and introduces products and services into the stream of commerce that incorporate infringing technology, knowing that they would be sold in this judicial district and elsewhere in the United States.

14. Upon information and belief, Defendant CommScope Holding Company, Inc. is a corporation organized and existing under the laws of the State of Delaware, with a place of

business at 1100 CommScope Place, SE, Hickory, North Carolina 28602, and can be served through its counsel of record or registered agent, Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808.

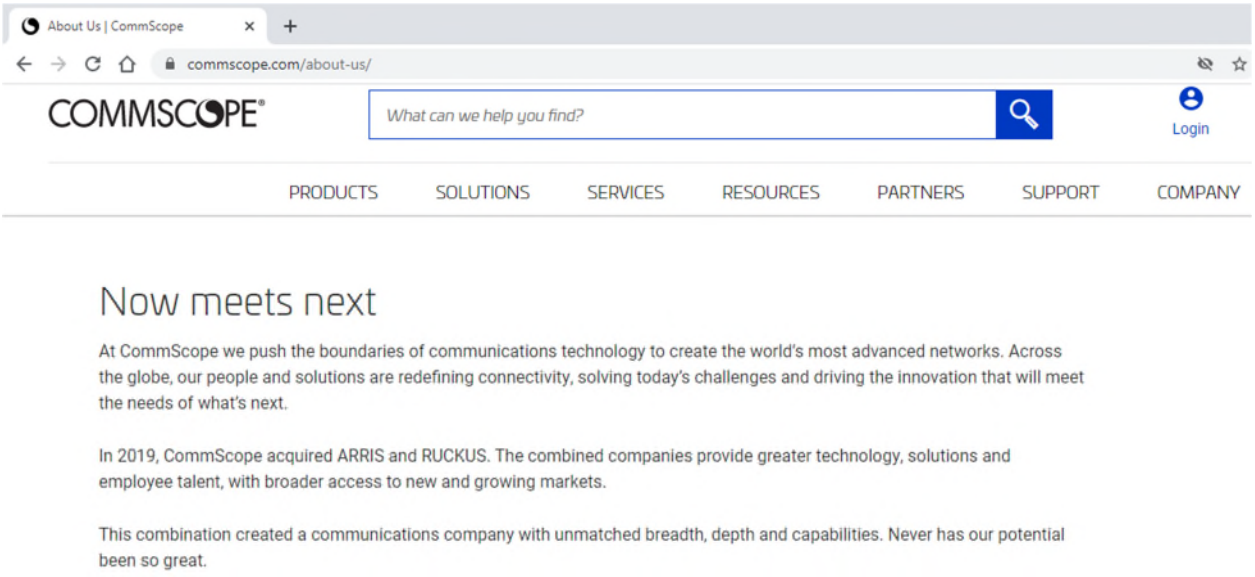
15. Upon information and belief, Defendant CommScope Inc. is a corporation organized and existing under the laws of the State of Delaware, with a place of business at 1100 CommScope Place, SE, Hickory, North Carolina 28602, and can be served through its counsel of record or registered agent, Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808. Upon information and belief, CommScope Inc. is a wholly owned subsidiary of CommScope Holding Company, Inc. (collectively "CommScope"). Upon information and belief, CommScope is doing business, either directly or through its agents, on an ongoing basis in this judicial district and has a regular and established place of business in this judicial district. For example, CommScope maintains and offers the CommScope web domain (www.commscope.com) that advertises the accused products and directs customers and/or potential customers in this district as to where to purchase those products.

16. Upon information and belief, CommScope acquired ARRIS and Ruckus in 2019.

17. Upon information and belief, CommScope controls ARRIS and Ruckus and their decisions regarding importation, manufacture, sale, and/or offers for sale of their products and services throughout the United States. For example, in the CommScope "combined company" the members of the ARRIS leadership team joined the combined company under the direction of the president and chief executive officer of CommScope. For example, in a press release dated February 15, 2019, CommScope's Chief Operating Officer, Morgan Kurk, explained that "[t]he addition of ARRIS and Ruckus to form the new CommScope will enhance our technology leadership throughout the network from the core, through the access, to the edge," and that "he

look[s] forward to helping unlock this potential by driving tighter integration across the company and leadership through the ecosystem."

18. Upon information and belief, Defendants deliberately hold themselves out as a single combined "CommScope" company. The online websites for Defendants are combined into a single "CommScope" presence, which is maintained and offered by CommScope, Inc. For example, the ARRIS web domain (www.arris.com) re-directs the public to the CommScope web domain (www.commscope.com) that explains that the world's leading portfolio of networking solutions include CommScope/Ruckus-branded and CommScope/ARRIS-branded products. Similarly, the former Ruckus web domain (www.ruckuswireless.com) re-directs the public to the CommScope web domain (www.commscope.com) that showcases Defendants' CommScope/Ruckus-branded products and solutions. The CommScope web domain further explains that the companies operate as "combined companies" that provide their technologies, solutions, and products, such as by importation, manufacture, sale, and/or offers for sale of their products and services throughout the United States:



(https://www.commscope.com/about-us). The CommScope web domain also promotes the sale of the accused products, providing instructions and information regarding "how to buy" the products of ARRIS and Ruckus (https://www.commscope.com/resources/how-to-buy/). As another example, ARRIS International's LinkedIn page (https://www.linkedin.com/company/arris), and Ruckus Network's LinkedIn page (https://www.linkedin.com/company/ruckus-networks/), both instruct its visitors to instead visit and follow CommScope's LinkedIn page (http://www.linked.in.com/company/commscope) for news, updates, and job postings. The CommScope webdomain and "Social Networks" that facilitate the above combined presence are maintained and offered by CommScope Inc. (https://www.commscope.com/globalassets/digizuite/3427-terms-and-conditions-for-the-use-of-the-website.pdf). Furthermore, job postings to join the "Ruckus Wireless engineering team" and for "Ruckus Networks, a Commscope company" are found on CommScope's job listings website (*e.g.*, https://jobs.commscope.com/job/Sunnyvale-Director%2C-Wirleess-Hardware-Engineering-Cali/687776400/, and https://jobs.commscope.com/job/Sunnyvale-Principal-Software-Engineer-Cali/684407100/). In addition, a Google search shows various job postings for ARRIS in CommScope's Richardson, Texas location.

19. CommScope is doing business, either directly or through its agents, on an ongoing basis in this judicial district and has a regular and established place of business in this judicial district.

NATURE OF THE ACTION, JURISDICTION, AND VENUE

20. SIPCO brings this action for patent infringement under the patent laws of the United States, 35 U.S.C. § 271 *et seq*.

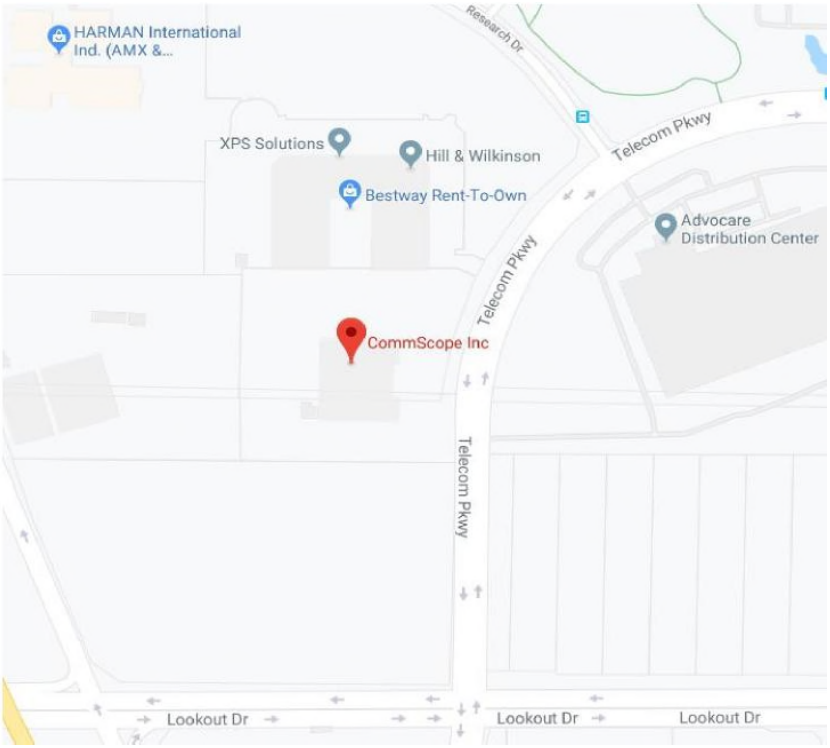
21. This Court has subject matter jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because the action arises under the patent laws of the United States.

22. The Court has personal jurisdiction over the Defendants because, *inter alia* SIPCO's claims arise in whole or in part from Defendants' conduct in Texas, including making, using, offering to sell and/or selling accused products in Texas, and/or importing accused products into Texas, and/or inducing others to commit acts of patent infringement in Texas. For example, CommScope operates offices at which it does business in Texas at 2601 Telecom Parkway, Richardson, Texas 70852; 11312 S. Pipeline Road, Eulees, Texas 76040; and 4101 W. Military Highway A, McAllen Texas 78053.

23. Venue is proper under 28 U.S.C. § 1400(b) and 28 U.S.C. § 1391(b) for at least the same reasons stated above. Plaintiff is informed and believes, and on that basis alleges, that CommScope has committed acts of infringement and has a regular and established place of business in this judicial district.

24. Plaintiff is informed and believes, and on that basis alleges, that CommScope has a regular and established physical place of business in the Eastern District of Texas, including at 2601 Telecom Parkway, Richardson Texas 70852, as depicted below.

(Image showing CommScope's offices at 2601 Telecom Parkway, Richardson TX 75082)



(Map Image showing the location of CommScope's offices at 2601 Telecom Parkway, Richardson TX 75082)

25. CommScope's commission of acts of infringement here, on behalf of itself and the other Defendants, and the presence of a sizeable office at which CommScope does business in the Eastern District of Texas, establishes venue over it under 28 U.S.C. § 1400(b). *See In re Cray, Inc.*, 871 F.3d 1355, 1362 (Fed. Cir. 2017) (describing location sufficient to establish venue as a "physical, geographical location in the district from which the business of the defendant is carried out").

26. Venue in this judicial district is proper as to all Defendants pursuant to 28 U.S.C. § 1391(b)(3) for at least the reason that CommScope, Inc., a defendant in this matter, is subject to the Court's personal jurisdiction with respect to this action.

27. This suit is commenced against Defendants pursuant to 35 U.S.C. § 299 in a single action because (a) a right to relief is asserted against the parties jointly, severally, or in the alternative with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences relating to the making, using, importing into the United States, offering for sale, and/or selling of the same accused products or processes, and (b) questions of fact common to all Defendants will arise in the action.

28. Upon information and belief, Defendants manufacture, sell and/or offer for sale the same products and processes accused in this action.

PATENTS-IN-SUIT

29. Plaintiff, as assignee, is the owner of all right, title, and interest in United States Patent No. 8,924,587, titled "Systems and Methods for Controlling Communication Between a Host Computer and Communication Devices," a true and correct copy of which is attached hereto as Exhibit 1 (the "'587 Patent"). The '587 Patent was duly and legally issued by the USPTO on December 30, 2014.

30. Plaintiff, as assignee, is the owner of all right, title, and interest in United States Patent No. 6,891,838, titled "System and Method for Monitoring and Controlling Residential Devices," a true and correct copy of which is attached hereto as Exhibit 2 (the "'838 Patent"). The '838 Patent was duly and legally issued by the USPTO on May 10, 2005.

31. Plaintiff, as assignee, is the owner of all right, title, and interest in United States Patent No. 7,480,501, titled "System and Method for Transmitting an Emergency Message Over an Integrated Wireless Network," a true and correct copy of which is attached hereto as Exhibit 3 (the "'501 Patent"). The '501 Patent was duly and legally issued by the USPTO no later than January 20, 2009.

32. Plaintiff, as assignee, is the owner of all right, title, and interest in United States Patent No. 8,606,284, titled "Terminal Having Transfer Mode and Network Connection Method," a true and correct copy of which is attached hereto as Exhibit 4 (the "'284 Patent"). The '284 Patent was duly and legally issued by the USPTO on December 10, 2013.

33. Plaintiff, as assignee, is the owner of all right, title, and interest in United States Patent No. 8,666,357, titled "System and Method for Transmitting an Emergency Message Over an Integrated Wireless Network," a true and correct copy of which is attached hereto as Exhibit 5 (the "'357 Patent"). The '357 Patent was duly and legally issued by the USPTO on March 4, 2014.

34. Plaintiff, as assignee, is the owner of all right, title, and interest in United States Patent No. 7,697,492, titled "Systems and Methods for Monitoring and Controlling Remote Devices," a true and correct copy of which is attached hereto as Exhibit 6 (the "'492 Patent"). The '492 Patent was duly and legally issued by the USPTO on April 13, 2010.

35. Collectively, the'587 Patent, '838 Patent, '501 Patent, '284 Patent, '357 Patent, and '492 Patent are referred to herein as the "Patents-in-Suit."

COUNT 1 - INFRINGEMENT OF U.S. PATENT NO. 8,924,587

36. SIPCO incorporates paragraphs 1 through 35 above by reference.

37. Defendants have infringed at least claims 3-8, 13-14, and 16 the '587 Patent in violation of 35 U.S.C. § 271, directly by at least using, manufacturing, importing, supplying, distributing, selling and/or offering for sale products and/or systems, including the Accused Products. .

38. For example, Defendants have infringed at least claim 3 of the '587 Patent literally and/or under the doctrine of equivalents, including by way of example offering for sale and selling (1) Defendants' CommScope/Ruckus-branded IoT-ready Access Points ("APs") supporting

Zigbee in combination with ZoneDirector or SmartZone Controller; and (2) Defendants' CommScope/Ruckus-branded APs supporting Zigbee in unleashed mode (collectively, the "Accused '587 Products"). Exemplary Accused '587 Products include at least the CommScope/Ruckus-branded APs R850, R750, R730, R650, R550, R720, R710, R610, R510, M510, H510, C110, T750, T610, T310, T811-CM, and E510, either with or without Ruckus IoT Module, *e.g.*, i100.

39. Each of the Accused '587 Products can function as a site controller when used in an IEEE802.15.4/Zigbee network ("a wireless communication network") together with compatible third-party Zigbee IoT devices (*e.g.*, Zigbee door lock in ASSA ABLOY Hospitality solution).

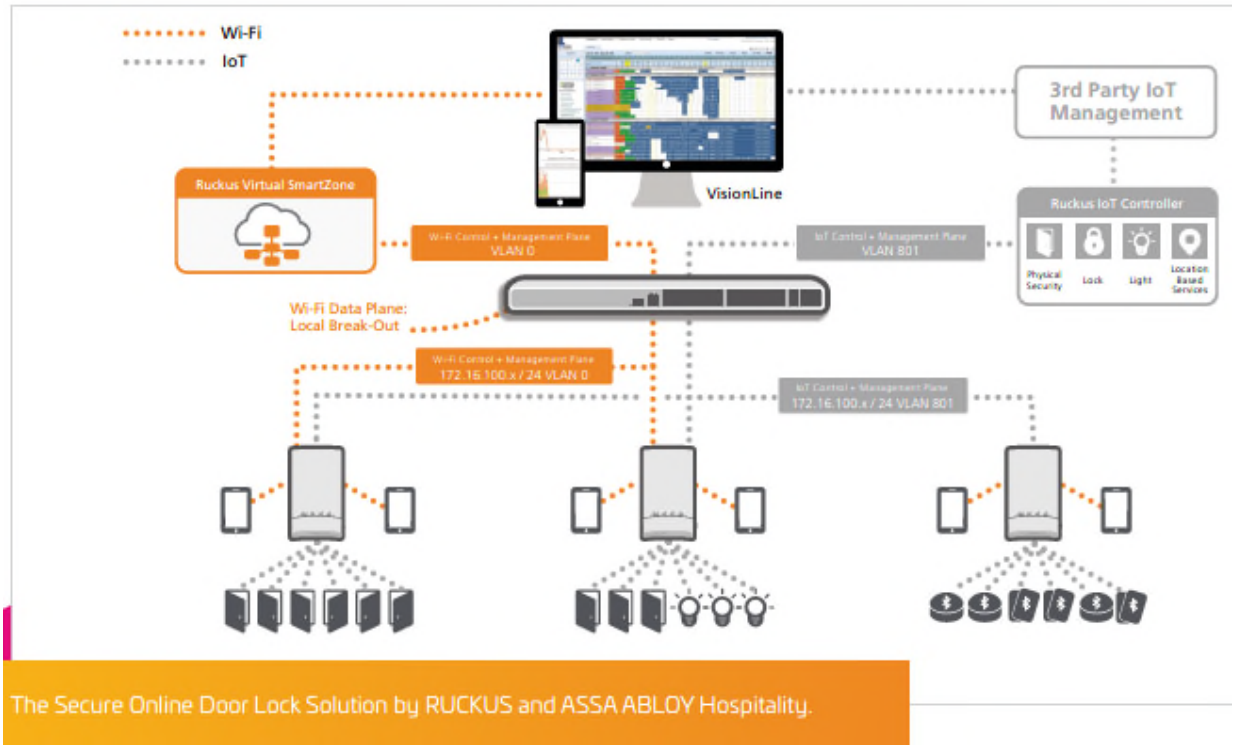
40. Each of the Accused '587 Products includes a transceiver (*e.g.*, a ZigBee radio) configured to receive data messages from one or more wireless transceivers (*e.g.*, the Zigbee radios of compatible third-party Zigbee IoT devices such as the Zigbee door lock in ASSA ABLOY Hospitality solution) of the wireless communication network, each of the one or more wireless transceivers having a unique identifier (*e.g.*, Source IEEE address/Source Address in Zigbee NWK Frame) and configured to receive a sensor data signal from a remote device (*e.g.*, the associated third-party Zigbee IoT devices), the data messages comprising the sensor data signal (*e.g.*, frame payload in Zigbee NWK Frame) and the unique identifier of the corresponding wireless transceiver.

41. Each of the Accused '587 Products further includes a network interface device configured to provide communication between the site controller and a wide area network (*e.g.*, the Internet via Ethernet, Wi-Fi, or cellular connection).

42. Each of the Accused '587 Products is configured to identify remote devices associated with the sensor data signals of the received data messages (*e.g.*, using the Source Address and Source IEEE Address).

43. Each of the Accused '587 Products is further configured to provide information related to the sensor data signals to the wide area network (*e.g.*, the Internet via Ethernet, Wi-Fi, or cellular connection) for access by a network device (*e.g.*, a computer running Defendants' CommScope/Ruckus-branded IoT management software, IoT cloud services, or ASSA ABLOY's Visionline Server).

44. Each of the Accused '587 Products is further configured to transmit a status message (*e.g.*, IEEE802.15.4/Zigbee frames including "Read Attributes Command") to one or more of the remote devices requesting current operating status of the one or more remote devices, wherein the operating status comprises information indicative of a condition monitored and/or controlled (*e.g.*, on/off, closures, temperature, etc.) by the one or more remote devices, receive a first response message (*e.g.*, IEEE/Zigbee frames including "Read Attributes Response Command") comprising the current operating status and identification information of the one or more remote devices, provide information corresponding to the operating status and identification information of the one or more remote devices to the wide area network (*e.g.*, the Internet via Ethernet, Wi-Fi, or cellular connection) for access by the network device (*e.g.*, a computer running Defendants' CommScope/Ruckus-branded IoT management software, IoT cloud services, or ASSA ABLOY's Visionline Server), and determine (*e.g.*, via Zigbee route discovery) and store (*e.g.*, in Zigbee routing tables) upstream and downstream communication paths for the one or more wireless transceivers of the wireless communication network.



(CommScope Ruckus Solution Brief: ASSA ABLOY Delivering Simplified Online Door Lock Solutions, at 2.)

45. The features and capabilities of Defendants' Accused Products reflect Defendants' direct infringement by satisfying every element of at least the aforementioned claims 3-8 of the '587 Patent, under 35 U.S.C. § 271(a).

46. As another example, Defendants have infringed at least claims 13-16 of the '587 Patent, directed to a "site controller for use in a wireless communication network," literally and/or under the doctrine of equivalents, including by way of example installing, setting up, using, and operating the Accused '587 Products within IEEE802.15.4/Zigbee networks, including the (1) CommScope/Ruckus-branded ZoneDirector Series Network Controllers and their associated software, such as the ZoneDirector OS; (2) CommScope/Ruckus-branded SmartZone Series Network Controllers, including their associated software; (3) the CommScope/Ruckus-branded

Cloud service; and (4) the Ruckus APs in "Unleashed" mode, including their associated software, in networks that also include compatible ZigBee IoT devices. Defendants specifically incorporated third-party Zigbee IoT devices to IEEE802.15.4/Zigbee networks including the Accused '587 Products and monitored and controlled the incorporated third-party Zigbee IoT devices using the Accused '587 Products. (*See, e.g.*, https://www.youtube.com/watch?v=JKxriG1fllM (dated June 19, 2019); https://www.youtube.com/watch?v=oqze7km_WlY (dated June 20, 2019).)

47. SIPCO has complied with the provisions of 35 U.S.C. § 287(a) by requiring licensees of its patents to comply with marking requirements, including by requiring licensees of its patents to mark retail products with patent numbers and/or listing products and/or patent numbers on publicly available websites, and undertaking reasonable measures to ensure compliance by its licensees. On information and belief, Defendants gained actual or constructive knowledge of the '587 Patent as a result of this patent marking, and Defendants have therefore been on notice of the '587 Patent.

48. On information and belief, Defendants undertook and continued their infringing actions despite an objectively high likelihood that such activities infringed the '587 Patent, which has been duly issued by the USPTO, and is presumed valid. For example, since, at least the time which Defendants had notice of the '587 Patent and its applicability to their products, Defendants have been aware of an objectively high likelihood that its actions constituted and continue to constitute infringement of the '587 Patent, and that the '587 Patent is valid. On information and belief, Defendants could not reasonably, subjectively believe that its actions do not constitute infringement of the '587 Patent, nor could they reasonably, subjectively believe that the patent is invalid. Despite that knowledge and subjective belief, and despite the objectively high likelihood

that its actions constitute infringement, Defendants have continued its infringing activities. As such, Defendants willfully infringe the ’587 Patent.

49. SIPCO has been damaged by Defendants’ infringement of the ’587 Patent.

COUNT 2 - INFRINGEMENT OF U.S. PATENT NO. 6,891,838

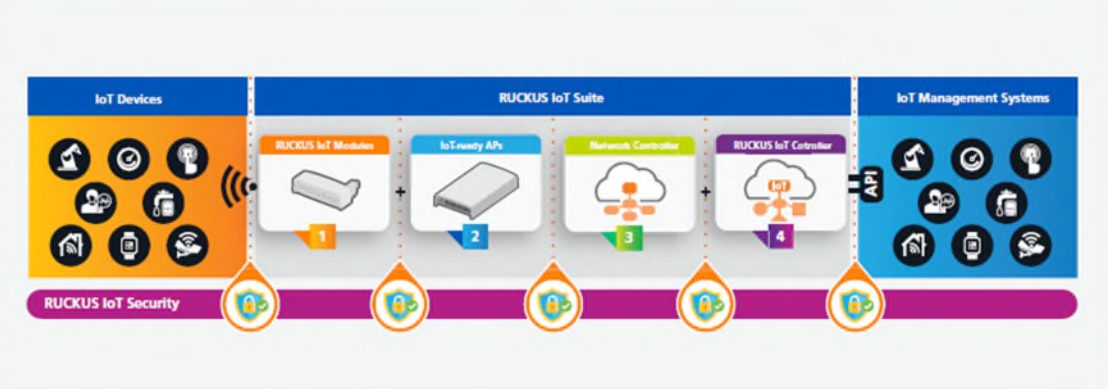
50. SIPCO incorporates paragraphs 1 through 52 above by reference.

51. Defendants have infringed and continue to infringe the ’838 Patent in violation of 35 U.S.C. § 271, directly and/or indirectly by at least using, manufacturing, importing, supplying, distributing, selling and/or offering for sale products and/or systems, including the Accused Products, and/or by contributing to or inducing infringement by others with the intent to cause infringement of the ’838 Patent.

52. For example, Defendants have infringed and continue to infringe at least claim 40 of the ’838 Patent, directed to a “distributed data monitoring and control system,” literally and/or under the doctrine of equivalents, including by way of example offering for sale and selling (1) Defendants’ CommScope/Ruckus-branded IoT-Ready and SmartMesh-enabled APs; (2) Defendants’ CommScope/ARRIS-branded IoT-Ready HomeAssure gateways, and (3) Defendants’ CommScope/ARRIS-branded IoT-Ready Smart Media Devices (collectively, the “Accused ’838 Products”). Exemplary Accused ’838 Products include at least Defendants’ CommScope/Ruckus-branded APs R850, R750, R730, R650, R550, R720, R710, R610, R510, M510, H510, C110, T750, T610, T310, T811-CM, E510, either with or without a Ruckus IoT Module, *e.g.*, i100; Defendants’ CommScope/ARRIS-branded HomeAssure gateways (*e.g.*, NVG558, NVG578, etc.); and Defendants’ IoT-Ready Smart Media Devices.

53. Each of the Accused ’838 Products create a distributed data monitoring and control system suitable for distinct residential automation applications. For example, each of the Accused

’838 Products is an AP with a built-in IoT radio with onboard BLE and Zigbee capabilities that can function as part of an IoT Suite Ecosystem.

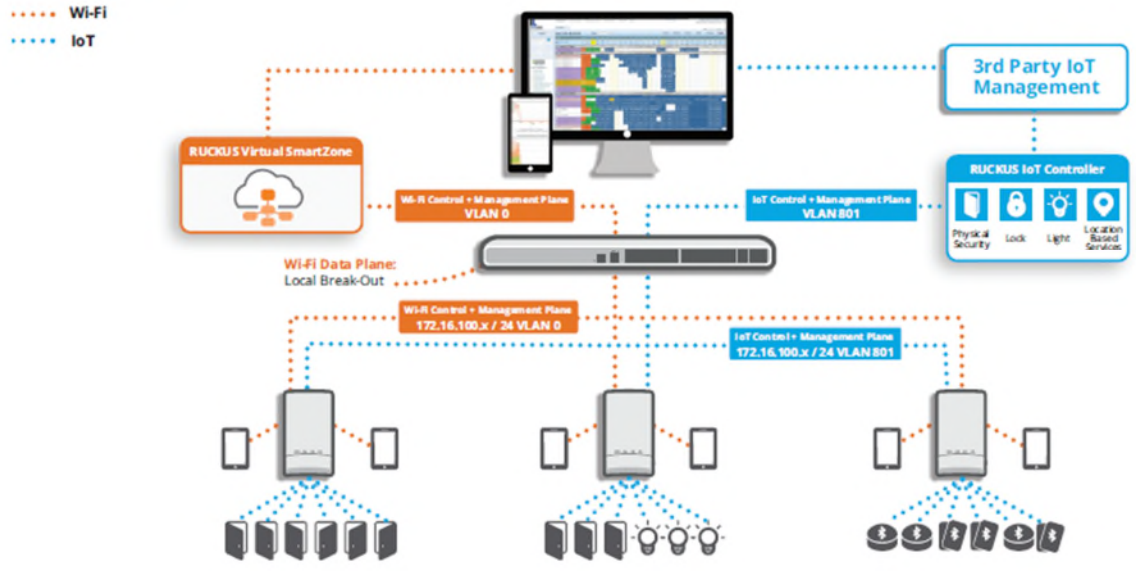


Use Cases and the RUCKUS IoT Suite Ecosystem

Integrations with industry-leading operational technology (OT) and customer technology (CT) solution providers enable organizations to use the RUCKUS IoT Controller to establish cross-solution policy rules while easily allowing for the use of 3rd party analytics tools and services tc increase IoT investment benefits.

The RUCKUS IoT Suite serves as the access network between IoT devices and their respective IoT management systems. By leveraging and extending the existing network infrastructure with multi-radio standards support, and multi-layered IoT security the RUCKUS IoT Suite can address a variety of IoT requirements.

An IoT Deployment



(*CommScope Ruckus IoT Suite Data Sheet, at 4-5.*)

54. Each of the Accused ’838 Products create a distributed data monitoring and control system with a first sensor configured to provide a first sensor data signal from a first local control system. For example, each of the products are APs or gateways that form a distributed data monitoring and control system for IoT sensors such as remote key cards and locks, intrusion, air, water and pollution quality, connected transit and bike shares, smart lighting and smart locks, and others.

55. Each of the Accused ’838 Products create a distributed data monitoring and control system with a first wireless communication device communicatively coupled to the first sensor, configured to receive the first sensor data signal from the first sensor, and configured to format and transmit a first encoded data signal. For example, the IoT sensors are coupled to wireless communication devices to communicate IoT sensor data using the BLE or Zigbee standards.

56. Each of the Accused ’838 Products create a distributed data monitoring and control system (*e.g.*, operating using the BLE standard) wherein the first encoded data signal (*e.g.*, BLE Network PDU) comprises a first wireless communication device identifier (*e.g.*, a Source Address), and comprises a first function code mapped from the received first sensor data signal (*e.g.*, a Light LC occupancy sensor status reported by the IoT occupancy sensors).

57. Each of the Accused ’838 Products create a distributed data monitoring and control system wherein the first function code is selected from a generic set of function codes configured for distinct applications, such that the first sensor data signal from the first local control system is mapped to a corresponding function code of the generic set of function codes. For example, by operating according to the Bluetooth Specification Mesh Model, a first function code included in the first encoded data signal is mapped from the first sensor data signal from the first local control system (*e.g.*, occupancy status detected and reported from an occupancy sensor) to a corresponding

function code of the generic set of function code (*e.g.*, Light LC Occupancy binary state which has the values of Generic On/Off state).

58. Each of the Accused '838 Products creates a distributed data monitoring and control system wherein the first wireless communication device is configured to transmit the first encoded data signal over a wireless transmission media to a gateway communicatively coupled to a wide area network. For example, the products are APs or gateways that form a distributed data monitoring and control system and that are connected to a wide area network such as the Internet.

59. Each of the Accused '838 Products create a distributed data monitoring and control system wherein the gateway is configured to receive and translate the first encoded data signal into a wide area network data transfer protocol for transmission to a computing device configured to collect, process, and store, the first encoded data signal. For example, each of the Accused '838 Products are APs or gateways configured to receive and translate the first encoded data signal (*e.g.*, a BLE message) into a wide area network data transfer protocol (*e.g.*, a 802.11 data message) for transmission (*e.g.*, via the Internet over Ethernet or over cellular LTE network, either directly or via other Ruckus APs in the network) to a computer device (*e.g.*, a computer running IoT Management software, analytics software or IoT cloud services, or a server) which is configured to collect, process and store the first encoded data signal (*e.g.*, collect, process, and store an IoT occupancy sensor status signal).

60. The features and capabilities of Defendants' Accused Products reflect Defendants' direct infringement by satisfying every element of at least the aforementioned claim of the '838 Patent, under 35 U.S.C. § 271(a).

61. Where acts constituting direct infringement of the '838 Patent are not performed by Defendants, such acts constituting direct infringement of the '838 Patent are performed by

Defendants' customers and/or end-users who act at the direction and/or control of Defendants, with Defendants' knowledge.

62. Plaintiff is informed and believes, and on that basis alleges, that Defendants are indirectly infringing one or more claims of the '838 Patent by active inducement in violation of 35 U.S.C. § 271(b), by at least using, manufacturing, supplying, distributing, selling and/or offering for sale the Accused Products to their customers with the knowledge and intent that use of those products would constitute direct infringement of the '838 Patent.

63. For example, Defendants direct their customers how to install, configure and operate the Accused '838 Products, including providing instructions, documentation, and technical support for customers to install and operate the Accused '492 Products in a SmartMesh network with IoT sensors. This includes instruction, documentation and technical support for installing, setting up, and operating the SmartMesh Network itself, including operation of (1) CommScope/Ruckus-branded IoT-ready APs, (2) CommScope/Ruckus-branded IoT Modules; (3) CommScope/Ruckus-branded SmartZone Controller; and (4) CommScope/Ruckus-branded IoT Controller. This includes but is not limited to the information and materials on Defendants' website.

64. Defendants specifically direct their customers on how to create a IoT Suite Ecosystem to establish cross-solution policy rules for various deployment examples, while allowing for the use of analytic tools and services to monitor and control IoT systems, including testing, setting up, and adjusting a network infrastructure with multi-radio standards support to address a variety of IoT requirements. This also includes but is not limited to the information and materials on Defendants' website.

65. Defendants have indirectly infringed one or more claims of the ’838 Patent, by, among other things, contributing to the direct infringement of others, including customers of the ’838 Accused Products by making, offering to sell, or selling, in the United States, or importing a component of a patented machine, manufacture, or combination, or an apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in infringement of the ’838 Patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use. Thus, Defendants are liable for infringement of the ’838 Patent pursuant to 35 U.S.C. § 271(c).

66. SIPCO has complied with the provisions of 35 U.S.C. § 287(a) by requiring licensees of its patents to comply with marking requirements, including by requiring licensees of its patents to mark retail products with patent numbers and/or listing products and/or patent numbers on publicly available websites, and undertaking reasonable measures to ensure compliance by its licensees. On information and belief, Defendants gained actual or constructive knowledge of the ’838 Patent as a result of this patent marking. In addition, Defendants have been on notice of the ’838 Patent since at least June 1, 2020. By the time of trial, Defendants will thus have known and intended (since receiving such notice), that their continued actions would actively induce and contribute to actual infringement of one or more claims of the ’838 Patent.

67. Defendants undertook and continued their infringing actions despite an objectively high likelihood that such activities infringed the ’838 Patent, which has been duly issued by the USPTO, and is presumed valid. For example, since, at least the time which Defendants had notice of the ’838 Patent and its applicability to their products, Defendants have been aware of an objectively high likelihood that its actions constituted and continue to constitute infringement of the ’838 Patent, and that the ’838 Patent is valid. On information and belief, Defendants could not

reasonably, subjectively believe that its actions do not constitute infringement of the ’838 Patent, nor could they reasonably, subjectively believe that the patent is invalid. As noted above, Defendants became aware of the ’838 Patent and its infringement of the ’838 Patent no later than June 1, 2020 when CommScope Holding Co., Inc. received SIPCO's notice letter dated May 27, 2020 and sent via Federal Express that same day, and would have become aware of their infringement then or shortly thereafter. Further, SIPCO sent a follow-up letter to Defendants on October 30, 2020, by overnight mail to the legal departments for CommScope Holding Co., Inc., ARRIS Solutions, Inc., and Ruckus Wireless Inc.’s, specifically directing them to claim 40 of the ’838 Patent and by e-mail to the legal department for CommScope Holding Co., Inc., including a claim chart setting forth in detail the basis for the infringement of that claim. Despite that knowledge and subjective belief, and despite the objectively high likelihood that its actions constitute infringement, Defendants have continued its infringing activities. As such, Defendants willfully infringe the ’838 Patent.

68. SIPCO has been damaged by Defendants’ infringement of the ’838 Patent.

COUNT 3 - INFRINGEMENT OF U.S. PATENT NO. 7,480,501

69. SIPCO incorporates paragraphs 1 through 71 above by reference.

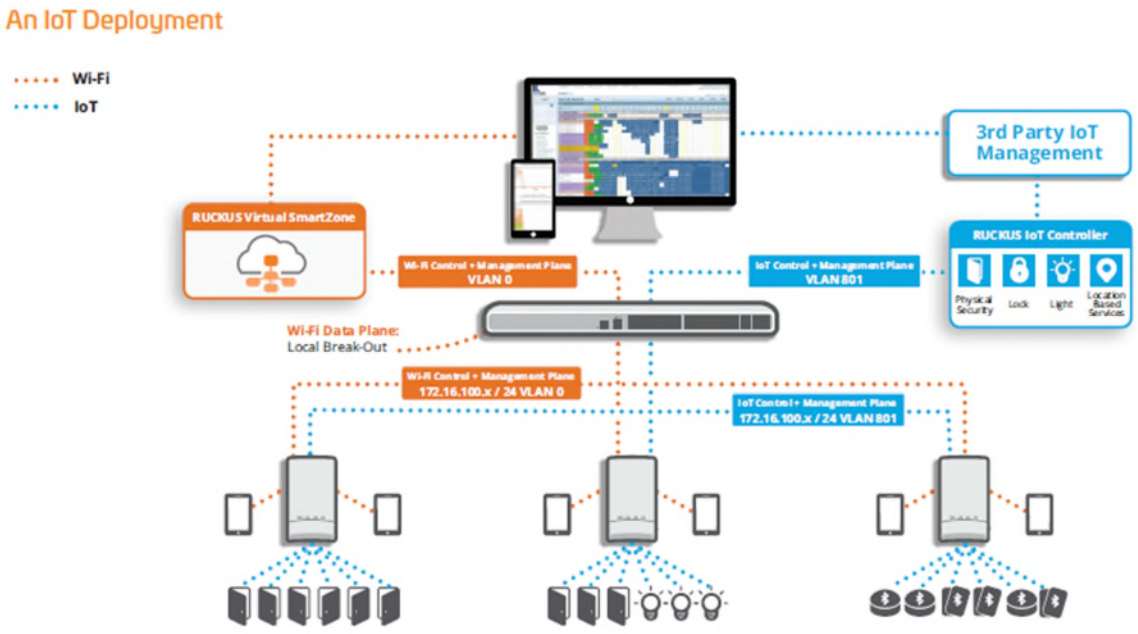
70. Defendants have infringed and continue to infringe the ’501 Patent in violation of 35 U.S.C. § 271, directly and/or indirectly by at least using, manufacturing, importing, supplying, distributing, selling and/or offering for sale products and/or systems, including the Accused Products, and/or by contributing to or inducing infringement by others with the intent to cause infringement of the ’501 Patent.

71. For example, Defendants have infringed and continue to infringe at least claim 17 of the ’501 Patent, directed to a “wireless communication network adapted for use in an automated

monitoring system," literally and/or under the doctrine of equivalents, including by way of example offering for sale and selling (1) Defendants' CommScope/Ruckus-branded cellular-ready APs with ZoneDirector (collectively, the "Accused '501 Products"). Exemplary Accused '501 Products include at least Defendants' CommScope/Ruckus-branded APs R850, R750, R730, R650, R550, R720, R710, R610, R510, M510, H510, C110, T750, T610, T310, T811-CM, E510.

72. Each of the Accused '501 Products includes a method for communicating emergency messages and cellular communications. For example, each product is a wireless AP or gateway that has integrated or add-on cellular communication capabilities (*e.g.,* 3G/4G/LTE and/or WiMAX) and communicates messages between it and one or more wireless APs, including communicating emergency messages such as network messages based on information from, as non-limiting examples, the state of smart locks, forced room entry conditions, andBLE panic buttons.

73. Each of the Accused '501 Products include predetermining a path for an emergency message by broadcasting path information to components of a transceiver network, such that each component stores the path information in its memory and configures itself to react to a signal for which the component is part of the predetermined path. For example, each of the Accused '501 Products is a gateway or AP that includes Smart Mesh, ZoneFlex and/or ZoneDirector, and that determines, ahead of time, the "best" mesh node with which to communicate network messages with by choosing a path from a plurality of paths in a tree topology.



(*CommScope Ruckus IoT Suite Data Sheet, at 5*.)

74. Each of the Accused ’501 Products includes receiving an emergency message broadcasted from an emergency message transceiver, the emergency message having at least an identification code uniquely assigned to the emergency message transceiver. For example, each of the Accused ’501 Products communicates, in the predetermined path, emergency information such as, for example, from IoT devices that use the BLE and Zigbee standards. The emergency message comprises an identification code uniquely assigned to the emergency message transceiver (*e.g.*, a Source Address field).

75. Each of the Accused ’501 Products includes determining information relevant to the received emergency message (*e.g.*, its Source) by associating the information with the identification code of the emergency message transceiver (*e.g.*, a Source Address field).

76. Each of the Accused ’501 Products includes communicating the emergency message and the relevant information along a predetermined path selected from a plurality of possible paths over a network of transceivers (*e.g.*, in a network using Smart Mesh, ZoneFlex

and/or ZoneDirector) such that assistance is summoned in response to the received emergency message.

77. Each of the Accused '501 Products includes receiving cellular communications from a cellular transceiver configured to communicate with a cellular communications network (*e.g.*, using built-in or added on cellular radio or a cellular wireless to receive cellular communications from a service provider's 3G/4G/LTE and/or WiMAX network).

78. The features and capabilities of Defendants' Accused Products reflect Defendants' direct infringement by satisfying every element of at least the aforementioned claim of the '501 Patent, under 35 U.S.C. § 271(a).

79. Where acts constituting direct infringement of the '501 Patent are not performed by Defendants, such acts constituting direct infringement of the '501 Patent are performed by Defendants' customers and/or end-users who act at the direction and/or control of Defendants, with Defendants' knowledge.

80. Plaintiff is informed and believes, and on that basis alleges, that Defendants are indirectly infringing one or more claims of the '501 Patent by active inducement in violation of 35 U.S.C. § 271(b), by at least using, manufacturing, supplying, distributing, selling and/or offering for sale the Accused Products to their customers with the knowledge and intent that use of those products would constitute direct infringement of the '501 Patent.

81. For example, Defendants direct their customers how to install, configure and operate the Accused '501 Products, including providing instructions, documentation, and technical support for customers to install and operate the Accused '501 Products in a SmartMesh network and with devices that communicate emergency messages. This includes instruction, documentation and technical support for installing, setting up, and operating the SmartMesh Network itself,

including the (1) CommScope/Ruckus-branded ZoneDirector Series Network Controllers and their associated software, such as the ZoneDirector OS; (2) CommScope/Ruckus-branded SmartZone Series Network Controllers, including their associated software; (3) the CommScope/Ruckus-branded Cloud service; and (4) the CommScope/Ruckus-branded APs in "Unleashed" mode, including their associated software. This includes but is not limited to the information and materials on Defendants' website.

82. Defendants specifically direct their customers on how to create a IoT Suite Ecosystem to establish cross-solution policy rules for various deployment examples, while allowing for the use of analytic tools and services to monitor and control IoT systems that communicate emergency messages such as from IoT panic buttons, including testing, setting up, and adjusting a network infrastructure with multi-radio standards support to address a variety of IoT requirements. This also includes but is not limited to the information and materials on Defendants' website.

83. Defendants have indirectly infringed one or more claims of the '501 Patent, by, among other things, contributing to the direct infringement of others, including customers of the '501 Accused Products by making, offering to sell, or selling, in the United States, or importing a component of a patented machine, manufacture, or combination, or an apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in infringement of the '501 Patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use. Thus, Defendants are liable for infringement of the '501 Patent pursuant to 35 U.S.C. § 271(c).

84. SIPCO has complied with the provisions of 35 U.S.C. § 287(a) by requiring licensees of its patents to comply with marking requirements, including by requiring licensees of

its patents to mark retail products with patent numbers and/or listing products and/or patent numbers on publicly available websites, and undertaking reasonable measures to ensure compliance by its licensees. On information and belief, Defendants gained actual or constructive knowledge of the ’501 Patent as a result of this patent marking. In addition, Defendants have been on notice of the ’501 Patent since at least June 1, 2020. By the time of trial, Defendants will thus have known and intended (since receiving such notice), that their continued actions would actively induce and contribute to actual infringement of one or more claims of the ’501 Patent.

85. Defendants undertook and continued their infringing actions despite an objectively high likelihood that such activities infringed the ’501 Patent, which has been duly issued by the USPTO, and is presumed valid. For example, since, at least the time which Defendants had notice of the ’501 Patent and its applicability to their products, Defendants have been aware of an objectively high likelihood that its actions constituted and continue to constitute infringement of the ’501 Patent, and that the ’501 Patent is valid. On information and belief, Defendants could not reasonably, subjectively believe that its actions do not constitute infringement of the ’501 Patent, nor could they reasonably, subjectively believe that the patent is invalid. As noted above, Defendants became aware of the ’501 Patent and its infringement of the ’501 Patent no later than June 1, 2020 when CommScope Holding Co., Inc. received SIPCO’s notice letter dated May 27, 2020 and sent via Federal Express that same day, and would have become aware of their infringement then or shortly thereafter. Despite that knowledge and subjective belief, and despite the objectively high likelihood that its actions constitute infringement, Defendants have continued its infringing activities. As such, Defendants willfully infringe the ’501 Patent.

86. SIPCO has been damaged by Defendants’ infringement of the ’501 Patent.

COUNT 4 - INFRINGEMENT OF U.S. PATENT NO. 8,606,284

87. SIPCO incorporates paragraphs 1 through 89 above by reference.

88. Defendants have infringed and continue to infringe at least claims 1, 12, 16-18, and 28-29 (the "Asserted Claims") of the '284 Patent in violation of 35 U.S.C. § 271, directly and/or indirectly by at least using, manufacturing, importing, supplying, distributing, selling and/or offering for sale products and/or systems, including the Accused Products, and/or by contributing to or inducing infringement by others with the intent to cause infringement of the '284 Patent.

89. The Asserted Claims of the '284 Patent are directed to a specific and concrete method for connecting wireless devices to a network. As recited in claim 1 and reflected in claim 18, the method encompasses the specific approach of detecting received signal strength indication (RSSI) information reflecting RSSI levels via a RSSI detecting unit, determining candidate devices based on those having the N-highest RSSI levels detected by the RSSI detecting unit, and connecting the candidate devices to the network. '284 Patent at claims 1 and 18. The Asserted Claims specify a particular metric, RSSI levels, and specify that only those with the N-highest levels detected are determined to be candidate devices and connected to the network. *Id.*

90. The specific and concrete nature of the Asserted Claims is further apparent in view of the various other metrics and approaches that may be used to determine whether to connect devices to a network. As explained in the '284 Patent itself, instead of using RSSI levels a terminal may use location information to determine candidate devices. *Id.* at 5:8-12. Other known metrics that may be used to determine whether to connect a device to a wireless network include the device type, the communication protocol(s) supported by the device type, the authentication status, the location of the device, whether the device has previously been connected to the network, and a large variety of other access restriction metrics and protocols. Even with respect to the metric of

RSSI levels, the Asserted Claims offer a specific approach among many possible approaches of only accepting the N-highest RSSI levels. As explained in the '284 Patent itself, other possible approaches to connecting wireless devices based on RSSI levels include setting a threshold RSSI level and determining all wireless devices having an RSSI level greater than the critical level to be candidate devices, or, alternatively, determining only those wireless devices with an RSSI level with a given range to be candidate devices. *Id*. at 5:30-39.

91. The Asserted Claims of the '284 Patent provide technical improvements and advantages to wireless networks by overcoming known issues resulting from over-association of wireless devices to single terminals or APs. In traditional wireless networks, such as WiFi, the wireless end devices, or wireless client stations (STAs), tend to select the AP having the highest RSSI level (such as the closest AP terminal). This basic selection approach may result in an "overconnected" or "overcrowded" AP—when a high concentration of end devices establish a connection to a single AP even if an adjacent AP remains unutilized. This is particularly true for wireless networks in public places such as public institutions, to which the '284 Patent is generally directed. *See, e.g.*, '284 Patent at 9:17-20. The Asserted Claims address this problem by implementing a control mechanisms at the terminal where the terminal only establishes a connection with candidate devices having the *N*-highest RSSI. By avoiding overcrowding, the Asserted Claims also help to avoid the uncontrolled "ping-pong" effect in wireless network environments.

92. In addition, limiting the candidate devices to those with the N-highest RSSI also facilitates "load balancing" between the multiple wireless devices that form the wireless network. *See, e.g.*, '284 Patent at 3:33-36, 3:36-40, 3:48-53, 4:11-12, Figs. 3-6. By identifying as candidate devices only those having the N-highest RSSI, the approach embodied in the Asserted Claims

forces other devices to connect to other APs that may not be as close but have a smaller number of connected devices, thus spreading the traffic load over the area more uniformly. In this way, the Asserted Claims ensure that the wireless network functions to more evenly distributes traffic, allowing higher throughput per network and per individual devices, and enabling a stable network operation with uniform traffic distribution across the area.

93. The Asserted Claims also serve to create wireless networks that are capable of higher and more satisfactory data transfer rates to wireless devices, and are less susceptible to fluctuations in the overall network topology. As noted in the '284 Patent, when RSSI levels are high, the data transfer state is such that a large amount of data can be provided to candidate devices; whereas when RSSI levels are low, only a small amount of data is capable of being provided. '284 Patent at 5:57-61. In addition, lower RSSI levels tend to exhibit greater fluctuations than higher RSSI levels. Use of a simple "threshold" RSSI level to identify candidate devices can result in wireless networks involving connections between a terminal and other wireless devices characterized by lower RSSI levels. By identifying as candidate devices only those having the N-highest RSSI, the approach embodied in the Asserted Claims helps to avoid the low data throughput and fluctuations associated with lower RSSI levels, and can better ensure that the connections in the network are at higher RSSI levels, where data transfers are satisfactory and can allow for larger amounts of data to be transferred.

94. The claimed features and functionality of the Asserted Claims are also not "generic" or "conventional." Although the use of RSSI was known at the time, it was used in a manner very different from that of the Asserted Claims. In particular, to the extent any use of RSSI was "conventional" in connection with wireless networks, such use was in a highly suboptimal manner wherein individual wireless end device selected, for example, the AP with the

highest RSSI level—thereby causing a host of problems, as explained above. Even years after the priority date of the '284 Patent these problems were identified and discussed in the art, which sought proposed load balancing solutions to address these issues. The '284 Patent provides a wholly different approach than any "conventional" use of RSSI levels by the individual wireless end devices. Indeed, the Asserted Claims recite a use of RSSI levels that is the *opposite* of so-called "conventional" approaches. The Asserted Claims are directed to controlling the network connectivity at the *terminal* and based on the selection of candidate devices with N-highest RSSI levels, rather than leaving that decision to end devices, or STAs, that instead tend to automatically select the AP with the greatest RSSI level, as in the conventional art. In this way, Asserted Claims as a whole operate in a manner that would be considered entirely *unconventional*.

95. Selecting "N-highest RSSI level devices" as in the Asserted Claims of the '284 Patent was not routine, conventional, or generic. To the contrary, this represents a novel approach to connectivity control in wireless networks, overcoming problems and issues found in the conventional approaches at the time, and enabling stable and optimized network throughputs. Moreover, additional advanced features provided by the '284 patent, such as in RSSI ranges, enabled even more sophisticated throughput and data transfer rate control. As such, the '284 Patent laid the groundwork and facilitated the development of modern devices with load balancing features.

96. The Expert Declaration of Branimir Vojcic, D.Sc. Regarding the Patentability Under 35 U.S.C. § 101 of the Asserted Claims of U.S. Patent No. 8,606,284, attached hereto as Exhibit 7, supports the above allegations and provides additional details that establish that: (1) the Asserted Claims of the '284 Patent focus on specific means or methods to achieve a desired result; (2) the Asserted Claims of the '284 Patent provide technological improvements to the relevant

technology existing at the time of the application for the ’284 Patent; and (3) the Asserted Claims are not directed to purely well-understood, routine, conventional activities at the time of the application for the ’284 Patent, and are instead unconventional in nature.

97. For example, Defendants have infringed and continue to infringe at least claim 18 of the ’284 Patent, directed to a “network connection method of a terminal,” literally and/or under the doctrine of equivalents, including by way of example offering for sale and selling (1) Defendants’ CommScope/Ruckus-branded APs with ZoneDirector (collectively, the “Accused ’284 Products”). Exemplary Accused ’284 Products include at least Defendants’ CommScope/Ruckus-branded APs R850, R750, R730, R650, R550, R720, R710, R610, R510, M510, H510, C110, T750, T610, T310, T811-CM, E510.

98. Each of the Accused ’284 Products contain a network connection method of a terminal, *e.g.*, that implement a network connection method that supports load balancing (*e.g.*, ZoneDirector supports management of APs and RF management, including Load Balancing).

99. Each of the Accused ’284 Products includes searching for devices, for example by performing channel scans of other adjacent APs.

100. Each of the Accused ’284 Products includes detecting a received signal strength indication (RSSI) level information of the searched devices, the RSSI level information indicating an RSSI level. For example, ZoneDirector load balancing performs channels scans to detect RSSI level information of APs by measuring the RSSI during channel scans.

101. Each of the Accused ’284 Products includes determining candidate devices to receive data using the RSSI level. For example, the products load balance client devices by determining client RSSI level information, and determine adjacent candidate APs by measuring their RSSI level information.

102. Each of the Accused ’284 Products includes connecting the determined candidate devices to a network, wherein the determining of the candidate devices is based on the candidate devices having an RSSI level among the N-highest RSSI levels detected. For example, the products include or exclude candidate devices to the network based on the RSSI levels detected, such as by ZoneDirector determining candidate APs by measuring the RSSI level information from devices and connecting candidate devices to a network based on the detected RSSI level by enforcing desired client limits.

103. The features and capabilities of Defendants’ Accused Products reflect Defendants’ direct infringement by satisfying every element of at least the aforementioned claim of the ’284 Patent, under 35 U.S.C. § 271(a).

104. Where acts constituting direct infringement of the ’284 Patent are not performed by Defendants, such acts constituting direct infringement of the ’284 Patent are performed by Defendants’ customers and/or end-users who act at the direction and/or control of Defendants, with Defendants’ knowledge.

105. Plaintiff is informed and believes, and on that basis alleges, that Defendants are indirectly infringing one or more claims of the ’284 Patent by active inducement in violation of 35 U.S.C. § 271(b), by at least using, manufacturing, supplying, distributing, selling and/or offering for sale the Accused Products to their customers with the knowledge and intent that use of those products would constitute direct infringement of the ’284 Patent.

106. For example, Defendants direct their customers how to install, configure and operate the Accused ’284 Products, including providing instructions, documentation, and technical support for customers to install and operate the Accused ’284 Products in a SmartMesh network. This includes instruction, documentation and technical support for installing, setting up, and

operating the SmartMesh Network itself, including the (1) CommScope/Ruckus-branded ZoneDirector Series Network Controllers and their associated software, such as the ZoneDirector OS; (2) CommScope/Ruckus-branded SmartZone Series Network Controllers, including their associated software; (3) the CommScope/Ruckus-branded Cloud service; and (4) the CommScope/Ruckus-branded APs in "Unleashed" mode, including their associated software. This includes but is not limited to the information and materials on Defendants' website.

107. Defendants specifically direct their customers on how to monitor network health characteristics, such as failure of APs, how to and how to change and then restore system settings relating to "self-healing" functionality, "Smart Uplink Selection," load balancing, and backhauling, including testing, setting up, and adjusting load balancing and backhauling functionality. This also includes but is not limited to the information and materials on Defendants' website.

108. Defendants have indirectly infringed one or more claims of the '284 Patent, by, among other things, contributing to the direct infringement of others, including customers of the '284 Accused Products by making, offering to sell, or selling, in the United States, or importing a component of a patented machine, manufacture, or combination, or an apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in infringement of the '284 Patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use. Thus, Defendants are liable for infringement of the '284 Patent pursuant to 35 U.S.C. § 271(c).

109. Defendants have been on notice of the '284 Patent since at least as of the filing of the original Complaint in this matter. By the time of trial, Defendants will thus have known and

intended (since receiving such notice), that their continued actions would actively induce and contribute to actual infringement of one or more claims of the ’284 Patent.

110. Defendants undertook and continued their infringing actions despite an objectively high likelihood that such activities infringed the ’284 Patent, which has been duly issued by the USPTO, and is presumed valid. For example, since, at least the time which Defendants had notice of the ’284 Patent and its applicability to their products, Defendants have been aware of an objectively high likelihood that its actions constituted and continue to constitute infringement of the ’284 Patent, and that the ’284 Patent is valid. On information and belief, Defendants could not reasonably, subjectively believe that its actions do not constitute infringement of the ’284 Patent, nor could they reasonably, subjectively believe that the patent is invalid. As noted above, Defendants have been aware of the ’284 Patent and its infringement of the ’284 Patent no later than the filing of the original Complaint in this matter. Despite that knowledge and subjective belief, and despite the objectively high likelihood that its actions constitute infringement, Defendants have continued its infringing activities. As such, Defendants willfully infringe the ’284 Patent.

111. SIPCO has been damaged by Defendants’ infringement of the ’284 Patent.

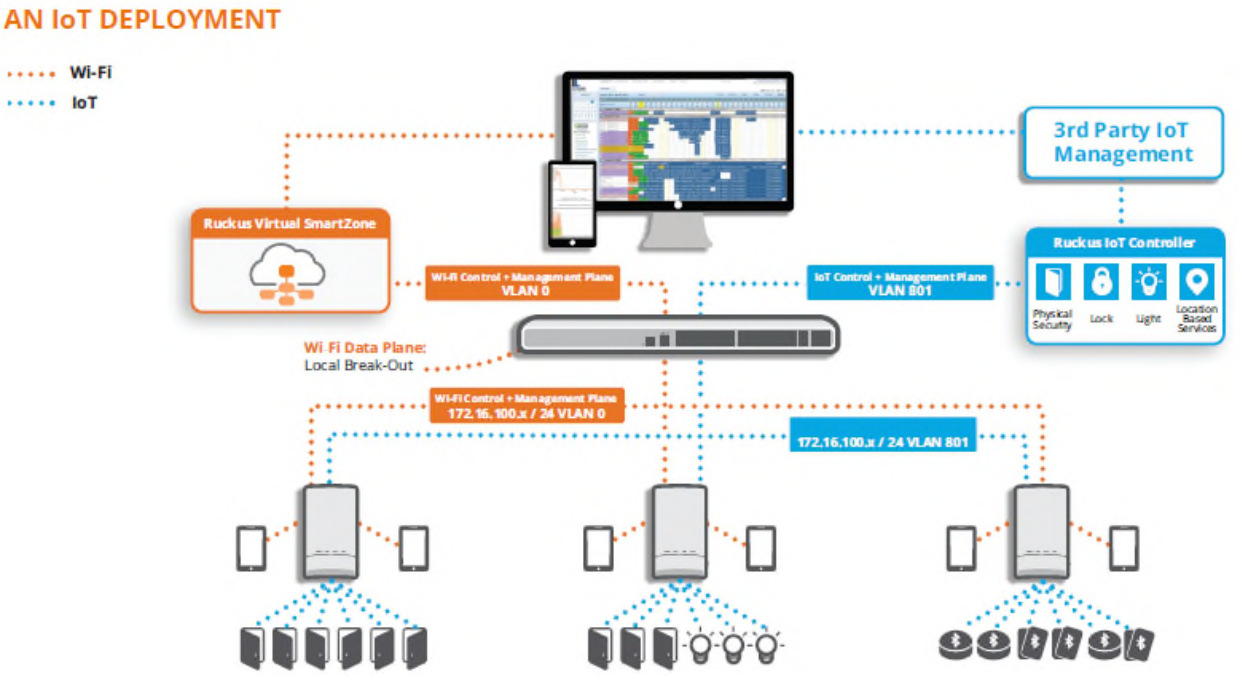
COUNT 5 - INFRINGEMENT OF U.S. PATENT NO. 8,666,357

112. SIPCO incorporates paragraphs 1 through 106 above by reference.

113. Defendants have infringed and continue to infringe the ’357 Patent in violation of 35 U.S.C. § 271, directly and/or indirectly by at least using, manufacturing, importing, supplying, distributing, selling and/or offering for sale products and/or systems, and/or by contributing to or inducing infringement by others with the intent to cause infringement of the ’357 Patent.

114. For example, Defendants have infringed and continue to infringe at least claim 9 of the ’357 Patent, directed to a “wireless communication device” in a “system for communicating emergency messages,” literally and/or under the doctrine of equivalents, including by way of example offering for sale and selling (1) Defendants’ CommScope/Ruckus-branded IoT-Ready and SmartMesh-enabled APs (collectively, the “Accused ’357 Products”). Exemplary Accused ’357 Products include at least Defendants’ CommScope/Ruckus-branded APs R850, R750, R730, R650, R550, R720, R710, R610, R510, M510, H510, C110, T750, T610, T310, T811-CM, and E510, either with or without a Ruckus IoT Module, *e.g.*, i100.

115. Each of the Accused ’357 Products is a wireless communications device in a system for communicating emergency message that includes a network of wireless communication devices (*e.g.*, a network of Defendants’ APs using Ruckus “SmartMesh” networking technology). The system, such as a Ruckus SmartMesh network, is a system for communicating emergency messages such as network messages based on information from, as non-limiting examples, the state of smart locks, forced room entry conditions, and BLE panic buttons.



DEPLOYMENT EXAMPLES

Hospitality

Hotels can more easily enhance security and convenience for guests through remote key card management and offering smart-home amenities to improve guest satisfaction. Additionally, lock audit trails, canceling or changing key card room access and alerting staff in cases of a forced room entry all build a safer and better guest experience.

Smart Cities

Cities can more easily implement a range of citizen-centric quality-of-life solutions ranging from parking location assistance to more efficient trash collection. Cities can monitor air, water and pollution quality to improve public health.

Smart Campuses

IoT-enabled Smart Campuses make colleges and universities safer and more efficient, through wayfinding, connected transit and bike shares, and smart parking applications. Connected CCTV, smart lighting and smart locks make everyone on campus safer.

Building Owners

Building owners and operators are using IoT applications to create new smart-home and smart-office experiences that attract new residents and tenants and help their properties compete. Amenities like smart lighting, environmental controls, and connected security make buildings safer, increasing property values and rents, while reducing operational costs.

(Ruckus IoT Suite Data Sheet, at 4.)

116. The network of wireless communication devices also includes a site controller. For example, a network includes: (1) a CommScope/Ruckus-branded ZoneDirector Series Network Controller, including its firmware and software, such as the ZoneDirector OS; (2) a CommScope/Ruckus-branded SmartZone Series Network Controller, whether a physical or Virtual device, including its firmware and software; (3) the CommScope/Ruckus-branded Cloud

service; or (4) a CommScope/Ruckus-branded Unleashed AP serving as a "Master" AP, including its firmware and software. Each of the foregoing, together with circuitry, firmware and/or software running on the Accused '357 Products, is configured to monitor communication paths in the SmartMesh network (*e.g.*, by detecting failure of APs and monitoring other network health characteristics); and redefine the communication paths, such as the wireless hops, when the failure of a network transceiver (*e.g.*, CommScope/Ruckus-branded AP) along a communication path is detected (*e.g.*, by at least the SmartMesh "self-healing" functionality, "Smart Uplink Selection," load balancing, and backhauling).

117. Each of the Accused '357 Products includes a transceiver (*e.g.*, two-way radio) to send and receive one or more emergency messages via one or more devices in the network (*e.g.*, other CommScope/Ruckus-branded APs).

118. Each of the Accused '357 Products also includes a controller (*e.g.*, a CPU) operatively coupled to the radio, and configured to communicate with at least one other remote wireless device (*e.g.*, CommScope/Ruckus-branded AP) via the transceiver with an emergency message. The radio is further configured to transmit an emergency message generated by the Accused '357 Product and to relay an emergency message generated by at least one other remote wireless device (*e.g.*, another CommScope/Ruckus-branded AP).

119. Each of the Accused '357 Products also contains a memory (*e.g.*, RAM) for storing communication path information for use in transmitting the one or more emergency messages. The communication path information comprises identification codes (*e.g.*, Source Addresses (SRCs)) associated with devices in the network (*e.g.*, CommScope/Ruckus-branded APs) and defining transmission paths for wireless communication.

120. The features and capabilities of Defendants' Accused Products reflect Defendants' direct infringement by satisfying every element of at least the aforementioned claim of the '357 Patent, under 35 U.S.C. § 271(a).

121. Where acts constituting direct infringement of the '357 Patent are not performed by Defendants, such acts constituting direct infringement of the '357 Patent are performed by Defendants' customers and/or end-users who act at the direction and/or control of Defendants, with Defendants' knowledge.

122. Plaintiff is informed and believes, and on that basis alleges, that Defendants are indirectly infringing one or more claims of the '357 Patent by active inducement in violation of 35 U.S.C. § 271(b), by at least using, manufacturing, supplying, distributing, selling and/or offering for sale the Accused '357 Products to their customers with the knowledge and intent that use of those products would constitute direct infringement of the '357 Patent.

123. For example, Defendants direct their customers how to install, configure and operate the Accused '357 Products, including providing instructions, documentation, and technical support for customers to install and operate the Accused '357 Products using Ruckus SmartMesh networking technology, as part of a SmartMesh network. This includes instruction, documentation and technical support for installing, setting up, and operating the SmartMesh network itself, including the (1) CommScope/Ruckus-branded ZoneDirector Series Network Controllers and their associated software, such as the ZoneDirector OS; (2) CommScope/Ruckus-branded SmartZone Series Network Controllers, including their associated software; (3) the CommScope/Ruckus-branded Cloud service; and (4) the CommScope/Ruckus-branded APs in "Unleashed" mode, including their associated software. Defendants specifically direct their customers how to monitor network health characteristics, such as failure of CommScope/Ruckus-branded APs, how to

change and then restore system settings relating to "self-healing" functionality, "Smart Uplink Selection," load balancing, and backhauling, including testing, setting up, and adjusting load balancing and backhauling functionality. Defendants also provide services as "virtual" site controllers, such as the CommScope/Ruckus-branded Cloud service and the "Virtual" SmartZone Network Controllers. The foregoing includes but is not limited to the information and materials on Defendants' websites, including videos, user guides, administrator guides, data sheets, feature sheets, and forums where Defendants' employees respond to users' questions and comments.

124. Defendants have indirectly infringed one or more claims of the '357 Patent, by, among other things, contributing to the direct infringement of others, including customers of the '357 Accused Products by importing into, or making, offering to sell, or selling, in the United States, or importing a component of a patented machine, manufacture, or combination, or an apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in infringement of the '357 Patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use. Thus, Defendants are liable for infringement of the '357 Patent pursuant to 35 U.S.C. § 271(c).

125. SIPCO has complied with the provisions of 35 U.S.C. § 287(a) by requiring licensees of its patents to comply with marking requirements, including by requiring licensees of its patents to mark retail products with patent numbers and/or listing products and/or patent numbers on publicly available websites, and undertaking reasonable measures to ensure compliance by its licensees. On information and belief, Defendants gained actual or constructive knowledge of the '357 Patent as a result of this patent marking. In addition, Defendants have been on notice of the '357 Patent since at least June 1, 2020. Defendants have therefore known and

intended (since receiving such notice), that their continued actions would actively induce and contribute to actual infringement of one or more claims of the ’357 Patent.

126. Defendants undertook and continued their infringing actions despite an objectively high likelihood that such activities infringed the ’357 Patent, which has been duly issued by the USPTO, and is presumed valid. For example, since, at least the time that Defendants had notice of the ’357 Patent and its applicability to their products, Defendants have been aware of an objectively high likelihood that their actions constituted and continue to constitute infringement of the ’357 Patent, and that the ’357 Patent is valid. On information and belief, Defendants could not reasonably, subjectively believe that their actions do not constitute infringement of the ’357 Patent, nor could they reasonably, subjectively believe that the patent is invalid. As noted above, Defendants became aware of the ’357 Patent no later than June 1, 2020 when CommScope Holding Co., Inc. received SIPCO’s notice letter dated May 27, 2020 and sent via Federal Express that same day, and would have become aware of their infringement then or shortly thereafter. Further, SIPCO sent a follow-up letter to Defendants on October 30, 2020, by overnight mail to the legal departments for CommScope Holding Co., Inc., ARRIS Solutions, Inc., and Ruckus Wireless Inc.’s, specifically directing them to claim 9 of the ’357 Patent and by e-mail to the legal department for CommScope Holding Co., Inc. Despite that knowledge and subjective belief, and despite the objectively high likelihood that their actions constitute infringement, Defendants have continued their infringing activities. As such, Defendants willfully infringe the ’357 Patent.

127. SIPCO has been damaged by Defendants’ infringement of the ’357 Patent.

COUNT 6 - INFRINGEMENT OF U.S. PATENT NO. 7,697,492

128. SIPCO incorporates paragraphs 1 through 122 above by reference.

129. Defendants have infringed and continue to infringe the ’492 Patent in violation of 35 U.S.C. § 271, directly and/or indirectly by at least using, manufacturing, importing, supplying, distributing, selling and/or offering for sale products and/or systems, including the Accused Products, and/or by contributing to or inducing infringement by others with the intent to cause infringement of the ’492 Patent.

130. For example, Defendants have infringed and continue to infringe at least claim 14 of the ’492 Patent, directed to a “wireless communication device for use in a communication system,” literally and/or under the doctrine of equivalents, including by way of example offering for sale and selling (1) Defendants’ CommScope/Ruckus-branded IoT-Ready APs supporting Zigbee, (2) Defendants’ CommScope/ARRIS-branded IoT-Ready HomeAssure gateways supporting Zigbee, and (3) Defendants’ CommScope/ARRIS-branded IoT-Ready Smart Media Devices supporting Zigbee (collectively, the “Accused ’492 Products”). Exemplary Accused ’492 Products include at least Defendants’ CommScope/Ruckus-branded APs R850, R750, R730, R650, R550, R720, R710, R610, R510, M510, H510, C110, T750, T610, T310, T811-CM, E510, either with or without a Ruckus IoT Module (*e.g.*, i100), Defendants’ CommScope/ARRIS-branded gateway models NVG558 and NVG578 with Zigbee radio, and Defendants’ IoT-Ready Smart Media Devices with Zigbee radio.

131. Each of the Accused ’492 Products is a wireless communication device for use in a communication system to communicate command and sensed data between remote wireless communication devices (*e.g.*, between Defendants’ products supporting Zigbee and third-party compatible Zigbee IoT devices such as Zigbee door locks).

132. Each of the above Accused ’492 Products includes a transceiver (*e.g.*, Zigbee radio) configured to send and receive wireless communications (*e.g.*, IEEE802.15.4/Zigbee frames).

133. Each of the above Accused '492 Products further includes a controller (*e.g.*, a microprocessor/CPU/controlling circuit) configured to communicate with at least one other remote wireless device (*e.g.*, Zigbee radio of compatible third-party Zigbee IoT devices) via the transceiver with a preformatted message (*e.g.*, IEEE802.15.4/Zigbee frames), the controller is further configured to format a message comprising a receiver address (*e.g.*, Destination Address in IEEE802.15.4/Zigbee frames) comprising a scalable address of at least one remote wireless device; a command indicator (*e.g.*, Command Identifier in IEEE802.15.4/Zigbee frames) comprising a command code; a data value comprising a scalable message (*e.g.*, variable payload in IEEE802.15.4/Zigbee frames).

134. The features and capabilities of Defendants' Accused '492 Products reflect Defendants' direct infringement by satisfying every element of at least the aforementioned claim of the '492 Patent, under 35 U.S.C. § 271(a).

135. Where acts constituting direct infringement of the '492 Patent are not performed by Defendants, such acts constituting direct infringement of the '492 Patent are performed by Defendants' customers and/or end-users who act at the direction and/or control of Defendants, with Defendants' knowledge.

136. Plaintiff is informed and believes, and on that basis alleges, that Defendants are indirectly infringing one or more claims of the '492 Patent by active inducement in violation of 35 U.S.C. § 271(b), by at least using, manufacturing, supplying, distributing, selling and/or offering for sale the Accused Products to their customers with the knowledge and intent that use of those products would constitute direct infringement of the '492 Patent.

137. For example, Defendants direct their customers how to install, configure and operate the Accused '492 Products, including providing instructions, documentation, and technical

support for customers to install and operate the Accused '492 Products in an IEEE802.15.4/Zigbee network. Defendants specifically direct their customers on how to incorporate Zigbee IoT devices to IEEE802.15.4/Zigbee networks including the Accused '492 Products and how to monitor and control the incorporated third-party Zigbee IoT devices using the Accused '492 Products, thereby communicating command and sensed data between the Accused '492 Products and the third-party Zigbee IoT devices. This includes but is not limited to the information and materials on Defendants' website and training/instruction videos posted by Defendants on the Internet. (*See, e.g.*, https://www.youtube.com/watch?v=JKxriG1fllM (dated June 19, 2019); https://www.youtube.com/watch?v=oqze7km_WlY (dated June 20, 2019).) Following Defendants' instructions and directions, their customers directly infringe the claims (including method claims) of the '492 Patent by using and operating the Accused '492 Products within IEEE802.15.4/Zigbee networks that also include compatible third-party Zigbee IoT devices.

138. Defendants have indirectly infringed one or more claims of the '492 Patent, by, among other things, contributing to the direct infringement of others, including customers of the '492 Accused Products by making, offering to sell, or selling, in the United States, or importing a component of a patented machine, manufacture, or combination, or an apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in infringement of the '492 Patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use. Thus, Defendants are liable for infringement of the '492 Patent pursuant to 35 U.S.C. § 271(c).

139. SIPCO has complied with the provisions of 35 U.S.C. § 287(a) by requiring licensees of its patents to comply with marking requirements, including by requiring licensees of its patents to mark retail products with patent numbers and/or listing products and/or patent

numbers on publicly available websites, and undertaking reasonable measures to ensure compliance by its licensees. On information and belief, Defendants gained actual or constructive knowledge of the '492 Patent as a result of this patent marking. In addition, Defendants have been on notice of the '492 Patent since at least June 1, 2020. By the time of trial, Defendants will thus have known and intended (since receiving such notice), that their continued actions would actively induce and contribute to actual infringement of one or more claims of the '492 Patent.

140. Defendants undertook and continued their infringing actions despite an objectively high likelihood that such activities infringed the '492 Patent, which has been duly issued by the USPTO, and is presumed valid. For example, since, at least the time which Defendants had notice of the '492 Patent and its applicability to their products, Defendants have been aware of an objectively high likelihood that its actions constituted and continue to constitute infringement of the '492 Patent, and that the '492 Patent is valid. On information and belief, Defendants could not reasonably, subjectively believe that its actions do not constitute infringement of the '492 Patent, nor could they reasonably, subjectively believe that the patent is invalid. As noted above, Defendants became aware of the '492 Patent and its infringement of the '492 Patent no later than June 1, 2020, when CommScope Holding Co., Inc. received SIPCO's notice letter dated May 27, 2020 and sent via Federal Express that same day, and would have become aware of their infringement then or shortly thereafter. Despite that knowledge and subjective belief, and despite the objectively high likelihood that its actions constitute infringement, Defendants have continued its infringing activities. As such, Defendants willfully infringe the '492 Patent.

141. SIPCO has been damaged by Defendants' infringement of the '492 Patent.

PRAYER FOR RELIEF

WHEREFORE, SIPCO prays for relief as follows:

1. A judgment declaring that Defendants have infringed and is infringing one or more claims of the ’587 Patent, ’838 Patent, ’501 Patent, ’284 Patent, ’357 Patent, and ’492 Patent;

2. A judgment awarding SIPCO compensatory damages as a result of Defendants’ infringement of one or more claims of the ’587 Patent, ’838 Patent, ’501 Patent, ’284 Patent, ’357 Patent, and ’492 Patent, together with interest and costs, consistent with lost profits and in no event less than a reasonable royalty;

3. A judgment awarding SIPCO treble damages, pre-judgment, and post-judgment interest under 35 U.S.C. § 284 and as otherwise allowed by law as a result of Defendants’ willful and deliberate infringement of one or more claims of the ’587 Patent, ’838 Patent, ’501 Patent, ’284 Patent, ’357 Patent, and ’492 Patent;

4. A judgment declaring that this case is exceptional and awarding SIPCO its expenses, costs, and attorneys’ fees in accordance with 35 U.S.C. §§ 284 and 285 and Rule 54(d) of the Federal Rules of Civil Procedure;

5. A grant of preliminary and permanent injunctions enjoining Defendant from further acts of infringement of one or more claims of the ’587 Patent, ’838 Patent, ’501 Patent, ’284 Patent, ’357 Patent, and ’492 Patent; and

6. Such other and further relief as the Court deems just and proper.

JURY TRIAL DEMANDED

SIPCO hereby demands a trial by jury.

Dated: May 21, 2021

By: */s/ Michael J. Word*
Geoff Culbertson
Kelly Tidwell
PATTON, TIDWELL & CULBERTSON, LLP
2800 Texas Boulevard (75503)

Post Office Box 5398
Texarkana, TX 75505-5398
Telephone: (903) 792-7080
Facsimile: (903) 792-8233
gpc@texarkanalaw.com
kbt@texarkanalaw.com

James A. (Tripp) Fussell
Jamie B. Beaber
Alison T. Gelsleichter
Sen (Alex) Wang
MAYER BROWN LLP
1999 K Street, N.W.
Washington, D.C. 20006
Telephone: (202) 263-3000
Facsimile: (202) 263-3300
jfussell@mayerbrown.com
jbeaber@mayerbrown.com
AGelsleichter@mayerbrown.com
awang@mayerbrown.com

Michael J. Word
Luiz Miranda
MAYER BROWN LLP
71 S. Wacker Drive
Chicago, Illinois 60606
Telephone: (312) 782-0600
Facsimile: (312) 701-7711
mword@mayerbrown.com
lmiranda@mayerbrown.com

Cliff A. Maier
Gray Buccigross
MAYER BROWN LLP
Two Palo Alto Square
Suite 300
3000 El Camino Real
Palo Alto, CA 94306
Telephone: (650) 331-2000
Facsimile: (650) 331-2060
cmaier@mayerbrown.com
gbuccigross@mayerbrown.com

Attorneys for Plaintiff SIPCO, Inc.

CERTIFICATE OF SERVICE

I hereby certify that as of this day all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via electronic mail.

Dated: May 21, 2021

/Michael J. Word/
Michael J. Word