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

STINGRAY IP SOLUTIONS LLC,	§	
	§	
Plaintiff,	§	
	§	
v.	§	JURY TRIAL DEMANDED
	§	
JOHNSON CONTROLS	§	
INTERNATIONAL PLC, JOHNSON	§	CIVIL ACTION NO. _____
CONTROLS, INC., and JOHNSON	§	
CONTROLS SECURITY SOLUTIONS	§	
LLC,	§	
	§	
Defendants.	§	

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Stingray IP Solutions LLC ("Stingray") files this Complaint in this Eastern District

of Texas (the "District") against Defendants Johnson Controls International plc, Johnson Controls,

Inc., and Johnson Controls Security Solutions LLC (collectively, "Defendants" or "Johnson

Controls") for infringement of U.S. Patent No. 7,224,678 (the "'678 patent"), U.S. Patent No.

7,440,572 (the "'572 patent"), and U.S. Patent No. 7,616,961 ("the "'961 patent").

THE PARTIES

1.   Stingray IP Solutions LLC ("Stingray" or "Plaintiff") is a Texas limited liability

company, located at 6136 Frisco Sq. Blvd., Suite 400, Frisco, TX 75034.

2.   On information and belief, Defendant Johnson Controls International plc ("JCI

PLC") is a public limited company organized under the laws of Ireland, with its principal place of

business and registered office located at One Albert Quay, Cork, Ireland, T12 X8N6.

3.   On information and belief, Defendant Johnson Controls, Inc. ("JC Inc.") is a company

organized under the laws of Wisconsin, with its principal place of business located at 5757 N

Green Bay Ave, Milwaukee, Wisconsin, USA 53209-4408. JCI PLC and JC Inc. share the same world headquarters in Cork, Ireland. Moreover, JC Inc. is a wholly owned and controlled subsidiary of JCI PLC, and JC Inc. is part of a multi-national group of companies operating under the name "Johnson Controls" of which JCI PLC is the parent and controlling entity.

4.   On information and belief, Defendant Johnson Controls Security Solutions LLC ("JC Security") is a company organized under the laws of Delaware, with its principal place of business located at 6600 Congress Ave, Boca Raton, FL 33487-1213. JCI PLC and JC Security share the same world headquarters in Cork, Ireland. Moreover, JC Security is a wholly owned and controlled subsidiary of JCI PLC, and JC Security is part of a multi-national group of companies operating under the name "Johnson Controls" of which JCI PLC is the parent and controlling entity.

5.   "Johnson Controls was originally incorporated in the state of Wisconsin in 1885 as Johnson Electric Service Company to manufacture, install and service automatic temperature regulation systems for buildings and was renamed to Johnson Controls, Inc. in 1974. In 2005, Johnson Controls acquired York International, a global supplier of heating, ventilating, air-conditioning ("HVAC") and refrigeration equipment and services. In 2014, Johnson Controls acquired Air Distribution Technologies, Inc., one of the largest independent providers of air distribution and ventilation products in North America. . . . In 2016, Johnson Controls, Inc. and Tyco completed their combination (the "Merger"), combining Johnson Controls portfolio of building efficiency solutions with Tyco's portfolio of fire and security solutions. Following the Merger, Tyco changed its name to 'Johnson Controls International plc.'" *See Form 10-K Annual Financial Report For the Fiscal Year Ended September 30, 2021,* p. 3, JOHNSON CONTROLS INTERNATIONAL PLC, *available for download at* https://investors.johnsoncontrols.com/financial-

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT – Page 2

information/johnson-sec-filings (last visited Sep. 26, 2022) [hereinafter "Annual Financial Report"].

6.   JCI PLC states that "Johnson Controls International plc, headquartered in Cork, Ireland, is a global leader in smart, healthy and sustainable buildings, serving a wide range of customers in more than 150 countries." *Id*. at p. 3. JCI PLC further states that Johnson Controls' "products, services, systems and solutions advance the safety, comfort and intelligence of spaces to serve people, places and the planet," and Johnson Controls "is committed to helping its customers win and creating greater value for all of its stakeholders through its strategic focus on buildings." *Id*. JCI PLC additionally states that Johnson Controls "is a global leader in engineering, manufacturing and commissioning building products and systems, including residential and commercial HVAC equipment, industrial refrigeration systems, controls, security systems, fire-detection systems and fire-suppression solutions. The Company further serves customers by providing technical services, including maintenance, management, repair, retrofit and replacement of equipment (in the HVAC, industrial refrigeration, security and fire-protection space), energy-management consulting and data-driven 'smart building' services and solutions powered by its OpenBlue software platform and capabilities." *Id.* at 4.

7.   JCI PLC states that Johnson Controls "has properties in over 60 countries throughout the world, with its world headquarters located in Cork, Ireland and its North American operational headquarters located in Milwaukee, Wisconsin USA." *Id*. at p. 25. According to JCI PLC, Johnson Controls' wholly- and majority-owned facilities primarily consist of manufacturing, sales and service offices, research and development facilities, monitoring centers, and assembly and/or warehouse centers." *Id*. at p. 25. Johnson Controls, including parent JCI PLC along with its subsidiaries, are engaged in research and development, manufacturing, importation, distribution,

sales, and related technical services for: (i) "HVAC, controls, building management, refrigeration, integrated electronic security and integrated fire-detection and suppression systems," with each activity being conducted "for commercial, industrial, retail, small business, institutional and governmental customers in the United States and Canada;" (ii) "HVAC equipment, controls software and software services for residential and commercial applications to commercial, industrial, retail, residential, small business, institutional and governmental customers worldwide;" and (iii) "fire protection, fire suppression and security products, including intrusion security, anti-theft devices, access control, and video surveillance and management systems, for commercial, industrial, retail, residential, small business, institutional and governmental customers worldwide." *See Id.* at 102-03. Johnson Controls' products are (i) manufactured outside the U.S. and then imported into the United States or (ii) manufactured inside the U.S. and distributed, and sold to end-users via the internet, brick-and-mortar stores and/or via dealers in the U.S., in Texas and the Eastern District of Texas.

8.   On information and belief, Johnson Controls has business segments including Building Solutions North America and Global Products. *Id.* at 102. "Building Solutions North America designs, sells, installs and services HVAC, controls, building management, refrigeration, integrated electronic security and integrated fire-detection and suppression systems for commercial, industrial, retail, small business, institutional and governmental customers in the United States and Canada. Building Solutions North America also provides energy efficiency solutions and technical services, including inspection, scheduled maintenance, and repair and replacement of mechanical and controls systems, as well as data-driven 'smart building' solutions, to non-residential building and industrial applications in the United States and Canadian marketplace." *Id.* "Global Products designs, manufactures and sells HVAC equipment, controls

software and software services for residential and commercial applications to commercial, industrial, retail, residential, small business, institutional and governmental customers worldwide. In addition, Global Products designs, manufactures and sells refrigeration equipment and controls globally. The Global Products business also designs, manufactures and sells fire protection, fire suppression and security products, including intrusion security, anti-theft devices, access control, and video surveillance and management systems, for commercial, industrial, retail, residential, small business, institutional and governmental customers worldwide." *Id.* at 102-03.

9.   On information and belief, Johnson Controls maintains a corporate presence in the United States, including in Texas and in this District, via at least its North American operational headquarters located in Milwaukee, Wisconsin, USA and its wholly owned and controlled U.S.-based subsidiaries, including JC Inc., which is a Delaware company and JC Security, which is a Wisconsin company. *See Exhibit 21.1*, *Annual Financial Report,* p. 183. On behalf and for the benefit of Defendants, Johnson Controls coordinates the importation, distribution, marketing, offers for sale, sale, and use of the Johnson Controls' products in the U.S. For example, Johnson Controls maintains distribution channels in the U.S. for Johnson Controls' products via online stores, distribution partners, retailers, reseller partners, dealers, and other related service providers. *See Where to buy*, JOHNSONCONTROLS.COM, https://www.johnsoncontrols.com/locations (accessible via menu "ABOUT US" and link for "Locations,") (last visited Sep. 26, 2022).

10.   As a result, via at least Johnson Controls' established distribution channels operated and maintained by at least Defendant JCI PLC and Johnson Controls' U.S. based subsidiaries, including wholly owned and controlled Defendants JC Inc. and JC Security, Johnson Controls products are distributed, sold, advertised, and used nationwide, including being sold to consumers

via Johnson Controls dealers operating in Texas and this District. Thus, Defendants do business in the U.S., the state of Texas, and in this District.

<div align="center">**JURISDICTION AND VENUE**</div>

11.   This action arises under the patent laws of the United States, namely 35 U.S.C. §§ 271, 281, and 284-285, among others.

12.   This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

A.   Defendant JCI PLC

13.   On information and belief, JCI PLC is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, and/or consumers. For example, JCI PLC is related to, owns, and/or controls subsidiaries (such as JC Inc. and JC Security), business segments (such as its Building Solutions North America segment and Global Products segment) and additional business and/or brands (such as its Johnson Controls, Lux, York, DSC, Tyco, Visonic, and Qolsys brands) that have a significant business presence in the U.S. and in Texas. Such a presence furthers

the development, design, manufacture, importation, distribution, sale, and use (including by inducement) of infringing Johnson Controls products in Texas, including in this District.

14.   This Court has personal jurisdiction over Defendant JCI PLC, directly and/or through the activities of JCI PLC's intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including through the activities of Defendants JC Inc. and JC Security, other members, segments, companies and/or brands of Johnson Controls, and U.S. based subsidiaries. Through direction and control of these entities, JCI PLC has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over JCI PLC would not offend traditional notions of fair play and substantial justice.

15.   On information and belief, JCI PLC controls or otherwise directs and authorizes all activities of its subsidiaries and related entities, including, but not limited to Defendants JC Inc. and JC Security, and other members, segments, companies and/or brands of Johnson Controls. *See, e.g., Legal*, JOHNSONCONTROLS.COM, https://www.johnsoncontrols.com/legal/terms (last visited Sep. 28, 2022) ("This website (the 'Site') is provided by Johnson Controls International plc and its affiliated companies ('Johnson Controls')."); *Annual Financial Report* at pp. 4, 13-14, Exhibit 21.1;   *Our   Brands*,   JOHNSONCONTROLS.COM, https://www.johnsoncontrols.com/en_sg/buildings_legacy-back-up/our-brands (last visited Sep. 28, 2022). Directly via its agents in the U.S. and via at least distribution partners, retailers, reseller partners, dealers, professional installers, and other service providers, JCI PLC has placed and continues to place infringing Johnson Controls products into the U.S. stream of commerce. Examples include the manufacture and/or importation of Johnson Controls products into the

United States. *See Annual Financial Report* at pp. 4, 13-14. JCI PLC has placed such products into the stream of commerce with the knowledge and understanding that such products are, will be, and continue to be sold, offered for sale, and/or imported into this District and the State of Texas. *See Litecubes, LLC v. Northern Light Products, Inc.*, 523 F.3d 1353, 1369-70 (Fed. Cir. 2008) ("[T]he sale [for purposes of § 271] occurred at the location of the buyer."); *see also Semcon IP Inc. v. Kyocera Corporation*, No. 2:18-cv-00197-JRG, 2019 WL 1979930, at *3 (E.D. Tex. May 3, 2019) (denying accused infringer's motion to dismiss because plaintiff sufficiently plead that purchases of infringing products outside of the United States for importation into and sales to end users in the U.S. may constitute an offer to sell under § 271(a)).

16.   On information and belief, Johnson Controls utilizes established distribution channels to distribute, market, offer for sale, sell, service, and/or warrant infringing products directly to consumers and other users, including providing links via its own website to online stores, retailers, detailers, resellers, distributors, and dealers offering such products and related services for sale. *See Where to buy*, JOHNSONCONTROLS.COM, https://www.johnsoncontrols.com/locations (accessible via menu "ABOUT US" and link for "Locations,") (last visited Sep. 29, 2022); *Our Brands*, JOHNSONCONTROLS.COM, https://www.johnsoncontrols.com/en_sg/buildings_legacy-back-up/our-brands (last visited Sep. 28, 2022). Such Johnson Controls products and/or services have been sold from and/or in both brick-and-mortar and/or online retail stores within this District and in Texas, with examples being Johnson Controls Beaumont Office located in Beaumont, Texas, other locations listed on the Johnson Controls website, nationwide dealers or distributors, and nationwide online retailers. *See., e.g., Where to buy*, JOHNSONCONTROLS.COM, https://www.johnsoncontrols.com/locations (accessible via menu "ABOUT US" and link for "Locations,") (last visited Sep. 28, 2022)

(showing that at least Johnson Controls services are provided from the office located at 4683 College Street, Beaumont, TX 77707 i.e., in this District); *HVAC TB Controls Tech*, LINKEDIN, https://www.linkedin.com/jobs/johnson-controls-jobs-beaumont-tx?keywords=Johnson%20Controls&location=United%20States&locationId=&geoId=103644278&f_TPR=&f_PP=102249749&position=1&pageNum=0 (last visited Sep. 28, 2022) (indicating that JCI PLC sells product in Beaumont via HVAC TB Controls Tech employees and listing responsibilities for employees in this position that include: "Under general supervision, conducts preventive maintenance, repair, installation, and commissioning and general servicing of systems (including detailed troubleshooting of systems," while noting "Johnson Controls International plc. is an equal employment opportunity . . . employer."). Additionally, Johnson Controls products, including infringing products and/or services, are sold nationwide, in Texas and this District via, for example, direct sales, online retailers and Lux Pro partners. *See, e.g., LUX Pro Catalogue*, p. 7, LUX PRODUCTS CORPORATION, *available for download at* https://pro.luxproducts.com/pro-catalog/ (last accessed, Sep. 28, 2022) (showing, e.g., the LUX CS1 Smart Thermostat for sale to professionals from "Johnson Controls Inc."); LUX, LUXPRODUCTS.COM, https://pro.luxproducts.com/ (last visited Sep. 28, 2022) (offering the LUX CS1 smart thermostat to professionals and providing a link to "GET A QUOTE"); *Lux Thermostat and Timers*, JOHNSONCONTROLS.COM, https://www.johnsoncontrols.com/residential-and-smart-home/lux-thermostat-and-timers (last visited Sep. 28, 2022). Johnson Controls thermostats, including at least Lux thermostats, are offered for sale in this District at least at S. Mckinney Lowe's, 8550 S.H. 121, McKinney, TX 75070, and online at least by SupplyHouse.com. *Lux Kono Smart White Thermostat with Wi-Fi Compatibility*, LOWE'S, https://www.lowes.com/pd/Lux-Kono-Smart-White-Smart-Thermostat-with-Wi-Fi-Compatibility/1000663267 (showing availability in this

District at S. Mckinney Lowe's, 8550 S.H. 121, McKinney, TX 75070); *CS1 Smart Thermostat –*

White (2 Heat – 1 Cool), SUPPLYHOUSE.COM, https://www.supplyhouse.com/Lux-CS1-WH1-

B04-CS1-Smart-Thermostat-White-2-Heat-1-Cool (last visited Sep. 28, 2022). JCI PLC, via its

wholly owned and controlled subsidiaries, also provides application software ("apps") for

download and use in conjunction with and as a part of the wireless communication network that

connects Johnson Controls products and other network devices. *See, e.g., Get Connected,* LUX,

https://www.luxproducts.com/app/ (last visited Sep. 28, 2022) ("Works With: CS1, KONO, &

GEO devices."). These apps are available via digital distribution platforms operated, for example,

by Apple Inc. and Google for download by users and execution on smartphone devices. *Id*.

17.   Based on JCI PLC's connections and relationship with manufacturers, dealers,

retailers, and digital distribution platforms, JCI PLC knows that Texas is a termination point of the

established distribution channel, namely online and brick-and-mortar stores offering Johnson

Controls products and related services and software to third-party manufacturers, distribution

partners, retailers (including national retailers), reseller partners, dealers, service providers,

consumers, and other users in Texas. JCI PLC, therefore, has purposefully directed its activities at

Texas, and should reasonably anticipate being brought in this Court, at least on this basis. *See Icon*

Health & Fitness, Inc. v. Horizon Fitness, Inc., 2009 WL 1025467, at (E.D. Tex. 2009) (finding

that "[a]s a result of contracting to manufacture products for sale in" national retailers' stores, the

defendant "could have expected that it could be brought into court in the states where [the national

retailers] are located").

18.   On information and belief, JCI PLC alone and in concert with other related entities

such as Defendants JC Inc. and JC Security, and subsidiaries, and members, segments, companies

and/or brands of Johnson Controls, manufactures and purposefully places infringing Johnson

Controls products in established distribution channels in the stream of commerce, including in Texas, via third-party manufacturers, distributors, dealers, and reseller partners, such as at least those operating online and/or those listed on Johnson Controls' website. As an example, JCI PLC manufactures Johnson Controls products in Texas and/or imports Johnson Controls products to Texas directly and/or through a related entity or subsidiary and directly sells and offers for sale infringing Johnson Controls products in Texas to resellers or dealers. For example, Johnson Controls Lux Kono thermostats are offered for sale and pickup at least at a Lowe's store located in this District at 8550 S.H. 121, McKinney, TX 75070. *Lux Thermostat and Timers*, JOHNSONCONTROLS.COM, https://www.johnsoncontrols.com/residential-and-smart-home/lux-thermostat-and-timers (last visited Sep. 28, 2022); *Lux Kono Smart White Thermostat with Wi-Fi Compatibility*, LOWE'S, https://www.lowes.com/pd/Lux-Kono-Smart-White-Smart-Thermostat-with-Wi-Fi-Compatibility/1000663267 (showing availability in this District at S. Mckinney Lowe's, 8550 S.H. 121, McKinney, TX 75070). These suppliers, distributors, dealers, and/or resellers import, advertise, offer for sale and/or sell Johnson Controls products and/or related services, such as consultation and installation, via their own websites to U.S. consumers, including to consumers in Texas and this District. Based on JCI PLC's connections and relationship, including supply contracts and other agreements with the U.S. and Texas-based suppliers, distributors, dealers, and/or resellers, such as at least The Home Depot and Lowe's, JCI PLC knows and has known that Texas is a termination point of the established distribution channels for Johnson Controls products. JCI PLC, alone and in concert with subsidiaries Defendants JC Inc. and JC Security, and U.S.-based Members, segments, companies and/or brands of Johnson Controls has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court, at least on this additional basis. *See Ultravision Technologies, LLC v.*

Holophane Europe Limited, 2020 WL 3493626, at *5 (E.D. Tex. 2020) (finding sufficient to make a *prima facie* showing of personal jurisdiction allegations that "Defendants either import the products to Texas themselves or through a related entity"); *see also Bench Walk Lighting LLC v. LG Innotek Co., Ltd et al.*, Civil Action No. 20-51-RGA, 2021 WL 65071, at *7-8 (D. Del., Jan. 7, 2021) (denying motion to dismiss for lack of personal jurisdiction based on the foreign defendant entering into supply contract with U.S. distributor and the distributor sold and shipped defendant's products from the U.S. to the a customer in the forum state).

19.   In the alternative, this Court has personal jurisdiction over JCI PLC under Federal Rule of Civil Procedure 4(k)(2), because the claims for patent infringement in this action arise under federal law, JCI PLC is not subject to the jurisdiction of the courts of general jurisdiction of any state, and exercising jurisdiction over JCI PLC is consistent with the U.S. Constitution.

20.   Venue is proper in this District with respect to Defendant JCI PLC, for example, pursuant to 28 U.S.C. § 1391. Defendant JCI PLC is a foreign entity and may be sued in any district under 28 U.S.C. § 1391(c). *See also In re HTC Corporation*, 889 F.3d 1349, 1357 (Fed. Cir. 2018) ("The Court's recent decision in *TC Heartland* does not alter" the alien-venue rule.).

B.   Defendant JC Inc.

21.   On information and belief, Defendant JC Inc. is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents

and residents of this District vicariously through and/or in concert with its partners, alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. For example, JC Inc. and parent Defendant JCI PLC and JCI PLC's U.S.-based subsidiaries, and members, segments, companies and/or brands of Johnson Controls manufacture, import, distribute, offer for sale, sell, and induce infringing use of Johnson Controls products to distribution partners, retailers (including national retailers), resellers, dealers, service providers, consumers, and other users.

22.   On information and belief, this Court has personal jurisdiction over JC Inc., directly and/or indirectly via the activities of JC Inc.'s intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including parent Defendant JCI PLC and U.S.-based subsidiaries, and members, segments, companies and/or brands of Johnson Controls.

23.   On information and belief, JC Inc. utilizes established distribution channels to distribute, market, offer for sale, sell, service, and/or warrant infringing products directly to consumers and other users, including offering such products and/or related services for sale. Johnson Controls products and services have been sold from and/or in both brick-and-mortar stores and online retail stores by entities within this District and in Texas. Alone and in concert with or via direction and control of or by at least these entities, JC Inc. has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within the United States, giving rise to this action and/or has established minimum contacts with Texas. For example, JC Inc. operates within a global network of sales and distribution of Johnson Controls products that includes subsidiaries of Johnson Controls, retail stores and showrooms, dealers, resellers, professional installers, and distributors operating in Texas, including this District.

24.   As another example, on information and belief, JC Inc. maintains an office in this District through at least one brick-and-mortar location at 4689 College Street, Beaumont, Texas, which location is adjacent to and/or forms at least a part of a Johnson Controls Beaumont Office located at 4683 College Street, Beaumont, Texas 77707. *See., e.g., Where to buy*, JOHNSONCONTROLS.COM, https://www.johnsoncontrols.com/locations (accessible via menu "ABOUT US" and link for "Locations,") (last visited Sep. 28, 2022) (showing that Johnson Controls services are provided from the office located at 4683 College Street, Beaumont, TX 77707, i.e., in this District); *Property ID: 207096 For Year 2022*, JEFFERSON CAD, https://esearch.jcad.org/Property/View/207096 (showing that "Johnson Controls Inc." owns property located at 4689 College Street, Beaumont, TX); *HVAC TB Controls Tech*, LINKEDIN, https://www.linkedin.com/jobs/johnson-controls-jobs-beaumont-

tx?keywords=Johnson%20Controls&location=United%20States&locationId=&geoId=103644278&f_TPR=&f_PP=102249749&position=1&pageNum=0 (last visited Sep. 28, 2022) ("Under general supervision, conducts preventive maintenance, repair, installation, and commissioning and general servicing of systems (including detailed troubleshooting of systems. . . . Johnson Controls International plc. is an equal employment opportunity . . . employer.").

25.   On information and belief, as a part of Johnson Controls' global manufacturing and distribution network, JC Inc. also purposefully places infringing Johnson Controls products in established distribution channels in the stream of commerce, including in Texas, via distribution partners, retailers (including national retailers), resellers, dealers, brand ambassadors, service providers, consumers, and other users. *See, e.g., LUX Pro Catalogue*, p. 7, LUX PRODUCTS CORPORATION, *available for download at* https://pro.luxproducts.com/pro-catalog/ (last accessed, Sep. 28, 2022) (showing, e.g., the LUX CS1 Smart Thermostat for sale to professionals from

"Johnson Controls Inc."); LUX, LUXPRODUCTS.COM, https://pro.luxproducts.com/ (last visited Sep. 28, 2022) (offering the LUX CS1 smart thermostat to professionals and providing a link to "GET A QUOTE"); *Lux Thermostat and Timers*, JOHNSONCONTROLS.COM, https://www.johnsoncontrols.com/residential-and-smart-home/lux-thermostat-and-timers (last visited Sep. 28, 2022); *CS1 Smart Thermostat – White (2 Heat – 1 Cool)*, SUPPLYHOUSE.COM, https://www.supplyhouse.com/Lux-CS1-WH1-B04-CS1-Smart-Thermostat-White-2-Heat-1-Cool (last visited Sep. 28, 2022).   For example, JC Inc. provides infringing Johnson Controls product under the York brand. As stated in the 2021 annual 10-K report of JCI PLC, "Johnson Controls . . . was renamed to Johnson Controls, Inc. in 1974. In 2005, Johnson Controls acquired York International, a global supplier of heating, ventilating, air-conditioning ("HVAC") and refrigeration equipment and services." *Annual Financial Report,* p. 3. Furthermore, York Hx3 Thermostats are offered for sale in this District by at least one nationwide online retailer, for example, EXPRESSOVERSTOCK. *York Hx3 Touch Screen WiFi Thermostat (White) THXU430W*, EXPRESSOVERSTOCK, https://www.expressoverstock.com/york-hx3-touch-screen-wifi-thermostat-white-thxu430w.html (last visited Sep. 29, 2022).   Therefore, JC Inc., alone and in concert with other members, segments, companies and/or brands of Johnson Controls, its parent entity Defendant JCI PLC and its U.S. based Johnson Controls subsidiaries has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court, at least on this basis. Through its own conduct and through direction and control of its subsidiaries or control by other Defendant JCI PLC, JC Inc. has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over JC Inc. would not offend traditional notions of fair play and substantial justice.

26.   Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). As alleged herein, Defendant JC Inc. has committed acts of infringement in this District. As further alleged herein, Defendant JC Inc., via its own operations and/or employees, has a regular and established place of business in this District, for example, in Jefferson County and at 4683 College Street, Beaumont, TX 77707, among other Johnson Controls locations owned, leased and/or operated in this District. Accordingly, JC Inc. may be sued in this district under 28 U.S.C. § 1400(b).

C.   Defendant JC Security

27.   On information and belief, Defendant JC Security is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its partners, alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. For example, JC Security and parent Defendant JCI PLC and JCI PLC's U.S.-based subsidiaries, and members, segments, companies and/or brands of Johnson Controls manufacture, import, distribute, offer for sale, sell, and induce infringing use of Johnson Controls products to distribution partners, retailers (including national retailers), resellers, dealers, service providers, consumers, and other users.

28.   On information and belief, this Court has personal jurisdiction over JC Security, directly and/or indirectly via the activities of JC Security's intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including parent Defendant JCI PLC and U.S.-based subsidiaries, and members, segments, companies and/or brands of Johnson Controls.

29.   On information and belief, JC Security utilizes established distribution channels to distribute, market, offer for sale, sell, service, and/or warrant infringing products directly to consumers and other users, including offering such products and/or related services for sale. Johnson Controls products and services have been sold from and/or in both brick-and-mortar stores and online retail stores by entities within this District and in Texas. Alone and in concert with or via direction and control of or by at least these entities, JC Security has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within the United States, giving rise to this action and/or has established minimum contacts with Texas. For example, JC Security operates within a global network of sales and distribution of Johnson Controls products that includes subsidiaries of Johnson Controls, retail stores and showrooms, dealers, resellers, professional installers, and distributors operating in Texas, including this District.

30.   As another example, on information and belief, JC Security maintains an office in this District, including at least a location in Beaumont, Texas, as at least a part of a Johnson Controls Beaumont Office located at 4683 College Street, Beaumont, Texas 77707. *See., e.g., "Johnson Controls Security" Search Results*, JEFFERSON CAD, https://esearch.jcad.org/Search/Result?keywords=Johnson%20Controls (last visited Sep. 30, 2022) (showing that "Johnson Controls Security" owns property located in this District at least in Beaumont, TX); *Where to buy*, JOHNSONCONTROLS.COM,

https://www.johnsoncontrols.com/locations (accessible via menu "ABOUT US" and link for "Locations,") (last visited Sep. 28, 2022) (showing that Johnson Controls services are provided from the office located at 4683 College Street, Beaumont, TX 77707, i.e., in this District); *Annual Financial Report* at 102-03 (Johnson Controls' "Building Solutions North America designs, sells, installs and services . . . controls, building management, . . . integrated electronic security and integrated fire-detection and suppression systems for commercial, industrial, retail, small business, institutional and governmental customers in the United States and Canada. . . . The Global Products business also designs, manufactures and sells fire protection, fire suppression and security products, including intrusion security, anti-theft devices, access control, and video surveillance and management systems, for commercial, industrial, retail, residential, small business, institutional and governmental customers worldwide.")

31.   On information and belief, as a part of Johnson Controls' global manufacturing and distribution network, JC Security also purposefully places infringing Johnson Controls products in established distribution channels in the stream of commerce, including in Texas, via distribution partners, retailers (including national retailers), resellers, dealers, brand ambassadors, service providers, consumers, and other users. *See, e.g., DSC Product Catalog*, p. 16, JOHNSON CONTROLS, *available for download at* https://cms.dsc.com/download.php?t=8&id=27 (last visited, Sep. 30, 2022) (showing Johnson Controls' Tyco DSC Iotega WS900x security panel for sale from "Johnson Controls", "Tyco", and "DSC"); *DSC WS900-91S IOTEGA WIRELESS*, SILARIUS, https://silarius.com/products/dsc-ws900-91s-iotega-wireless (last visited Sep. 30, 2022) (offering the DSC Iotega WS900-91S wireless security panel for sale to individuals in the United States, including individuals in Texas and this District).   For example, JC Security, directly and/or indirectly via the activities of JC Security's intermediaries, agents, related entities, distributors,

importers, customers, subsidiaries, and/or consumers, including parent Defendant JCI PLC and

U.S.-based subsidiaries, and members, segments, companies and/or brands of Johnson Controls.

provides infringing Johnson Controls product under the brand Johnson Controls, Tyco, DSC,

and/or Iotega. Furthermore, DSC SN-750EF1 security cameras with built-in Wi-Fi support are

offered for sale in this District by at least one nationwide online retailer, for example, JMAC

Supply   Corp.   *See,   e.g.,   DSC   SN-750EF1*,   JMAC   SUPPLY   CORP,

https://www.jmac.com/DSC_SN_750EF1_p/tyco-dsc-sn-750ef1.htm (last visited Sep. 30, 2022);

720P   HD   (1MP)   IP   Security   Camera   -   SN-750EF1,   DSC,

https://www.dsc.com/index.php?n=products&o=view&id=2635 (last visited Sep. 30, 2022)

(noting "Wi-Fi support built in").   Therefore, JC Security, alone and in concert with other

members, segments, companies and/or brands of Johnson Controls, its parent entity Defendant JCI

PLC and its U.S. based Johnson Controls subsidiaries has purposefully directed its activities at

Texas, and should reasonably anticipate being brought in this Court, at least on this basis. Through

its own conduct and through direction and control of its subsidiaries or control by other Defendant

JCI PLC, JC Security has committed acts of direct and/or indirect patent infringement within

Texas, and elsewhere within the United States, giving rise to this action and/or has established

minimum contacts with Texas such that personal jurisdiction over JC Security would not offend

traditional notions of fair play and substantial justice.

32.   Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). As

alleged herein, Defendant JC Security has committed acts of infringement in this District. As

further alleged herein, Defendant JC Security, via its own operations and/or employees has a

regular and established place of business in this District at least in Jefferson County, for example,

Beaumont, TX, among other Johnson Controls locations owned, leased and/or operated in this

District.   Examples include a "Jefferson Controls Beaumont Office" at 4683 College Street, Beaumont, TX 77707 in this District and various locations listed in the Jefferson County and Collin County property records, some of which are listed below:

7	2689810 P-9000-213-3972-1	JOHNSON CONTROLS SECURITY SOLUTIONS LLC	Various Locations Crc Spl	BPP at Various Locations Crc Spl	Currently Unavailable
8	2689813 P-9000-213-3973-1	JOHNSON CONTROLS SECURITY SOLUTIONS LLC	Various Locations Cwy Swy	BPP at Various Locations Cwy Swy	Currently Unavailable
9	2702451 P-9000-214-3457-1	JOHNSON CONTROLS SECURITY SOLUTIONS LLC	Various Locations Cmc Sfr	BPP at Various Locations Cmc Sfr	Currently Unavailable
10	2702452 P-9000-214-3458-1	JOHNSON CONTROLS SECURITY SOLUTIONS LLC	Various Locations Cml Sml	BPP at Various Locations Cml Sml	Currently Unavailable
11	2702453 P-9000-214-3459-1	JOHNSON CONTROLS SECURITY SOLUTIONS LLC	Various Locations Cmr Spl	BPP at Various Locations Cmr Spl	Currently Unavailable
12	2702454 P-9000-214-3460-1	JOHNSON CONTROLS SECURITY SOLUTIONS LLC	Various Locations Cpl Sfr	BPP at Various Locations Cpl Sfr	Currently Unavailable
13	2702455 P-9000-214-3461-1	JOHNSON CONTROLS SECURITY SOLUTIONS LLC	Various Locations Cpr Spr	BPP at Various Locations Cpr Spr	Currently Unavailable
14	2755928 P-9000-217-4323-1	JOHNSON CONTROLS SECURITY SOLUTIONS LLC	Various Locations Cmc Sal	BPP at Various Locations Cmc Sal	Currently Unavailable
15	2850929 P-9000-222-3725-1	JOHNSON CONTROLS SECURITY SOLUTIONS LLC	Various Locations Cfr Spr	BPP at Various Locations Cfr Spr	Currently Unavailable
16	2850930 P-9000-222-3726-1	JOHNSON CONTROLS SECURITY SOLUTIONS LLC	Various Locations Cla Sco	BPP at Various Locations Cla Sco	Currently Unavailable

Property Search, COLLINCAD.ORG,

https://www.collincad.org/propertysearch?owner_name=johnson_controls (last visited Oct. 3,

2022). Accordingly, JC Security may be sued in this district under 28 U.S.C. § 1400(b).

33.   On information and belief, Defendants JCI PLC, JC Inc. and JC Security each have

significant ties to, and presence in, the State of Texas and this District, making venue in this District

both proper and convenient for this action.

THE ASSERTED PATENTS AND TECHNOLOGY

34.   The Asserted Patents cover various aspects of monitoring, detecting intrusions, and encrypting and decrypting wireless communications networks, including networks created between Defendants' smart home devices.

35.   The '678 patent involves detecting intrusions into a wireless local or metropolitan area network. The disclosed intrusion detection techniques include monitoring transmission between stations of the network, where each station has its own media access layer (MAC) address. The monitoring is done to detect failed attempts to authenticate the MAC addresses. Upon detection of a number of failed attempts to authenticate, an intrusion alert may be generated.

36.   The '961 patent involves allocating channels in mobile ad hoc networks. The patent describes dynamic channel allocation in such networks to efficiently make use of a plurality of channels. In such networks, wireless communication links connect wireless mobile nodes over multiple separate channels at different frequencies. The disclosed techniques for channel allocation include monitoring link performance on one channel based on a quality of service (QoS) threshold. When the monitored link performance falls below the QoS threshold, other available separate channels are scouted. Scouting may include switching to a second separate channel at a different frequency. A channel activity query may be broadcast to determine link performance of the second separate channel. Replies to the query are processed to determine the link performance, and channel activity may be updated for each separate channel based on the replies.

37.   The '572 patent involves providing secure wireless local area networks (LAN). A device for securing such a LAN may include a housing with a wireless transceiver carried by the housing. A medium access controller (MAC) is also carried by the housing. A cryptography circuit may be connected to the MAC controller and the transceiver. The circuit may encrypt both address

and data information by at least adding a plurality of encrypting bits to be transmitted. And the cryptography circuit may decrypt both address and data information upon reception.

38.   On information and belief, a significant portion of the operating revenue of Defendants is derived from the manufacture, distribution, sale, and use of home and business networking, IoT, and smart home products and components, which are manufactured in or imported into the United States, distributed to resellers, dealers, and third-party manufacturers, and ultimately sold to and used by U.S. consumers. For example, Johnson Controls reported that Building Solutions North America had 8,685 million dollars (8.685 billion dollars) in sales and Global Products had 8,602 million dollars in sales (8.602 billion U.S. dollars) in the year ended September 30, 2021. *See Annual Financial Report,* p. 35.

39.   The Asserted Patents cover Defendants' home and business IoT and smart home products and components, software, services, and processes related to same that generally connect to other devices in a network or other networks using a wireless protocol, such as ZigBee and Wi-Fi. *See, e.g., Residential and Smart Home*, JOHNSONCONTROLS.COM, https://www.johnsoncontrols.com/residential-and-smart-home (last visited Sep. 30, 2022); *LUX Products Corp. Joins the ZigBee Alliance*, LUX, https://www.luxproducts.com/lux-products-corp-joins-the-zigbee-alliance/ (July 6, 2016) (last visited Sep. 30, 2022) ("'We are excited to be a part of the ZigBee Alliance.' . . . . LUX is a privately-held company based in Philadelphia, Pennsylvania with an R&D center in Hong Kong, manufacturing in Asia and packaging and distribution plant in Laredo, Texas. . . . The company sells more than one million thermostats each year."). Defendants' infringing Johnson Controls products include, but are not limited to, devices enabled or compliant with Wi-Fi and/or ZigBee, including without limitation thermostats (for example, LUX CS1, LUX GEO, LUX KONO, LUX KONOz, YORK Hx and YORK Hx3

thermostats); security cameras (for example, Johnson Controls and/or DSC SN-629F1, SN-750EF1, and 631PT1 security cameras); security system panels, modules or hubs (for example, Johnson Controls and/or DSC and/or IOTEGA WS900x panels; Johnson Controls and/or DSC and/or PowerSeries ProHSM3WIFI WiFi adapter modules; and Johnson Controls and/or DSC and/or Telguard ASG1000-1T5NAS interactive hubs); wireless alarm and/or home automation gateways (for example, Johnson Controls and/or Tyco and/or Visonic PowerMaster-360R Modern Wireless Alarm and Home Automation Gateways); home security panels (for example, Johnson Controls and/or Qolsys IQ Panel 4 and IQ Panel 2+ security panels); smart remotes and routers (for example, Johnson Controls and/or Qolsys IQ Remotes, IQ WiFi 6 and IQ WiFi security panels); intrusion detectors (for example, Johnson Controls and/or Tyco and/or Visonic intrusion detectors); Visonic ZigBee solutions and products (for example, ZigBee compatible GB-540, MCT-350, MCT-370, MP-840 and MP-841 intrusion detectors); field bus systems (for example, Johnson Controls FX-ZFR Series Wireless Field Bus System, which can use ZigBee); ZigBee and/or WiFi modules and interfaces (for example, smartphone and tablet Wi-Fi interfaces); and related accessories and software (all collectively referred to as the "Accused Products"). These Accused Products infringe the Asserted Patents by at least their manufacture, importation, distribution, sale, and use in the U.S.

40.   The Asserted Patents cover Accused Products of Johnson Controls that use the ZigBee protocol to communicate with other devices on a communication network, including those of third-party manufacturers. Examples of the Johnson Controls' ZigBee products include the KONOz Smart thermostat (including model number KN-Z-WH1-B04) which "uses the Zigbee protocol to easily communicate with your home automation hub," and "makes controlling KONOz from existing apps a snap," which is shown below:
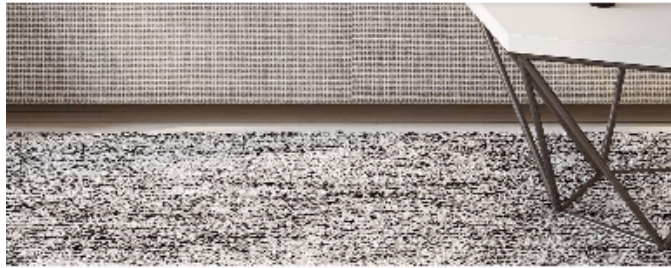
Get Connected

Seamless Integration with Your Smart Home

KONOz is compatible with the leading connected home platforms so you can expand with the peace of mind of not having to run another home automation system. KONOz uses the Zigbee protocol to easily communicate with your home automation hub. This makes controlling KONOz from existing apps a snap! KONOz will be the solution to your Smart Home Automation needs with Zero Degrees of Difficulty
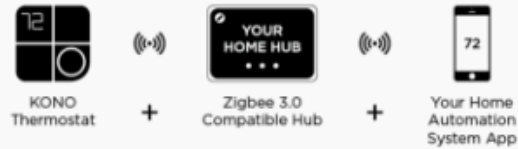
Product Features

Model Number
KN-Z-WH1-B04

Power Source
4 AA Alkaline Batteries ,
Wall – Powered (24Vac C-Wire)
LUX Power Bridge

Heating / Cooling
Universal compatibility with conventional forced air, gas, oil & electric furnaces up to 2H/1C, heat pumps with or without Aux/Emergency heat and Hydronic (hot water) heat

Accessories

Decor Snap Covers™ Available separately

See LUX KONOz, HTTPS://WWW.LUXPRODUCTS.COM/KONOZ/ (last visited Sep. 30, 2022).

41.   ZigBee protocols, which are covered by the Asserted Patents and utilized by certain Accused Products, are based on the IEEE 802.15.4 standard for wireless network communication.

Below is an excerpt from the technical specification for ZigBee protocols describing the basic

architecture and standards that enable wireless network communication.

1.1   Protocol Description

The ZigBee Alliance has developed a very low-cost, very low-power-consumption, two-way, wireless communications standard. Solutions adopting the ZigBee standard will be embedded in consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor applications, toys, and games.

1.1.3   Stack Architecture

The ZigBee stack architecture is made up of a set of blocks called layers. Each layer performs a specific set of services for the layer above. A data entity provides a data transmission service and a management entity provides all other services. Each service entity exposes an interface to the upper layer through a service access point (SAP), and each SAP supports a number of service primitives to achieve the required functionality.

The IEEE 802.15.4 standard defines the two lower layers: the physical (PHY) layer and the medium access control (MAC) sub-layer. The ZigBee Alliance builds on this foundation by providing the network (NWK) layer and the framework for the application layer. The application layer framework consists of the application support sub-layer (APS) and the ZigBee device objects (ZDO). Manufacturer-defined application objects use the framework and share APS and security services with the ZDO.

The PHY layer operates in two separate frequency ranges: 868/915 MHz and 2.4 GHz. The lower frequency PHY layer covers both the 868 MHz European band and the 915 MHz band, used in countries such as the United States and Australia. The higher frequency PHY layer is used virtually worldwide. A complete description of the PHY layers can be found in [B1].

ZigBee Specification, revision r21 at 1, THE ZIGBEE ALLIANCE, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf (August 5, 2015).

42.   The IEEE 802.15.4 standard based mobile ad-hoc network, utilized by the Accused Products, is a type of Low-Rate Wireless Personal Area Network (LR-WPAN) that allows transmission of data between plurality of network nodes.

IEEE STANDARDS ASSOCIATION   ◈**IEEE**

**IEEE Standard for
Local and metropolitan area networks—**

**Part 15.4: Low-Rate Wireless Personal Area
Networks (LR-WPANs)**

4. General description

4.1 General

An LR-WPAN is a simple, low-cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements. The main objectives of an LR-WPAN are ease of installation, reliable data transfer, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol.

Two different device types can participate in an IEEE 802.15.4 network: a full-function device (FFD) and a reduced-function device (RFD). An FFD is a device that is capable of serving as a personal area network (PAN) coordinator or a coordinator. An RFD is a device that is not capable of serving as either a PAN coordinator or a coordinator. An RFD is intended for applications that are extremely simple, such as a light switch or a passive infrared sensor; it does not have the need to send large amounts of data and only associates with a single FFD at a time. Consequently, the RFD can be implemented using minimal resources and memory capacity.

4.2 Components of the IEEE 802.15.4 WPAN

A system conforming to this standard consists of several components. The most basic is the device. Two or more devices communicating on the same physical channel constitute a WPAN. However, this WPAN includes at least one FFD, which operates as the PAN coordinator.

Page 8, http://ecee.colorado.edu/~liue/teaching/comm_standards/2015S_zigbee/802.15.4-2011.pdf

43.   In the ZigBee network of the Accused Products, a network device/node is configured to monitor the performance of a channel-in-use based on its energy measurement. As described

below, if the measurement value is higher than the value on other channels (threshold), it indicates

interference is present on the channel, consequently resulting in transmission failures.

ANNEX E   OPERATING NETWORK MANAGER AS NETWORK CHANNEL MANAGER FOR INTERFERENCE REPORTING AND RESOLUTION

A single device can become the Network Channel Manager. This device acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default address of the network manager is the coordinator, however this can be updated by sending a Mgmt_NWK_Update_req command with a different short address for the network channel manager. The device that is the Network Channel Manager shall set the network manager bit in the server mask in the node descriptor and shall respond to System_Server_Discovery_req commands.

Each router or coordinator is responsible for tracking transmit failures using the TransmitFailure field in the neighbor table and also keeping a NIB counter for total transmissions attempted. A device that detects a significant number of transmission failures may take action to determine if interference is a cause.   The following steps are an example of that procedure[1]:

1. Conduct an energy scan on all channels within the current PHY. If this energy scan does not indicate higher energy on the current channel then other channels, no action is taken. The device should continue to operate as normal and the message counters are not reset. However, repeated energy scans are not desirable as the device is off the network during these scans and therefore implementations should limit how often a device with failures conducts energy scans.

2. If the energy scan does indicate increased energy on the channel in use, a Mgmt_NWK_Update_notify should be sent to the Network Manager to indicate interference is present. This report is sent as an APS Unicast with acknowledgement and once the acknowledgment is received the total transmit and transmit failure counters are reset to zero.

Page 516, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

44.   As described below, the network manager node facilitates switching to a different

channel, i.e., scouting available separate channels, if the performance on the channel-in-use falls

below a threshold (i.e., when the current channel's energy is higher than channels, indicating

increased interference, and thereby resulting in multiple transmission failures). The network nodes

switch to a new (second) channel whose energy level is lowest or below an acceptable threshold.

ZigBee
Control your world

A single device can become the Network Channel Manager. This device acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default address of the network manager is the coordinator, however this can be updated by sending a Mgmt_NWK_Update_req command with a different short address for the network channel manager. The device that is the Network Channel Manager shall set the network manager bit in the server mask in the node descriptor and shall respond to System_Server_Discovery_req commands.

Each router or coordinator is responsible for tracking transmit failures using the TransmitFailure field in the neighbor table and also keeping a NIB counter for total transmissions attempted. A device that detects a significant number of transmission failures may take action to determine if interference is a cause.   The following steps are an example of that procedure[1]:

1.   Conduct an energy scan on all channels within the current PHY. If this energy scan does not indicate higher energy on the current channel then other channels, no action is taken. The device should continue to operate as normal and the message counters are not reset. However, repeated energy scans are not desirable as the device is off the network during these scans and therefore implementations should limit how often a device with failures conducts energy scans.

2.   If the energy scan does indicate increased energy on the channel in use, a Mgmt_NWK_Update_notify should be sent to the Network Manager to indicate interference is present. This report is sent as an APS Unicast with acknowledgement and once the acknowledgment is received the total transmit and transmit failure counters are reset to zero.

3.   To avoid a device with communication problems from constantly sending reports to the network manager, the device should not send a Mgmt_NWK_Update_notify more than 4 times per hour.

Upon receipt of an unsolicited Mgmt_NWK_Update_notify, the network manager must evaluate if a channel change is required in the network. The specific mechanisms the network manager uses to decide upon a channel change are left to the implementers. It is expected that implementers will apply different methods to best determine when a channel change is required and how to select the most appropriate channel. The following is offered as guidance for implementation.

Comment: Zigbee network further allows network devices/nodes to function as Network Channel Manager. The network manager node facilitates switching to a different channel if the performance on the channel-in-use falls below a threshold (i.e., when the current channel's energy is higher than channels, indicating increased interference, and thereby resulting in multiple transmission failures).

Page 516, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

45.   With reference to the above graphic and as further described below, the ZigBee

network of the Accused Products further allows using the command to request interference reports,

i.e., broadcasts a channel activity query, from the network nodes, which involves scanning the

energy level on all the channels including the newly switched (second) channel. The interference

report will represent determining the performance for the second channel. In addition, the most recent energy level value and failure rate (indicative of the channel performance/activity) corresponding to the channels is stored, i.e., the channel activity is updated.

The network manager may do the following:

1. Wait and evaluate if other reports from other devices are received. This may be appropriate if there are no other failures reported. In this case the network manager should add the reporting device to a list of devices that have reported interference. The number of devices on such a list would depend on the size of the network. The network manager can age devices out of this list.

2. Request other interference reports using the Mgmt_NWK_Update_req command. This may be done if other failures have been reported or the network manager device itself has failures and a channel change may be desired. The network manager may request data from the list of devices that have reported interference plus other randomly selected routers in the network. The network manager should not request an update from the device that has just reported interference since this data is fresh already.

3. Upon receipt of the Mgmt_NWK_Update_notify, the network manager shall determine if a channel change is required using whatever implementation specific mechanisms are considered appropriate. The network manager device with just one channel allowed in the *apsChannelMask* parameter must not issue the Mgmt_Nwk_Update_Req command to request other devices to change the current channel. However, the network manager may report channel quality issues to the application.

4. If the above data indicate a channel change should be considered, the network manager completed the following:

   a. Select a single channel based on the Mgmt_NWK_Update_notify based on the lowest energy. This is the proposed new channel. If this new channel does not have an energy level below an acceptable threshold, a channel change should not be done. Additionally, a new channel shall not belong to a PHY different from the one on which a network manager is operating now.

5. Prior to changing channels, the network manager should store the energy scan value as the last energy scan value and the failure rate from the existing channel as the last failure rate. These values are useful to allow comparison of the failure rate and energy level on the previous channel to evaluate if the network is causing its own interference.

6. The network manager should broadcast a Mgmt_NWK_Update_req notifying devices of the new channel. The broadcast shall be to all devices with RxOnWhenIdle equal to TRUE. The network manager is responsible for incrementing the *nwkUpdateId* parameter from the NIB and including it in the Mgmt_NWK_Update_req. The network manager shall set a timer based on the value of *apsChannelTimer* upon issue of a Mgmt_NWK_Update_req that changes channels and shall not issue another such command until this timer expires. However, during this period, the network manager can complete the above analysis. However, instead of changing channels, the network manager would report to the local application using Mgmt_NWK_Update_notify and the application can force a channel change using the Mgmt_NWK_Update_req.

Upon receipt of a Mgmt_NWK_Update_req with a change of channels, the local network manager shall set a timer equal to the *nwkNetworkBroadcastDeliveryTime* and shall switch channels upon expiration of this timer. Each node shall also increment the *nwkUpdateId* parameter and also reset the total transmit count and the transmit failure counters.

Page 517, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

46.   The Asserted Patents also cover Accused Products of Johnson Controls that utilize the Wi-Fi protocol. Examples of such products include the LUX CS1 Smart Thermostat and LUX App. As shown below, the LUX CS1 and LUX App are Wi-Fi (IEEE 802.11) compliant:

CS1, LUX, https://pro.luxproducts.com/cs1/ (last visited Sep. 30, 2022).

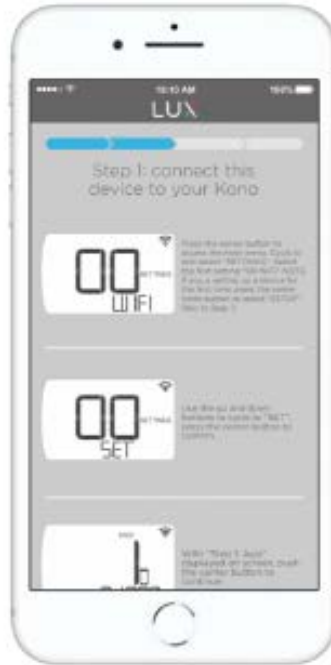**PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT** – Page 32

So Smart its Simple

The new LUX App is packed full of enhanced smart features to make your life both easy and comfortable. The app is user friendly and includes an informative home screen, an intuitive smart scheduling interface, Home and Away Aware smart geofencing, and even the Accuweather so you can always be one step ahead. Smart technology has never been this simple. The LUX App is compatible with the LUX Smart suite of thermostats the all new and affordable CS1 Smart Thermostat, KONO, and GEO devices all utilize the smart app available on IOS & Android devices. Best of all, its free to download!

So Smart its Simple, LUX, *https://www.luxproducts.com/app/* (last visited Sep. 30, 2022).

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT – Page 33

The app will present a set of instructions specific to your device.
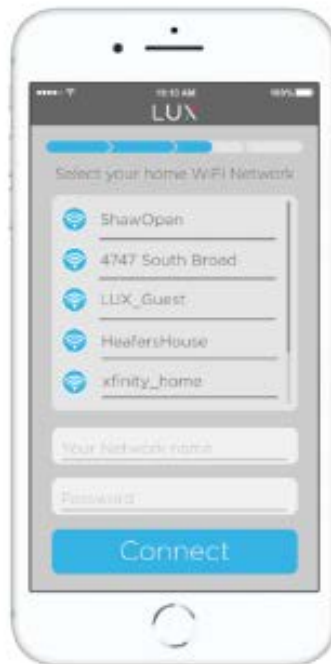
After connecting to the thermostat network, return to the LUX
app and connect to your home wifi network.

See Frequently Asked Questions, LUX, https://www.luxproducts.com/faqs/#1591276519431-a8400425-c02e (last visited Sep. 30, 2022).

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT – Page 34

47.   The Accused Products include an intrusion detection method for a local or metropolitan area. As described below, the IEEE 802.11 authentication methods utilized by the Accused Products utilize a TKIP that includes a "MIC" to defend against active attacks.

IEEE Std 802.11™-2007
(Revision of
IEEE Std 802.11-1999)

8.3.2.3 TKIP MIC

Flaws in the IEEE 802.11 WEP design cause it to fail to meet its goal of protecting data traffic content from casual eavesdroppers. Among the most significant WEP flaws is the lack of a mechanism to defeat message forgeries and other active attacks. To defend against active attacks, TKIP includes a MIC, named Michael. This MIC offers only weak defenses against message forgeries, but it constitutes the best that can be achieved with the majority of legacy hardware. TKIP uses different MIC keys depending on the direction of the transfer as described in 8.6.1 and 8.6.2.

Annex H contains an implementation of the TKIP MIC. It also provides test vectors for the MIC.

8.3.2.3.1 Motivation for the TKIP MIC

Before defining the details of the MIC, it is useful to review the context in which this mechanism operates. Active attacks enabled by the original WEP design include the following:

— Bit-flipping attacks
— Data (payload) truncation, concatenation, and splicing
— Fragmentation attacks
— Iterative guessing attacks against the key
— Redirection by modifying the MPDU DA or RA field
— Impersonation attacks by modifying the MPDU SA or TA field

The MIC makes it more difficult for any of these attacks to succeed.

All of these attacks remain at the MPDU level with the TKIP MIC. The MIC, however, applies to the MSDU, so it blocks successful MPDU-level attacks. TKIP applies the MIC to the MSDU at the transmitter and verifies it at the MSDU level at the receiver. If a MIC check fails at the MSDU level, the implementation shall discard the MSDU and invoke countermeasures (see 8.3.2.4).

Page 217, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

48.   Stations (STAs) in an IEEE 802.11 network of the Accused Products associate with each other using a robust security network association (RSNA). As described below, RSNA supports intrusion detection by employing authentication mechanisms and data frame protection mechanisms (such as, temporal key integrity protocol - TKIP) between the STAs. Data is

exchanged between the STAs in the form of MPDUs (medium access control (MAC) protocol data units). The MAC frame (MPDU) comprises a MSDU (information frame) in the frame body, and four addresses that identify, among others, source MAC address (SA) and destination MAC address (DA) for the MSDU.

IEEE Std 802.11™-2007
(Revision of
IEEE Std 802.11-1999)

5.1.1.4 Interaction with other IEEE 802® layers

IEEE Std 802.11 is required to appear to higher layers [logical link control (LLC)] as a wired IEEE 802 LAN. This requires that the IEEE 802.11 network handle STA mobility within the MAC sublayer. To meet reliability assumptions (that LLC makes about lower layers), it is necessary for IEEE Std 802.11 to incorporate functionality that is untraditional for MAC sublayers.

In a robust security network association (RSNA), IEEE Std 802.11 provides functions to protect data frames, IEEE Std 802.1X-2004 provides authentication and a Controlled Port, and IEEE Std 802.11 and IEEE Std 802.1X-2004 collaborate to provide key management. All STAs in an RSNA have a corresponding IEEE 802.1X entity that handles these services. This standard defines how an RSNA utilizes IEEE Std 802.1X-2004 to access these services.

3.126 robust security network (RSN): A security network that allows only the creation of robust security network associations (RSNAs). An RSN can be identified by the indication in the RSN information element (IE) of Beacon frames that the group cipher suite specified is not wired equivalent privacy (WEP).

3.127 robust security network association (RSNA): The type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-Way Handshake. Note that the existence of an RSNA by a pair of devices does not of itself provide robust security. Robust security is provided when all devices in the network use RSNAs.

5.2.3.2 RSNA

An RSNA defines a number of security features in addition to wired equivalent privacy (WEP) and IEEE 802.11 authentication. These features include the following:

— Enhanced authentication mechanisms for STAs
— Key management algorithms
— Cryptographic key establishment
— An enhanced data cryptographic encapsulation mechanism, called Counter mode with Cipher-block chaining Message authentication code Protocol (CCMP), and, optionally, Temporal Key Integrity Protocol (TKIP).

Page 72, 61, 75 https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

49.   In the TKIP protocol of the Accused Products, an MSDU transmitter STA calculates cryptographic message integrity code (MIC) using the MAC addresses (SA & DA) corresponding

to the MSDU. As described below, the transmission is monitored if the MIC (which is obtained using the MAC addresses) is verified/authenticated at the receiver. MSDUs with invalid MICs are discarded and countermeasures are invoked.

8.3 RSNA data confidentiality protocols

8.3.1 Overview

This standard defines two RSNA data confidentiality and integrity protocols: TKIP and CCMP. Implementation of CCMP shall be mandatory in all IEEE 802.11 devices claiming RSNA compliance. Implementation of TKIP is optional for an RSNA. A design aim for TKIP was that the algorithm should be implementable within the capabilities of most devices supporting only WEP, so that many such devices would be field-upgradeable by the supplier to support TKIP.

8.3.2 Temporal Key Integrity Protocol (TKIP)

8.3.2.1 TKIP overview

The TKIP is a cipher suite enhancing the WEP protocol on pre-RSNA hardware. TKIP modifies WEP as follows:

a) A transmitter calculates a keyed cryptographic message integrity code (MIC) over the MSDU SA and DA, the MSDU priority (see 8.3.2.3), and the MSDU plaintext data. TKIP appends the computed MIC to the MSDU data prior to fragmentation into MPDUs. The receiver verifies the MIC after decryption, ICV checking, and defragmentation of the MPDUs into an MSDU and

discards any received MSDUs with invalid MICs. TKIP's MIC provides a defense against forgery attacks.

b) Because of the design constraints of the TKIP MIC, it is still possible for an adversary to compromise message integrity; therefore, TKIP also implements countermeasures. The countermeasures bound the probability of a successful forgery and the amount of information an attacker can learn about a key.

Page 213, 214 https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

50.   The TKIP MIC implementation of the Accused Products prevents intrusion attacks, such as, message redirection by modifying destination/receiver MAC address (DA or RA) and impersonation by modifying the source/transmitter MAC address (SA or TA). As described below, the transmission is monitored if the MIC (which is obtained using the MAC addresses) is

verified/authenticated at the receiver. MSDU with an invalid MIC will indicate a modified MAC

address (SA or DA), thereby resulting in discarding the MSDU and invoking the countermeasures.

8.3.2.3 TKIP MIC

Flaws in the IEEE 802.11 WEP design cause it to fail to meet its goal of protecting data traffic content from casual eavesdroppers. Among the most significant WEP flaws is the lack of a mechanism to defeat message forgeries and other active attacks. To defend against active attacks, TKIP includes a MIC, named Michael. This MIC offers only weak defenses against message forgeries, but it constitutes the best that can be achieved with the majority of legacy hardware. TKIP uses different MIC keys depending on the direction of the transfer as described in 8.6.1 and 8.6.2.

Annex H contains an implementation of the TKIP MIC. It also provides test vectors for the MIC.

8.3.2.3.1 Motivation for the TKIP MIC

Before defining the details of the MIC, it is useful to review the context in which this mechanism operates. Active attacks enabled by the original WEP design include the following:

— Bit-flipping attacks
— Data (payload) truncation, concatenation, and splicing
— Fragmentation attacks
— Iterative guessing attacks against the key
— Redirection by modifying the MPDU DA or RA field
— Impersonation attacks by modifying the MPDU SA or TA field

The MIC makes it more difficult for any of these attacks to succeed.

All of these attacks remain at the MPDU level with the TKIP MIC. The MIC, however, applies to the MSDU, so it blocks successful MPDU-level attacks. TKIP applies the MIC to the MSDU at the transmitter and verifies it at the MSDU level at the receiver. If a MIC check fails at the MSDU level, the implementation shall discard the MSDU and invoke countermeasures (see 8.3.2.4).

Page 217, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

51.   Upon detecting a first MIC failure, as described below, a countermeasure timer is

initiated, and a failure event (alert) is reported to the AP by sending a Michael MIC Failure Report

frame. Upon detecting a second consecutive MIC failure within 60 seconds, i.e., detecting a

number of failed attempts, the participating STAs are deauthenticated, wherein deauthentication

involves sending a notification (i.e., generating an alert) to deauthenticate due to an intrusion (2 consecutive MIC failures has occurred).

8.3.2.4 TKIP countermeasures procedures

The TKIP MIC trades off security in favor of implementability on pre-RSNA devices. Michael provides only weak protection against active attacks. A failure of the MIC in a received MSDU indicates a probable active attack. A successful attack against the MIC would mean an attacker could inject forged data frames and perform further effective attacks against the encryption key itself. If TKIP implementation detects a probable active attack, TKIP shall take countermeasures as specified in this subclause. These countermeasures accomplish the following goals:

— MIC failure events *should* be logged as a security-relevant matter. A MIC failure is an almost certain indication of an active attack and warrants a follow-up by the system administrator.

— The rate of MIC failures *must* be kept below two per minute. This implies that STAs and APs detecting two MIC failure events within 60 s must disable all receptions using TKIP for a period of 60 s. The slowdown makes it difficult for an attacker to make a large number of forgery attempts in a short time.

A single counter or timer shall be used to log MIC failure events. These failure events are defined as follows:

— For an Authenticator:
   — Detection of a MIC failure on a received unicast frame.
   — Receipt of Michael MIC Failure Report frame.

— For a Supplicant:
   — Detection of a MIC failure on a received unicast or broadcast/multicast frame.
   — Attempt to transmit a Michael MIC Failure Report frame.

The number of MIC failures is accrued independent of the particular key context. Any single MIC failure, whether detected by the Supplicant or the Authenticator and whether resulting from a group MIC key failure or a pairwise MIC key failure, shall be treated as cause for a MIC failure event.

The Supplicant uses a single Michael MIC Failure Report frame to report a MIC failure event to the Authenticator. A Michael MIC Failure Report is an EAPOL-Key frame with the following Key Information

The first MIC failure shall be logged, and a timer initiated to enable enforcement of the countermeasures. If the MIC failure event is detected by the Supplicant, it shall also report the event to the AP by sending a Michael MIC Failure Report frame.

If a subsequent MIC failure occurs within 60 s of the most recent previous failure, then a STA whose IEEE 802.1X entity has acted as a Supplicant shall deauthenticate (as defined in 11.3.1.3) itself or deauthenticate all the STAs with a security association if its IEEE 802.1X entity acted as an Authenticator. For an IBSS STA, both Supplicant and Authenticator actions shall be taken. Furthermore, the device shall not receive or transmit any TKIP-encrypted data frames, and shall not receive or transmit any unencrypted data frames other than IEEE 802.1X messages, to or from any peer for a period of at least 60 s after it detects the second failure. If the device is an AP, it shall disallow new associations using TKIP during this 60 s period; at the

Page 219, 220, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

52.   The Asserted Patents also cover Johnson Controls' Wi-Fi compliant devices, which support WPA and WPA2, and WPA3 security mechanisms, as described below and in the

following paragraph. Of the WPA, WPA2 and WPA3 security mechanism used by the Accused

Products, such as Johnson Controls' smart home Wi-Fi devices, the WPA is based on Temporal

Key Integrity Protocol (TKIP), while the WPA2 and WPA3 are based on Counter Mode Cipher

Block Chaining Message Authentication Code Protocol (CCMP). Shown below are exemplary

IEEE 802.11 compliant smart remotes and routers. The devices each have a housing.

IQ REMOTE

The IQ Remote is a secondary tablet that pairs with the IQ Panel 4, IQ Hub and IQ Panel 2 Plus. Not only does it provide a way to arm and disarm your Panel and see sensor status, but it gives you the features you don't get in your mobile app like chimes, emergency panics, and a siren. The IQ Remote can be upgraded over the air as new software upgrades are released.

QW9104-840

IQ Remote, QOLSYS, https://qolsys.com/iq-remote-2/ (last visited Sep. 30, 2022).

CONNECTING THE IQ REMOTE TO WIFI

The IQ Remote pairs with the IQ Panel 2 over a secure WIFI Network (802.11 B, G, N, AC) and must be connected to the same 2.4 or 5 GHz network as the IQ Panel 2 before you can add it to the system. To connect to a secure WIFI:

Touch "Activate WIFI"

Select network from available list. — Whitehouse / Your Neighbor

Enter WIFI credentials — Password

IMPORTANT: Please check that the IQ Remote can successfully connect to the network in the chosen installation location

IQ Remote Quick Guide, p. 1, QOLSYS, *available for download at* https://qolsys.com/wp-

content/uploads/2019/01/IQ-RemoteV3-Quick-Guide.pdf (last visited Sep. 30, 2022)

SPECIFICATIONS	
Items	**IQ WIFI 6**
Wireless Band	Dual IEEE 802.11 b/g/n/ax 2.4GHz IEEE 802.11 a/n/ac/ax 5GHz – AX1800
Ethernet	1x LAN / 1x WAN Gigabit Ethernet Ports
Security	WPA2 and WPA 3 Encryption
Expandable Mesh	Add up to 8 nodes (1 controller & 7 agents).
DHCP	Server, Client
Protocols	IPv4 and IPv6
Guest Network	2.4GHz/5GHz
WPS	Physical button is on the back of the device
Power Supply AC–DC	AC (110V 60Hz / 240V 50Hz), 12 DC (12V/1A) – Barrel jack
Operating Temperature	32°F to 104°F (0°C – 40°C)
Operating Distance	Up to 1,500 square feet per point
Weight	425g
Size	151.4mm x 150.4mm x 55.4mm
Part Number	IQWF6

IQ WIFI 6 Specification Sheet, p. 1 QOLSYS, available for download at https://qolsys.com/wp-content/uploads/2022/08/IQ-WiFi-6-Flyer-SpeckSheet-07-19-22.pdf (last visited Sep. 30, 2022) (listing the brands Qolsys, DSC, PowerG, and Johnson Controls in a footer of the specification sheets).

53.   As shown above, the Accused Products provide 2.4 GHz and 5 GHz Wi-Fi speeds. This capability ascertains the presence of a Wi-Fi antenna and transceiver in the device and provides a secure wireless LAN.

54.   Shown below is a block diagram of TKIP (used with WPA) based cryptography circuit utilized in the Accused Products. The circuit shown encrypts both address (destination address (DA), source address (SA)) and data information (plaintext MSDU) by adding encryptions bits (MIC key) to both the address and data. The cryptography circuit of the Accused Products is also configured to decrypt the encrypted address and data information.

IEEE Std 802.11™-2007
(Revision of
IEEE Std 802.11-1999)

8.3.2 Temporal Key Integrity Protocol (TKIP)

8.3.2.1.1 TKIP cryptographic encapsulation

TKIP enhances the WEP cryptographic encapsulation with several additional functions, as depicted in Figure 8-4.
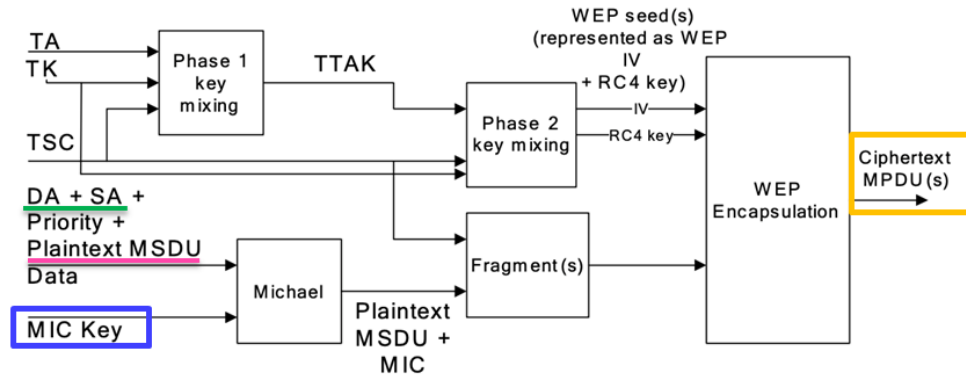
Figure 8-4—TKIP encapsulation block diagram

a) TKIP MIC computation protects the MSDU Data field and corresponding SA, DA, and Priority fields. The computation of the MIC is performed on the ordered concatenation of the SA, DA, Priority, and MSDU Data fields. The MIC is appended to the MSDU Data field. TKIP discards any MIC padding prior to appending the MIC.

b) If needed, IEEE Std 802.11 fragments the MSDU with MIC into one or more MPDUs. TKIP assigns a monotonically increasing TSC value to each MPDU, taking care that all the MPDUs generated from the same MSDU have the same value of extended IV (see 8.3.2.2).

c) For each MPDU, TKIP uses the key mixing function to compute the WEP seed.

d) TKIP represents the WEP seed as a WEP IV and ARC4 key and passes these with each MPDU to WEP for generation of the ICV (see 7.1.3.6), and for encryption of the plaintext MPDU, including all or part of the MIC, if present. WEP uses the WEP seed as a WEP default key, identified by a key identifier associated with the temporal key.

Page 213, 214, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

COUNT I

(INFRINGEMENT OF U.S. PATENT NO. 7,224,678)

55.   Plaintiff incorporates paragraphs 1 through 54 herein by reference.

56.   Plaintiff is the assignee of the '678 patent, entitled "Wireless local or metropolitan

area network with intrusion detection features and related methods," with ownership of all

substantial rights in the '678 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

57.   The '678 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '678 patent issued from U.S. Patent Application No. 10/217,042.

58.   Johnson Controls has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '678 patent in this District and elsewhere in Texas and the United States.

59.   On information and belief, Johnson Controls designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Johnson Controls and its parent, subsidiaries, members, segments, companies, brands and/or related entities, such as Defendants JCI PLC, JC Inc., and JC Security and U.S.-based subsidiaries, members, segments, companies and/or brands of Johnson Controls.

60.   Defendants each directly infringe the '678 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '678 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, and/or consumers. Furthermore, on information and belief, Defendants make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, customers and other related service providers in the United States, or in the case that it delivers the Accused Products outside of the United States it does so intending and/or knowing that those products are destined for the

United States and/or designing those products for sale and use in the United States, thereby directly infringing the '678 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to "whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)").

61.   Furthermore, Johnson Controls directly infringes the '678 patent through its direct involvement in the activities of its parent, subsidiaries, and related entities, including Defendants JCI PLC, JC Inc., and JC Security, and U.S.-based subsidiaries, members, segments, companies and/or brands of Johnson Controls, including by selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. On information and belief, U.S.-based subsidiaries, including at least JC Inc. and JC Security, conduct activities that constitute direct infringement of the '678 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants. Johnson Controls and parent JCI PLC are vicariously liable for the infringing conduct of Defendants JC Inc. and JC Security and U.S.-based subsidiaries, members, segments, companies and/or brands of Johnson Controls (under both the alter ego and agency theories). On information and belief, Defendants JCI PLC, JC Inc., and JC Security and U.S. based subsidiaries members, segments, companies and/or brands of Johnson Controls Johnson Controls are essentially the same company, comprising members, segments, companies and/or brands of Johnson Controls. Moreover, JCI PLC, as the parent company, along with its related entities, has the right and ability to control the infringing activities of those subsidiary entities such that Defendants receive a direct financial benefit from that infringement.

62.   For example, Johnson Controls infringes claim 51 of the '678 patent via the Accused

Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to LUX CS1, LUX GEO,

LUX KONO, LUX KONOz, YORK Hx and YORK Hx3 thermostats; Johnson Controls and/or

DSC SN-629F1, SN-750EF1, and 631PT1 security cameras; Johnson Controls and/or DSC and/or

IOTEGA WS900x security system panels; Johnson Controls and/or DSC and/or PowerSeries

ProHSM3WIFI WiFi adapter modules; Johnson Controls and/or DSC and/or Telguard ASG1000-

1T5NAS interactive hubs; Johnson Controls and/or Tyco and/or Visonic PowerMaster-360R

Modern Wireless Alarm and Home Automation Gateways; Johnson Controls and/or Qolsys IQ

Panel 4 and IQ Panel 2+ security panels; Johnson Controls and/or Qolsys IQ Remotes, IQ WiFi 6

and IQ WiFi security panels; Lux App; and related accessories and software.

63.   Those Accused Products include "[a]n intrusion detection method for a wireless local

or metropolitan area network comprising a plurality of stations" comprising the limitations of

claim 51. The technology discussion above and the example Accused Products provide context for

Plaintiff's allegations that each of those limitations are met. For example, the Accused Products

include the steps of transmitting data between the plurality of stations using a media access layer

(MAC), each of the stations having a respective MAC address associated therewith; monitoring

transmissions among the plurality of stations to detect failed attempts to authenticate MAC

addresses; and generating an intrusion alert based upon detecting a number of failed attempts to

authenticate a MAC address.

64.   At a minimum, Johnson Controls has known of the '678 patent at least as early as the

filing date of this complaint. In addition, Johnson Controls has known about infringement of an

L3Harris ("Harris") patent portfolio that was acquired by Stingray, which includes the '678 patent,

since at least its receipt of a letter dated July 7, 2020, from Acacia Research Corp, working with

Acacia Research Group LLC and on behalf of Stingray. The letter notifies Tyco Integrated Security

that its products practice the technologies covered by Stingray's Harris patent portfolio. Further,

Tyco Integrated Security is now a Johnson Controls company. *See Tyco is now Johnson Controls*,

TYCOIS.COM, https://www.tycois.com/home ("Tyco Integrated Security is now Johnson Controls,

the world leader in fire protection, security, HVAC, building controls and energy storage"); *see*

also id. (including a link to Terms of Use for Johnson Controls at

https://www.johnsoncontrols.com/legal/terms, said Terms of Use stating, "This website (the

'Site') is provided by Johnson Controls International plc and its affiliated companies ('Johnson

Controls')."); *WNC1800/FX-ZFR182x Pro Series Wireless Field Bus System Technical Bulletin*,

JOHNSONCONTROLS.COM, https://docs.johnsoncontrols.com/bas/r/Facility-Explorer/en-

US/WNC1800/FX-ZFR182x-Pro-Series-Wireless-Field-Bus-System-Technical-Bulletin (last

visited Oct. 4, 2022). Follow-up correspondence on behalf of Stingray, regarding Stingray's Harris

patent portfolio, was sent directly to Johnson Controls, including, for example, correspondence in

February 2021. Johnson Controls did not respond. On March 16, 2022, a letter was sent on behalf

of Stingray (a wholly owned subsidiary of Acacia Research Group LLC) to Johnson Controls again

notifying Johnson Controls of and providing Johnson Controls with the opportunity to license

Stingray's "premier [Harris] patent portfolio in wireless networking." Again, Johnson Controls did

not respond.

65.   On information and belief, since at least the above-mentioned date when Johnson

Controls was on notice of its infringement, Defendants have each actively induced, under U.S.C.

§ 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers,

consumers, and other related service providers that import, distribute, purchase, offer for sale, sell,

or use the Accused Products that include or are made using all of the limitations of one or more

claims of the '678 patent to directly infringe one or more claims of the '678 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, Defendants each do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '678 patent. On information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, consumers, and other related service providers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing wireless networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g.*, *Services and Support*, JOHNSONCONTROLS.COM, https://www.johnsoncontrols.com/services-and-support (last visited Sep. 30, 2022) (providing consumers with "HVAC Operations, Maintenance, and Repair Services" and "Security Maintenance and Support"); *see also Lux Products Corporation*, YOUTUBE.COM, https://www.youtube.com/channel/UCOE9M13g5cBxst2blF29C5g/videos (providing consumers with Johnson Controls- and/or LUX- produced how-to videos related to Johnson Controls and/or LUX products) (last visited Sep. 30, 2022). Furthermore, Johnson Controls markets smartphone and tablet interfaces and its application software as providing remote control for Johnson Controls products and working with Google Assistant, Amazon Alexa, Apple HomeKit, Apple Home App or Siri to control Johnson Controls Products with voice commands or connect with other connected products. *See Frequently Asked Questions*, LUX,

https://www.luxproducts.com/faqs/ (scroll down and access "Smart Home") (last visited Sep. 30, 2022). Such compatibility provides convenience and added functionality that induces consumers to use Johnson Controls products, including the smartphone and tablet Wi-Fi interfaces utilizing WiFi protocols in networks with other third-party devices, and thus further infringe the '678 patent.

66.   On information and belief, despite having knowledge of the patent portfolio including the '678 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the portfolio, Johnson Controls has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants infringing activities relative to the '678 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

67.   Plaintiff Stingray has been damaged as a result of Johnson Controls' infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for Johnson Controls' infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

<div align="center">

COUNT II

(INFRINGEMENT OF U.S. PATENT NO. 7,440,572)

</div>

68.   Plaintiff incorporates paragraphs 1 through 67 herein by reference.

69.   Plaintiff is the assignee of the '572 patent, entitled "Secure wireless LAN device and associated methods," with ownership of all substantial rights in the '572 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

70.   The '572 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '572 patent issued from U.S. Patent Application No. 09/760,619.

71.   Johnson Controls has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '572 patent in this District and elsewhere in Texas and the United States.

72.   On information and belief, Johnson Controls designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Johnson Controls and its parent, subsidiaries, members, segments, companies, brands and/or related entities, such as Defendants JCI PLC, JC Inc., and JC Security and U.S.-based subsidiaries, members, segments, companies and/or brands of Johnson Controls.

73.   Defendants each directly infringe the '572 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '572 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, and/or consumers. Furthermore, on information and belief, Defendants make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, customers and other related service providers in the United States, or in the case that it delivers the Accused Products outside of the United States it does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the '572 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell*

Semiconductor, Inc., 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to "whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)").

74.   Furthermore, Defendant Johnson Controls directly infringes the '572 patent through direct involvement in the activities of Johnson Controls and its parent, subsidiaries or related entities, such as Defendants JCI PLC, JC Inc., and JC Security and U.S.-based subsidiaries, members, segments, companies and/or brands of Johnson Controls, including by selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. On information and belief, U.S.-based subsidiaries, members, segments, companies and/or brands of Johnson Controls, including at least JC Inc. and JC Security, conduct activities that constitute direct infringement of the '572 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants. JCI PLC is vicariously liable for the infringing conduct of Defendants JC Inc. and JC Security and U.S.-based subsidiaries, members, segments, companies and/or brands of Johnson Controls (under both the alter ego and agency theories). On information and belief, Defendants JCI PLC and JC Inc. and U.S.-based subsidiaries, members, segments, companies and/or brands of Johnson Controls are essentially the same company, comprising some members, segments, companies and/or brands of Johnson Controls. Moreover, JCI PLC, as the parent company, along with its related entities, has the right and ability to control the infringing activities of those subsidiary entities such that Defendants receive a direct financial benefit from that infringement.

75.   For example, Johnson Controls infringes claim 1 of the '572 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to LUX CS1, LUX GEO, LUX KONO, LUX KONOz, YORK Hx and YORK Hx3 thermostats; Johnson Controls and/or DSC SN-629F1, SN-750EF1, and 631PT1 security cameras; Johnson Controls and/or DSC and/or IOTEGA WS900x security system panels; Johnson Controls and/or DSC and/or PowerSeries ProHSM3WIFI WiFi adapter modules; Johnson Controls and/or DSC and/or Telguard ASG1000-1T5NAS interactive hubs; Tyco and/or Visonic PowerMaster-360R Modern Wireless Alarm and Home Automation Gateways; Johnson Controls and/or Qolsys IQ Panel 4 and IQ Panel 2+ security panels; Johnson Controls and/or Qolsys IQ Remotes, IQ WiFi 6 and IQ WiFi security panels; Lux App; and related accessories and software.

76.   Those Accused Products include "[a] secure wireless local area network (LAN) device" comprising the limitations of claim 1. The technology discussion above and the example Accused Products provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Products include a housing; a wireless transceiver carried by said housing; a medium access controller (MAC) carried by said housing; and a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver for encrypting both address and data information for transmission by at least adding a plurality of encrypting bits to both the address and the data information, and for decrypting both the address and the data information upon reception.

77.   Johnson Controls further infringes the '572 patent via 35 U.S.C. § 271(g) by selling, offering to sell, and/or importing IoT and smart home devices, their components, and/or products containing same, that are made by a process covered by the '572 patent. On information and belief, the infringing IoT and smart home devices, their components, and/or products containing

same are not materially changed by subsequent processes, and they are neither trivial nor nonessential components of another product.

78.   Johnson Controls further infringes based on the importation, sale, offer for sale, or use of the Accused Products that are made from a process covered by the '572 patent. To the extent that Plaintiff made reasonable efforts to determine whether the patented processes of the '572 patent were used in the production of the Accused Products but was not able to so determine, the Accused Products should be presumed by this Court to have been so made, pursuant to 35 U.S.C. § 295.

79.   At a minimum, Johnson Controls has known of the '572 patent at least as early as the filing date of this complaint. In addition, Johnson Controls has known about infringement of an L3Harris ("Harris") patent portfolio that was acquired by Stingray, which includes the '572 patent, since at least its receipt of a letter dated July 7, 2020, from Acacia Research Corp, working with Acacia Research Group and on behalf of Stingray. The letter notifies Tyco Integrated Security that its products practice the technologies covered by Stingray's Harris patent portfolio. Further, Tyco Integrated Security is now a Johnson Controls company. *See Tyco is now Johnson Controls*, TYCOIS.COM, https://www.tycois.com/home ("Tyco Integrated Security is now Johnson Controls, the world leader in fire protection, security, HVAC, building controls and energy storage"); *see also id*. (including a link to Terms of Use for Johnson Controls at https://www.johnsoncontrols.com/legal/terms, said Terms of Use stating, "This website (the 'Site') is provided by Johnson Controls International plc and its affiliated companies ('Johnson Controls')."); *WNC1800/FX-ZFR182x Pro Series Wireless Field Bus System Technical Bulletin*, JOHNSONCONTROLS.COM, https://docs.johnsoncontrols.com/bas/r/Facility-Explorer/en-US/WNC1800/FX-ZFR182x-Pro-Series-Wireless-Field-Bus-System-Technical-Bulletin (last

visited Oct. 4, 2022). Follow-up correspondence on behalf of Stingray, regarding Stingray's Harris

patent portfolio, was sent directly to Johnson Controls, including, for example, correspondence in

February 2021. Johnson Controls did not respond. On March 16, 2022, a letter was sent on behalf

of Stingray (a wholly owned subsidiary of Acacia Research Group LLC) to Johnson Controls again

notifying Johnson Controls of and providing Johnson Controls with the opportunity to license

Stingray's "premier [Harris] patent portfolio in wireless networking." Again, Johnson Controls did

not respond.

80.   On information and belief, since at least the above-mentioned date when Johnson

Controls was on notice of its infringement, Defendants have each actively induced, under U.S.C.

§ 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers,

consumers, and other related service providers that import, distribute, purchase, offer for sale, sell,

or use the Accused Products that include or are made using all of the limitations of one or more

claims of the '572 patent to directly infringe one or more claims of the '572 patent by using,

offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided

on the above-mentioned date, Defendants each do so with knowledge, or with willful blindness of

the fact, that the induced acts constitute infringement of the '572 patent. On information and belief,

Defendants each intend to cause, and have taken affirmative steps to induce, infringement by

importers, online stores, distribution partners, retailers, reseller partners, dealers, consumers, and

other related service providers by at least, *inter alia*, creating advertisements that promote the

infringing use of the Accused Products, creating and/or maintaining established distribution

channels for the Accused Products into and within the United States, manufacturing the Accused

Products in conformity with U.S. laws and regulations, distributing or making available

instructions or manuals for these products to purchasers and prospective buyers, testing wireless

networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g.*, *Services and Support*, JOHNSONCONTROLS.COM, https://www.johnsoncontrols.com/services-and-support (last visited Sep. 30, 2022) (providing consumers with "HVAC Operations, Maintenance, and Repair Services" and "Security Maintenance and Support"); *see also Lux Products Corporation*, YOUTUBE.COM, https://www.youtube.com/channel/UCOE9M13g5cBxst2blF29C5g/videos (providing consumers with Johnson Controls- and/or LUX- produced how-to videos related to Johnson Controls and/or LUX products) (last visited Sep. 30, 2022). Furthermore, Johnson Controls markets smartphone and tablet interfaces and its application software as providing remote control for Johnson Controls products and working with Google Assistant, Amazon Alexa, Apple HomeKit, Apple Home App or Siri to control Johnson Controls Products with voice commands or connect with other connected products. *See Frequently Asked Questions*, LUX, https://www.luxproducts.com/faqs/ (scroll down and access "Smart Home") (last visited Sep. 30, 2022). Such compatibility provides convenience and added functionality that induces consumers to use Johnson Controls products, including the smartphone and tablet Wi-Fi interfaces utilizing WiFi protocols in networks with other third-party devices, and thus further infringe the '572 patent.

81.   On information and belief, despite having knowledge of the patent portfolio including the '572 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the portfolio, Johnson Controls has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants infringing activities relative to the '572 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct

beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

82.   Plaintiff Stingray has been damaged as a result of Johnson Controls' infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for Johnson Controls' infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT III

(INFRINGEMENT OF U.S. PATENT NO. 7,616,961)

83.   Plaintiff incorporates paragraphs 1 through 82 herein by reference.

84.   Plaintiff is the assignee of the '961 patent, entitled "Allocating channels in a mobile ad hoc network," with ownership of all substantial rights in the '961 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

85.   The '961 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '961 patent issued from U.S. Patent Application No. 10/134,862.

86.   Johnson Controls has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '961 patent in this District and elsewhere in Texas and the United States.

87.   On information and belief, Johnson Controls designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Johnson Controls and its parent, subsidiaries, members, segments, companies, brands and/or

related entities, such as Defendants JCI PLC, JC Inc., and JC Security and U.S.-based subsidiaries, members, segments, companies and/or brands of Johnson Controls.

88.   Defendants each directly infringe the '961 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '961 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, and/or consumers. Furthermore, on information and belief, Defendants make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, customers and other related service providers in the United States, or in the case that it delivers the Accused Products outside of the United States it does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the '961 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to "whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)").

89.   Furthermore, Defendant Johnson Controls directly infringes the '961 patent through direct involvement in the activities of its parent, subsidiaries and related entities, including Defendants JCI PLC, JC Inc., and JC Security and U.S.-based subsidiaries, members, segments, companies and/or brands of Johnson Controls, including by selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the

United States for its related entities. On information and belief, U.S. based subsidiaries, members, segments, companies and/or brands of Johnson Controls including at least JC Inc. and JC Security, conduct activities that constitute direct infringement of the '961 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants. JCI PLC is vicariously liable for the infringing conduct of Defendants JC Inc. and JC Security, and U.S.-based subsidiaries, members, segments, companies and/or brands of Johnson Controls (under both the alter ego and agency theories). On information and belief, Defendants JCI PLC, JC Inc., JC Security and U.S.-based subsidiaries, members, segments, companies and/or brands of Johnson Controls are essentially the same company, comprising members, segments, companies and/or brands of Johnson Controls. Moreover, JCI PLC, as the parent company, along with its related entities, has the right and ability to control the infringing activities of those subsidiary entities such that Defendants receive a direct financial benefit from that infringement.

90.   For example, Johnson Controls infringes claim 1 of the '961 patent via the Accused Products that utilize ZigBee protocols, including, but not limited to Johnson Controls and/or LUX KONOz thermostats; Johnson Controls and/or Tyco and/or Visonic ZigBee compatible ZigBee compatible GB-540, MCT-350, MCT-370, MP-840 and MP-841 intrusion detectors; Johnson Controls FX-ZFR Series Wireless Field Bus System; ZigBee modules and interfaces; and related accessories and software.

91.   Those Accused Products include a "method for dynamic channel allocation in a mobile ad hoc network comprising a plurality of wireless mobile nodes and a plurality of wireless communication links connecting the plurality of wireless mobile nodes together over a plurality of separate channels at different frequencies" comprising the limitations of claim 1. The technology

discussion above and the example Accused Products provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Products include the steps of at each node, monitoring link performance on a first channel, link performance being based upon at least one quality of service (QoS) threshold; at each node, scouting one or more other available separate channels at different frequencies when the monitored link performance on the first channel falls below the QoS threshold by at least switching to a second separate channel at a different frequency, broadcasting a channel activity query to determine link performance for the second separate channel, and processing replies to the channel activity query to determine the link performance for the second separate channel; and at each node, updating respective channel activity for the first and second separate channels at different frequencies based upon the processed replies.

92.   At a minimum, Johnson Controls has known of the '961 patent at least as early as the filing date of this complaint. In addition, Johnson Controls has known about infringement of an L3Harris ("Harris") patent portfolio that was acquired by Stingray, which includes the '961 patent, since at least its receipt of a letter dated July 7, 2020, from Acacia Research Corp, working with Acacia Research Group LLC and on behalf of Stingray. The letter notifies Tyco Integrated Security of its infringing use of Stingray's Harris patent portfolio including, for example, "mesh networking used in wireless control of home automation devices," in at least the "advanced ZigBee intrusion detectors, which are sold under Tyco's Visonic brand, as well as [Tyco Integrated Security's] WNC1800/ZFR182x Pro Series Wireless Field Bus System using low power 802.15.4 mesh technology." The letter notifies Tyco Integrated Security that its products practice the technologies covered by the Stingray patent portfolio. Further, Tyco Integrated Security is now a Johnson Controls company. *See Tyco is now Johnson Controls*, TYCOIS.COM, https://www.tycois.com/home ("Tyco Integrated Security is now Johnson Controls, the world

leader in fire protection, security, HVAC, building controls and energy storage"); *see also id.* (including a link to Terms of Use for Johnson Controls at https://www.johnsoncontrols.com/legal/terms, said Terms of Use stating, "This website (the 'Site') is provided by Johnson Controls International plc and its affiliated companies ('Johnson Controls')."); *WNC1800/FX-ZFR182x Pro Series Wireless Field Bus System Technical Bulletin*, JOHNSONCONTROLS.COM, https://docs.johnsoncontrols.com/bas/r/Facility-Explorer/en-US/WNC1800/FX-ZFR182x-Pro-Series-Wireless-Field-Bus-System-Technical-Bulletin (last visited Oct. 4, 2022) Follow-up correspondence on behalf of Stingray, regarding Stingray's Harris patent portfolio, was sent directly to Johnson Controls, including, for example, correspondence in February 2021. Johnson Controls did not respond. On March 16, 2022, a letter was sent on behalf of Stingray (a wholly owned subsidiary of Acacia Research Group LLC), to Johnson Controls again notifying Johnson Controls of and providing Johnson Controls with the opportunity to license Stingray's "premier [Harris] patent portfolio in wireless networking, including patents related to the Zigbee . . . standards crucial to the blossoming Internet of Things (IoT)." Johnson Controls again did not respond.

93.   On information and belief, since at least the above-mentioned date when Johnson Controls was on notice of its infringement, Defendants have each actively induced, under U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, consumers, and other related service providers that import, distribute, purchase, offer for sale, sell, or use the Accused Products that include or are made using all of the limitations of one or more claims of the '961 patent to directly infringe one or more claims of the '961 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, Defendants each do so with knowledge, or with willful blindness of

the fact, that the induced acts constitute infringement of the '961 patent. On information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, consumers, and other related service providers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing wireless networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g.*, *Services and Support*, JOHNSONCONTROLS.COM, https://www.johnsoncontrols.com/services-and-support (last visited Sep. 30, 2022) (providing consumers with "HVAC Operations, Maintenance, and Repair Services" and "Security Maintenance and Support"); *see also KONOz Installation Manual*, LUX, https://www.luxproducts.com/installation/#1524081905498-6d73ce08-ebce (providing consumers with Johnson Controls- and/or LUX- produced instruction manual related to Johnson Controls and/or LUX products) (last visited Sep. 30, 2022). Furthermore, Johnson Controls markets its LUX Konoz thermostat as being compatible with a smart hub and smart hub app and working with Google Assistant and Amazon Alexa to control Johnson Controls Products with voice commands. *See LUX KONOz*, LUX, https://www.luxproducts.com/konoz/ (last visited Sep. 30, 2022). Such compatibility provides convenience and added functionality that induces consumers to use Johnson Controls products, including the smartphone and tablet Wi-Fi interfaces utilizing ZigBee and/or WiFi protocols in networks with other third-party devices, and thus further infringe the '961 patent.

94.   On information and belief, despite having knowledge of the patent portfolio including the '961 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the portfolio, Johnson Controls has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants infringing activities relative to the '961 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

95.   Plaintiff Stingray has been damaged as a result of Johnson Controls' infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for Johnson Controls' infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

CONCLUSION

96.   Plaintiff is entitled to recover from Defendants the damages sustained by Plaintiff as a result of Defendants' wrongful acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court.

97.   Plaintiff has incurred and will incur attorneys' fees, costs, and expenses in the prosecution of this action. The circumstances of this dispute may give rise to an exceptional case within the meaning of 35 U.S.C. § 285, and Plaintiff is entitled to recover its reasonable and necessary attorneys' fees, costs, and expenses.

JURY DEMAND

98.   Plaintiff hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules

of Civil Procedure.

PRAYER FOR RELIEF

99.   Plaintiff requests that the Court find in its favor and against Defendants, and that the Court grant Plaintiff the following relief:

1. A judgment that Defendants have infringed the Asserted Patents as alleged herein, directly and/or indirectly by way of inducing infringement of such patents;

2. A judgment for an accounting of damages sustained by Plaintiff as a result of the acts of infringement by Defendants;

3. A judgment and order requiring Defendants to pay Plaintiff damages under 35 U.S.C. § 284, including up to treble damages as provided by 35 U.S.C. § 284, and any royalties determined to be appropriate;

4. A judgment and order requiring Defendants to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;

5. A judgment and order finding this to be an exceptional case and requiring Defendants to pay the costs of this action (including all disbursements) and attorneys' fees as provided by 35 U.S.C. § 285; and

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

Dated: October 7, 2022

Respectfully submitted,

/s/ Jeffrey R. Bragalone __
  Jeffrey R. Bragalone (lead attorney)
  Texas Bar No. 02855775
  E-mail: jbragalone@bosfirm.com
  Terry A. Saad
  Texas Bar No. 24066015
  E-mail: tsaad@bosfirm.com
  Marcus Benavides
  Texas Bar No. 24035574
  E-mail: mbenavides@bosfirm.com
  Brandon Zuniga
  Texas Bar no. 24088720
  E-mail: bzuniga@bosfirm.com
  Paul Stevenson
  Texas Bar No. 24117098
  E-mail: pstevenson@bosfirm.com
BRAGALONE OLEJKO SAAD PC
901 Main Street
Suite 3800
Dallas, Texas 75202
Telephone: (214) 785-6670
Facsimile: (214) 785-6680

Wesley Hill
Texas Bar No. 24032294
E-mail: wh@wsfirm.com
WARD, SMITH, & HILL, PLLC
P.O. Box 1231
Longview, Texas 75606
Telephone: (903) 757-6400
Facsimile: (903) 757-2323

**ATTORNEYS FOR PLAINTIFF
STINGRAY IP SOLUTIONS LLC**

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT – Page 64