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

STINGRAY IP SOLUTIONS LLC,	§	
	§	
Plaintiff,	§	
	§	
v.	§	CIVIL ACTION NO. _____
	§	
ASSA ABLOY AB,	§	JURY TRIAL DEMANDED
	§	
Defendant.	§	
	§	
	§	
	§	
	§	

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 Defendant Assa Abloy AB ("Defendant" or "Assa Abloy") for infringement of U.S. Patent No. 7,224,678 (the "'678 patent"), U.S. Patent No. 7,440,572 (the "'572 patent"), U.S. Patent No. 7,441,126 (the "'126 patent"), and U.S. Patent No. 7,616,961 ("the "'961 patent") (collectively, the "Asserted Patents").

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 Assa Abloy AB is Swedish corporation, with its principal place of business and registered office located at Klarabergsviadukten 90, SE-10723, Stockholm, Sweden. Assa Abloy AB may be served via its agents and its alter egos, including, for example, Assa Abloy Global Solutions, Inc., a Texas corporation, Assa Abloy Sales and Marketing Group, Inc., a Delaware corporation, Assa Abloy Americas Residential Inc., a Delaware corporation, Assa Abloy Entrance Systems US Inc., a Connecticut corporation, Assa Abloy

Fenestration, LLC, a New York company, and Assa Abloy High Security Group Inc., a Virginia corporation, all having registered agent C T Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX 75201-3136, USA. Assa Abloy AB may also be served via its agent and alter ego Assa Abloy Inc., an Oregon corporation, having registered agent C T Corporation System, 780 Commercial St. SE, Ste. 100, Salem, Oregon, 97301-3465, USA, being a wholly owned subsidiary of Assa Abloy AB, and owning 100% of at least Assa Abloy Global Solutions, Inc., Assa Abloy Sales and Marketing Group, Inc., Assa Abloy Entrance Systems US Inc., and Assa Abloy High Security Group Inc.

3. Assa Abloy AB is a Swedish public limited liability company with its registered office in Stockholm, Sweden, and whose Series B shares are listed on Nasdaq Stockholm. *See Annual Report 2022*, ASSA ABLOY, pp. 51-52, available for download at https://www.assaabloy.com/group/en/investors (last visited Jan. 11, 2024) [hereinafter "Annual Report"]. Assa Abloy provides access solutions for physical and digital places and operates as a single global company with local business units. *Id.* at 6.

4. Assa Abloy offers products that are compatible with Wi-Fi and/or Zigbee protocols. For example, Assa Abloy offers "ASSA ABLOY Intelligent WiFi locks and exit devices" and a Zigbee-enabled "RFID cylindrical lock." *See Intelligent WiFi,* ASSA ABLOY, https://www.intelligentopenings.com/en/products/by-category/wireless/intelligent-wifi-access-control (last visited Jan. 11, 2024); *RFID cylindrical lock,* ASSA ABLOY, https://www.intelligentopenings.com/en/solutions/by-market/multi-resident-access-control/off-campus-student-housing/rfid-cylindrical-lock (last visited Jan. 11, 2024); *see also Door Opening Solutions for Off-Campus Student Housing*, ASSA ABLOY, pp. 3-4, available for download at https://storage.googleapis.com/aa-americas/dam/AADSS1176443.pdf (last visited Jan. 11, 2024).

5. Assa Abloy has "operations in more than 70 countries" including "local manufacturing and assembly lines in both mature and emerging markets." Annual Report at 11. According to Assa Abloy's Annual Report, Assa Abloy has more employees in the United States than any other country, averaging 12,674 U.S. employees for the year 2022. *See* Annual Report, p. 38. Additionally, the U.S. market accounted for approximately half of Assa Abloy's sales in 2022, namely, 54,093 million Swedish kronor ("SEK M") out of total sales of 120,793 SEK M. *Id.* at pp. 2, 40 ("The US market, where we have around half of our geographical exposure, was very strong during the year [2022]), 45, 79. Using an exchange rate of 1 SEK to 0.0959 USD as of December 31, 2022, Assa Abloy's 2022 U.S. sales were approximately U.S. $ 5.19 billion. *See, e.g.*, *Swedish Krona (SEK) to US Dollar (USD) Historical Exchange Rates on 31st December 2022*, EXCHANGE RATES.ORG.UK, https://www.exchangerates.org.uk/SEK-USD-31_12_2022-exchange-rate-history.html (last visited Jan. 11, 2024).

6. At least some of Assa Abloy's manufacturing facilities are in the United States. *Id.* at 24. Other Assa Abloy manufacturing facilities are located outside the United States. *Id.* Assa Abloy products, including products sold by their subsidiaries, 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.

7. On information and belief, Assa Abloy operates its business and offers products via five divisions, using various brands and subsidiaries collectively referred to as the Assa Abloy Group. *Id.* at 6, 78. Assa Abloy AB is the "[Assa Abloy] Group's Parent company." *Id.* Assa Abloy AB "is responsible for Group management and provides Group-wide functions." *Id.*

8. Assa Abloy uses its global divisions to "manufacture and sell access solutions, identification products and entrance automation in the global market." *Id.* at 6. Assa Abloy's two global divisions are "Global Technologies," and "Entrance Systems." *Id.*

9. Assa Abloy uses its regional divisions to "manufacture and sell mechanical and electromechanical locks, digital door locks, cylinders and security doors, adapted to the local market's standards and security requirements." *Id.* Assa Abloy's three regional divisions are "Opening Solutions Americas," "Opening Solutions EMEIA," and "Opening Solutions Asia Pacific." *Id.*

10. Assa Abloy uses its local business units to optimize its resources and optimize "products according to . . . local conditions[,] demand," and applicable local standards. *Id.*

11. Assa Abloy's 2022 Annual Report states that it sells products under approximately 190 brands globally. *Id.* ASSA ABLOY is Assa Abloy's "employer brand and main brand for commercial openings and entrance automation." *Id.* Assa Abloy's past and/or present brands also include, for example, HID for identification and access management and Yale for the residential market. *Id*; *see also Brand overview*, ASSA ABLOY, https://www.assaabloy.com/group/en/about-us/our-brands/brand-overview (last visited Jan. 11, 2024) (listing "135" brands).

12. On information and belief, Assa Abloy maintains a corporate presence in the United States, including in Texas and in this District, via at least making, using, importing, offering to sale, and/or selling Assa Abloy products in or into the United States, including, for example, on behalf of, in conjunction with, for and/or via customers in the United States and Assa Abloy's alter egos, related entities and/or wholly controlled U.S.-based subsidiaries, including, without limitation, Assa Abloy Global Solutions, Inc., Assa Abloy Sales and Marketing Group, Inc., Assa Abloy Americas Residential Inc., Assa Abloy Entrance Systems US Inc., Assa Abloy Fenestration,

LLC, Assa Abloy High Security Group Inc, and/or Door Security Solutions of the Southwest. On behalf and for the benefit of Defendant and the Assa Abloy Group, Assa Abloy AB (including, for example, via at least one shared executive, e.g., Lucas Boselli, President of Assa Abloy Americas Residential Inc. and Executive Vice President and Head of Assa Abloy Americas division) engages in, controls, orders, provides for, induces, jointly participates in, and/or coordinates the importation, distribution, marketing, offers for sale, sale, and use of Assa Abloy's products in the U.S. For example, Assa Abloy AB maintains distribution and support channels in the U.S. for Assa Abloy products via manufacturing facilities, online stores, distribution partners, retailers, reseller partners, dealers, and other related service providers. *See, e.g., Opening Solutions*, ASSA ABLOY, https://www.assaabloydss.com/en/support/contact-sales/find-a-sales-office (last visited Jan. 26, 2024) (stating "ASSA ABLOY Door Security Solutions represents more than 20 leading door, frame and hardware brands, and product lines that create a total door opening solution for any environment," listing brands including Assa Abloy, Sargent, Yale Commercial, and Securitron, and listing a Door Security Solutions of the Southwest location at 6817 K Ave., Suite 101, Plano, TX 75074, in Collin County and in this District); *Door Security Solutions of the Southwest*, ASSA ABLOY, https://www.linkedin.com/company/assa-abloy-door-security-solutions-of-the-southwest (last visited Jan. 26, 2024) (stating "ASSA ABLOY Door Security Solutions of the Southwest is a manufacturer's representative company and architectural consulting firm that employs 20 persons with a combined 100+ years experience in the commercial openings industry. We provide sales and marketing support for the ASSA ABLOY DSS group of commercial openings products in the North Texas, Oklahoma[,] Arkansas, and Northern Louisiana. . . . DSS of the Southwest promotes its manufacturer's product lines by creating demand for them through the end-user channel."); Annual Report, p. 6, 24, 45, 79; *Contact support*, ASSA ABLOY,

https://www.assaabloydss.com/en/support/product-technical-support (last visited Jan. 11, 2024) (stating "[o]ur product support teams are ready to assist with your technical questions" and providing links to "Support tools" and "Technical Support teams" for numerous listed "product brands"); *Where to Buy*, ASSA ABLOY, https://www.corbinrusswin.com/en/contact-us/where-to-buy (last visited Jan. 11, 2024) (indicating Assa Abloy's Corbin Russwin products, including at least Wi-Fi-enabled devices (e.g., IN120 PED5400 Series WiFi locks), "can be purchased through [] channel partners" and instructing website users to "[u]se the locator below to find the correct partner for the desired products and services"); *Where to Buy*, ASSA ABLOY, https://www.intelligentopenings.com/en/support/where-to-buy (last visited Jan. 11, 2024) (listing Contract Hardware Distributors in the United States, in Texas and in this District, including, for example, Commercial Lock Services, located at 5540 Oak Bend Trail, Prosper Texas, 75078, USA in Collin County, Texas); *Gateman ASSA ABLOY G-Touch Digital Vertibolt Rim Lock - Traceless Super Slim Body, Master Mode, Forced Lock, Automatic Locking, Volume Control, Silent Low Battery Alarm, Emergency Power Support*, VEISE, https://www.amazon.com/Gateman-ASSA-ABLOY-G-Touch-Vertibolt/dp/B09PZ6VFYT/ (last visited Jan. 11, 2024); *Zigbee Endnode Kit w/cable for Signature and Essence*, ASSA ABLOY, https://estore.assaabloyglobalsolutions.com/us/hospitality/zigbee-rf-online-communication-module-for-locks-and-remote-readers-(2006-stack---ams-only).html (last visited Jan. 11, 2024); *About Kwikset*, KWIKSET, https://www.kwikset.com/about-kwikset (last visited Jan. 26, 2024) (stating "Kwikset is the leading residential lock manufacturer," "Kwikset is part of the Hardware and Home Improvement (HHI) division of ASSA ABLOY (STO: AAY.ST)," and "Kwikset products are sold online and through retailers and distributors throughout the U.S."); *Kwikset Wifi*, HOME DEPOT, https://www.homedepot.com/s/kwikset%20wifi?NCNI-5 (last visited Jan. 26,

2024) (indicating the "N Frisco" Home Depot located at 5995 Eldorado Pkwy, Frisco, TX 75033, in Collin County and this District, sells Kwikset WiFi smart locks.).

13. As a result, via at least Assa Abloy's established distribution channels operated and maintained by at least Defendant Assa Abloy AB and Assa Abloy's U.S.-based subsidiaries, Assa Abloy's products are distributed, sold, advertised, and used nationwide, including being sold to consumers via Assa Abloy dealers operating in Texas and this District. Thus, Defendant does business in the United States, the State of Texas, and in this District.

JURISDICTION AND VENUE

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

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

A. Defendant Assa Abloy AB

16. On information and belief, Assa Abloy AB 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, subsidiaries, members, divisions, segments, companies, brands, and/or consumers. For example, at relevant times for

infringement of the Asserted Patents, Assa Abloy AB is related to, has been related to, owns, has owned, controls and/or has controlled subsidiaries, businesses, divisions and/or brands (including but not limited to Assa Abloy Americas Residential, Inc., Assa Abloy Door Security Solutions of the Southwest, Yale, Kwikset, Sargent, and Corbin Russwin) 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 Assa Abloy products in Texas, including in this District.

17. This Court has personal jurisdiction over Defendant Assa Abloy AB, directly and/or through the activities of Assa Abloy AB's alter egos, intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including through the activities of those based in the U.S. Through direction and control of these entities, Assa Abloy AB 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 Assa Abloy AB would not offend traditional notions of fair play and substantial justice.

18. On information and belief, Assa Abloy AB controls or otherwise directs and authorizes all activities of its alter egos, subsidiaries and related entities, including, but not limited to members, divisions, segments, companies and/or brands of Assa Abloy, for example, Assa Abloy Door Security Solutions and Kwikset. *See, e.g., Contact Us*, ASSA ABLOY, https://www.assaabloy.com/group/en/contact (clicking on the "Locations" link and selecting the "United States" from a drop down menu showcases Assa Abloy Door Security Solutions as a contact for Assa Abloy Group) (last visited Jan. 26, 2024); Annual Report, p. 30 (disclosing Assa Abloy organization structure, America being the largest regional division); *Company History*,

KWIKSET, https://www.kwikset.com/about-kwikset (last visited Feb. 28, 2024) ("The Kwikset Denison, TX facility broke ground and since then, there have been two plant expansions. Kwikset Denison manufactures component parts for Kwikset lock-sets, Price-Pfister faucets, and Black & Decker tools. The plant is the largest zinc user in the United States."). Directly via its alter egos and/or agents in the U.S. and via at least distribution partners, retailers, reseller partners, dealers, professional installers, and other service providers, Assa Abloy AB has placed and continues to place infringing Assa Abloy products into the U.S. stream of commerce. Examples include the manufacture and/or importation of Assa Abloy products in and into the United States. *See* Annual Report, p. 34; *Company History*, KWIKSET, https://www.kwikset.com/about-kwikset (last visited Feb. 28, 2024) ("The Kwikset Denison, TX facility"); *Property Search*, GRAYSON CAD, https://esearch.graysonappraisal.org/Search/Result?keywords=assa%20abloy (last visited Feb. 28, 2024) (showing real property owned by "Assa Abloy Americas Residential Inc" at 2600 N HWY 91, Denison, Texas 75020 in 2024); *Search*, ASSA ABLOY, https://jobs1.hhicareers.com/jobs?pageIndex=2 (last visited Feb. 28, 2024) (job search results showing jobs for Assa Abloy in Texas, including but not limited to Denison, Texas). Assa Abloy AB 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)).

19. On information and belief, Assa Abloy AB 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, vendors, resellers, distributors, and/or dealers offering such products and related services for sale. *See* Annual Report, pp. 34 (Under the heading "Overview Americas," indicating that the America's division is "[o]rganized into 13 business areas and market regions, by product category"), 40 (Under the heading "*What explains the very strong growth in 2022?*" noting that "The US market, where [Assa Abloy] ha[s] around half of [its] geographical exposure, was very strong during the year. [Assa Abloy's] Residential, Industrial and Perimeter security segments all performed very strongly."); *Assa Abloy*, ASSA ABLOY, https://www.assaabloy.com/group/en (last visited Jan. 26, 2024) (Under the heading "*We are your local partner with a global presence,*" stating that "With 52,000 colleagues around the world, we have an expert wherever you are."); *Our Organization*, ASSA ABLOY, https://www.assaabloy.com/group/en/about-us/how-we-are-organized (Under the heading "*Opening Solutions Americas,*" stating that "In the US and Canada around 80% of our sales are to businesses, organizations and institutions like schools and hospitals, and the rest is for homes."). Assa Abloy 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, at least, The Home Depot, nationwide dealers or distributors, and nationwide online retailers. *See., e.g., Kwikset Wifi*, HOME DEPOT, https://www.homedepot.com/s/kwikset%20wifi?NCNI-5 (last visited Jan. 26, 2024) (indicating the "N Frisco" Home Depot located at 5995 Eldorado Pkwy, Frisco, TX 75033, in Colling County and this District, sells Kwikset WiFi smart locks.); *Yale Assure 2 Smart Lock Black Suede Keyed Wi-Fi Single Cylinder Deadbolt with Touchscreen Keypad*, HOME DEPOT,

https://www.homedepot.com/p/Yale-Assure-2-Smart-Lock-Black-Suede-Keyed-Wi-Fi-Single-Cylinder-Deadbolt-with-Touchscreen-Keypad-YRD420-WF1-BSP/322081820 (last visited Jan. 12, 2024) (Being offered for sale to individuals in zip code 75033 in Frisco, Collin County, Texas in this District and being assigned Model # YRD420-WF1-BSP and Internet # 322081820); *Yale Lifetime Limited Warranty*, ASSA ABLOY, *https://images.thdstatic.com/catalog/pdfImages/68/68cf3722-48f2-4f01-b3fe-134eeaf62a61.pdf* (last visited Jan. 12, 2024) (indicating that Assa Abloy provides the manufacturer's warranty for the Yale Assure Wi-Fi lock sold at Home Depot in Frisco and assigned Model # YRD420-WF1-BSP and Internet # 322081820). Additionally, Assa Abloy products, including infringing products and/or services, are sold nationwide, in Texas and this District via, for example, direct sales, online retailers, and Assa Abloy's subsidiaries and/or brands, for example, Assa Abloy Door Security Solutions and or Door Security Solutions of the Southwest. *See, e.g., Opening Solutions*, ASSA ABLOY, https://www.assaabloydss.com/en/support/contact-sales/find-a-sales-office (last visited Jan. 26, 2024) (stating "ASSA ABLOY Door Security Solutions represents more than 20 leading door, frame and hardware brands, and product lines that create a total door opening solution for any environment," listing brands including Assa Abloy, Sargent, Yale Commercial, and Securitron, and listing a Door Security Solutions of the Southwest location at 6817 K Ave., Suite 101, Plano, TX 75074, in Collin County and in this District); *Door Security Solutions of the Southwest*, ASSA ABLOY, https://www.linkedin.com/company/assa-abloy-door-security-solutions-of-the-southwest (last visited Jan. 26, 2024) (stating "ASSA ABLOY Door Security Solutions of the Southwest is a manufacturer's representative company and architectural consulting firm that employs 20 persons with a combined 100+ years experience in the commercial openings industry. We provide sales and marketing support for the ASSA ABLOY DSS group of

commercial openings products in the North Texas, Oklahoma[,] Arkansas, and Northern Louisiana. . . . DSS of the Southwest promotes its manufacturer's product lines by creating demand for them through the end-user channel."); Annual Report, p. 6, 24, 45, 79; *Contact support*, ASSA ABLOY, https://www.assaabloydss.com/en/support/product-technical-support (last visited Jan. 11, 2024) (stating "[o]ur product support teams are ready to assist with your technical questions" and providing links to "Support tools" and "Technical Support teams" for numerous listed "product brands"); *Where to Buy*, ASSA ABLOY, https://www.corbinrusswin.com/en/contact-us/where-to-buy (last visited Jan. 11, 2024) (indicating Assa Abloy's Corbin Russwin products, including at least Wi-Fi-enabled devices (e.g., IN120 PED5400 Series WiFi locks), "can be purchased through [] channel partners" and instructing website users to "[u]se the locator below to find the correct partner for the desired products and services"); *Where to Buy*, ASSA ABLOY, https://www.intelligentopenings.com/en/support/where-to-buy (last visited Jan. 11, 2024) (listing Contract Hardware Distributors in the United States, in Texas and in this District, including, for example, Commercial Lock Services, located at 5540 Oak Bend Trail, Prosper Texas, 75078, USA in Collin County, Texas); *Gateman ASSA ABLOY G-Touch Digital Vertibolt Rim Lock - Traceless Super Slim Body, Master Mode, Forced Lock, Automatic Locking, Volume Control, Silent Low Battery Alarm, Emergency Power Support*, VEISE, https://www.amazon.com/Gateman-ASSA-ABLOY-G-Touch-Vertibolt/dp/B09PZ6VFYT/ (last visited Jan. 11, 2024); *Zigbee Endnode Kit w/cable for Signature and Essence*, ASSA ABLOY, https://estore.assaabloyglobalsolutions.com/us/hospitality/zigbee-rf-online-communication-module-for-locks-and-remote-readers-(2006-stack---ams-only).html (last visited Jan. 11, 2024); *About Kwikset*, KWIKSET, https://www.kwikset.com/about-kwikset (last visited Jan. 26, 2024) (stating "Kwikset is the leading residential lock manufacturer," "Kwikset is part of the Hardware

and Home Improvement (HHI) division of ASSA ABLOY (STO: AAY.ST),” and “Kwikset products are sold online and through retailers and distributors throughout the U.S.”); *Kwikset Wifi*, HOME DEPOT, https://www.homedepot.com/s/kwikset%20wifi?NCNI-5 (last visited Jan. 26, 2024) (indicating the “N Frisco” Home Depot located at 5995 Eldorado Pkwy, Frisco, TX 75033, in Colling County and this District, sells Kwikset WiFi smart locks.).

20. Assa Abloy AB, 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 Assa Abloy products and other network devices. These apps are available via digital distribution platforms operated, for example, by Assa Abloy, Apple Inc., and/or Google for download by users and execution on smartphone devices. *See, e.g.*, *Kwikset App,* KWIKSET, https://www.kwikset.com/smart-locks/app#! (last visited Jan. 26, 2024) (indicating the Kwikset App is available at the Apple App Store and Google Play and works with various Halo Wi-Fi Smart Locks); *IN120 PE8800 Series,* SARGENT ASSA ABLOY, https://www.sargentlock.com/en/commercial-locks-products/electronic-access-control/wireless/intelligent-wi-fi/product-details.aehpdp-in120-pe8800-series-aeh_sargent_846487 (last visited Jan. 26, 2024) (Under a heading entitled “IN120 PE8800 Series” stating, “This innovative WiFi lock makes it easy and affordable to expand your access control system by incorporating the two products together and utilizing your existing WiFi infrastructure” and indicates this lock provides support for “HID Mobile Access®.”); *HID Mobile Access*, APPLE, https://apps.apple.com/us/app/hid-mobile-access/id843238107 (last visited Jan. 26, 2024) (“HID Mobile Access® merges security with convenience by enabling a smartphone or other mobile device to securely open a door or gate.”).

21. Based on Assa Abloy AB's connections and relationship with its U.S. subsidiaries, manufacturers, dealers, retailers, and digital distribution platforms, Assa Abloy AB knows that Texas is a termination point of the established distribution channel, namely online and brick-and-mortar stores offering Assa Abloy 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. Assa Abloy AB, 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").

22. On information and belief, Assa Abloy AB alone and in concert with other related entities such as subsidiaries, and members, divisions, segments, companies and/or brands of Assa Abloy, manufactures and purposefully places infringing Assa Abloy 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 Assa Abloy's website. As an example, Assa Abloy AB, directly and/or through a related entity or subsidiary, manufactures infringing Assa Abloy products in Texas, imports infringing Assa Abloy products to Texas and/or sells or offers for sale infringing Assa Abloy products in Texas to resellers or dealers. At least components of Assa Abloy and/or Kwikset products are or have been manufactured in Denison, Texas, and/or Richardson, Texas, during times relevant to the allegations in this complaint. *See, e.g.*, *Company History*, KWIKSET, https://www.kwikset.com/about-kwikset (last visited Feb. 28, 2024) ("The Kwikset Denison, TX

facility broke ground and since then, there have been two plant expansions. Kwikset Denison manufactures component parts for Kwikset lock-sets, Price-Pfister faucets, and Black & Decker tools. The plant is the largest zinc user in the United States."); *Connect with Assa Abloy Global Solutions | US*, ASSA ABLOY, https://campaigns.assaabloyglobalsolutions.com/us-info (last visited Feb. 28, 2024) ("Connect with ASSA ABLOY Global Solutions | US: 631 International Parkway, Suite 100 Richardson, TX 75081"); *Assa Abloy Global Solutions Manufacturing and Distribution*, https://business.richardsonchamber.com/list/member/assa-abloy-global-solutions-24803 (last visited Feb. 28, 2024) (referring to "Assa Abloy Global Solutions Manufacturing and distribution," listing an address at "631 International Parkway STE 100, Richardson, TX 75081," and listing product and service offerings related to "openings, such as locks, doors, gates and entrance automation systems."). Kwikset wi-fi enabled smart locks are offered for sale and pickup at least at a Home Depot store located in this District at 5995 Eldorado Pkwy, Frisco, TX 75033. *See., e.g., Kwikset Wifi*, HOME DEPOT, https://www.homedepot.com/s/kwikset%20wifi?NCNI-5 (last visited Jan. 26, 2024) (indicating the "N Frisco" Home Depot located at 5995 Eldorado Pkwy, Frisco, TX 75033, in Collin County and this District, sells Kwikset WiFi smart locks, including, for example, Model# 99390-001 and 939WIFITSCR514S.). These suppliers, distributors, dealers, and/or resellers import, advertise, offer for sale and/or sell Assa Abloy 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 Assa Abloy AB'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, Assa Abloy AB knows and has known that Texas is a termination point of the established distribution channels for Assa Abloy products. Assa Abloy AB, alone and in concert with related entities, subsidiaries,

members, divisions, segments, companies and/or brands, including U.S.-based subsidiaries, members, divisions, segments, companies and/or brands of Assa Abloy 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).

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

24. Venue is proper in this District with respect to Defendant Assa Abloy AB, for example, pursuant to 28 U.S.C. § 1391. Defendant Assa Abloy AB 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.).

25. Additionally, venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and/or 1400(b). As alleged herein, Defendant Assa Abloy AB has committed acts of infringement

in this District. As further alleged herein, Defendant Assa Abloy AB, via its own operations, employees, and/or through the activities of Assa Abloy AB's alter egos, agents, related entities, and/or subsidiaries, has a regular and established place of business in this District, for example, at 2600 N HWY 91, Denison, Texas 75020 in Grayson County, Texas among any other Assa Abloy locations owned, leased and/or operated in this District. Accordingly, Assa Abloy AB may be sued in this district under 28 U.S.C. § 1400(b).

26. On information and belief, Defendant Assa Abloy AB has 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

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

28. 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.

29. 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.

30. 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.

31. The ’126 patent provides a secure wireless local area network (LAN) utilizing a LAN device. This device may include a housing that carries a wireless transceiver and a media access controller (MAC). A cryptography circuit carried by the housing may be connected to the MAC and the wireless transceiver. And the cryptography circuit may comprise a volatile memory provided for storing cryptography information and may also comprise a battery provided for maintaining the cryptography information stored on the volatile memory.

32. On information and belief, a significant portion of the operating revenue of Defendant 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, Assa Abloy reported that they had over 54 billion Swedish Kronor in sales in the U.S. market during the 2022 reporting period. *See* Annual Report pp. 2, 40, 45, 79.

33. The Asserted Patents cover Defendant's home and business IoT and smart 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., Persona Campus™ Online*, ASSA ABLOY, https://www.intelligentopenings.com/en/solutions/by-platform/persona-campus, (last visited Jan. 29, 2024) (under heading entitled "Comprehensive campus solutions," listing "IEEE 802.11b/g/n WiFi locks," "IEEE 802.15.4 Aperio® wireless locks and devices"); *ASSA ABLOY Joins the Alliance Board of Directors,* CONNECTIVITY STANDARDS ALLIANCE, https://csa-iot.org/newsroom/assa-abloy-joins-board/ (last visited Jan. 29, 2024) (stating "The Zigbee Alliance, an organization of hundreds of companies creating, maintaining, and delivering open, global standards for the Internet of Things (IoT), today announced ASSA ABLOY Group – the global leader in access solutions – has joined the Alliance's Board of Directors," and quoting Martin Huddart, Head of Smart Residential at Assa Abloy, as stating, "As a major manufacturer of residential and commercial access solutions, our product lines depend on efficient, reliable, and secure communications to operate effectively"); *Intelligent WiFi*, ASSA ABLOY, https://www.intelligentopenings.com/en/products/by-category/wireless/intelligent-wifi-access-control (last visited Jan. 29, 2024) (listing Assa Abloy WiFi-enabled products); *Complete access management for off-campus student housing*, ASSA ABLOY, https://www.intelligentopenings.com/en/solutions/by-market/multi-resident-access-control/off-campus-student-housing (last visited Jan. 29, 2024) ("Online solutions can be created by combining wired Ethernet and wireless Zigbee locks to create the most efficient setup for your individual needs."). Defendant's infringing products include, but are not limited to, devices enabled or compliant with Wi-Fi and/or ZigBee, including without limitation access control (for

example, Assa Abloy's Corbin Russwin IN120 Intelligent WIFI Access Control, Assa Abloy's Sargent IN120 PE8800 Series access control, Assa Abloy's Kwikset Halo Matte Black Touchscreen WiFi Keypad Electronic Single-Cylinder Smart Lock Deadbolt, Assa Abloy's August WiFi Smart Lock, Assa Abloy's Zigbee-enabled VingCard Classic RFID Electronic Lock, Assa Abloy's Zigbee-enabled DL100 lock, and Assa Abloy's Zigbee-enabled Securitron® R100 Aperio® Wireless Card Reader); connected modules, gateways, routers, and/or bridges (for example, Asa Abloy's Wi-Fi-enabled Connect Bridge Plus, Assa Abloy's Yale MD-05 BLE/WiFi transceiver module for door locks, Assa Abloy's Yale Wi-Fi Smart Module, Assa Abloy's Yale Zigbee Smart Module, Assa Abloy's Zigbee Module PCBA 1731, Assa Abloy's Zigbee Endnode Kit w/cable for Signature and Essence, Assa Abloy's Yale Assure Door Lock Range Zigbee Module, and devices that include any Wi-Fi- or Zigbee-enabled module); keypads (for example, Assa Abloy's Kwikset Halo Matte Black Touchscreen WiFi Keypad Electronic Single-Cylinder Smart Lock Deadbolt and Assa Abloy's Kwikset 916 SmartCode Traditional Electronic Deadbolt with Zigbee Technology); 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.

34. The Asserted Patents cover Accused Products of Assa Abloy that use the ZigBee protocol to communicate with other devices on a communication network, including those of third-party manufacturers. Examples of Assa Abloy's ZigBee products include the Assa Abloy VingCard Class RFID electronic lock, which uses the Zigbee protocol for "Online compatibility" and is shown below:

VingCard Classic RFID
Electronic Lock

Classic RFID offers the latest Radio Frequency Identification (RFID) technology and the quickest path to go contactless if you currently have standard Classic VingCard electronic locks installed.

TECHNICAL DATA

. . . .

Online compatibility	Wireless (based on ZigBee protocol) in Visionline.

See VingCard Classic RFID Electronic Lock, ASSA ABLOY (updated Sep. 2020), available for download at https://www.assaabloyglobalsolutions.com/downloadables/product-sheets/electronic-locks/vingcard-classic/VingCard%20Classic%20RFID%20Product%20Sheet%20English.pdf (last visited Feb. 1, 2024).

35. 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

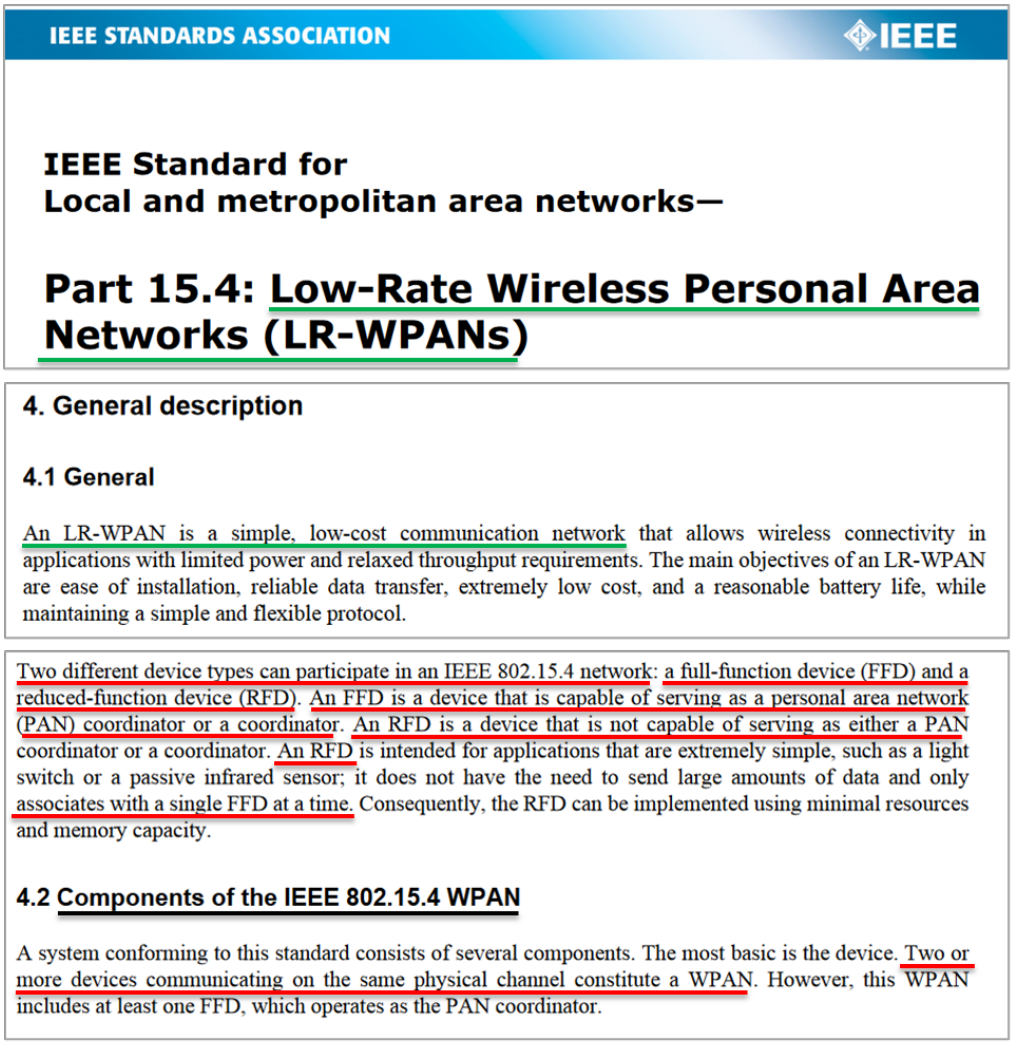
The ZigBee stack architecture is made up of a set of blocks called layers. Each layer performs a specific set of services for the layer above. A data entity provides a data transmission service and a management entity provides all other services. Each service entity exposes an interface to the upper 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).

36. 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 a 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

37. 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.

ZigBee Control your world

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.

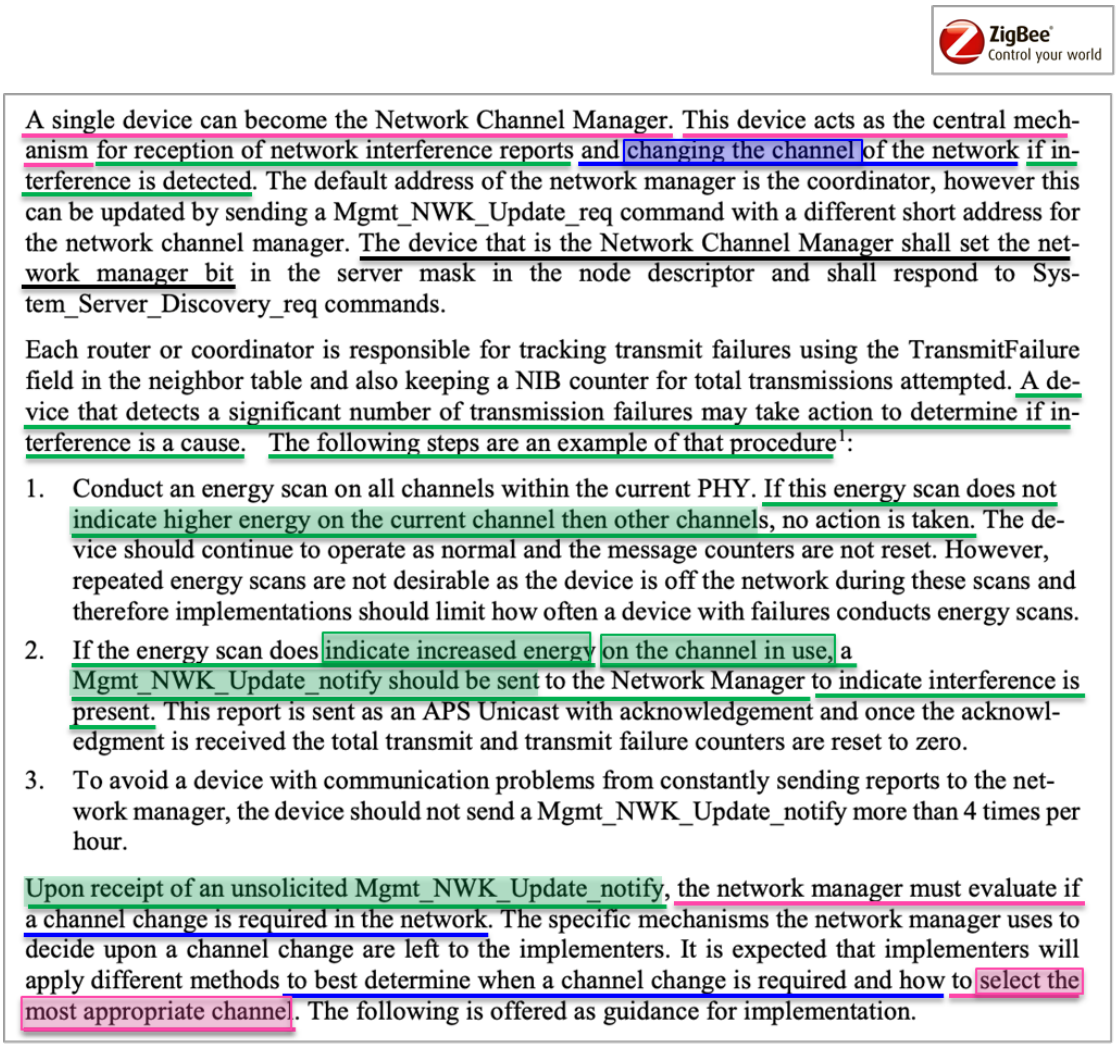
Each router or coordinator is responsible for tracking transmit failures using the TransmitFailure field in the neighbor table and also keeping a NIB counter for total transmissions attempted. A device that detects a significant number of transmission failures may take action to determine if interference 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

38. 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.



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.

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

39. 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

40. The Asserted Patents also cover Accused Products of Assa Abloy that utilize the Wi-Fi protocol. Examples of such products include Assa Abloy's Corbin Russwin IN120 Intelligent WiFi Access Control and the HID Mobile Access® powered by SEOS® application for mobile devices. As shown below, the IN120 Intelligent WiFi Access Control and the HID Mobile Access® app are Wi-Fi (IEEE 802.11) compliant:

Corbin Russwin
ASSA ABLOY

Security:
› AES 128-bit encryption
› Supports current WiFi network security standards, including:
- WEP, WPA and WPA2
- 802.1x (e.g. EAP, PEAP, PAP)

IN120 Intelligent WiFi Access Control

The Corbin Russwin IN120 pairs a sleek, attractive design with the latest in access control technology to address the evolving needs of today's facilities.

Featuring multiCLASS SE® technology and an optional keypad, it supports multiple credential types, including mobile devices, for a future-proof solution that is convenient and secure.

› 6 AA batteries

Features	Benefits
Utilizes IEEE 802.11 WiFi infrastructure	• Significantly reduces installation costs • Eliminates the need for any proprietary equipment • Ideal for hard-to-wire locations
multiCLASS SE® Technology from HID Global®	• Provides heightened security • Supports: – Multiple credential technologies, offering easy migration to higher security credentials or consolidation of mixed credentials – Optional keypad for dual authentication requirements or one-time PIN usage – HID Mobile Access® powered by Seos®, for both iOS® and Android™ devices – PIV/PIV-I variants support HID PROX, iCLASS and iCLASS SE
Field-upgradable 802.11b/g/n radio	• Interoperability with other WiFi equipment • Future proof for constantly evolving WiFi standards

Corbin Russwin IN120 WiFI Sell Sheet, CORBIN RUSSWIN ASSA ABLOY (2020) available at https://www.corbinrusswin.com/en/commercial-locks-products/electronic-access-

control/wireless/intelligent-wi-fi/product-details.aehpdp-mechanical-locks-and-exit-devices-mortise-locks-m-l2000-series-in120-ml2000-series-171255-aeh_corbin_russwin_171255 (last visited Feb. 1, 2024).

How does ASSA ABLOY support mobile access in their access control locks?

ASSA ABLOY offers support for:

HID Mobile Access®

HID Mobile Access, which leverages Seos® as its underlying credential technology, offers these key benefits:

- **User Convenience:** Users can now use their mobile device to access facilities. Highly intuitive "Tap" and "Twist and Go" gestures make for convenient and efficient access.
- **Operational Efficiency and Cost Effectiveness:** Using HID Global's highly stable online management portal, administrators can create, manage, issue and revoke credentials through the cloud. Organizations can efficiently scale up or down in response to business needs.
- **Higher Security:** HID Mobile Access is powered by Seos credential technology and follows best practices in data integrity to bind each mobile ID to the device and protect the data at rest and in motion.

ASSA ABLOY products supporting mobile access

Wireless

Real-Time Wireless (Aperio) and Intelligent WiFi

Adams Rite DL100 Aperio wireless deadlatch

VIew product >

Corbin Russwin IN100 Aperio wireless lock

View product >

Corbin Russwin IN120 WiFi lock

View product >

HES ES100 Aperio wireless strike

View product >

HES K100 Aperio wireless cabinet lock

View product >

HES KS100 Aperio wireless server cabinet lock

View product >

SARGENT IN100 Aperio wireless lock

View product >

SARGENT IN120 WiFi lock

View product >

Securitron R100 Aperio wireless reader

View product >

Securitron DR100 wireless card reader with relay

View product >

Mobile Access, ASSA ABLOY, https://www.intelligentopenings.com/en/solutions/by-challenge/access-control-technologies-and-trends/mobile-access-control (last visited Sep. 30, 2023).

41. As can be seen, Assa Abloy supports mobile access for their access control devices, including Wi-Fi-enabled control locks via their HID Mobile Access® app for mobile devices.

42. 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.

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

43. 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

44. 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

45. 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

46. 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.

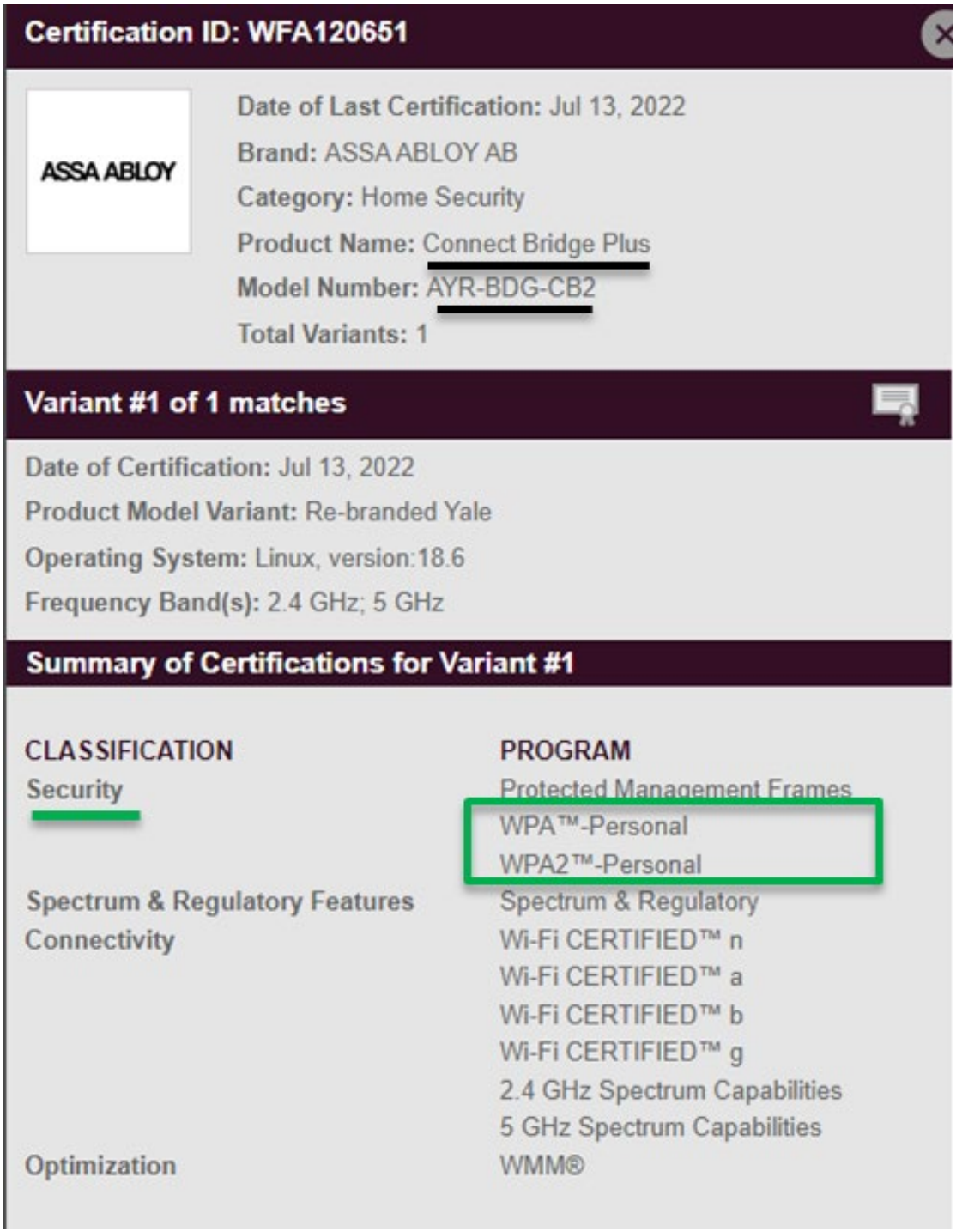
If a subsequent MIC failure occurs within 60 s of the most recent previous failure, then a STA whose IEEE 802.1X entity has acted as a Supplicant shall deauthenticate (as defined in 11.3.1.3) itself or deauthenticate all the STAs with a security association if its IEEE 802.1X entity acted as an Authenticator. 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

47. The Asserted Patents also cover Assa Abloy's 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 Assa Abloy's smart access control 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 Assa Abloy devices. Each of the devices has a housing.

Corbin Russwin IN120 WiFI Sell Sheet, CORBIN RUSSWIN ASSA ABLOY (2020) available at https://www.corbinrusswin.com/en/commercial-locks-products/electronic-access-control/wireless/intelligent-wi-fi/product-details.aehpdp-mechanical-locks-and-exit-devices-mortise-locks-m-l2000-series-in120-ml2000-series-171255-aeh_corbin_russwin_171255 (last visited Feb. 1, 2024).



Certification ID: WFA120651

ASSA ABLOY

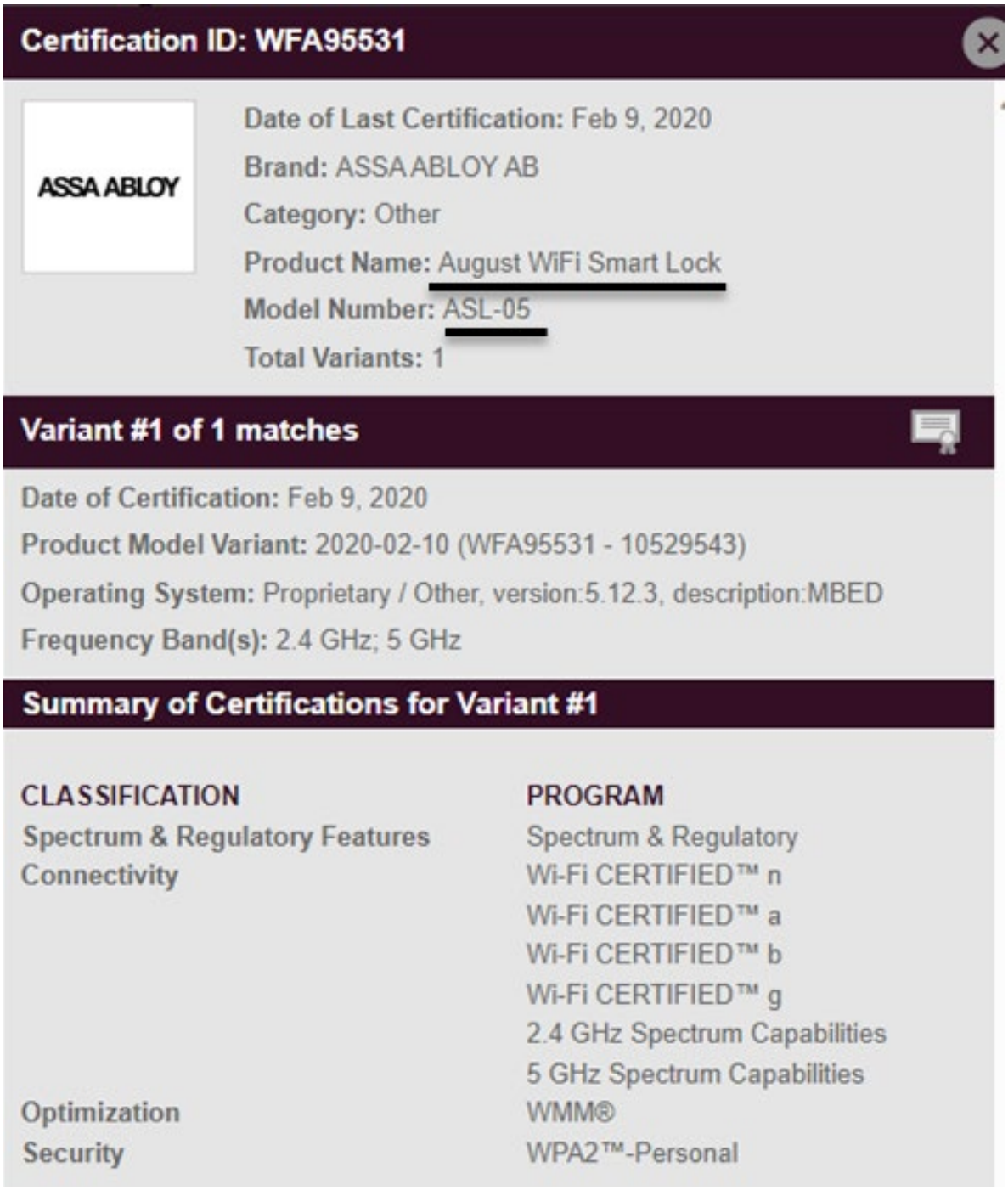
Date of Last Certification: Jul 13, 2022
Brand: ASSA ABLOY AB
Category: Home Security
Product Name: Connect Bridge Plus
Model Number: AYR-BDG-CB2
Total Variants: 1

Variant #1 of 1 matches

Date of Certification: Jul 13, 2022
Product Model Variant: Re-branded Yale
Operating System: Linux, version:18.6
Frequency Band(s): 2.4 GHz; 5 GHz

Summary of Certifications for Variant #1

CLASSIFICATION	PROGRAM
Security	Protected Management Frames
	WPA™-Personal
	WPA2™-Personal
Spectrum & Regulatory Features	Spectrum & Regulatory
Connectivity	Wi-Fi CERTIFIED™ n
	Wi-Fi CERTIFIED™ a
	Wi-Fi CERTIFIED™ b
	Wi-Fi CERTIFIED™ g
	2.4 GHz Spectrum Capabilities
	5 GHz Spectrum Capabilities
Optimization	WMM®



Certification ID: WFA95531

ASSA ABLOY

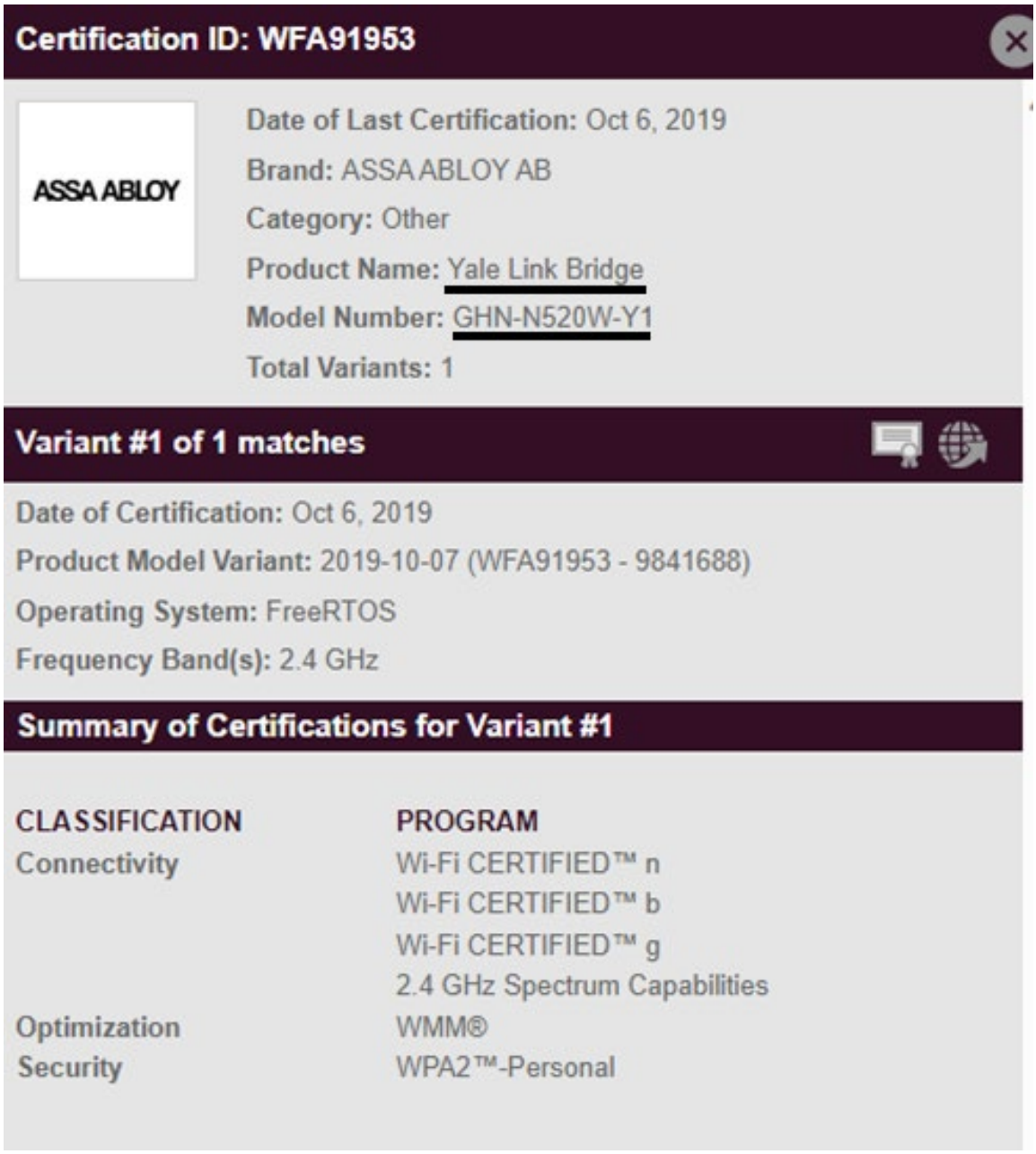
Date of Last Certification: Feb 9, 2020
Brand: ASSA ABLOY AB
Category: Other
Product Name: August WiFi Smart Lock
Model Number: ASL-05
Total Variants: 1

Variant #1 of 1 matches

Date of Certification: Feb 9, 2020
Product Model Variant: 2020-02-10 (WFA95531 - 10529543)
Operating System: Proprietary / Other, version:5.12.3, description:MBED
Frequency Band(s): 2.4 GHz; 5 GHz

Summary of Certifications for Variant #1

CLASSIFICATION	PROGRAM
Spectrum & Regulatory Features	Spectrum & Regulatory
Connectivity	Wi-Fi CERTIFIED™ n
	Wi-Fi CERTIFIED™ a
	Wi-Fi CERTIFIED™ b
	Wi-Fi CERTIFIED™ g
	2.4 GHz Spectrum Capabilities
	5 GHz Spectrum Capabilities
Optimization	WMM®
Security	WPA2™-Personal



Product Finder, WIFI ALLIANCE, https://www.wi-fi.org/product-finder-results?sort_by=certified&sort_order=desc&companies=2665 (last visited Feb. 1, 2024) (filter for "Assa Abloy" as the "Brand").

48. WPA and WPA2 security encryption systems are used in conjunction with 802.11 b/g/n Wi-Fi connections standards, which as illustrated above are utilized across Defendant's Accused Product line.

49. As illustrated above, the Wi-Fi-enabled Accused Products provide 2.4 and/or 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.

50. 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.

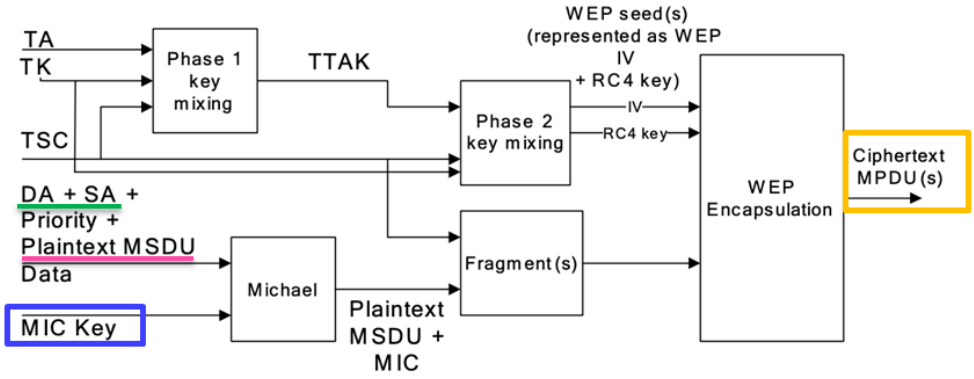


Figure 8-4—TKIP encapsulation block diagram

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

51. On information and belief, Defendant also infringes the ’126 patent via products that utilize a volatile memory for storing cryptography information utilized in the cryptography circuit and a battery for maintaining the cryptography information in the volatile memory. As examples, Assa Abloy’s Corbin Russwin IN120 Intelligent WIFI Access Control (see discussion *supra*), Wi-Fi-enabled Sargent IN120 PE8800 Series access control, Kwikset HALO WI-FI

Touchscreen Smart Lock, and Wi-Fi-enabled Yale MD-05 module each utilize a battery that provides power to maintain data, including cryptographic information in the product's internal (volatile) memory. Such cryptographic information allows data encryption to be carried out over a secure wireless 802.11 network.

SARGENT
ASSA ABLOY

IN120 PE8800 Series

The IN120-PE8800 Series pairs a sleek, attractive design in access control technology with our heavy duty, wide-stile rim exit device. This innovative WiFi lock makes it easy and affordable to expand your access control system by incorporating the two products together and utilizing your existing WiFi infrastructure. Featuring multiCLASS SE® technology from HID Global, it provides heightened security as well as simultaneous support for multiple credential types and HID Mobile Access® powered by Seos®.

- **Batteries Required:** 6 AA Alkaline Batteries

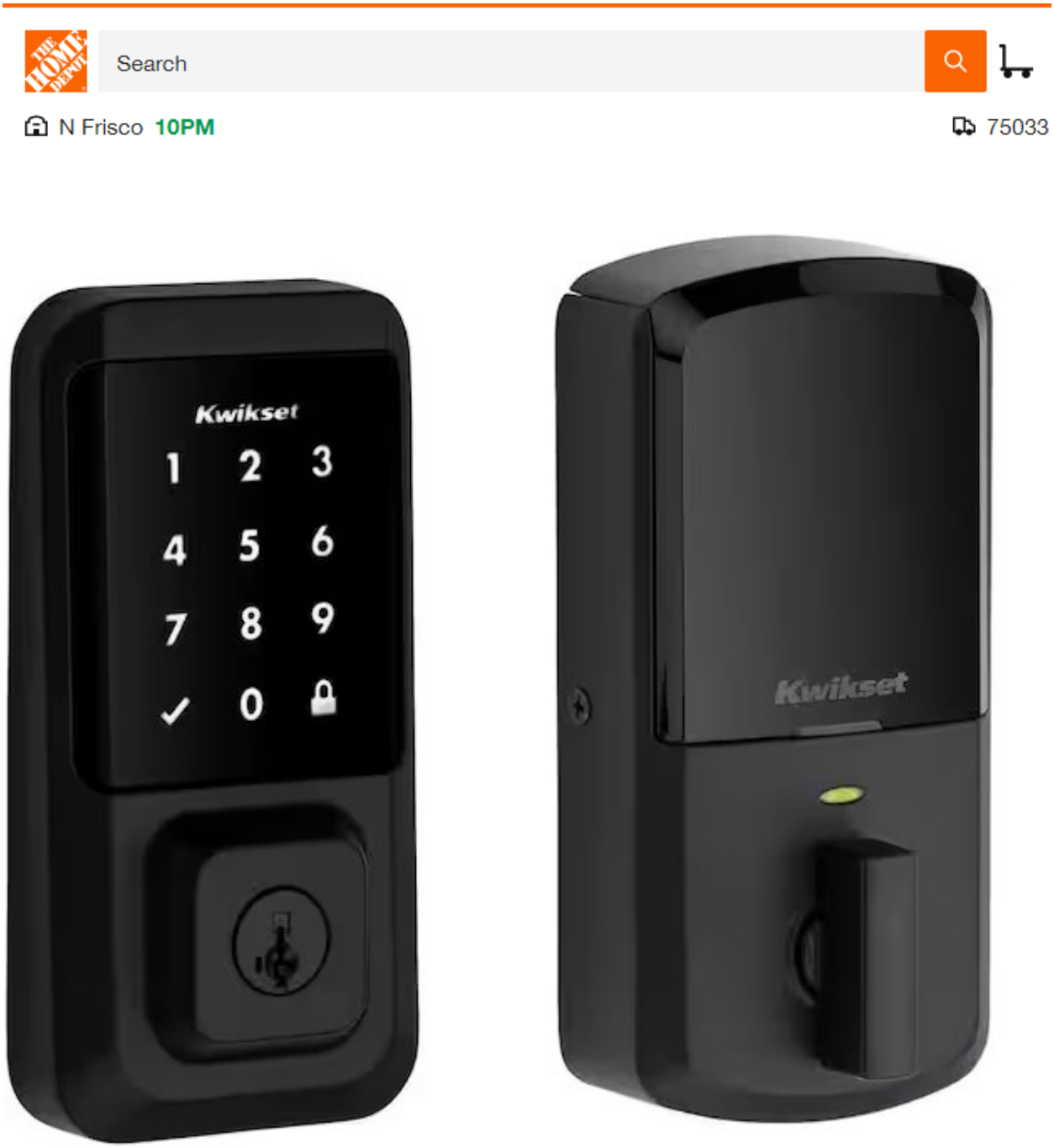
Features

- Utilizes IEEE 802.11 WiFi infrastructure
- 802.11b/g/n radio

Benefits

- Provides heightened security by supporting offerings such as multiple credential technologies, offering easy migration to higher security credentials or consolidation of mixed credentials– Optional keypad for dual authentication requirements or one-time PIN usage– HID Mobile Access® powered by Seos®, for both iOS® and Android™ devices– PIV/PIV-I variants support HID PROX, iCLASS and iCLASS SE
- Allows for interoperability with other WiFi equipment which evolves with constantly changing WiFi standards

IN120 PE8800 Series, SARGENT ASSA ABLOY, https://www.sargentlock.com/en/commercial-locks-products/electronic-access-control/wireless/intelligent-wi-fi/product-details.aehpdp-in120-pe8800-series-aeh_sargent_846487 (last visited Feb. 1, 2024).



Details

Battery Type	AA Battery
Connectivity	Wifi

Kwikset HALO Matte Black Touchscreen WiFi Keypad Electronic Single-Cylinder Smart Lock Deadbolt featuring SmartKey Security, HOME DEPOT, https://www.homedepot.com/p/Kwikset-HALO-Matte-Black-Touchscreen-WiFi-Keypad-Electronic-Single-Cylinder-Smart-Lock-Deadbolt-featuring-SmartKey-Security-939WIFITSCR514S/311532384 (last visited Feb. 1, 2024).

August 18, 2021

ASSA ABLOY

Federal Communications Commission
7435 Oakland Mills Road
Columbia, MD
21046-1609 CC:
Curtis-Straus LLC
TCB

Re: Single Modular Approval Request

We, ASSA ABLOY Inc., are applying for a **full modular approval** for our device with **FCC ID: U4A-WF1MRUS**

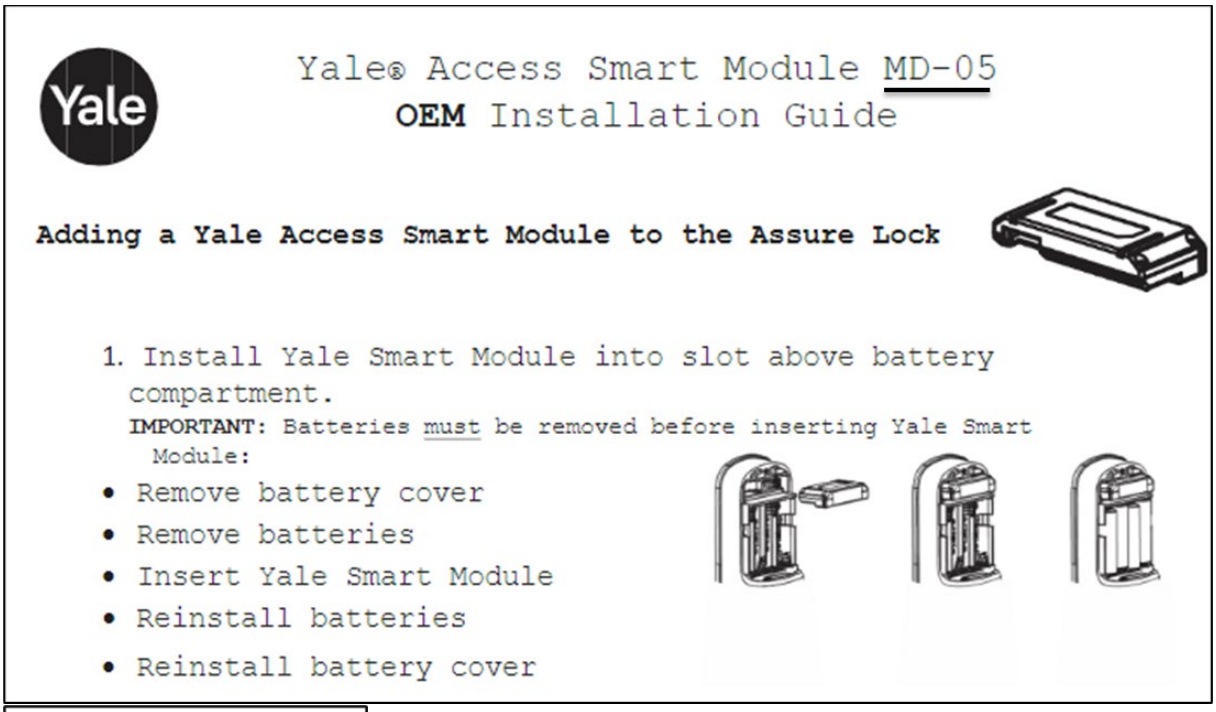
Please note that, this module is to be installed only by us in our end products and will not be marketed to any other party. Installation will be under our control and therefore full compliance of the end product will always be ensured.

https://fccid.io/U4A-WF1MRUS/Letter/Modular-Request-Letter-5426379

2.2 Description of EUT

The MD-05 is a module containing a BLE/WiFi transceiver that is used in Yale door locks. The MD-05 is powered by the batteries in the lock. For testing purposes, the MD-05 was powered by a Phihong PSA05A-050QL6 power supply. The MD-05 uses a Murata Type 1LV BLE/WiFi transceiver module with an inverted F trace antenna. The 802.11bgn transceiver uses 11 channels as shown in the table below.

https://fccid.io/U4A-WF1MRUS/Test-Report/TR-Sub-C-2-4GHz-WiFi-5426392



Yale® Access Smart Module MD-05
OEM Installation Guide

Adding a Yale Access Smart Module to the Assure Lock

1. Install Yale Smart Module into slot above battery compartment.
IMPORTANT: Batteries must be removed before inserting Yale Smart Module:
- Remove battery cover
- Remove batteries
- Insert Yale Smart Module
- Reinstall batteries
- Reinstall battery cover

FCC:
FCC ID: U4A-WF1MRUS

https://fccid.io/U4A-WF1MRUS/Users-Manual/User-Manual-Installation-Manual-5426397

52. As shown in the non-limiting examples of above, several Accused Products utilize a battery to maintain cryptography information involved in a secure wireless 802.11 network.

COUNT I

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

53. Plaintiff incorporates paragraphs 1 through 52 herein by reference.

54. 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.

55. 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.

56. Assa Abloy 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.

57. On information and belief, Assa Abloy designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Assa Abloy and its subsidiaries, members, divisions, segments, companies, brands and/or related entities, including U.S.-based subsidiaries, members, divisions, segments, companies and/or brands of Assa Abloy.

58. Defendant directly infringes the '678 patent via 35 U.S.C. § 271(a) by manufacturing (including via contract manufacturers), 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, subsidiaries, members, divisions, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, (i) Defendant designs the Accused Products for U.S. consumers; (ii) Defendant makes, uses, and/or sells the Accused Products inside the United States; and/or (iii) Defendant makes and sells the Accused Products outside of the United States and delivers those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, integrators, installers, customers and/or other related service providers in the United States, or in the case that Defendant 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)").

59. Furthermore, Defendant Assa Abloy AB directly infringes the '678 patent through its direct involvement in the activities of its subsidiaries, and related entities, including U.S.-based subsidiaries, members, divisions, segments, companies and/or brands of Assa Abloy, including by designing the Accused Products for U.S. consumers; making the Accused Products in the United States; using the Accused Products in the United States; selling and offering for sale the Accused Products directly to U.S. consumers and its related entities; and/or importing the Accused Products into the United States for sale and/or for its related entities. On information and belief, Assa Abloy's U.S.-based subsidiaries and/or brands, including at least Assa Abloy Global Solutions, Inc., Assa Abloy Sales and Marketing Group, Assa Abloy Americas Residential Inc., and/or Door Security Solutions of the Southwest, conduct activities that constitute direct infringement of the '678 patent under 35 U.S.C. § 271(a) by making, importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendant. Defendant Assa Abloy AB is vicariously liable for the infringing conduct of Assa Abloy Global Solutions, Inc., Assa Abloy Sales and Marketing Group, Assa Abloy Americas Residential Inc., and/or Door Security Solutions of the Southwest, and other U.S.-based subsidiaries, members, related entities, divisions, segments, companies and/or brands of Assa Abloy (under both the alter ego and agency theories). On information and belief, Defendant Assa Abloy AB, and related entities and subsidiaries, including U.S.-based subsidiaries members, divisions, segments, companies and/or brands of Assa Abloy are essentially the same company (i.e., "Assa Abloy"), operating in the U.S.

via, for example, one or more of the brands, divisions, segments, mergers, and/or acquisitions of Assa Abloy listed in this complaint. Moreover, Assa Abloy AB, as the parent company, along with its related entities, has the right and ability to control and/or delegate the control of the infringing activities of those subsidiary entities such that Defendant receives a direct financial benefit from that infringement.

60. For example, Assa Abloy infringes claim 51 of the '678 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to access control (for example, Assa Abloy's Corbin Russwin IN120 Intelligent WIFI Access Control, Assa Abloy's Wi-Fi-enabled Sargent IN120 PE8800 Series access control, Assa Abloy's Kwikset Halo Matte Black Touchscreen WiFi Keypad Electronic Single-Cylinder Smart Lock Deadbolt, and Assa Abloy's August WiFi Smart Lock); connected modules, gateways, routers, and/or bridges (for example, Asa Abloy's Wi-Fi-enabled Connect Bridge Plus, Assa Abloy's Yale MD-05 BLE/WiFi transceiver module for door locks, Assa Abloy's Yale Wi-Fi Smart Module, and devices including any WiFi-enabled module); keypads (for example, Assa Abloy's Kwikset Halo Matte Black Touchscreen WiFi Keypad Electronic Single-Cylinder Smart Lock Deadbolt); and related accessories and software.

61. 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.

62. At a minimum, Assa Abloy has known of the '678 patent at least as early as the filing date of this complaint. In addition, Assa Abloy 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 May 8, 2018, from North Forty Consulting LLC, working with Harris Corporation. The letter notifies Assa Abloy (via its Kwikset subsidiary and/or brand) of Harris Corporation's (now L3 Harris Technologies, Inc.) ownership of patents relating to wireless communication networks, network management/security, as well as innovations pertinent to the IEEE 802.11 and Zigbee standards. Further, Assa Abloy has been on notice about infringement of the Harris patent portfolio and the '678 patent, since at least its receipt (via Kwikset) of a presentation and licensing proposal dated on or around March 2019, from North Forty Consulting LLC, working with Harris Corporation.

63. Additional correspondence sent by Acacia Research Group LLC on behalf of Stingray (a wholly owned subsidiary of Acacia Research Group LLC), regarding Stingray's acquisition of and attempt to license the Harris patent portfolio (which Assa Abloy had notice of at least by May 8, 2018), was sent directly to Assa Abloy, for example, via correspondence to Mr. Nico Delvaux, President and CEO of Assa Abloy, and correspondence to Mr. Lucas Boselli, Head of Americas Division of Assa Abloy, with a copy to Ms. Page Heslin, General Counsel and Secretary of Assa Abloy Americas, both items of correspondence dated June 16, 2020. Acacia Research Group LLC, on behalf of Stingray, also sent further correspondence to Assa Abloy via Kwikset regarding Stingray's acquisition of and attempt to license the Harris patent portfolio. For example, correspondence dated August 21, 2020, was addressed to Mr. John Lundgren, Chief

Executive Officer of Kwikset, pointing out the lack of response to earlier correspondence dated June 16, 2020, and again offering to discuss licensing the Harris patent portfolio. These examples of notice provided to Assa Abloy are not exhaustive, and Assa Abloy has also received additional notice of infringement in connection with the Asserted Patents.

64. On information and belief, since at least the above-mentioned date or dates when Defendant was on notice of its infringement, Defendant has actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, integrators, installers, OEMs, consumers, other users, and other related service providers that make, 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 making, using, offering for sale, selling, and/or importing the Accused Products. Since at least the date or dates of notice provided above, Defendant conducts infringing activities with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '678 patent. On information and belief, Defendant intends to cause, and has taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMS, integrators, installers, consumers, other users, 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. Moreover, Defendant manufactures, tests, and certifies the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendant distributes or makes available instructions or manuals for these products to consumers, installers, purchasers and/or prospective

buyers, tests and certifies the wireless networking features (with for example the Wi-Fi Alliance and/or for FCC compliance) in the Accused Products, and provides technical support, product files, videos, and/or related services for these products to purchasers in the United States. *See, e.g., Product Finder Filtered Results*, WIFI ALLIANCE, https://www.wi-fi.org/product-finder-results?keywords=Assa Abloy (last visited Feb. 5, 2024) (showing Assa Abloy's WiFi Certified™ products include, for example, the "August connect" with model number "AC-R2" and "Last Certified Date: 2022-10-24," the "Connect Bridge Plus" with model number "AYR-BDG-CB2" and "Last Certified Date: 2022-07-14," and the "Yale Link Bridge," with model number "GHN-N520W-Y1" and "Last Certified Date: 2019-10-07"); *Test Report Certification pursuant to FCC Part 15, Subpart C for Assa Abloy's Yale MD-05 BLE/WiFi transceiver module for door locks*, VPI LABORATORIES (Aug. 3, 2021), available at https://fccid.io/U4A-WF1MRUS/Test-Report/TR-Sub-C-2-4GHz-WiFi-5426392 (last visited Feb. 5, 2024); *Yale® Access Smart Module MD-05 OEM Installation Guide*, YALE, available at https://fccid.io/U4A-WF1MRUS/Users-Manual/User-Manual-Installation-Manual-5426397 (last visited Feb. 5, 2024); *ASSA ABLOY IN120 WiFi Access Control Lock*, SARGENT ASSA ABLOY, https://www.youtube.com/watch?v=Lc_vsMBcC_U (last visited Feb. 6, 2024) (including a description that states "The IN120 WiFi lock, available from ASSA ABLOY Group brands Corbin Russwin and SARGENT, offers the ease and flexibility of WiFi in a new streamlined design, setting a new standard for aesthetics and performance," and "The IN120 uses 802.11b/g/n WiFi infrastructure . . . .").

65. Furthermore, Defendant induces infringement by installers, integrators, consumers and other users of Assa Abloy's products by designing, developing, marketing, and offering smartphone, tablet, and/or mobile device interfaces as application software (i.e., apps) such as the

HID Mobile Access® App to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, including Wi-Fi and ZigBee networks. *See, e.g.*, *Mobile Access*, ASSA ABLOY, https://www.intelligentopenings.com/en/solutions/by-challenge/access-control-technologies-and-trends/mobile-access-control (last visited Feb. 5, 2024).

66. Assa Abloy's apps also induce infringing use of the Accused Products by providing compatibility between Assa Abloy products and third-party products that share or access the same wireless networks. *See, e.g., HID Mobile Access – Compatible Devices*, HID, https://www.hidglobal.com/mobile-access-compatible-devices (last visited Feb. 5, 2024) (stating "[t]his list of mobile devices is regularly updated to show those deemed to be compatible with the latest version of the HID® Mobile Access® app" and listing devices from numerous brands). Such compatibility provides convenience and added functionality that induces consumers to use the Defendant's products, including via apps and other interfaces utilizing Wi-Fi and/or ZigBee protocols in networks with other third-party devices. Thus, these activities further infringe or induce infringement of the '678 patent.

67. On information and belief, despite having knowledge of the '678 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '678 patent, Defendant has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendant's 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.

68. Plaintiff Stingray has been damaged as a result of Assa Abloy's infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for their 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 II

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

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

70. 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.

71. 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.

72. Assa Abloy 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.

73. On information and belief, Assa Abloy designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Assa Abloy and its subsidiaries, members, divisions, segments, companies, brands and/or related entities, including U.S.-based subsidiaries, members, divisions, segments, companies and/or brands of Assa Abloy.

74. Defendant directly infringes the '572 patent via 35 U.S.C. § 271(a) by manufacturing (including via contract manufacturers), 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, subsidiaries, members, divisions, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, (i) Defendant designs the Accused Products for U.S. consumers; (ii) Defendant makes, uses, and/or sells the Accused Products inside the United States; and/or (iii) Defendant makes and sells the Accused Products outside of the United States and delivers those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, integrators, installers, customers and/or other related service providers in the United States, or in the case that Defendant 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)").

75. Furthermore, Defendant Assa Abloy AB directly infringes the '572 patent through its direct involvement in the activities of its subsidiaries, and related entities, including U.S.-based subsidiaries, members, divisions, segments, companies and/or brands of Assa Abloy, including by designing the Accused Products for U.S. consumers; making the Accused Products in the United States; using the Accused Products in the United States; selling and offering for sale the Accused Products directly to U.S. consumers and its related entities; and/or importing the Accused Products

into the United States for sale and/or for its related entities. On information and belief, Assa Abloy's U.S.-based subsidiaries and/or brands, including at least Assa Abloy Global Solutions, Inc., Assa Abloy Sales and Marketing Group, Assa Abloy Americas Residential Inc., and/or Door Security Solutions of the Southwest, conduct activities that constitute direct infringement of the '572 patent under 35 U.S.C. § 271(a) by making, importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendant. Defendant Assa Abloy AB is vicariously liable for the infringing conduct of Assa Abloy Global Solutions, Inc., Assa Abloy Sales and Marketing Group, Assa Abloy Americas Residential Inc., and/or Door Security Solutions of the Southwest, and other U.S.-based subsidiaries, members, related entities, divisions, segments, companies and/or brands of Assa Abloy (under both the alter ego and agency theories). On information and belief, Defendant Assa Abloy AB, and related entities and subsidiaries, including U.S.-based subsidiaries members, divisions, segments, companies and/or brands of Assa Abloy are essentially the same company (i.e., "Assa Abloy"), operating in the U.S. via, for example, one or more of the brands, divisions, segments, mergers, and/or acquisitions of Assa Abloy listed in this complaint. Moreover, Assa Abloy AB, as the parent company, along with its related entities, has the right and ability to control and/or delegate the control of the infringing activities of those subsidiary entities such that Defendant receives a direct financial benefit from that infringement.

76. For example, Assa Abloy infringes claim 1 of the '572 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to access control (for example, Assa Abloy's Corbin Russwin IN120 Intelligent WIFI Access Control, Assa Abloy's Wi-Fi-enabled Sargent IN120 PE8800 Series access control, Assa Abloy's Kwikset Halo Matte Black Touchscreen WiFi Keypad Electronic Single-Cylinder Smart Lock Deadbolt, and Assa

Abloy's August WiFi Smart Lock); connected modules, gateways, routers, and/or bridges (for example, Asa Abloy's Wi-Fi-enabled Connect Bridge Plus, Assa Abloy's Yale MD-05 BLE/WiFi transceiver module for door locks, Assa Abloy's Yale Wi-Fi Smart Module, and devices including any WiFi-enabled module); keypads (for example, Assa Abloy's Kwikset Halo Matte Black Touchscreen WiFi Keypad Electronic Single-Cylinder Smart Lock Deadbolt); and related accessories and software.

77. 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.

78. Assa Abloy 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 make a secure wireless local area network 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.

79. Assa Abloy 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.

80. At a minimum, Assa Abloy has known of the '572 patent at least as early as the filing date of this complaint. In addition, Assa Abloy 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 May 8, 2018, from North Forty Consulting LLC, working with Harris Corporation. The letter notifies Assa Abloy (via its Kwikset subsidiary and/or brand) of Harris Corporation's (now L3 Harris Technologies, Inc.) ownership of patents relating to wireless communication networks, network management/security, as well as innovations pertinent to the IEEE 802.11 and Zigbee standards. Further, Assa Abloy has been on notice about infringement of the Harris patent portfolio and the '572 patent, since at least its receipt (via Kwikset) of a presentation and licensing proposal dated on or around March 2019, from North Forty Consulting LLC, working with Harris Corporation.

81. Additional correspondence sent by Acacia Research Group LLC on behalf of Stingray (a wholly owned subsidiary of Acacia Research Group LLC), regarding Stingray's acquisition of and attempt to license the Harris patent portfolio (which Assa Abloy had notice of at least by May 8, 2018), was sent directly to Assa Abloy, for example, via correspondence to Mr. Nico Delvaux, President and CEO of Assa Abloy, and correspondence to Mr. Lucas Boselli, Head of Americas Division of Assa Abloy, with a copy to Ms. Page Heslin, General Counsel and Secretary of Assa Abloy Americas, both items of correspondence dated June 16, 2020. Acacia Research Group LLC, on behalf of Stingray, also sent further correspondence to Assa Abloy via Kwikset regarding Stingray's acquisition of and attempt to license the Harris patent portfolio. For

example, correspondence dated August 21, 2020, was addressed to Mr. John Lundgren, Chief Executive Officer of Kwikset, pointing out the lack of response to earlier correspondence dated June 16, 2020, and again offering to discuss licensing the Harris patent portfolio. These examples of notice provided to Assa Abloy are not exhaustive, and Assa Abloy has also received additional notice of infringement in connection with the Asserted Patents.

82. On information and belief, since at least the above-mentioned date or dates when Defendant was on notice of its infringement, Defendant has actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, integrators, installers, OEMs, consumers, other users, and other related service providers that make, 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 making, using, offering for sale, selling, and/or importing the Accused Products. Since at least the date or dates of notice provided above, Defendant conducts infringing activities with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the ’572 patent. On information and belief, Defendant intends to cause, and has taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMS, integrators, installers, consumers, other users, 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. Moreover, Defendant manufactures, tests, and certifies the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendant distributes or makes available

instructions or manuals for these products to consumers, installers, purchasers and/or prospective buyers, tests and certifies the wireless networking features (with for example the Wi-Fi Alliance and/or for FCC compliance) in the Accused Products, and provides technical support, product files, videos, and/or related services for these products to purchasers in the United States. *See, e.g., Product Finder Filtered Results*, WIFI ALLIANCE, https://www.wi-fi.org/product-finder-results?keywords=Assa Abloy (last visited Feb. 5, 2024) (showing Assa Abloy's WiFi Certified™ products include, for example, the "August connect" with model number "AC-R2" and "Last Certified Date: 2022-10-24," the "Connect Bridge Plus" with model number "AYR-BDG-CB2" and "Last Certified Date: 2022-07-14," and the "Yale Link Bridge," with model number "GHN-N520W-Y1" and "Last Certified Date: 2019-10-07"); *Test Report Certification pursuant to FCC Part 15, Subpart C for Assa Abloy's Yale MD-05 BLE/WiFi transceiver module for door locks*, VPI LABORATORIES (Aug. 3, 2021), available at https://fccid.io/U4A-WF1MRUS/Test-Report/TR-Sub-C-2-4GHz-WiFi-5426392 (last visited Feb. 5, 2024); *Yale® Access Smart Module MD-05 OEM Installation Guide*, YALE, available at https://fccid.io/U4A-WF1MRUS/Users-Manual/User-Manual-Installation-Manual-5426397 (last visited Feb. 5, 2024); *ASSA ABLOY IN120 WiFi Access Control Lock*, SARGENT ASSA ABLOY, https://www.youtube.com/watch?v=Lc_vsMBcC_U (last visited Feb. 6, 2024) (including a description that states "The IN120 WiFi lock, available from ASSA ABLOY Group brands Corbin Russwin and SARGENT, offers the ease and flexibility of WiFi in a new streamlined design, setting a new standard for aesthetics and performance," and "The IN120 uses 802.11b/g/n WiFi infrastructure . . . .").

83. Furthermore, Defendant induces infringement by installers, integrators, consumers and other users of Assa Abloy's products by designing, developing, marketing, and offering

smartphone, tablet, and/or mobile device interfaces as application software (i.e., apps) such as the HID Mobile Access® App to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, including Wi-Fi and ZigBee networks. *See, e.g.*, *Mobile Access*, ASSA ABLOY, https://www.intelligentopenings.com/en/solutions/by-challenge/access-control-technologies-and-trends/mobile-access-control (last visited Feb. 5, 2024).

84. Assa Abloy's apps also induce infringing use of the Accused Products by providing compatibility between Assa Abloy products and third-party products that share or access the same wireless networks. *See, e.g., HID Mobile Access – Compatible Devices*, HID, https://www.hidglobal.com/mobile-access-compatible-devices (last visited Feb. 5, 2024) (stating "[t]his list of mobile devices is regularly updated to show those deemed to be compatible with the latest version of the HID® Mobile Access® app" and listing devices from numerous brands). Such compatibility provides convenience and added functionality that induces consumers to use the Defendant's products, including via apps and other interfaces utilizing Wi-Fi and/or ZigBee protocols in networks with other third-party devices. Thus, these activities further infringe or induce infringement of the '572 patent.

85. On information and belief, despite having knowledge of the '572 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '572 patent, Defendant has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendant's 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.

86. Plaintiff Stingray has been damaged as a result of Assa Abloy's infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for their 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)

87. Plaintiff incorporates paragraphs 1 through 86 herein by reference.

88. 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.

89. 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.

90. Assa Abloy 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.

91. On information and belief, Assa Abloy designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Assa Abloy and its subsidiaries, members, divisions, segments, companies, brands and/or related entities, including U.S.-based subsidiaries, members, divisions, segments, companies and/or brands of Assa Abloy.

92. Defendant directly infringes the '961 patent via 35 U.S.C. § 271(a) by manufacturing (including via contract manufacturers), 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, subsidiaries, members, divisions, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, (i) Defendant designs the Accused Products for U.S. consumers; (ii) Defendant makes, uses, and/or sells the Accused Products inside the United States; and/or (iii) Defendant makes and sells the Accused Products outside of the United States and delivers those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, integrators, installers, customers and/or other related service providers in the United States, or in the case that Defendant 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)").

93. Furthermore, Defendant Assa Abloy AB directly infringes the '961 patent through its direct involvement in the activities of its subsidiaries, and related entities, including U.S.-based subsidiaries, members, divisions, segments, companies and/or brands of Assa Abloy, including by designing the Accused Products for U.S. consumers; making the Accused Products in the United

States; using the Accused Products in the United States; selling and offering for sale the Accused Products directly to U.S. consumers and its related entities; and/or importing the Accused Products into the United States for sale and/or for its related entities. On information and belief, Assa Abloy's U.S.-based subsidiaries and/or brands, including at least Assa Abloy Global Solutions, Inc., Assa Abloy Sales and Marketing Group, Assa Abloy Americas Residential Inc., and/or Door Security Solutions of the Southwest, conduct activities that constitute direct infringement of the '961 patent under 35 U.S.C. § 271(a) by making, importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendant. Defendant Assa Abloy AB is vicariously liable for the infringing conduct of Assa Abloy Global Solutions, Inc., Assa Abloy Sales and Marketing Group, Assa Abloy Americas Residential Inc., and/or Door Security Solutions of the Southwest, and other U.S.-based subsidiaries, members, related entities, divisions, segments, companies and/or brands of Assa Abloy (under both the alter ego and agency theories). On information and belief, Defendant Assa Abloy AB, and related entities and subsidiaries, including U.S.-based subsidiaries members, divisions, segments, companies and/or brands of Assa Abloy are essentially the same company (i.e., "Assa Abloy"), operating in the U.S. via, for example, one or more of the brands, divisions, segments, mergers, and/or acquisitions of Assa Abloy listed in this complaint. Moreover, Assa Abloy AB, as the parent company, along with its related entities, has the right and ability to control and/or delegate the control of the infringing activities of those subsidiary entities such that Defendant receives a direct financial benefit from that infringement.

94. For example, Assa Abloy infringes claim 1 of the '961 patent via the Accused Products that utilize ZigBee protocols, including, but not limited to access control (for example, Assa Abloy's Zigbee-enabled VingCard Classic RFID Electronic Lock, Assa Abloy's Zigbee-

enabled DL100 lock, and Assa Abloy's Zigbee-enabled Securitron® R100 Aperio® Wireless Card Reader); connected modules, gateways, routers, and/or bridges (for example, Assa Abloy's Yale Zigbee Smart Module, Assa Abloy's Zigbee Module PCBA 1731, Assa Abloy's Zigbee Endnode Kit w/cable for Signature and Essence, Assa Abloy's Yale Assure Door Lock Range Zigbee Module, and devices including any Zigbee-enabled module); keypads (for example, Assa Abloy's Kwikset 916 SmartCode Traditional Electronic Deadbolt with Zigbee Technology); and related accessories and software.

95. 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.

96. At a minimum, Assa Abloy has known of the '961 patent at least as early as the filing date of this complaint. In addition, Assa Abloy 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 May 8, 2018, from North Forty Consulting LLC, working with Harris Corporation. The letter notifies Assa Abloy (via its Kwikset subsidiary and/or brand) of Harris Corporation's (now L3 Harris Technologies, Inc.) ownership of patents relating to wireless communication networks, network management/security, as well as innovations pertinent to the IEEE 802.11 and Zigbee standards. Further, Assa Abloy has been on notice about infringement of the Harris patent portfolio and the '961 patent, since at least its receipt (via Kwikset) of a presentation and licensing proposal dated on or around March 2019, from North Forty Consulting LLC, working with Harris Corporation.

97. Additional correspondence sent by Acacia Research Group LLC on behalf of Stingray (a wholly owned subsidiary of Acacia Research Group LLC), regarding Stingray's acquisition of and attempt to license the Harris patent portfolio (which Assa Abloy had notice of at least by May 8, 2018), was sent directly to Assa Abloy, for example, via correspondence to Mr. Nico Delvaux, President and CEO of Assa Abloy, and correspondence to Mr. Lucas Boselli, Head of Americas Division of Assa Abloy, with a copy to Ms. Page Heslin, General Counsel and Secretary of Assa Abloy Americas, both items of correspondence dated June 16, 2020. Acacia Research Group LLC, on behalf of Stingray, also sent further correspondence to Assa Abloy via Kwikset regarding Stingray's acquisition of and attempt to license the Harris patent portfolio. For example, correspondence dated August 21, 2020, was addressed to Mr. John Lundgren, Chief Executive Officer of Kwikset, pointing out the lack of response to earlier correspondence dated June 16, 2020, and again offering to discuss licensing the Harris patent portfolio. These examples of notice provided to Assa Abloy are not exhaustive, and Assa Abloy has also received additional notice of infringement in connection with the Asserted Patents.

98. On information and belief, since at least the above-mentioned date or dates when Defendant was on notice of its infringement, Defendant has actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, integrators, installers, OEMs, consumers, other users, and other related service providers that make, 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 making, using, offering for sale, selling, and/or importing the Accused Products. Since at least the date or dates of notice provided above, Defendant conducts infringing activities with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '961 patent. On information and belief, Defendant intends to cause, and has taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMS, integrators, installers, consumers, other users, 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. Moreover, Defendant manufactures, tests, and certifies the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendant distributes or makes available instructions or manuals for these products to consumers, installers, purchasers and/or prospective buyers, tests and certifies the wireless networking features (with for example the Connectivity Standards Alliance, i.e., for ZigBee certification, and/or for FCC compliance) in the Accused Products, and provides technical support, product files, videos, and/or related services for these products to purchasers in the United States. *See, e.g.*, Certified Products Search, Connectivity

Standards Alliance, https://csa-iot.org/csa-iot_products/?p_keywords&p_type%5B0%5D=17&p_type%5B1%5D=14&p_type%5B2%5D=1053&p_certificate&p_company%5B0%5D=736&p_family#post-feed-block-4b75856a1cb81c23f4249ff4dfa85044 (last visited Feb. 6, 2024) (showing Assa Abloy's Zigbee products certified by the Connectivity Standards Alliance showing 21 different products, systems, and/or certificates); *User Manual Online Option*, ASSA ABLOY, available at https://fccid.io/Y7V-683081150C1/User-Manual/Users-Manual-3402004 (last visited Feb. 6, 2024) (stating "[t]hese devices comply with Part 15 of the FCC Rules," "[t]his equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules," and "[t]he online option is based on the ZigBee standard, a standard for transmission of data via radio" that is "based on IEEE 802.15.4 (Open ISM 2.4GHz band; ISM = industrial, scientific and medical"); *Visionline – The complete system solution for hotels*, ASSA ABLOY GLOBAL SOLUTIONS OFFICIAL, https://www.youtube.com/watch?v=3BHZqPsaEMM (last visited Feb. 6, 2024) ("ASSA ABLOY Hospitality's Visionline is a software for wireless locking systems. It integrates stand-alone electronic hotel locks operating in online mode through Radio Frequency (RF-online) that is based on Zigbee high security open platform.").

99. Furthermore, Defendant induces infringement by installers, integrators, consumers and other users of Assa Abloy's products by designing, developing, marketing, and offering smartphone, tablet, and/or mobile device interfaces as application software (i.e., apps) such as the HID Mobile Access® App to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, including Wi-Fi and ZigBee networks. *See, e.g.*, *Mobile Access*, ASSA ABLOY, https://www.intelligentopenings.com/en/solutions/by-

challenge/access-control-technologies-and-trends/mobile-access-control (last visited Feb. 5, 2024).

100. Assa Abloy's apps also induce infringing use of the Accused Products by providing compatibility between Assa Abloy products and third-party products that share or access the same wireless networks. *See, e.g., HID Mobile Access – Compatible Devices*, HID, https://www.hidglobal.com/mobile-access-compatible-devices (last visited Feb. 5, 2024) (stating "[t]his list of mobile devices is regularly updated to show those deemed to be compatible with the latest version of the HID® Mobile Access® app" and listing devices from numerous brands). Such compatibility provides convenience and added functionality that induces consumers to use the Defendant's products, including via apps and other interfaces utilizing Wi-Fi and/or ZigBee protocols in networks with other third-party devices. Thus, these activities further infringe or induce infringement of the '961 patent.

101. On information and belief, despite having knowledge of the '961 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '961 patent, Defendant has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendant's 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.

102. Plaintiff Stingray has been damaged as a result of Assa Abloy's infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for their 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 IV

(INFRINGEMENT OF U.S. PATENT NO. 7,441,126)

103. Plaintiff incorporates paragraphs 1 through 102 herein by reference.

104. Plaintiff is the assignee of the '126 patent, entitled "Secure wireless LAN device including tamper resistant feature and associated method," with ownership of all substantial rights in the '126 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements

105. The '126 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '126 patent issued from U.S. Patent Application No. 09/761,173.

106. Assa Abloy has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '126 patent in this District and elsewhere in Texas and the United States.

107. On information and belief, Assa Abloy designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Assa Abloy and its subsidiaries, members, divisions, segments, companies, brands and/or related entities, including U.S.-based subsidiaries, members, divisions, segments, companies and/or brands of Assa Abloy.

108. Defendant directly infringes the '126 patent via 35 U.S.C. § 271(a) by manufacturing (including via contract manufacturers), 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 '126 patent to, for example, its alter egos, agents, intermediaries,

related entities, distributors, dealers, importers, customers, subsidiaries, members, divisions, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, (i) Defendant designs the Accused Products for U.S. consumers; (ii) Defendant makes, uses, and/or sells the Accused Products inside the United States; and/or (iii) Defendant makes and sells the Accused Products outside of the United States and delivers those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, integrators, installers, customers and other related service providers in the United States, or in the case that Defendant 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 '126 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)").

109. Furthermore, Defendant Assa Abloy AB directly infringes the '126 patent through its direct involvement in the activities of its subsidiaries, and related entities, including U.S.-based subsidiaries, members, divisions, segments, companies and/or brands of Assa Abloy, including by designing the Accused Products for U.S. consumers; making the Accused Products in the United States; using the Accused Products in the United States; selling and offering for sale the Accused Products directly to U.S. consumers and its related entities; and/or importing the Accused Products into the United States for sale and/or for its related entities. On information and belief, Assa Abloy's U.S.-based subsidiaries and/or brands, including at least Assa Abloy Global Solutions,

Inc., Assa Abloy Sales and Marketing Group, Assa Abloy Americas Residential Inc., and/or Door Security Solutions of the Southwest, conduct activities that constitute direct infringement of the '126 patent under 35 U.S.C. § 271(a) by making, importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendant. Defendant Assa Abloy AB is vicariously liable for the infringing conduct of Assa Abloy Global Solutions, Inc., Assa Abloy Sales and Marketing Group, Assa Abloy Americas Residential Inc., and/or Door Security Solutions of the Southwest, and other U.S.-based subsidiaries, members, related entities, divisions, segments, companies and/or brands of Assa Abloy (under both the alter ego and agency theories). On information and belief, Defendant Assa Abloy AB, and related entities and subsidiaries, including U.S.-based subsidiaries members, divisions, segments, companies and/or brands of Assa Abloy are essentially the same company (i.e., "Assa Abloy"), operating in the U.S. via, for example, one or more of the brands, divisions, segments, mergers, and/or acquisitions of Assa Abloy listed in this complaint. Moreover, Assa Abloy AB, as the parent company, along with its related entities, has the right and ability to control and/or delegate the control of the infringing activities of those subsidiary entities such that Defendant receives a direct financial benefit from that infringement.

110. For example, Assa Abloy infringes claim 1 of the '126 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to Defendant's infringing Accused Products that are enabled or compliant with Wi-Fi and that utilize a battery and a volatile memory for the storage of device data, including cryptographic data. Such Accused Products include, but are not limited to access control (for example, Assa Abloy's Corbin Russwin IN120 Intelligent WIFI Access Control, Assa Abloy's Wi-Fi-enabled Sargent IN120 PE8800 Series access control, Assa Abloy's Kwikset Halo Matte Black Touchscreen WiFi Keypad Electronic

Single-Cylinder Smart Lock Deadbolt, and Assa Abloy's August WiFi Smart Lock); connected modules, gateways, routers, and/or bridges (for example, Assa Abloy's Yale MD-05 BLE/WiFi transceiver module for door locks, Assa Abloy's Yale Wi-Fi Smart Module, and devices including any WiFi-enabled module); keypads (for example, Assa Abloy's Kwikset Halo Matte Black Touchscreen WiFi Keypad Electronic Single-Cylinder Smart Lock Deadbolt); and related accessories and software.

111. 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 media access controller (MAC) carried by said housing; and a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver, said cryptography circuit comprising at least one volatile memory for storing cryptography information, and a battery for maintaining the cryptography information in said at least one volatile memory.

112. At a minimum, Assa Abloy has known of the '126 patent at least as early as the filing date of this complaint. In addition, Assa Abloy has known about infringement of an L3Harris ("Harris") patent portfolio that was acquired by Stingray, which includes the '126 patent, since at least its receipt of a letter dated May 8, 2018, from North Forty Consulting LLC, working with Harris Corporation. The letter notifies Assa Abloy (via its Kwikset subsidiary and/or brand) of Harris Corporation's (now L3 Harris Technologies, Inc.) ownership of patents relating to wireless communication networks, network management/security, as well as innovations pertinent to the IEEE 802.11 and Zigbee standards. Further, Assa Abloy has been on notice about infringement of

the Harris patent portfolio and the '126 patent, since at least its receipt (via Kwikset) of a presentation and licensing proposal dated on or around March 2019, from North Forty Consulting LLC, working with Harris Corporation.

113. Additional correspondence sent by Acacia Research Group LLC on behalf of Stingray (a wholly owned subsidiary of Acacia Research Group LLC), regarding Stingray's acquisition of and attempt to license the Harris patent portfolio (which Assa Abloy had notice of at least by May 8, 2018), was sent directly to Assa Abloy, for example, via correspondence to Mr. Nico Delvaux, President and CEO of Assa Abloy, and correspondence to Mr. Lucas Boselli, Head of Americas Division of Assa Abloy, with a copy to Ms. Page Heslin, General Counsel and Secretary of Assa Abloy Americas, both items of correspondence dated June 16, 2020. Acacia Research Group LLC, on behalf of Stingray, also sent further correspondence to Assa Abloy via Kwikset regarding Stingray's acquisition of and attempt to license the Harris patent portfolio. For example, correspondence dated August 21, 2020, was addressed to Mr. John Lundgren, Chief Executive Officer of Kwikset, pointing out the lack of response to earlier correspondence dated June 16, 2020, and again offering to discuss licensing the Harris patent portfolio. These examples of notice provided to Assa Abloy are not exhaustive, and Assa Abloy has also received additional notice of infringement in connection with the Asserted Patents.

114. On information and belief, since at least the above-mentioned date or dates when Defendant was on notice of its infringement, Defendant has actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, integrators, installers, OEMs, consumers, other users, and other related service providers that make, 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 '126 patent to directly infringe

one or more claims of the '126 patent by making, using, offering for sale, selling, and/or importing the Accused Products. Since at least the date or dates of notice provided above, Defendant conducts infringing activities with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '126 patent. On information and belief, Defendant intends to cause, and has taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMS, integrators, installers, consumers, other users, 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. Moreover, Defendant manufactures, tests, and certifies the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendant distributes or makes available instructions or manuals for these products to consumers, installers, purchasers and/or prospective buyers, tests and certifies the wireless networking features (with for example the Wi-Fi Alliance and/or for FCC compliance) in the Accused Products, and provides technical support, product files, videos, and/or related services for these products to purchasers in the United States. *See, e.g.*, *Product Finder Filtered Results*, WIFI ALLIANCE, https://www.wi-fi.org/product-finder-results?keywords=Assa Abloy (last visited Feb. 5, 2024) (showing Assa Abloy's WiFi Certified™ products include, for example, the "August connect" with model number "AC-R2" and "Last Certified Date: 2022-10-24," the "Connect Bridge Plus" with model number "AYR-BDG-CB2" and "Last Certified Date: 2022-07-14," and the "Yale Link Bridge," with model number "GHN-N520W-Y1" and "Last Certified Date: 2019-10-07"); *Test Report Certification pursuant to FCC Part 15, Subpart C for Assa Abloy's Yale MD-05 BLE/WiFi transceiver module for door locks*,

VPI LABORATORIES (Aug. 3, 2021), available at https://fccid.io/U4A-WF1MRUS/Test-Report/TR-Sub-C-2-4GHz-WiFi-5426392 (last visited Feb. 5, 2024); *Yale® Access Smart Module MD-05 OEM Installation Guide*, YALE, available at https://fccid.io/U4A-WF1MRUS/Users-Manual/User-Manual-Installation-Manual-5426397 (last visited Feb. 5, 2024); *ASSA ABLOY IN120 WiFi Access Control Lock*, SARGENT ASSA ABLOY, https://www.youtube.com/watch?v=Lc_vsMBcC_U (last visited Feb. 6, 2024) (including a description that states "The IN120 WiFi lock, available from ASSA ABLOY Group brands Corbin Russwin and SARGENT, offers the ease and flexibility of WiFi in a new streamlined design, setting a new standard for aesthetics and performance," and "The IN120 uses 802.11b/g/n WiFi infrastructure . . . .").

115. Furthermore, Defendant induces infringement by installers, integrators, consumers and other users of Assa Abloy's products by designing, developing, marketing, and offering smartphone, tablet, and/or mobile device interfaces as application software (i.e., apps) such as the HID Mobile Access® App to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, including Wi-Fi and ZigBee networks. *See, e.g.*, *Mobile Access*, ASSA ABLOY, https://www.intelligentopenings.com/en/solutions/by-challenge/access-control-technologies-and-trends/mobile-access-control (last visited Feb. 5, 2024).

116. Assa Abloy's apps also induce infringing use of the Accused Products by providing compatibility between Assa Abloy products and third-party products that share or access the same wireless networks. *See, e.g., HID Mobile Access – Compatible Devices*, HID, https://www.hidglobal.com/mobile-access-compatible-devices (last visited Feb. 5, 2024) (stating "[t]his list of mobile devices is regularly updated to show those deemed to be compatible with the

latest version of the HID® Mobile Access® app" and listing devices from numerous brands). Such compatibility provides convenience and added functionality that induces consumers to use the Defendant's products, including via apps and other interfaces utilizing Wi-Fi and/or ZigBee protocols in networks with other third-party devices. Thus, these activities further infringe or induce infringement of the '126 patent.

117. On information and belief, despite having knowledge of the '126 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '126 patent, Defendant has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendant's infringing activities relative to the '126 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.

118. Plaintiff Stingray has been damaged as a result of Assa Abloy's infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for their 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

119. Plaintiff is entitled to recover from Defendant the damages sustained by Plaintiff as a result of Defendant's 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.

120. 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

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

PRAYER FOR RELIEF

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

1. A judgment that Defendant has 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 Defendant;
3. A judgment and order requiring Defendant 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 Defendant 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 Defendant 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: March 7, 2024

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
Mark M. R. Douglass
Texas Bar No. 24131184
E-mail: mdouglass@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