

3. On information and belief, Defendant Schlage Lock Company LLC is a Delaware limited liability company, having registered agent Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, TX 78701, USA.

4. Allegion Public Limited Company is an Irish public limited liability company with its registered office in Dublin, Ireland, and whose ordinary shares are listed on the New York Stock Exchange under trading symbol ALLE. *See Annual Report 2023*, ALLEGION, p. 1, available for download at <https://investor.allegion.com/~media/Files/A/Allegion-IR/reports-and-presentations/2023-allegion-annual-report-10-k.pdf> (last visited May 14, 2024) [hereinafter “Annual Report”]. Allegion is a global provider of security products and solutions, offering “an extensive and versatile portfolio of security and access control products and solutions across a range of market-leading brands.” *Id.* at 4. Allegion’s principal products and services include, for example, “[d]oor controls and systems;” “[l]ocks, locksets, portable locks and key systems;” “[e]xit devices;” “[e]lectronic security products;” and “[s]oftware-enabled access control systems.” *Id.* Allegion “operate[s] and report[s] financial results for” its “Allegion Americas” segment, which sells products under Allegion Brands including: Dexter, Falcon, Kryptonite, Locknetics, Schlage, Isonas, LCN, Von Duprin, ADsystems, Stanley Access Technologies, Brio, Glynn-Johnson, Ives, Republic, Steelcraft, TGP, Zero International, yonomi, and zentra (collectively, the “Allegion Brands”). *See id.* at 4-6.

5. Allegion has offered and/or offers products in Plano, TX, Collin County, Texas, and this District that are compatible with Wi-Fi and/or Zigbee protocols. For example, via is Schlage brand, Allegion has offered the “Schlage Encode Plus™ Smart Wifi Deadbolt,” and “Schlage Connect™ Zigbee lock.” *Schlage Lock Company*, SCHLAGE, <https://www.amazon.com/stores/page/B25C357F-F6AB-40EC-87A1->

F5AEFB3B223C?ingress=2&visitId=4785205b-56b1-4b0c-bf98-2e139f345af7&store_ref=bl_ast_dp_brandLogo_sto&ref_=ast_bln (“Schlage Encode Plus™ Smart Wifi Deadbolt”); *Schlage Connect™ Zigbee*, SCHLAGE, <https://www.schlage.com/en/home/support/faqs/schlage-connect-zigbee.html> (last visited May 14, 2024); *Find a Retailer*, SCHLAGE, <https://www.schlage.com/en/home/where-to-buy.html> (last visited May 14, 2024) (providing links to “Find online” and “Find locally, listing retailers including “build with FERGUSON,” “THE HOME DEPOT,” “MENARDS,” “LOWE’S,” “amazon,” “Do it Best,” “True Value,” “wayfair,” and “ACE.”).

6. Allegion “manag[es] [a] network of production and assembly facilities” and “distribute[s] [its] products through a broad network of channel partners.” Annual Report at 11. Allegion “manufacture[s] products in several geographic markets around the world,” “operat[ing] 31 principal production and assembly facilities – 18 in [its] Allegion Americas segment.” *Id.* Allegion’s “strategy is to produce in the region of use, wherever appropriate, . . . to be closer to the end user and increase efficiency and timely product delivery.” *Id.* “Much of [Allegion’s] U.S. based residential portfolio is manufactured in the Baja region of Mexico under the Maquiladora, Manufacturing and Export Services Industry (“IMMEX”) program.” *Id.* Allegion also has U.S. production and assembly facilities in “Blue Ash, Ohio,” “Everett, Washington,” “Farmington, Connecticut,” “Greenfield, Indiana,” “Indianapolis, Indiana,” “Irving, Texas,” “Perrysburg, Ohio,” “Princeton, Illinois,” “Security, Colorado,” and “Snoqualmie, Washington.” *Id.* at 12.

7. Accordingly, at least some of Allegion’s manufacturing facilities are in the United States and other Allegion manufacturing facilities are located outside the United States. *See id.* Allegion 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.

8. According to Allegion's Annual Report, "[a]s of December 31, 2023, approximately 48% of [Allegion's 12,400 employees worldwide] are employed within the U.S." *Id.* Additionally, the "Allegion Americas" market accounted for the vast majority of Allegion's net revenues in 2023, namely, \$2.9136 billion out of total sales of \$3.650.8 billion. *Id.* at 34. In particular, the U.S. alone accounted for \$2.7547 billion of these total sales. *Id.* at F-32.

9. On information and belief, Allegion 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 Allegion 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 Allegion's alter egos, related entities and/or wholly controlled U.S.-based subsidiaries, including, without limitation, Defendant Schlage Lock Company LLC, a Delaware limited liability company having an office at 5200 Tennyson Pkwy, Suite 300, Plano, TX 75024, and Allegion Access Technologies LLC, a Delaware limited liability company, listing an address at 350 N Saint Paul St, Dallas, TX 75201. On behalf and for the benefit of Defendants, Allegion Public Limited Company engages in, controls, orders, provides for, induces, jointly participates in, and/or coordinates the importation, distribution, marketing, offers for sale, sale, and use of Allegion's products in the U.S. For example, Allegion Public Limited Company maintains distribution and support channels in the U.S. for Allegion products via manufacturing facilities, online stores, distribution partners, retailers, reseller partners, dealers, and other related service providers. *See, e.g., Allegion Locations*, ALLEGION, <https://www.allegion.com/corp/en/header/locations.html> (last visited May 14, 2024) (listing "Sales" location at "5200 Tennyson, Suite #300[,] Plano, TX 75024," in

Collin County and in this District); *Property Search*, Collin CAD, <https://www.collincad.org/propertysearch?prop=2598055&year=2024> (last visited May 14, 2024) (listing a “Owner Name(s)” of “Schlage Lock Company LLC” at “5200 Tennyson Pkwy #00300[,] Plano, TX 75024”); *“Schlage Wifi” Search Results*, THE HOME DEPOT, <https://www.homedepot.com/s/schlage%20wifi?NCNI-5> (last visited May 14, 2024) (indicating the “N Plano” Home Depot located at 4600 State Hwy 121, Plano, TX 75024, in Collin County and this District, sells Schlage Camelot, Encode and Encode Plus WiFi smart locks.).

10. As a result, via at least Allegion’s established distribution channels operated and maintained by at least Defendants Allegion Public Limited Company and Schlage Lock Company LLC and Allegion’s U.S.-based subsidiaries, Allegion’s products are distributed, sold, advertised, and used nationwide, including being sold to consumers via Allegion 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

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

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

A. Defendant Allegion Public Limited Company

13. On information and belief, Defendant Allegion Public Limited Company 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, Defendant Allegion Public Limited Company is related to, has been related to, owns, has owned, controls and/or has controlled subsidiaries, businesses, segments, divisions and/or brands (including but not limited Schlage Lock Company LLC, Allegion Access Technologies LLC, and the Allegion Brands) that have a significant business presence in the U.S. and in Texas. Such a presence furthers the development, design, manufacture, importation, distribution, sale, and use (including by inducement) of infringing Allegion products in Texas, including in this District.

14. This Court has personal jurisdiction over Defendant Allegion Public Limited Company, directly and/or through the activities of Allegion Public Limited Company'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, Allegion Public Limited Company 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 Allegion Public Limited Company would not offend traditional notions of fair play and substantial justice.

15. On information and belief, Allegion Public Limited Company 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 Allegion, for example, Schlage Lock Company LLC, Allegion Access Technologies LLC, and the Allegion Brands. *See, e.g., Allegion Locations*, ALLEGION, <https://www.allegion.com/corp/en/header/locations.html> (last visited May 14, 2024) (listing “Sales” location at “5200 Tennyson, Suite #300[,] Plano, TX 75024,” in Collin County and in this District); *Property Search*, Collin CAD, <https://www.collincad.org/propertysearch?prop=2598055&year=2024> (last visited May 14, 2024) (listing a “Owner Name(s)” of “Schlage Lock Company LLC” at “5200 Tennyson Pkwy #00300[,] Plano, TX 75024”); Annual Report, pp. 11-12, 34, F-32 (disclosing Allegion “manag[es] [a] network of production and assembly facilities” and “distribute[s] [its] products through a broad network of channel partners,” in locations around the globe but concentrated in the United States); *Find a Retailer*, SCHLAGE, <https://www.schlage.com/en/home/where-to-buy.html> (last visited May 14, 2024) (providing links to “Find online” and “Find locally, listing retailers including “build with FERGUSON,” “THE HOME DEPOT,” “MENARDS,” “LOWE’S,” “amazon,” “Do it Best,” “True Value,” “wayfair,” and “ACE.”); *Schlage Wifi” Search Results*, THE HOME DEPOT, <https://www.homedepot.com/s/schlage%20wifi?NCNI-5> (last visited May 14, 2024) (indicating the “N Plano” Home Depot located at 4600 State Hwy 121, Plano, TX 75024, in Collin County and this District, sells Schlage Camelot, Encode and Encode Plus WiFi smart locks.); *Schlage Lock Company*, SCHLAGE, https://www.amazon.com/stores/page/B25C357F-F6AB-40EC-87A1-F5AEFB3B223C?ingress=2&visitId=4785205b-56b1-4b0c-bf98-2e139f345af7&store_ref=bl_ast_dp_brandLogo_sto&ref_=ast_bln (“Schlage Encode Plus™ Smart Wifi Deadbolt”); *Schlage Connect™ Zigbee*, SCHLAGE,

<https://www.schlage.com/en/home/support/faqs/schlage-connect-zigbee.html> (last visited May 14, 2024). 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, Allegion Public Limited Company has placed and continues to place infringing Allegion products into the U.S. stream of commerce. Examples include the manufacture, sale, offering for sale, use and/or importation of Allegion products in and into the United States. *See id.*; *Search for jobs or keywords*, ALLEGION, <https://allegion.wd5.myworkdayjobs.com/careers/jobs> (last visited May 14, 2024) (showing Allegion job posting for “Early Careers Sale Development Program – Plano, TX” and “Sales Consultant – Distributor – Dallas/Ft. Worth, Texas” both listing a location in “Plano, TX”). Allegion Public Limited Company has placed such products into the stream of commerce with the knowledge and understanding that such products are, will be, and continue to be sold, offered for sale, and/or imported into this District and the State of Texas. *See Litecubes, LLC v. Northern Light Products, Inc.*, 523 F.3d 1353, 1369-70 (Fed. Cir. 2008) (“[T]he sale [for purposes of § 271] occurred at the location of the buyer.”); *see also Semcon IP Inc. v. Kyocera Corporation*, No. 2:18-cv-00197-JRG, 2019 WL 1979930, at *3 (E.D. Tex. May 3, 2019) (denying accused infringer’s motion to dismiss because plaintiff sufficiently plead that purchases of infringing products outside of the United States for importation into and sales to end users in the U.S. may constitute an offer to sell under § 271(a)).

16. On information and belief, Allegion Public Limited Company 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, e.g.*, Annual Report, pp. 11-12, 34, F-32 (disclosing Allegion

“manag[es] [a] network of production and assembly facilities” and “distribute[s] [its] products through a broad network of channel partners,” in locations around the globe but concentrated in the United States); *Find a Retailer*, SCHLAGE, <https://www.schlage.com/en/home/where-to-buy.html> (last visited May 14, 2024) (providing links to “Find online” and “Find locally, listing retailers including “build with FERGUSON,” “THE HOME DEPOT,” “MENARDS,” “LOWE’S,” “amazon,” “Do it Best,” “True Value,” “wayfair,” and “ACE.”). Allegion 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., “Schlage Wifi” Search Results*, THE HOME DEPOT, <https://www.homedepot.com/s/schlage%20wifi?NCNI-5> (last visited May 14, 2024) (indicating the “N Plano” Home Depot located at 4600 State Hwy 121, Plano, TX 75024, in Collin County and this District, sells Schlage Camelot, Encode and Encode Plus WiFi smart locks.). Additionally, Allegion products, including infringing products and/or services, are sold nationwide, in Texas and this District via, for example, direct sales, online retailers, and Allegion’s subsidiaries and/or brands, for example, Defendant Schlage Lock Company LLC and Allegion Access Technologies LLC. *See, e.g., Allegion Locations*, ALLEGION, <https://www.allegion.com/corp/en/header/locations.html> (last visited May 14, 2024) (listing “Sales” location at “5200 Tennyson, Suite #300[,] Plano, TX 75024,” in Collin County and in this District); *Property Search*, Collin CAD, <https://www.collincad.org/propertysearch?prop=2598055&year=2024> (last visited May 14, 2024) (listing a “Owner Name(s)” of “Schlage Lock Company LLC” at “5200 Tennyson Pkwy #00300[,] Plano, TX 75024”); *Search for jobs or keywords*, ALLEGION, <https://allegion.wd5.myworkdayjobs.com/careers/jobs> (last visited May 14, 2024) (showing

Allegion job posting for “Early Careers Sale Development Program – Plano, TX” and “Sales Consultant – Distributor – Dallas/Ft. Worth, Texas” both listing a location in “Plano, TX”); Annual Report at Ex. 21.1.

17. Allegion Public Limited Company, 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 Allegion products and other network devices. These apps are available via digital distribution platforms operated, for example, by Allegion, Apple Inc., and/or Google for download by users and execution on smartphone devices. *See, e.g., ENGAGE™ for Access Control*, SCHLAGE, <https://commercial.schlage.com/en/products/software/engage-for-access-control.html> (last visited May 15, 2024) (urging consumers to “[c]onnect compatible devices over Wi-Fi for periodic updates” and indicating the ENGAGE™ App is available at the Apple App Store and Google Play).

18. Based on Allegion Public Limited Company’s connections and relationship with its U.S. subsidiaries, manufacturers, dealers, retailers, and digital distribution platforms, Allegion Public Limited Company knows that Texas is a termination point of the established distribution channel, namely online and brick-and-mortar stores offering Allegion 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. Allegion Public Limited Company, 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”).

19. On information and belief, Defendant Allegion Public Limited Company alone and in concert with other related entities such as subsidiaries, members, divisions, segments, companies and/or brands of Allegion, manufactures and purposefully places infringing Allegion 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 Allegion’s website. As an example, Allegion Public Limited Company, directly and/or through a related entity or subsidiary, manufactures infringing Allegion products in Texas, imports infringing Allegion products to Texas and/or sells or offers for sale infringing Allegion products in Texas to resellers or dealers. At least components of Allegion and/or Schlage products are or have been offered for sale, sold, and/or imported in Plano, Texas, during times relevant to the allegations in this complaint. *See, e.g., Allegion Locations*, ALLEGION, <https://www.allegion.com/corp/en/header/locations.html> (last visited May 14, 2024) (listing “Sales” location at “5200 Tennyson, Suite #300[,] Plano, TX 75024,” in Collin County and in this District); *Property Search*, Collin CAD, <https://www.collincad.org/propertysearch?prop=2598055&year=2024> (last visited May 14, 2024) (listing a “Owner Name(s)” of “Schlage Lock Company LLC” at “5200 Tennyson Pkwy #00300[,] Plano, TX 75024”); *Find a Retailer*, SCHLAGE, <https://www.schlage.com/en/home/where-to-buy.html> (last visited May 14, 2024) (providing links to “Find online” and “Find locally, listing retailers including “build with FERGUSON,” “THE HOME DEPOT,” “MENARDS,” “LOWE’S,” “amazon,” “Do it Best,” “True Value,” “wayfair,” and “ACE.”); Annual Report, p. 11 (“Much of [Allegion’s] U.S. based residential portfolio is manufactured in the Baja region of

Mexico under the Maquiladora, Manufacturing and Export Services Industry ("IMMEX") program.”). Allegion’s Schlage wi-fi enabled smart locks are offered for sale and pickup at least at a Home Depot store located in this District at 4600 State Hwy 121, Plano, TX 75024. “*Schlage Wifi*” Search Results, THE HOME DEPOT, <https://www.homedepot.com/s/schlage%20wifi?NCNI-5> (last visited May 14, 2024) (indicating the “N Plano” Home Depot located at 4600 State Hwy 121, Plano, TX 75024, in Collin County and this District, sells Schlage Camelot, Encode and Encode Plus WiFi smart locks.). These suppliers, distributors, dealers, and/or resellers import, advertise, offer for sale and/or sell Allegion products and/or related services, such as delivery, consultation, and/or installation, via their own websites to U.S. consumers, including to consumers in Texas and this District. Based on Defendant Allegion Public Limited Company’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, Allegion Public Limited Company knows and has known that Texas is a termination point of the established distribution channels for Allegion products. Allegion Public Limited Company, 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 Allegion 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).

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

21. Venue is proper in this District with respect to Defendant Allegion Public Limited Company, for example, pursuant to 28 U.S.C. § 1391. Defendant Allegion Public Limited Company 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.).

22. Additionally, venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and/or 1400(b). As alleged herein, Defendant Allegion Public Limited Company has committed acts of infringement in this District. As further alleged herein, Defendant Allegion Public Limited Company, via its own operations, employees, and/or through the activities of Allegion Public Limited Company's alter egos, agents, related entities, and/or subsidiaries, has a regular and established place of business in this District, for example, at 5200 Tennyson, Suite #300, Plano, Texas 75024, in Collin County, Texas among any other Allegion locations owned, leased and/or operated in this District. Accordingly, Allegion Public Limited Company may be sued in this district under 28 U.S.C. § 1400(b).

23. On information and belief, Defendant Allegion Public Limited Company 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.

B. Defendant Schlage Lock Company LLC

24. On information and belief, Defendant Schlage Lock Company LLC 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, Defendant Schlage Lock Company LLC has been related to, has been owned by, has owned, has been controlled by, and/or has controlled its parent, subsidiaries, businesses, segments, divisions and/or brands (including but not limited at least some of Defendant Allegion Public Limited Company, Allegion Access Technologies LLC, and the Allegion Brands) that have a significant business presence in the U.S. and in Texas. Such a presence furthers the development, design, manufacture, importation, distribution, sale, and use (including by inducement) of infringing Allegion products in Texas, including in this District.

25. This Court has personal jurisdiction over Defendant Schlage Lock Company LLC, directly and/or through the activities of Schlage Lock Company LLC's parent, 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 and its own activities, Schlage Lock Company LLC 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 Schlage Lock Company LLC would not offend traditional notions of fair play and substantial justice.

26. On information and belief, Schlage Lock Company LLC 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 Allegion, for example, the Schlage Brand. *See, e.g., Allegion Locations*, ALLEGION, <https://www.allegion.com/corp/en/header/locations.html> (last visited May 14, 2024) (listing “Sales” location at “5200 Tennyson, Suite #300[,] Plano, TX 75024,” in Collin County and in this District); *Property Search*, Collin CAD, <https://www.collincad.org/propertysearch?prop=2598055&year=2024> (last visited May 14, 2024) (listing a “Owner Name(s)” of “Schlage Lock Company LLC” at “5200 Tennyson Pkwy #00300[,] Plano, TX 75024”); Annual Report, pp. 11-12, 34, F-32 (disclosing Allegion “manag[es] [a] network of production and assembly facilities” and “distribute[s] [its] products through a broad network of channel partners,” in locations around the globe but concentrated in the United States); *Find a Retailer*, SCHLAGE, <https://www.schlage.com/en/home/where-to-buy.html> (last visited May 14, 2024) (providing links to “Find online” and “Find locally, listing retailers including “build with FERGUSON,” “THE HOME DEPOT,” “MENARDS,” “LOWE’S,” “amazon,” “Do it Best,” “True Value,” “wayfair,” and “ACE.”); *Schlage Wifi” Search Results*, THE HOME DEPOT,

<https://www.homedepot.com/s/schlage%20wifi?NCNI-5> (last visited May 14, 2024) (indicating the “N Plano” Home Depot located at 4600 State Hwy 121, Plano, TX 75024, in Collin County and this District, sells Schlage Camelot, Encode and Encode Plus WiFi smart locks.); *Schlage Lock Company*, SCHLAGE, https://www.amazon.com/stores/page/B25C357F-F6AB-40EC-87A1-F5AEFB3B223C?ingress=2&visitId=4785205b-56b1-4b0c-bf98-2e139f345af7&store_ref=bl_ast_dp_brandLogo_sto&ref_=ast_bln (“Schlage Encode Plus™ Smart Wifi Deadbolt”); *Schlage Connect™ Zigbee*, SCHLAGE, <https://www.schlage.com/en/home/support/faqs/schlage-connect-zigbee.html> (last visited May 14, 2024). 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, Schlage Lock Company LLC has placed and continues to place infringing Allegion products into the U.S. stream of commerce. Examples include the manufacture, sale, offering for sale, use and/or importation of Allegion products, including but not limited to Schlage products, in and into the United States. *See id.*; *Search for jobs or keywords*, ALLEGION, <https://allegion.wd5.myworkdayjobs.com/careers/jobs> (last visited May 14, 2024) (showing Allegion job posting for “Early Careers Sale Development Program – Plano, TX” and “Sales Consultant – Distributor – Dallas/Ft. Worth, Texas” both listing a location in “Plano, TX”). Schlage Lock Company LLC 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).

27. On information and belief, Schlage Lock Company LLC 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, e.g.*, Annual Report, pp. 11-12, 34, F-32 (disclosing Allegion “manag[es] [a] network of production and assembly facilities” and “distribute[s] [its] products through a broad network of channel partners,” in locations around the globe but concentrated in the United States); *Find a Retailer*, SCHLAGE, <https://www.schlage.com/en/home/where-to-buy.html> (last visited May 14, 2024) (providing links to “Find online” and “Find locally, listing retailers including “build with FERGUSON,” “THE HOME DEPOT,” “MENARDS,” “LOWE’S,” “amazon,” “Do it Best,” “True Value,” “wayfair,” and “ACE.”). Allegion products and/or services (including, but not limited to Schlage 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.*, “Schlage Wifi” Search Results, THE HOME DEPOT, <https://www.homedepot.com/s/schlage%20wifi?NCNI-5> (last visited May 14, 2024) (indicating the “N Plano” Home Depot located at 4600 State Hwy 121, Plano, TX 75024, in Collin County and this District, sells Schlage Camelot, Encode and Encode Plus WiFi smart locks.). Additionally, Allegion products, including infringing products and/or services, are sold nationwide, in Texas and this District via, for example, direct sales, online retailers, and Allegion’s parent, subsidiaries

and/or brands, for example, Defendants Allegion Public Limited Company, Schlage Lock Company LLC, and/or Allegion Access Technologies LLC. *See, e.g., Allegion Locations*, ALLEGION, <https://www.allegion.com/corp/en/header/locations.html> (last visited May 14, 2024) (listing “Sales” location at “5200 Tennyson, Suite #300[,] Plano, TX 75024,” in Collin County and in this District); *Property Search*, Collin CAD, <https://www.collincad.org/propertysearch?prop=2598055&year=2024> (last visited May 14, 2024) (listing a “Owner Name(s)” of “Schlage Lock Company LLC” at “5200 Tennyson Pkwy #00300[,] Plano, TX 75024”); *Search for jobs or keywords*, ALLEGION, <https://allegion.wd5.myworkdayjobs.com/careers/jobs> (last visited May 14, 2024) (showing Allegion job posting for “Early Careers Sale Development Program – Plano, TX” and “Sales Consultant – Distributor – Dallas/Ft. Worth, Texas” both listing a location in “Plano, TX”); Annual Report at Ex. 21.1.

28. Schlage Lock Company LLC, 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 Allegion products and other network devices. These apps are available via digital distribution platforms operated, for example, by Allegion, Schlage, Apple Inc., and/or Google for download by users and execution on smartphone devices. *See, e.g., ENGAGE™ for Access Control*, SCHLAGE, <https://commercial.schlage.com/en/products/software/engage-for-access-control.html> (last visited May 15, 2024) (urging consumers to “[c]onnect compatible devices over Wi-Fi for periodic updates” and indicating the ENGAGE™ App is available at the Apple App Store and Google Play).

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

30. On information and belief, Defendant Schlage Lock Company LLC alone and in concert with other related entities such as its parent, subsidiaries, members, divisions, segments, companies and/or brands of Allegion, manufactures and purposefully places infringing Allegion 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 Allegion's website. As an example, Schlage Lock Company LLC, directly and/or through a related entity or subsidiary, manufactures infringing Allegion products in Texas, imports infringing Allegion products to Texas and/or sells or offers for sale infringing Allegion products in Texas to resellers or dealers. At least components of Allegion and/or Schlage products are or have been offered for sale, sold, and/or imported in Plano, Texas, during times relevant to the allegations in this complaint. *See, e.g., Allegion Locations*,

ALLEGION, <https://www.allegion.com/corp/en/header/locations.html> (last visited May 14, 2024) (listing “Sales” location at “5200 Tennyson, Suite #300[,] Plano, TX 75024,” in Collin County and in this District); *Property Search*, Collin CAD, <https://www.collincad.org/propertysearch?prop=2598055&year=2024> (last visited May 14, 2024) (listing a “Owner Name(s)” of “Schlage Lock Company LLC” at “5200 Tennyson Pkwy #00300[,] Plano, TX 75024”); *Find a Retailer*, SCHLAGE, <https://www.schlage.com/en/home/where-to-buy.html> (last visited May 14, 2024) (providing links to “Find online” and “Find locally, listing retailers including “build with FERGUSON,” “THE HOME DEPOT,” “MENARDS,” “LOWE’S,” “amazon,” “Do it Best,” “True Value,” “wayfair,” and “ACE.”); Annual Report, p. 11 (“Much of [Allegion’s] U.S. based residential portfolio is manufactured in the Baja region of Mexico under the Maquiladora, Manufacturing and Export Services Industry (“IMMEX”) program.”). Allegion’s Schlage wi-fi enabled smart locks are offered for sale and pickup at least at a Home Depot store located in this District at 4600 State Hwy 121, Plano, TX 75024. “*Schlage Wifi*” *Search Results*, THE HOME DEPOT, <https://www.homedepot.com/s/schlage%20wifi?NCNI-5> (last visited May 14, 2024) (indicating the “N Plano” Home Depot located at 4600 State Hwy 121, Plano, TX 75024, in Collin County and this District, sells Schlage Camelot, Encode and Encode Plus WiFi smart locks.). These suppliers, distributors, dealers, and/or resellers import, advertise, offer for sale and/or sell Allegion products and/or related services, such as delivery, consultation, and/or installation, via their own websites to U.S. consumers, including to consumers in Texas and this District. Based on Defendant Schlage Lock Company LLC’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, Schlage Lock Company LLC knows and has known that Texas is a termination point of the

established distribution channels for Allegion products. Schlage Lock Company LLC, 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 Allegion 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).

31. Additionally, venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and/or 1400(b). As alleged herein, Defendant Schlage Lock Company LLC has committed acts of infringement in this District. As further alleged herein, Defendant Schlage Lock Company LLC, via its own operations, employees, and/or through the activities of Schlage Lock Company LLC’s parent, alter egos, agents, related entities, and/or subsidiaries, has a regular and established place of business in this District, for example, at 5200 Tennyson, Suite #300, Plano, Texas 75024, in Collin County, Texas among any other Allegion locations owned, leased and/or operated in this District. Accordingly, Schlage Lock Company LLC may be sued in this district under 28 U.S.C. § 1400(b).

32. On information and belief, Defendant Schlage Lock Company LLC 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

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

34. 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.

35. 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.

36. 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.

37. 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.

38. On information and belief, a significant portion of the operating revenue of Defendants is derived from the manufacture, distribution, sale, and use of home and business networking, IoT, and smart security and access control solutions, 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, Allegion reported that they had over \$2.7547 billion in sales in the U.S. market during the 2023 reporting period. *See* Annual Report pp. 34, F-32.

39. The Asserted Patents cover Defendants' networking, IoT, smart, security and access control solutions, products, 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., Smart Deadbolt*, SCHLAGE, <https://www.schlage.com/en/home/products/products-smart-locks.html> (last visited May 14, 2024) (listing "Schlage Encode Plus™ Smart WiFi Deadbolt," "Schlage Encode™ Smart Wifi

Deadbolt,” and “Schlage Encode™ Smart WiFi Lever”); *With a pioneering spirit and partner-of-choice mindset, Allegion shapes the future of connected security and access*, ALLEGION, <https://www.allegion.com/corp/en/news/blog/2023/CSA-new-status.html> (last visited May 14, 2024) (“Allegion has been named a Promoter Member of the Connectivity Standards Alliance (the Alliance) and, with this elevated status, now has a seat on the Alliance Board of Directors.”); *Certified Products Search*, CONNECTIVITY STANDARDS ALLIANCE, https://csa-iot.org/csa-iot_products/?p_keywords=&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_company%5B%5D=781&p_family= (last visited May 14, 2024) (listing three different “Schlage Connect Smart Deadbolt” products as Zigbee certified); *Schlage Connect™ Zigbee*, SCHLAGE, <https://www.schlage.com/en/home/support/faqs/schlage-connect-zigbee.html> (last visited May 14, 2024). Defendants’ 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, Allegion’s Schlage Encode Plus™ Smart WiFi Deadbolt, Schlage Encode™ Smart Wifi Deadbolt, Schlage Encode™ Smart WiFi Lever, Schlage NDE wireless lock with Wi-Fi compatibility, and Schlage Connect™ Smart Deadbolt with Zigbee compatibility) and related accessories (for example, Schlage Sense™ Wi-Fi Adapter) and software (for example, Schlage Engage™ for Access Control) (all collectively referred to as the “Accused Products”). These Accused Products infringe the Asserted Patents by at least their manufacture, importation, distribution, sale, and use in the U.S.

40. The Asserted Patents cover Accused Products of Allegion that use the ZigBee protocol to communicate with other devices on a communication network, including those of third-party manufacturers. Examples of Allegion’s ZigBee products include Schlage Connect™ Zigbee

smart lock, which uses the Zigbee protocol for “enrollment with a compatible Zigbee-enabled smart home hub” as shown below:



With the Zigbee certified Schlage Connect, enrollment with a compatible Zigbee-enabled smart home hub is fast and easy with the Schlage Connect's 1-button enrollment. If you need help with installation or just want to learn more about Schlage's smart locks, we've collected the top FAQs and resources here.

See *Schlage Connect™ Zigbee*, SCHLAGE,

<https://www.schlage.com/en/home/support/faqs/schlage-connect-zigbee.html> (last visited May

14, 2024); see also *Certified Products Search*, CONNECTIVITY STANDARDS ALLIANCE, [https://csa-](https://csa-iot.org/csa-)

[iot_products/?p_keywords=&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_company%5B%5D=781&p_family=](https://csa-iot.org/csa-iot_products/?p_keywords=&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_company%5B%5D=781&p_family=) (last visited May 14, 2024) (listing three different “Schlage Connect Smart Deadbolt” products as Zigbee certified).

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

Below is an excerpt from the technical specification for ZigBee protocols describing the basic architecture and standards that enable wireless network communication.

1.1 Protocol Description

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

1.1.3 Stack Architecture

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

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

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

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

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

IEEE STANDARDS ASSOCIATION

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

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

4. General description

4.1 General

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

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

4.2 Components of the IEEE 802.15.4 WPAN

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

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

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

described below, if the measurement value is higher than the value on other channels (threshold), it indicates interference is present on the channel, consequently resulting in transmission failures.



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

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

Each router or coordinator is responsible for tracking transmit failures using the TransmitFailure field in the neighbor table and also keeping a NIB counter for total transmissions attempted. A device that detects a significant number of transmission failures may take action to determine if interference is a cause. The following steps are an example of that procedure¹:

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 acknowledgement is received the total transmit and transmit failure counters are reset to zero.

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

44. As described below, the network manager node facilitates switching to a different channel, i.e., scouting available separate channels, if the performance on the channel-in-use falls below a threshold (i.e., when the current channel's energy is higher than channels, indicating

increased interference, and thereby resulting in multiple transmission failures). The network nodes switch to a new (second) channel whose energy level is lowest or below an acceptable threshold.



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 procedure¹:

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 than 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 acknowledgement 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>

45. With reference to the above graphic and as further described below, the ZigBee network of the Accused Products further allows using the command to request interference reports, i.e., broadcasts a channel activity query, from the network nodes, which involves scanning the energy level on all the channels including the newly switched (second) channel. The interference report will represent determining the performance for the second channel. In addition, the most

recent energy level value and failure rate (indicative of the channel performance/activity) corresponding to the channels is stored, i.e., the channel activity is updated.

The network manager may do the following:

1. Wait and evaluate if other reports from other devices are received. This may be appropriate if there are no other failures reported. In this case the network manager should add the reporting device to a list of devices that have reported interference. The number of devices on such a list would depend on the size of the network. The network manager can age devices out of this list.
2. Request other interference reports using the `Mgmt_NWK_Update_req` command. This may be done if other failures have been reported or the network manager device itself has failures and a channel change may be desired. The network manager may request data from the list of devices that have reported interference plus other randomly selected routers in the network. The network manager should not request an update from the device that has just reported interference since this data is fresh already.
3. Upon receipt of the `Mgmt_NWK_Update_notify`, the network manager shall determine if a channel change is required using whatever implementation specific mechanisms are considered appropriate. The network manager device with just one channel allowed in the `apsChannelMask` parameter must not issue the `Mgmt_Nwk_Update_Req` command to request other devices to change the current channel. However, the network manager may report channel quality issues to the application.
4. If the above data indicate a channel change should be considered, the network manager completed the following:
 - a. Select a single channel based on the `Mgmt_NWK_Update_notify` based on the lowest energy. This is the proposed new channel. If this new channel does not have an energy level below an acceptable threshold, a channel change should not be done. Additionally, a new channel shall not belong to a PHY different from the one on which a network manager is operating now.
5. Prior to changing channels, the network manager should store the energy scan value as the last energy scan value and the failure rate from the existing channel as the last failure rate. These values are useful to allow comparison of the failure rate and energy level on the previous channel to evaluate if the network is causing its own interference.
6. The network manager should broadcast a `Mgmt_NWK_Update_req` notifying devices of the new channel. The broadcast shall be to all devices with `RxOnWhenIdle` equal to `TRUE`. The network manager is responsible for incrementing the `nwkUpdateId` parameter from the NIB and including it in the `Mgmt_NWK_Update_req`. The network manager shall set a timer based on the value of `apsChannelTimer` upon issue of a `Mgmt_NWK_Update_req` that changes channels and shall not issue another such command until this timer expires. However, during this period, the network manager can complete the above analysis. However, instead of changing channels, the network manager would report to the local application using `Mgmt_NWK_Update_notify` and the application can force a channel change using the `Mgmt_NWK_Update_req`.

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

46. The Asserted Patents also cover Accused Products of Allegion that utilize the Wi-Fi protocol. Examples of such products include Allegion’s Schlage Encode Plus™ Smart WiFi Deadbolt and Schlage’s ENGAGE™ cloud-based web and mobile applications. As shown below, the Schlage Encode Plus™ Smart WiFi Deadbolt and Schlage’s ENGAGE™ applications are Wi-Fi (IEEE 802.11) compatible:

Smart Deadbolt product categories.

No more worrying whether you locked the front door before you left. With a Schlage smart lock, you can enjoy peace of mind and freedom from keys. Depending on your specific system and home automation needs, Schlage has a wide selection of smart locks that fit with any smart home.



Smart Deadbolt, SCHLAGE, <https://www.schlage.com/en/home/products/products-smart-locks.html> (last visited May 14, 2024) (listing “Schlage Encode Plus™ Smart WiFi Deadbolt,” “Schlage Encode™ Smart Wifi Deadbolt,” and “Schlage Encode™ Smart WiFi Lever”).



Schlage Encode Plus™ Smart WiFi Deadbolt with Century Trim

BE499WB CEN 619

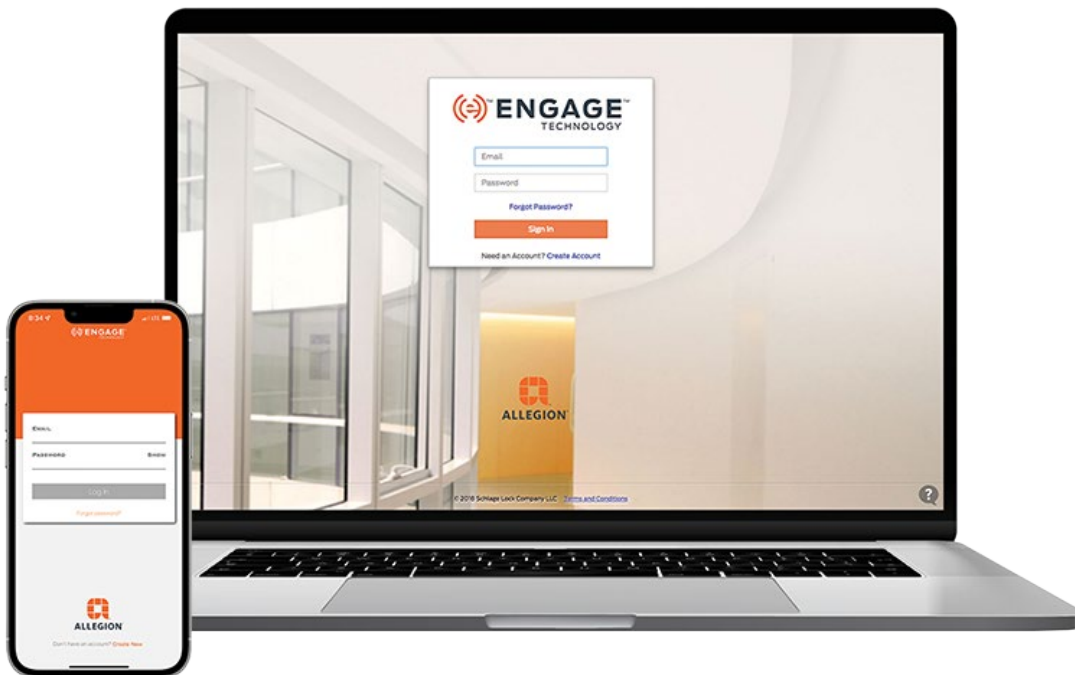


SPECIFICATIONS

- Battery: Uses 4 AA alkaline batteries
- WiFi compatibility: requires 2.4GHz WiFi network

Schlage Encode Plus™ Smart WiFi Deadbolt with Century Trim, SCHLAGE,

<https://www.schlage.com/en/home/products/BE499WBCENFFF.html> (last visited May 14, 2024) (listing battery and WiFi compatibility).



ENGAGE™ for Access Control

ENGAGE cloud-based web and mobile applications are ideal for basic access control within small businesses and multifamily properties. Connect compatible devices over Wi-Fi for periodic updates or use No-Tour which enables Schlage smart and mobile credentials to deliver updates to devices. ENGAGE for access control supports Schlage Control®, NDE, LE, XE360™, and CTE with MTB readers as well as Von Duprin RU and RM.

Looking for more information? Connect with an Allegion team member for help.

Connect with Allegion Team

ENGAGE™ for Access Control, SCHLAGE,

<https://commercial.schlage.com/en/products/software/engage-for-access-control.html> (last visited May 15, 2024) (urging consumers to “[c]onnect compatible devices over Wi-Fi for periodic updates” and indicating the ENGAGE™ App is available at the Apple App Store and Google Play).

47. As can be seen, Allegion supports mobile access for their access control devices, including Wi-Fi-enabled control locks via their ENGAGE™ App for mobile and other devices.

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

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

8.3.2.3 TKIP MIC

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

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

8.3.2.3.1 Motivation for the TKIP MIC

Before defining the details of the MIC, it is useful to review the context in which this mechanism operates.

Active attacks enabled by the original WEP design include the following:

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

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

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

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

49. 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>

50. 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>

51. 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>

52. 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.

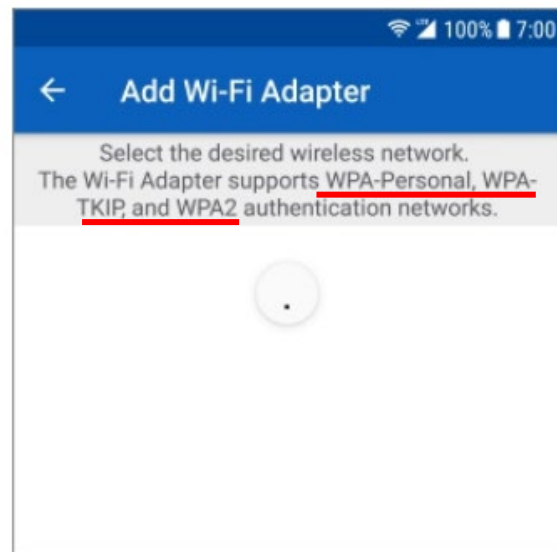
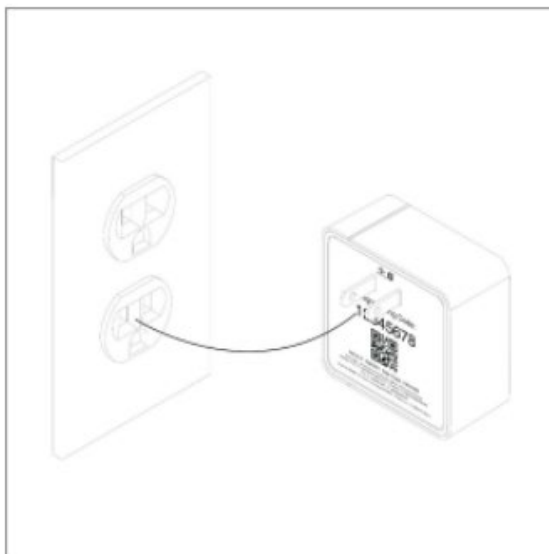
If a subsequent MIC failure occurs within 60 s of the most recent previous failure, then a STA whose IEEE 802.1X entity has acted as a Supplicant shall deauthenticate (as defined in 11.3.1.3) itself or deauthenticate all the STAs with a security association if its IEEE 802.1X entity acted as an Authenticator.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

53. The Asserted Patents also cover Allegion's Wi-Fi compliant devices, which support WPA, WPA2, and/or WPA3 security mechanisms, as described below and in the following paragraph. Of the WPA, WPA2 and/or WPA3 security mechanism used by the Accused Products, such as Allegion's smart access control Wi-Fi devices, the WPA security mechanism is based on

Temporal Key Integrity Protocol (TKIP), while the WPA2 and WPA3 security mechanisms are based on Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). Shown below are exemplary IEEE 802.11 compliant Allegion devices. Each of the devices has a housing.

- 6 Select your home Wi-Fi network to pair with.



Set up your Schlage Sense™ Wi-Fi Adapter, SCHLAGE,

<https://www.schlage.com/blog/categories/2017/11/schlage-sense-wi-fi-adapter-set-up.html> (last visited May 14, 2024).








NDE wireless lock specifications

Communication standards	<ul style="list-style-type: none">2.4 GHz Wi-Fi® (IEEE 802.11b/g/n)WPA2, WPA, WEP, 802.1x
Battery life*	Uses 4 AA batteries Up to 2 years

ENGAGE™ cloud-based
web and mobile applications

 ENGAGE™
TECHNOLOGY

The ENGAGE cloud-based web and mobile applications deliver simple and convenient site set-up with basic access management for users and locks. Please refer to the ENGAGE data sheet for additional detail.

NDE Wireless cylindrical lock, SCHLAGE, https://securiotec.com/wp-content/uploads/2020/10/Schlage_NDE_Series_Wireless_Lock_Data_Sheet_110409.pdf (last visited May 14, 2024) (specifications including: “2.4 GHz WiFi® (IEE 802.11b/g/n),” “WPA2, WPA, WEP, 802.1x,” and “4 AA batteries”).

54. 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 in products represented in Defendants’ Accused Product line.

55. 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.

56. 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.

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.

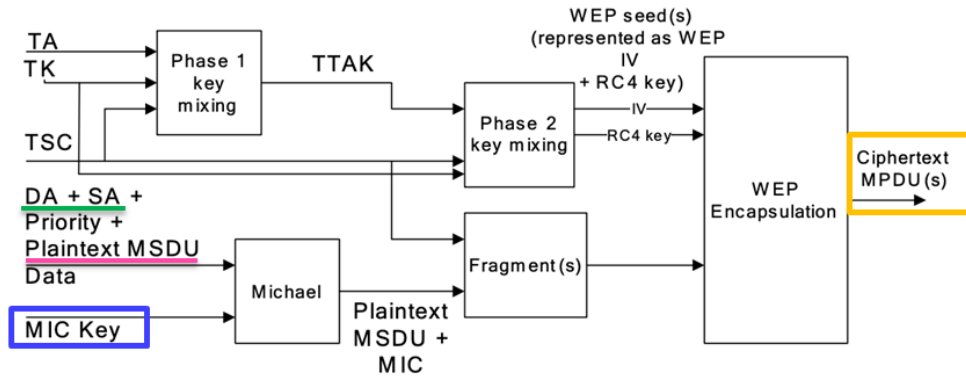


Figure 8-4—TKIP encapsulation block diagram

- 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>

57. On information and belief, Defendants also infringe 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 an example, Allegion's Schlage NDE wireless lock and Schlage Encode Plus™ Smart WiFi Deadbolt 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.




NDE wireless lock specifications


Communication standards	<ul style="list-style-type: none">▪ <u>2.4 GHz Wi-Fi® (IEEE 802.11b/g/n)</u>▪ <u>WPA2, WPA, WEP, 802.1x</u>
Battery life*	<u>Uses 4 AA batteries</u> Up to 2 years

ENGAGE™ cloud-based
web and mobile applications

 ENGAGE™
TECHNOLOGY

The ENGAGE cloud-based web and mobile applications deliver simple and convenient site set-up with basic access management for users and locks. Please refer to the ENGAGE data sheet for additional detail.

 Download on the
App Store

 ANDROID APP ON
Google play

NDE Wireless cylindrical lock, SCHLAGE, https://securiotec.com/wp-content/uploads/2020/10/Schlage_NDE_Series_Wireless_Lock_Data_Sheet_110409.pdf (last

visited May 14, 2024) (specifications including: “2.4 GHz WiFi® (IEEE 802.11b/g/n),” “WPA2, WPA, WEP, 802.1x,” and “4 AA batteries”).



Schlage Encode Plus™ Smart WiFi Deadbolt with Century Trim

BE499WB CEN 619



SPECIFICATIONS

- Battery: Uses 4 AA alkaline batteries
- WiFi compatibility: requires 2.4GHz WiFi network

Schlage Encode Plus™ Smart WiFi Deadbolt with Century Trim, SCHLAGE,

<https://www.schlage.com/en/home/products/BE499WBCENFFF.html> (last visited May 14, 2024) (listing battery and WiFi compatibility).

58. 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)

59. Plaintiff incorporates paragraphs 1 through 58 herein by reference.

60. 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.

61. 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.

62. Allegion has directly and/or indirectly infringed (by inducing infringement) one or more claims of the '678 patent in this District and elsewhere in Texas and the United States.

63. On information and belief, Allegion has designed, developed, manufactured, imported, distributed, offered to sell, sold, and used the Accused Products, including via the activities of Allegion 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 Allegion.

64. Defendants have directly infringed 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, subsidiaries, members, divisions, segments, companies, brands, distributors, importers, resellers, dealers, OEMs, integrators, installers, customers, and/or consumers. Furthermore, on information and belief, (i) Defendants have designed the Accused Products for U.S. consumers; (ii) Defendants have made, used, and/or sold the Accused Products inside the United States; and/or (iii) Defendants have made and sold the Accused Products outside of the United States and delivered 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 Defendants delivered the Accused Products outside of the United States they did so intending and/or knowing that those

products were 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)”).

65. Furthermore, Defendants have directly infringed the '678 patent through their direct involvement in the activities of their subsidiaries, and related entities, including U.S.-based subsidiaries, members, divisions, segments, companies and/or brands of Allegion, 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, Allegion's U.S.-based subsidiaries and/or brands, including at least Schlage Lock Company LLC, Allegion Access Technologies LLC, and/or the Allegion Brands, have conducted 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 Defendants. Defendants are vicariously liable for the infringing conduct of Schlage Lock Company LLC, Allegion Access Technologies LLC, and/or the Allegion Brands, and other U.S.-based subsidiaries, members, related entities, divisions, segments, companies and/or brands of Allegion (under both the alter ego and agency theories). On information and belief, Defendants, and related entities and subsidiaries, including U.S.-based subsidiaries members, divisions, segments, companies and/or brands of Allegion are essentially the same company (i.e., “Allegion”),

operating in the U.S. via, for example, one or more of the brands, divisions, segments, mergers, and/or acquisitions of Allegion listed in this complaint. Moreover, Allegion Public Limited Company, as the parent company, along with its related entities, has had the right and ability to control and/or delegate the control of the infringing activities of those subsidiary entities such that Defendants have received a direct financial benefit from that infringement.

66. As an example, Allegion 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, Allegion's Schlage Encode Plus™ Smart WiFi Deadbolt, Schlage Encode™ Smart Wifi Deadbolt, Schlage Encode™ Smart WiFi Lever, and Schlage NDE wireless lock with Wi-Fi compatibility); related accessories (for example, the Schlage Sense™ Wi-Fi Adapter); and related software (for example, Schlage Engage™ for Access Control); and devices including any WiFi-enabled module.

67. 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.

68. Allegion 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

correspondence dated July 21, 2020, from John Garland, working with Acacia Research Group LLC, on behalf of Stingray. The letter notifies Allegion of Stingray's ownership of patents relating to smart locks, wireless communication networks and ad-hoc mesh networking, as well as innovations pertinent to the Zigbee protocols and technology. Further, Allegion has been on notice about infringement of the Harris patent portfolio and the '678 patent, since at least a call dated on or around August 20, 2021, and its receipt of a corresponding presentation with claim charts for the Harris patent portfolio.

69. 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 was sent to Allegion, for example, on June 2, 2021, and July 27, 2021. These examples of notice provided to Allegion are not exhaustive, and Allegion has also received additional communications regarding notice of infringement in connection with the Asserted Patents.

70. On information and belief, since at least the above-mentioned date or dates when Defendants were on notice of their infringement, Defendants have 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, Defendants have conducted 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, Defendants

have intended to cause, and have 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, Defendants have manufactured, tested, and certified the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC regulations, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendants have distributed or made 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, the Connectivity Standards Alliance and/or for FCC compliance) in the Accused Products, and have provided technical support, product files, videos, and/or related services for these products to purchasers in the United States. *See, e.g., FCC ID XPB-BR400*, FCCID.IO, <https://fccid.io/XPB-BR400> (last visited May 15, 2024) (showing Allegion’s submissions to the FCC regarding the Schlage Sense Wi-Fi Adapter assigned ID BR400); *Testing of Electromagnetic Emissions per CFR Title 47, Part 15.247 etc., for Allegion, PLC’s BR400*, WILLOW RUN (WR) TEST LABS, INC. (March 16, 2017), available at <https://fccid.io/XPB-BR400/Test-Report/Test-Report-3331554> (last visited May 15, 2024); *Certified Products Search*, CONNECTIVITY STANDARDS ALLIANCE, https://csa-iot.org/csa-iot_products/?p_keywords=&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_company%5B%5D=781&p_family= (last visited May 14, 2024) (listing three different “Schlage Connect Smart Deadbolt” products as Zigbee certified); *How to Install the Schlage NDE Lock*, SCHLAGE, <https://www.youtube.com/watch?v=U6fUoLLH7Kw> (last

visited May 15, 2024) (including a description that states “This video demonstrates how to install the NDE Wireless lock,” “To view all of the training videos available for NDE and LE locks, go to our playlist: . . . ,” and “For more information on the NDE Series lock with ENGAGE technology, please visit our web site at <http://www.allegion.com/us>.”).

71. Furthermore, Defendants have induced infringement by installers, integrators, consumers and other users of Allegion’s products by designing, developing, marketing, and offering smartphone, tablet, and/or mobile device interfaces as application software (i.e., apps) such as Schlage’s ENGAGE™ app to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, and update compatible devices using a Wi-Fi network. *See, e.g., ENGAGE™ for Access Control*, SCHLAGE, <https://commercial.schlage.com/en/products/software/engage-for-access-control.html> (last visited May 15, 2024) (urging consumers to “[c]onnect compatible devices over Wi-Fi for periodic updates” and indicating the ENGAGE™ App is available at the Apple App Store and Google Play).

72. Allegion’s apps have also induced infringing use of the Accused Products by providing compatibility between Allegion products and third-party products that share or access the same wireless networks. *See, e.g., SCHLAGE ENGAGE Managed Property 8.1.0 User’s Guide*, ALLEGION, available at https://us.allegion.com/content/dam/allegion-us-2/web-documents-2/UserGuide/Schlage_ENGAGE_User_Guide_113180.pdf (last visited May 15, 2024) (stating “We support and test the flagship phone models from Apple, Samsung, LG, Motorola, and Google for the last two years,” and listing devices from numerous brands). Such compatibility has provided convenience and added functionality that has induced consumers to use the Defendants’ products, including via apps and other interfaces utilizing Wi-Fi and/or ZigBee protocols in

networks with other third-party devices. Thus, these activities have further infringed or induced infringement of the '678 patent.

73. On information and belief, despite having knowledge of the '678 patent and knowledge that it was directly and/or indirectly infringing one or more claims of the '678 patent, Defendants nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants' infringing activities relative to the '678 patent have been 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.

74. Plaintiff Stingray has been damaged as a result of Allegion'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)

75. Plaintiff incorporates paragraphs 1 through 74 herein by reference.

76. 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.

77. 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.

78. Allegion 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.

79. On information and belief, Allegion designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Allegion 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 Allegion.

80. Defendants directly infringe 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, subsidiaries, members, divisions, segments, companies, brands, distributors, importers, resellers, dealers, OEMs, integrators, installers, customers, and/or consumers. Furthermore, on information and belief, (i) Defendants design the Accused Products for U.S. consumers; (ii) Defendants make, use, and/or sell the Accused Products inside the United States; and/or (iii) Defendants make and sell the Accused Products outside of the United States and deliver 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 Defendants deliver the Accused Products outside of the United States they do 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)”).

81. Furthermore, Defendants directly infringe the '572 patent through their direct involvement in the activities of their subsidiaries, and related entities, including U.S.-based subsidiaries, members, divisions, segments, companies and/or brands of Allegion, 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, Allegion's U.S.-based subsidiaries and/or brands, including at least Schlage Lock Company LLC, Allegion Access Technologies LLC, and/or the Allegion Brands, 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 Defendants. Defendants are vicariously liable for the infringing conduct of Schlage Lock Company LLC, Allegion Access Technologies LLC, and/or the Allegion Brands, and other U.S.-based subsidiaries, members, related entities, divisions, segments, companies and/or brands of Allegion (under both the alter ego and agency theories). On information and belief, Defendants, and related entities and subsidiaries, including U.S.-based subsidiaries members, divisions, segments, companies and/or brands of Allegion are essentially the same company (i.e., “Allegion”), operating in the U.S. via, for example, one or more of the brands, divisions, segments, mergers, and/or acquisitions of Allegion listed in this complaint. Moreover, Allegion Public Limited

Company, 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 Defendants receive a direct financial benefit from that infringement.

82. As an example, Allegion 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, Allegion's Schlage Encode Plus™ Smart WiFi Deadbolt, Schlage Encode™ Smart Wifi Deadbolt, Schlage Encode™ Smart WiFi Lever, and Schlage NDE wireless lock with Wi-Fi compatibility); related accessories (for example, the Schlage Sense™ Wi-Fi Adapter); and related software (for example, Schlage Engage™ for Access Control); and devices including any WiFi-enabled module.

83. 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.

84. Allegion further infringes the '572 patent via 35 U.S.C. § 271(g) by selling, offering to sell, and/or importing networking, IoT, smart, security and access control solutions, products, components, software, services, and processes related to same, that make a secure wireless local area network by a process covered by the '572 patent. On information and belief, the infringing

networking, IoT, smart, security and access control solutions, products, components, software, services, and processes related to same are not materially changed by subsequent processes, and they are neither trivial nor nonessential components of another product.

85. Allegion 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.

86. At a minimum, Allegion has known of the '572 patent at least as early as the filing date of this complaint. In addition, Allegion 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 correspondence dated July 21, 2020, from John Garland, working with Acacia Research Group LLC, on behalf of Stingray. The letter notifies Allegion of Stingray's ownership of patents relating to smart locks, wireless communication networks and ad-hoc mesh networking, as well as innovations pertinent to the Zigbee protocols and technology. Further, Allegion has been on notice about infringement of the Harris patent portfolio and the '572 patent, since at least a call dated on or around August 20, 2021, and its receipt of a corresponding presentation with claim charts for the Harris patent portfolio.

87. 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 was sent to Allegion, for example, on June 2, 2021, and July 27, 2021. These examples of notice provided to Allegion are not

exhaustive, and Allegion has also received additional communications regarding notice of infringement in connection with the Asserted Patents.

88. On information and belief, since at least the above-mentioned date or dates when Defendants were on notice of their infringement, Defendants have 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, Defendants conduct 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, Defendants intend to cause, and have 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, Defendants manufacture, test, and certify the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC regulations, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendants distribute or make 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, the Connectivity Standards Alliance and/or for FCC compliance) in the Accused

Products, and provide technical support, product files, videos, and/or related services for these products to purchasers in the United States. *See, e.g., FCC ID XPB-BR400*, FCCID.IO, <https://fccid.io/XPB-BR400> (last visited May 15, 2024) (showing Allegion’s submissions to the FCC regarding the Schlage Sense Wi-Fi Adapter assigned ID BR400); *Testing of Electromagnetic Emissions per CFR Title 47, Part 15.247 etc., for Allegion, PLC’s BR400*, WILLOW RUN (WR) TEST LABS, INC. (March 16, 2017), available at <https://fccid.io/XPB-BR400/Test-Report/Test-Report-3331554> (last visited May 15, 2024); *Certified Products Search*, CONNECTIVITY STANDARDS ALLIANCE, https://csa-iot.org/csa-iot_products/?p_keywords=&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_company%5B%5D=781&p_family= (last visited May 14, 2024) (listing three different “Schlage Connect Smart Deadbolt” products as Zigbee certified); *How to Install the Schlage NDE Lock*, SCHLAGE, <https://www.youtube.com/watch?v=U6fUoLLH7Kw> (last visited May 15, 2024) (including a description that states “This video demonstrates how to install the NDE Wireless lock,” “To view all of the training videos available for NDE and LE locks, go to our playlist: . . . ,” and “For more information on the NDE Series lock with ENGAGE technology, please visit our web site at <http://www.allegion.com/us>.”).

89. Furthermore, Defendants induce infringement by installers, integrators, consumers and other users of Allegion’s products by designing, developing, marketing, and offering smartphone, tablet, and/or mobile device interfaces as application software (i.e., apps) such as Schlage’s ENGAGE™ app to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, and update compatible devices using a Wi-Fi network. *See, e.g., ENGAGE™ for Access Control*, SCHLAGE, <https://commercial.schlage.com/en/products/software/engage-for-access-control.html> (last visited

May 15, 2024) (urging consumers to “[c]onnect compatible devices over Wi-Fi for periodic updates” and indicating the ENGAGE™ App is available at the Apple App Store and Google Play).

90. Allegion’s apps also induce infringing use of the Accused Products by providing compatibility between Allegion products and third-party products that share or access the same wireless networks. *See, e.g., SCHLAGE ENGAGE Managed Property 8.1.0 User’s Guide, ALLEGION*, available at https://us.allegion.com/content/dam/allegion-us-2/web-documents-2/UserGuide/Schlage_ENGAGE_User_Guide_113180.pdf (last visited May 15, 2024) (stating “We support and test the flagship phone models from Apple, Samsung, LG, Motorola, and Google for the last two years,” and listing devices from numerous brands). Such compatibility provides convenience and added functionality that induces consumers to use the Defendants’ 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.

91. 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, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants’ infringing activities relative to the ’572 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

92. Plaintiff Stingray has been damaged as a result of Allegion'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)

93. Plaintiff incorporates paragraphs 1 through 92 herein by reference.

94. 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.

95. 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.

96. Allegion 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.

97. On information and belief, Allegion designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Allegion 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 Allegion.

98. Defendants directly infringe 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, subsidiaries, members, divisions, segments, companies, brands, distributors, importers, resellers, dealers, OEMs, integrators, installers, customers, and/or consumers. Furthermore, on information and belief, (i) Defendants design the Accused Products for U.S. consumers; (ii) Defendants make, use, and/or sell the Accused Products inside the United States; and/or (iii) Defendants make and sell the Accused Products outside of the United States and deliver 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 Defendants deliver the Accused Products outside of the United States they do 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)”).

99. Furthermore, Defendants directly infringe the '961 patent through their direct involvement in the activities of their subsidiaries, and related entities, including U.S.-based subsidiaries, members, divisions, segments, companies and/or brands of Allegion, 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, Allegion's U.S.-based subsidiaries and/or brands, including at least Schlage Lock Company LLC, Allegion Access Technologies LLC, and/or the Allegion Brands, 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 Defendants. Defendants are vicariously liable for the infringing conduct of Schlage Lock Company LLC, Allegion Access Technologies LLC, and/or the Allegion Brands, and other U.S.-based subsidiaries, members, related entities, divisions, segments, companies and/or brands of Allegion (under both the alter ego and agency theories). On information and belief, Defendants, and related entities and subsidiaries, including U.S.-based subsidiaries members, divisions, segments, companies and/or brands of Allegion are essentially the same company (i.e., "Allegion"), operating in the U.S. via, for example, one or more of the brands, divisions, segments, mergers, and/or acquisitions of Allegion listed in this complaint. Moreover, Allegion Public Limited Company, 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 Defendants receive a direct financial benefit from that infringement.

100. As an example, Allegion infringes claim 1 of the '961 patent via the Accused Products that utilize ZigBee protocols, including, but not limited to access control (for example, Allegion's Schlage Connect™ Zigbee lock)); and related accessories and software (for example, Schlage Engage™ for Access Control); and devices including any Zigbee-enabled module.

101. 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.

102. At a minimum, Allegion has known of the ’961 patent at least as early as the filing date of this complaint. In addition, Allegion 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 correspondence dated July 21, 2020, from John Garland, working with Acacia Research Group LLC, on behalf of Stingray. The letter notifies Allegion of Stingray’s ownership of patents relating to smart locks, wireless communication networks and ad-hoc mesh networking, as well as innovations pertinent to the Zigbee protocols and technology. Further, Allegion has been on notice about infringement of the Harris patent portfolio and the ’961 patent, since at least a call dated on or around August 20, 2021, and its receipt of a corresponding presentation with claim charts for the Harris patent portfolio.

103. 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 was sent to Allegion, for example, on June 2, 2021, and July 27, 2021. These examples of notice provided to Allegion are not exhaustive, and Allegion has also received additional communications regarding notice of infringement in connection with the Asserted Patents.

104. On information and belief, since at least the above-mentioned date or dates when Defendants were on notice of their infringement, Defendants have 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, Defendants conduct 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, Defendants intend to cause, and have 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, Defendants manufacture, test, and certify the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC regulations, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendants distribute or make 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, the Connectivity Standards Alliance and/or for FCC compliance) in the Accused Products, and provide technical support, product files, videos, and/or related services for these products to purchasers in the United States. *See, e.g., FCC ID XPB-BR400*, FCCID.IO, <https://fccid.io/XPB-BR400> (last visited May 15, 2024) (showing Allegion’s submissions to the FCC regarding the Schlage Sense Wi-Fi Adapter assigned ID BR400); *Testing of Electromagnetic Emissions per CFR Title 47, Part 15.247 etc., for Allegion, PLC’s BR400*, WILLOW RUN (WR) TEST LABS, INC. (March 16, 2017), available at <https://fccid.io/XPB-BR400/Test-Report/Test-Report-3331554> (last visited May 15, 2024); *Certified Products Search*, CONNECTIVITY STANDARDS ALLIANCE, https://csa-iot.org/csa-iot_products/?p_keywords=&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_company%5B%5D=781&p_family= (last visited May 14, 2024) (listing three different “Schlage Connect Smart Deadbolt” products as Zigbee certified); *How to Install the Schlage NDE Lock*, SCHLAGE, <https://www.youtube.com/watch?v=U6fUoLLH7Kw> (last visited May 15, 2024) (including a description that states “This video demonstrates how to install the NDE Wireless lock,” “To view all of the training videos available for NDE and LE locks, go to our playlist: . . . ,” and “For more information on the NDE Series lock with ENGAGE technology, please visit our web site at <http://www.allegion.com/us>.”); *Schlage Connect™ Smart Deadbolt, Zigbee Certified*, SCHLAGE, https://www.youtube.com/watch?v=_q-8PDvjRG8 (last visited May 15, 2024).

105. Furthermore, Defendants induce infringement by installers, integrators, consumers and other users of Allegion’s products by designing, developing, marketing, and offering smartphone, tablet, and/or mobile device interfaces as application software (i.e., apps) such as

Schlage's ENGAGE™ app to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, and update compatible devices using a Wi-Fi network. *See, e.g., ENGAGE™ for Access Control*, SCHLAGE, <https://commercial.schlage.com/en/products/software/engage-for-access-control.html> (last visited May 15, 2024) (urging consumers to “[c]onnect compatible devices over Wi-Fi for periodic updates” and indicating the ENGAGE™ App is available at the Apple App Store and Google Play).

106. Allegion's apps also induce infringing use of the Accused Products by providing compatibility between Allegion products and third-party products that share or access the same wireless networks. *See, e.g., SCHLAGE ENGAGE Managed Property 8.1.0 User's Guide*, ALLEGION, available at https://us.allegion.com/content/dam/allegion-us-2/web-documents-2/UserGuide/Schlage_ENGAGE_User_Guide_113180.pdf (last visited May 15, 2024) (stating “We support and test the flagship phone models from Apple, Samsung, LG, Motorola, and Google for the last two years,” and listing devices from numerous brands). Such compatibility provides convenience and added functionality that induces consumers to use the Defendants' 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.

107. 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, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants' infringing activities relative to the '961 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate,

consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

108. Plaintiff Stingray has been damaged as a result of Allegion'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)

109. Plaintiff incorporates paragraphs 1 through 108 herein by reference.

110. 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.

111. 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.

112. Allegion 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.

113. On information and belief, Allegion designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Allegion 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 Allegion.

114. Defendants directly infringe 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, subsidiaries, members, divisions, segments, companies, brands, distributors, importers, resellers, dealers, OEMs, integrators, installers, customers, and/or consumers. Furthermore, on information and belief, (i) Defendants design the Accused Products for U.S. consumers; (ii) Defendants make, use, and/or sell the Accused Products inside the United States; and/or (iii) Defendants make and sell the Accused Products outside of the United States and deliver 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 Defendants deliver the Accused Products outside of the United States they do 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)”).

115. Furthermore, Defendants directly infringe the '126 patent through their direct involvement in the activities of their subsidiaries, and related entities, including U.S.-based

subsidiaries, members, divisions, segments, companies and/or brands of Allegion, 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, Allegion's U.S.-based subsidiaries and/or brands, including at least Schlage Lock Company LLC, Allegion Access Technologies LLC, and/or the Allegion Brands, 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 Defendants. Defendants are vicariously liable for the infringing conduct of Schlage Lock Company LLC, Allegion Access Technologies LLC, and/or the Allegion Brands, and other U.S.-based subsidiaries, members, related entities, divisions, segments, companies and/or brands of Allegion (under both the alter ego and agency theories). On information and belief, Defendants, and related entities and subsidiaries, including U.S.-based subsidiaries members, divisions, segments, companies and/or brands of Allegion are essentially the same company (i.e., "Allegion"), operating in the U.S. via, for example, one or more of the brands, divisions, segments, mergers, and/or acquisitions of Allegion listed in this complaint. Moreover, Allegion Public Limited Company, 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 Defendants receive a direct financial benefit from that infringement.

116. As an example, Allegion infringes claim 1 of the '126 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to Defendants' 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, Allegion's Schlage Encode Plus™ Smart WiFi Deadbolt, Schlage Encode™ Smart Wifi Deadbolt, Schlage Encode™ Smart WiFi Lever, and Schlage NDE wireless lock with Wi-Fi compatibility); related accessories (for example, the Schlage Sense™ Wi-Fi Adapter); and related software (for example, Schlage Engage™ for Access Control); and devices including any WiFi-enabled module.

117. 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.

118. At a minimum, Allegion has known of the '126 patent at least as early as the filing date of this complaint. In addition, Allegion 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 correspondence dated July 21, 2020, from John Garland, working with Acacia Research Group LLC, on behalf of Stingray. The letter notifies Allegion of Stingray's ownership of patents relating to smart locks, wireless communication networks and ad-hoc mesh networking, as well as innovations pertinent to the Zigbee protocols and technology. Further, Allegion has been on notice about infringement of the Harris patent portfolio and the '126 patent, since at least a call

dated on or around August 20, 2021, and its receipt of a corresponding presentation with claim charts for the Harris patent portfolio.

119. 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 was sent to Allegion, for example, on June 2, 2021, and July 27, 2021. These examples of notice provided to Allegion are not exhaustive, and Allegion has also received additional communications regarding notice of infringement in connection with the Asserted Patents.

120. On information and belief, since at least the above-mentioned date or dates when Defendants were on notice of their infringement, Defendants have 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, Defendants conduct 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, Defendants intend to cause, and have 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, Defendants

manufacture, test, and certify the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC regulations, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendants distribute or make 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, the Connectivity Standards Alliance and/or for FCC compliance) in the Accused Products, and provide technical support, product files, videos, and/or related services for these products to purchasers in the United States. *See, e.g., FCC ID XPB-BR400*, FCCID.IO, <https://fccid.io/XPB-BR400> (last visited May 15, 2024) (showing Allegion’s submissions to the FCC regarding the Schlage Sense Wi-Fi Adapter assigned ID BR400); *Testing of Electromagnetic Emissions per CFR Title 47, Part 15.247 etc., for Allegion, PLC’s BR400*, WILLOW RUN (WR) TEST LABS, INC. (March 16, 2017), available at <https://fccid.io/XPB-BR400/Test-Report/Test-Report-3331554> (last visited May 15, 2024); *Certified Products Search*, CONNECTIVITY STANDARDS ALLIANCE, https://csa-iot.org/csa-iot_products/?p_keywords=&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_company%5B%5D=781&p_family= (last visited May 14, 2024) (listing three different “Schlage Connect Smart Deadbolt” products as Zigbee certified); *How to Install the Schlage NDE Lock*, SCHLAGE, <https://www.youtube.com/watch?v=U6fUoLLH7Kw> (last visited May 15, 2024) (including a description that states “This video demonstrates how to install the NDE Wireless lock,” “To view all of the training videos available for NDE and LE locks, go to our playlist: . . . ,” and “For more information on the NDE Series lock with ENGAGE technology, please visit our web site at <http://www.allegion.com/us>.”).

121. Furthermore, Defendants induce infringement by installers, integrators, consumers and other users of Allegion's products by designing, developing, marketing, and offering smartphone, tablet, and/or mobile device interfaces as application software (i.e., apps) such as Schlage's ENGAGE™ app to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, and update compatible devices using a Wi-Fi network. See, e.g., *ENGAGE™ for Access Control*, SCHLAGE, <https://commercial.schlage.com/en/products/software/engage-for-access-control.html> (last visited May 15, 2024) (urging consumers to “[c]onnect compatible devices over Wi-Fi for periodic updates” and indicating the ENGAGE™ App is available at the Apple App Store and Google Play).

122. Allegion's apps also induce infringing use of the Accused Products by providing compatibility between Allegion products and third-party products that share or access the same wireless networks. See, e.g., *SCHLAGE ENGAGE Managed Property 8.1.0 User's Guide*, ALLEGION, available at https://us.allegion.com/content/dam/allegion-us-2/web-documents-2/UserGuide/Schlage_ENGAGE_User_Guide_113180.pdf (last visited May 15, 2024) (stating “We support and test the flagship phone models from Apple, Samsung, LG, Motorola, and Google for the last two years,” and listing devices from numerous brands). Such compatibility provides convenience and added functionality that induces consumers to use the Defendants' 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.

123. 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,

Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants' 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.

124. Plaintiff Stingray has been damaged as a result of Allegion'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

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

126. 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

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

PRAYER FOR RELIEF

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

1. A judgment that Defendants have infringed the Asserted Patents as alleged herein, directly and/or indirectly by way of inducing infringement of such patents;
2. A judgment for an accounting of damages sustained by Plaintiff as a result of the acts of infringement by Defendants;
3. A judgment and order requiring Defendants to pay Plaintiff damages under 35 U.S.C. § 284, including up to treble damages as provided by 35 U.S.C. § 284, and any royalties determined to be appropriate;
4. A judgment and order requiring Defendants to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;
5. A judgment and order finding this to be an exceptional case and requiring Defendants to pay the costs of this action (including all disbursements) and attorneys' fees as provided by 35 U.S.C. § 285; and
6. Such other and further relief as the Court deems just and equitable.

Dated: May 31, 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