

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

STINGRAY IP SOLUTIONS LLC,

Plaintiff,

v.

**RESIDEO TECHNOLOGIES, INC. and
ADEMCO INC.,**

Defendants.

§
§
§
§
§
§
§
§
§
§
§
§
§
§
§
§
§
§
§
§
§

JURY TRIAL DEMANDED

CIVIL ACTION NO. _____

PLAINTIFF’S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Stingray IP Solutions LLC (“Stingray”) files this Complaint in this Eastern District of Texas (the “District”) against Defendants Resideo Technologies, Inc. and Ademco Inc. (collectively, “Defendants” or “Resideo”) for infringement of U.S. Patent No. 7,224,678 (the “’678 patent”) and U.S. Patent No. 7,440,572 (the “’572 patent”).

THE PARTIES

1. Stingray IP Solutions, LLC (“Stingray” or “Plaintiff”) is a Texas limited liability company, located at 6136 Frisco Sq. Blvd., Suite 400, Frisco, TX 75034.

2. On information and belief, Defendant Resideo Technologies, Inc. (“Resideo”) is a corporation formed and organized under the laws of Delaware with its principal executive offices and corporate headquarters located at 16100 N. 71st Street, Suite 550, Scottsdale, Arizona. Resideo is registered to do business in Texas. *See* TEXAS SECRETARY OF STATE, <https://direct.sos.state.tx.us/> at Filing No. 804269474 (showing Resideo’s application for registration to do business as a foreign

corporation in Texas) (last visited Oct. 4, 2022). Resideo’s registered agent in Texas is Corporation Service Company located at 211 E. 7th Street, Suite 620, Austin, TX 78701-3128.

3. On information and belief, Defendant Ademco Inc. (“Ademco”) is a corporation formed and organized under the laws of Delaware with its principal place of business at 115 Tabor Rd. Morris Plains, NJ 07950. Ademco is registered to do business in Texas and maintains Corporation Service Company located at 211 E. 7th Street, Suite 620, Austin, TX 78701-3128 as its registered agent. *See* TEXAS SECRETARY OF STATE, <https://direct.sos.state.tx.us/> at Filing No. 803012625 (showing Ademco’s 2021 Public Information Report in Texas) (last visited Oct. 4, 2022). Ademco is a wholly-owned subsidiary of Resideo.

4. In about October of 2018, Honeywell International Inc. completed a spin-off of its “Home” business into a new company—Resideo Technologies, Inc., which is a defendant in this action. Defendant Resideo became a public company, trading under the ticker symbol “REZI” of the New York Stock Exchange. Resideo describes itself as “a leading global manufacturer and developer of technology-driven products and solutions that provide critical comfort, residential thermal and security solutions to over 150 million homes globally” and also “the leading wholesale distributor of low-voltage security products including intrusion, access control and video products and participate significantly in the broader related markets of smart home, fire, power, audio, ProAV, networking, communications, wire and cable, enterprise connectivity, and structured wiring products.” *Resideo 2021 Annual Report*, at “Form 10-K”, *available for download at* <https://investor.resideo.com/financials/annual-reports/default.aspx> (last visited Oct. 3, 2022). Defendant Resideo operates via two business segments: “Products & Solutions” and “ADI Global Distribution.” *Id.* at 4 (citations are to the document’s internal pagination).

5. Resideo’s Products & Solutions segment offers “temperature and humidity control, thermal water and air solutions, as well as security panels, sensors, peripherals, wire and cable, communications devices, video cameras, awareness solutions, cloud infrastructure, installation and maintenance tools, and related software.” *Resideo 2021 Annual Report* at 4. These products offer “home connectivity” that provide “control, visibility, insights, and alerts to the end user.” The Products & Solutions segment “operate[s] manufacturing and distribution facilities throughout the world, including sites in Mexico, Czech Republic, Hungary, the United States, Germany, United Kingdom, Netherlands and China.” *Resideo 2021 Annual Report* at 5. This segment’s revenue is derived in significant part “from products manufactured in [Resideo’s] own facilities.” *Id.* And “manufacturing operations include printed circuit board (PCB) assembly, surface mount technologies (SMT), automatic and manual assembly and test, electrotechnical assembly and test, die casting and machining, calibration and final test.” *Id.* Resideo also sources “raw materials and commodities, electronic components and assemblies, and mechanical components and assemblies from a wide range of third-party suppliers worldwide.” *Id.* The Products & Solutions segment primarily sells Resideo’s products “through a network of professional contractors, distributors, OEMs, retailers and online merchants.” *Id.* at 10.

6. Resideo’s ADI Global Distribution segment utilizes “nearly 200 stocking locations in 16 countries” to “distributes[] more than 350,000 products from over 1,000 manufacturers to a customer base of over 100,000 contractors and is recognized for superior customer service.” *Resideo 2021 Annual Report* at 4. This segment distributes products, including Resideo’s own products, from “industry-leading manufacturers and carries a line of private label products.” These products are “delivered through a comprehensive network of professional contractors, distributors and OEMs, as well as major retailers and online merchants.” *Id.* at 28. Fourteen percent (14%) of

the segment's net revenue comes from the sale of products from Resideo's Products & Solutions segment. *Id.*

7. On information and belief, Defendant Ademco registered to use "Resideo" as an assumed name at least with the Secretary of State of Texas, and also does business in the U.S. as "ADI Global Distribution," also referred to as "ADI." *See, e.g., Standard Terms and Conditions, ADI, A RESIDEO COMPANY*, <https://www.adiglobaldistribution.us/TermsAndConditionsPage> (last visited Oct. 4, 2022) ("All sales by Ademco Inc., doing business as ADI Global Distribution ("Seller"), are expressly conditioned by and under these terms and conditions....").

8. Among Resideo's products, Resideo designs, manufactures, distributes, and sells products that specialize in smart home technology, including "air and temperature control solutions, security products, water monitoring product and energy solutions." *See Resideo, ADI, A RESIDEO COMPANY*, <https://www.adiglobaldistribution.us/Catalog/shop-brands/resideo> (summarizing the Resideo brand product offerings) (last visited Oct. 4, 2022). These products communicate with each other using network protocols, including 802.11-based protocols (referred to commonly as "Wi-Fi"). For example, Resideo offers "smart thermostats, programmable thermostats, non-programmable thermostats, air purifiers, humidifiers, [and] ventilation controls" as air and temperature solutions." Resideo also offers "door and window contacts, alarm communicators and control panels, security cameras, smoke detectors, heat detectors, CO detectors, [and] wireless keys" as security solutions. And Resideo offers "leak detectors, freeze detectors, water heater solutions, [and] hydronic zoning panels" as water safety solutions. Among power or energy solutions products, Resideo offers "smart thermostats, HVAC components and other home system essentials."

9. On information and belief, Defendants on their own and/or via subsidiaries, distributors, and affiliates maintain a corporate and commercial presence in the United States, including in Texas and this District. Defendants maintain their business presence in the U.S. and Texas via at least the following activities: 1) providing branch locations across the U.S. (including six in Texas) where consumers may pick-up purchased products; 2) maintaining an online presence (<https://www.resideo.com/us/en/products/>, <https://www.adiglobaldistribution.us/Catalog/shop-brands/resideo>, and <https://www.honeywellhome.com/us/en>) that solicits sales of Resideo products under at least the Resideo® and Honeywell Home™ brands; 3) distributing, via wholesale and retail channels, Resideo’s products and services, including utilizing national retailers in this District; 4) providing to U.S. consumers the “Resideo App,” the “Total Connect Comfort app” and the “ADI mobile app” (among other app software) for accessing product information, connecting to Wi-Fi networks, purchasing products, and other services related to Resideo products; 5) establishing a network of distributors, dealers, and qualified expert installers for the sale and use of Resideo products across the U.S.; and 6) employment of at least 3,300 persons in the United States, including residents of Texas and this District. For example, Defendants employ Texas residents in at least five (5) business locations in the Dallas / Fort Worth area, including at 12880 Valley Branch Lane Farmers Branch, TX 75234 (branch location); 5036 Saunders Rd., Fort Worth, TX 76119 (branch location), 750 W John Carpenter Freeway, Irving, TX, 75039, 346 Beltline Rd Unit 100, Coppell, TX, 75019, and 2601 Petty Place, Fort Worth, TX, 76177. *See, e.g., Why Join Us*, RESIDEO, <https://www.resideo.com/us/en/corporate/about/careers> (providing a link to Resideo’s job search portal, which identifies where Resideo is hiring). Thus, Defendants Resideo and Ademco do business in the United States, the state of Texas, and in the Eastern District of Texas.

JURISDICTION AND VENUE

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

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

A. Defendant Resideo

12. On information and belief, Defendant Resideo is subject to this Court’s specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein, including its registration to do business in Texas, 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, intermediaries, agents, distributors, importers, customers, subsidiaries, affiliates, and/or consumers.

13. For example, Resideo owns and/or controls multiple, subsidiaries, distributors, and affiliates including, but not limited to, Defendant Ademco. Ademco operates in the U.S. and in Texas under the assumed name “Resideo” and is also known as ADI Global Distribution or ADI. Resideo maintains a significant business presence in Texas by employing residents in at least six (6) branch locations where consumers may purchase and pick-up merchandise and other warehousing/distribution facilities, including locations in Austin, Houston, San Antonio, and the Dallas/Fort Worth Area. *See, e.g., Branch Locator, ADI, A RESIDEO COMPANY,*

<https://www.adiglobaldistribution.us/dealerlocator> (providing a search function for consumers to find branch locations in the U.S. and Texas). Resideo, via at least the operations of its ADI Global Distribution business segment, owns or leases a logistics and distribution facility in this District at 2601 Petty Place, Fort Worth, TX, 76177. *See Property Search Results > 1-7 of 7 for Year 2022, DENTON CAD, <https://propaccess.trueautomation.com/clientdb/SearchResults.aspx?cid=19>* (Search results for “Ademco” as owner) (last visited Oct. 4, 2022). Importantly, Resideo maintains its own employees or agents at this facility to conduct its business of at least distribution of Resideo products. *See, e.g., https://eh1.f.a.us6.oraclecloud.com/hcmUI/CandidateExperience/en/sites/CX_2/requisitions/preview/10237/?location=Coppell%2C+TX%2C+United+States&locationId=300000002483784&locationLevel=city&mode=location&radius=25&radiusUnit=MI* (showing a “Sr Human Resources Business Partner” position open for hiring at the 2601 Petty Place location) (last visited Oct. 4, 2022).

14. Such a corporate and commercial presence by Defendant Resideo furthers the development, design, manufacture, importation, distribution, and sale of Defendant’s infringing electronic devices in Texas, including in this District. Through utilization of its business segments and the direction and control of its subsidiaries and affiliates, Resideo has committed acts of direct and/or indirect patent infringement within Texas, this District, and elsewhere in the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over Resideo would not offend traditional notions of fair play and substantial justice.

15. On information and belief, Resideo controls or otherwise directs and authorizes all activities of its subsidiaries, distributors, and affiliates, including, but not limited to Defendant Ademco, which, significantly, have substantial business operations in Texas. Directly and via at

least these subsidiaries, distributors, and/or affiliates and via intermediaries, such as resellers, dealers, expert installers, and customers, Resideo has placed and continues to place infringing electronic devices, including Resideo's smart home devices, such as Resideo® and Honeywell Home™ branded devices, into the U.S. stream of commerce. Resideo 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, Defendant Resideo also purposefully places infringing smart home devices in established distribution channels in the stream of commerce by contracting with national retailers who sell Resideo's products in the U.S. via online and brick and mortar stores, including in Texas and this District. Resideo contracts with these companies with the knowledge and expectation that Resideo's smart home devices will be imported, distributed, advertised, offered for sale, and sold in the U.S. market. For example, at least Best Buy, Walmart, Home Depot, Lowe's, Target, and Amazon.com offer for sale and sell Resideo smart home devices, in and specifically for the U.S. market, via their own websites or retail stores located in and selling their products to consumers in Texas and this District. *See, e.g., Find A Resideo Retailer Near You*, RESIDEO, <https://www.resideo.com/us/en/find-a-retailer/> (showing where the Resideo's products are sold) (last visited Oct. 4, 2022). Moreover, Resideo products, such as at least Honeywell

Home™ branded products are offered for sale and sold in retail stores located in this District. *See, e.g., T9 WiFi 7-Day Programmable Smart Thermostat with Touchscreen Display and Smart Room Sensor*, HOME DEPOT, <https://www.homedepot.com/p/Honeywell-T9-WiFi-7-Day-Programmable-Smart-Thermostat-with-Touchscreen-Display-and-Smart-Room-Sensor-RCHT9610WFSW2003/312604036> (showing Resideo’s Honeywell Home product available for sale in Frisco). Resideo also provides its application software products and services, e.g., the “Resideo App,” the “Total Connect Comfort App,” and the “Total Connect 2.0 App” for download and use in conjunction with and as a part of smart home devices. *See Applications for Your Connected Products*, RESIDEO, <https://www.resideo.com/us/en/apps/> (listing available Resideo apps) (last visited Oct. 4, 2022). Resideo’s apps are available via digital distribution platforms operated by Apple Inc. and Google. *Id.*

17. Based on Defendant Resideo’s connections and relationship with its distributors, subsidiaries, including its wholly owned subsidiary Ademco, resellers, contractors, dealers, installers, local and U.S.- based national retailers, and digital distribution platforms, Resideo knows that Texas is a termination point of the established distribution channel for the sale and use of Resideo smart home products and related software to consumers in Texas. Resideo, therefore, has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court, at least on this basis. *See Icon Health & Fitness, Inc. v. Horizon Fitness, Inc.*, 2009 WL 1025467, at (E.D. Tex. 2009) (finding that “[a]s a result of contracting to manufacture products for sale in” national retailers’ stores, the defendant “could have expected that it could be brought into court in the states where [the national retailers] are located”).

18. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). As alleged herein, Defendant Resideo has committed acts of infringement in this District. As further

alleged herein, Defendant Resideo, via its own operations and employees located there and via ratification of Defendant Ademco's (i.e., ADI) presence and activities, including as an agent and alter ego of Resideo, has a regular and established place of business, in this District. Resideo's regular and established place of business is at 2601 Petty Place, Fort Worth, TX, 76177, which according to publicly available records is located in Denton County. Accordingly, Resideo may be sued in this district under 28 U.S.C. § 1400(b).

B. Defendant Ademco

19. On information and belief, Defendant Ademco is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. For example, Ademco is registered to do business in Texas, including registration to use the name "Resideo," which is the same name of its parent Resideo Technologies, Inc. Moreover, Ademco, including as an alter ego of parent company Resideo, owns and operates a logistics/ distribution facility where employees and/or agents of Defendants work to store, distribute, and sell Resideo products, including related administration of the business. This facility is located in Denton County at 2601 Petty Place, Fort Worth, TX, 76177.

20. Defendant Ademco further is responsible for importing, shipping, distributing, selling, offering for sale, delivering, and using Resideo's smart home devices, including Resideo® and Honeywell Home™ branded products and purposefully placing infringing smart home devices in established distribution channels in the stream of commerce in the U.S., including in Texas and this District. For example, Ademco, in concert with Resideo as part of the ADI Global Distribution segment, distributes its products to residents of Texas and this District, via distributors, professional contractors, original equipment manufacturers, dealers, retailers, and online merchants (including its own online store). *See Resideo, ADI, A RESIDEO COMPANY*, <https://www.adiglobaldistribution.us/Catalog/shop-brands/resideo> (showing Resideo products offered for sale via ADI's website) (last visited Oct. 4, 2022). Moreover, Ademco provides branch locations where residents of Texas and this District "shop and pick up anytime at an ADI locker" Resideo products sold to consumers via ADI's website. *See Shop Online, Pick Up Anytime, ADI, A RESIDEO COMPANY*, <https://www.adiglobaldistribution.us/pick-up-anytime> (last visited Oct. 6, 2022). Ademco also provides software applications such as the ADI app "for the easiest, fastest, access to products, account information and more." *See Access ADI Wherever You Go, ADI, A RESIDEO COMPANY*, <https://www.adiglobaldistribution.us/adi-app> (advertising that the app "makes browsing and shopping low-voltage products easier than ever"). Defendant Ademco, therefore, has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court.

21. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). As alleged herein, Defendant Ademco has committed acts of infringement in this District and has one or more regular and established places of business in this District, including the location listed above in Denton county. One such regular and established place of business is the Ademco facility located

at 2601 Petty Place, Fort Worth, TX, 76177, which Resideo and Ademco jointly utilize, via their employees and/or agents, to store, distribute, and sell Resideo products in this District, Texas, and the U.S. Accordingly, Defendant Ademco may be sued in this district under 28 U.S.C. § 1400(b).

22. On information and belief, Defendants Resideo and Ademco each have significant ties to, and presence in, the State of Texas and the Eastern District of Texas, making venue in this District both proper and convenient for this action.

THE ASSERTED PATENTS AND TECHNOLOGY

23. 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.

24. 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.

25. 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) 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.

26. On information and belief, a significant portion of the operating revenue of Defendants is derived from the manufacture and sale of smart home devices. For example, Defendant Resideo utilizes its distributors, subsidiaries, including its wholly owned subsidiary







Defendant Ademco, resellers, contractors, dealers, installers, retailers, and digital distribution platforms to provide smart home devices and related services to consumers. For the year 2020, Defendants reported \$2.46 billion in (external) revenue for the Products & Solutions segment and the ADI Global Distribution segment reported \$3.37 billion in external revenue with 14% of that supplied by the Products & Solutions segment. *See Resideo 2021 Annual Report* at 28, 32.

27. The Asserted Patents cover Defendants' smart home products and components, software, services, and processes related to same that generally connect to other devices in a network or other networks using a wireless protocol, such as Wi-Fi (collectively referred to herein as the "Accused Products"). *See All Smart Home Products*, RESIDEO, <https://www.resideo.com/us/en/products/> ("From WiFi connected, smart and programmable thermostats to humidifiers, home ventilation and air purifiers, shop Resideo to take control of what supports your home in making you feel more at home.") (last visited Oct. 4, 2022). Defendants' infringing Accused Products include, but are not limited to, devices enabled or compliant with Wi-Fi such as smart Wi-Fi connected and programmable thermostats and related kits, Wi-Fi security cameras, water leak & freeze detectors, Wi-Fi outdoor and indoor video cameras, video doorbells, security control panels and related accessories, including motion detectors, smoke detectors, communications modules. *See id.*

28. The Asserted Patents cover Accused Products of Defendants that utilize the Wi-Fi protocol. Examples of such products include Resideo's smart home "Air Products" such as Wi-Fi enabled thermostats, as shown below.

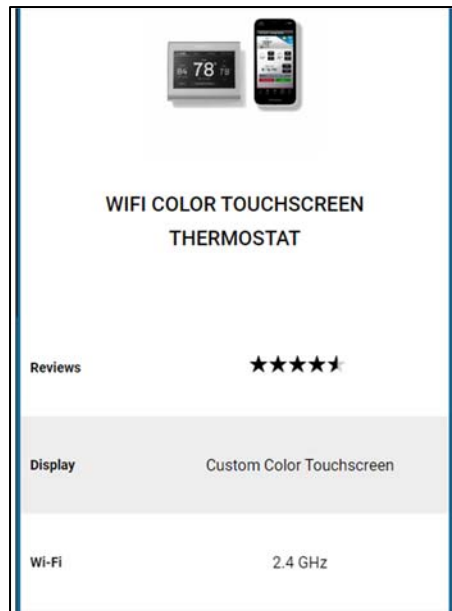
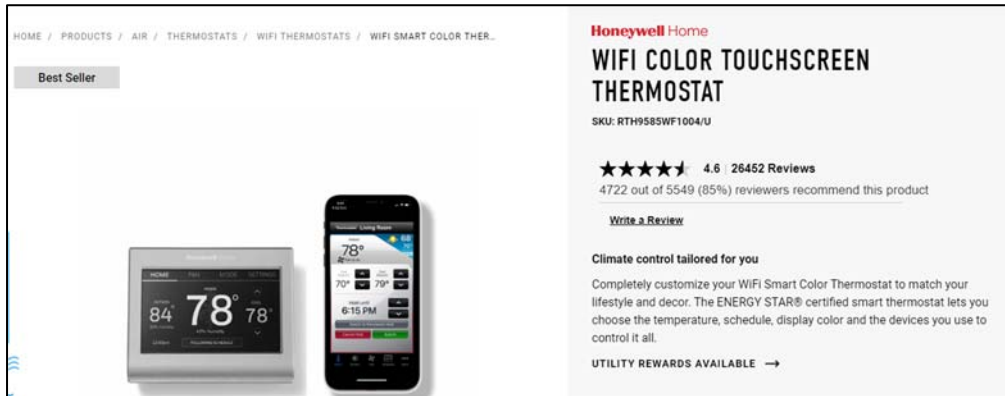
WIFI THERMOSTATS

With WiFi Thermostats like our Honeywell Home T9 Smart Thermostat, we bring you helpful, connected products so you can enjoy optimal comfort in your home. Shop online or connect with a Resideo Pro for consultation and installation to help manage energy costs while maintaining a comfortable temperature.

 <p>WIFI SMART COLOR THERMOSTAT \$179.99 ★★★★★ (26454)</p> <p><i>More options available</i></p> <p>ADD TO CART</p>	 <p>T9 SMART THERMOSTAT \$209.99 ★★★★★ (4783)</p> <p><i>More options available</i></p> <p>OUT OF STOCK</p>	 <p>T6 PRO SMART THERMOSTAT <i>Requires a pro for pricing, installation and warranty</i> ★★★★★ (108)</p> <p><i>More options available</i></p> <p>FIND A PRO</p>
 <p>WIFI 9000 COLOR TOUCHSCREEN THERMOSTAT <i>Requires a pro for pricing, installation and warranty</i> ★★★★★ (8753)</p> <p>FIND A PRO</p>	<p>Discontinued</p>  <p>THE ROUND® SMART THERMOSTAT \$249.00 ★★★★★ (100)</p> <p>FIND A RETAILER</p>	 <p>T5 SMART THERMOSTAT \$119.00 ★★★★★ (22)</p> <p><i>More options available</i></p> <p>ADD TO CART</p>

WiFi Thermostats, RESIDEO, <https://www.resideo.com/us/en/products/air/thermostats/wifi-thermostats/> (last accessed Oct. 5, 2022).

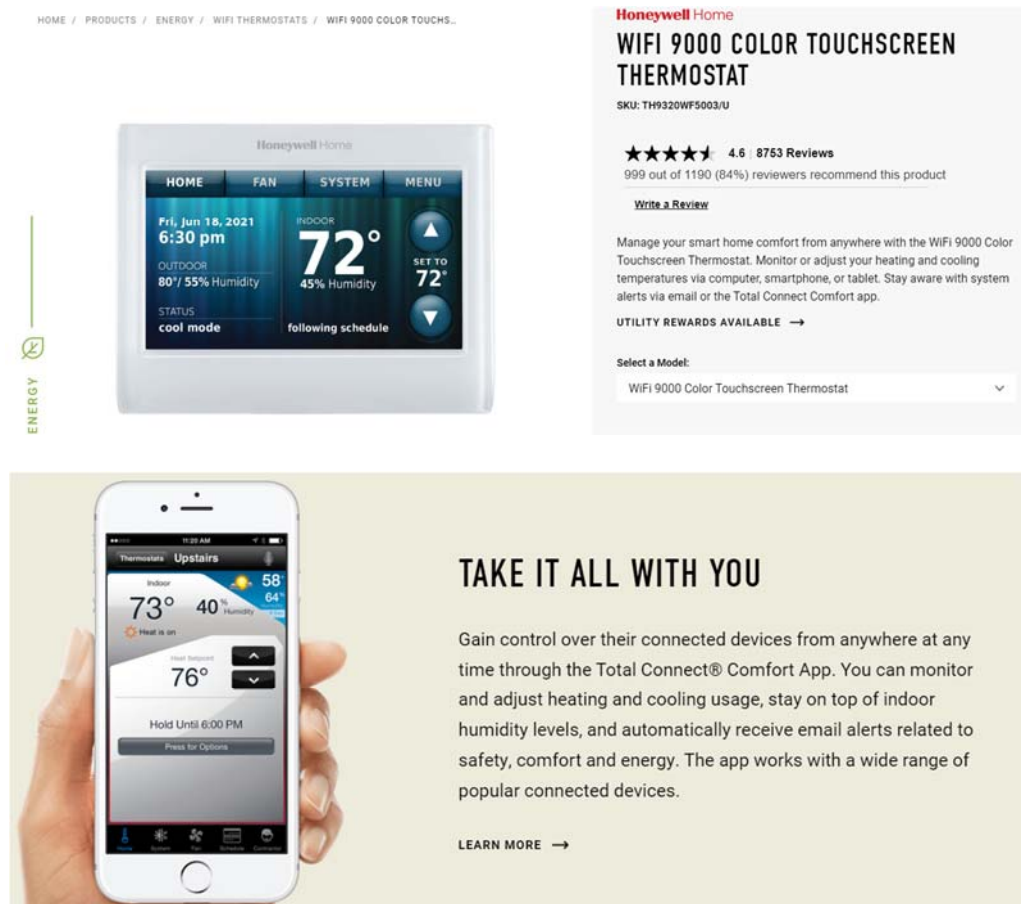
29. The Defendants’ Wi-Fi Color Touchscreen Thermostat, which functions with Resideo’s Total Connect Comfort App, is shown as Wi-Fi (IEEE 802.11) compliant.



WiFi Color Touchscreen Thermostat, RESIDEO,
<https://www.resideo.com/us/en/products/air/thermostats/wifi-thermostats/wifi-color-touchscreen-thermostat-rth9585wf1004-u/> (last accessed Oct. 5, 2022).

30. The Asserted Patents cover Accused Products of Defendants’ “Energy Wi-Fi Thermostats” which include products that are “WiFi connected [] to room sensors that constantly

monitor temperature.” For example, the WiFi 9000 Color Touchscreen Thermostat is shown as Wi-Fi enabled and is supported by Resideo’s Total Connect Comfort App.



WiFi 9000 Color Touchscreen Thermostat, RESIDEO,
<https://www.resideo.com/us/en/products/energy/wifi-thermostats/wifi-9000-color-touchscreen-thermostat-th9320wf5003-u/> (last visited Oct. 5, 2022).

31. Other examples of Defendants’ infringing products include Resideo’s smart home “Security Products” such as Wi-Fi security panels, cameras, and related kits, as shown below.

SECURITY SYSTEMS

Make your home or business security smarter with Honeywell Home security systems from Resideo. With connected options to automate system control, easy-to-use keypads and key fobs, wireless sensors and more, our security systems provide you with sophisticated solutions designed to work together seamlessly.

GOLD KIT \$608.95
★★★★★ (0)
ADD TO CART

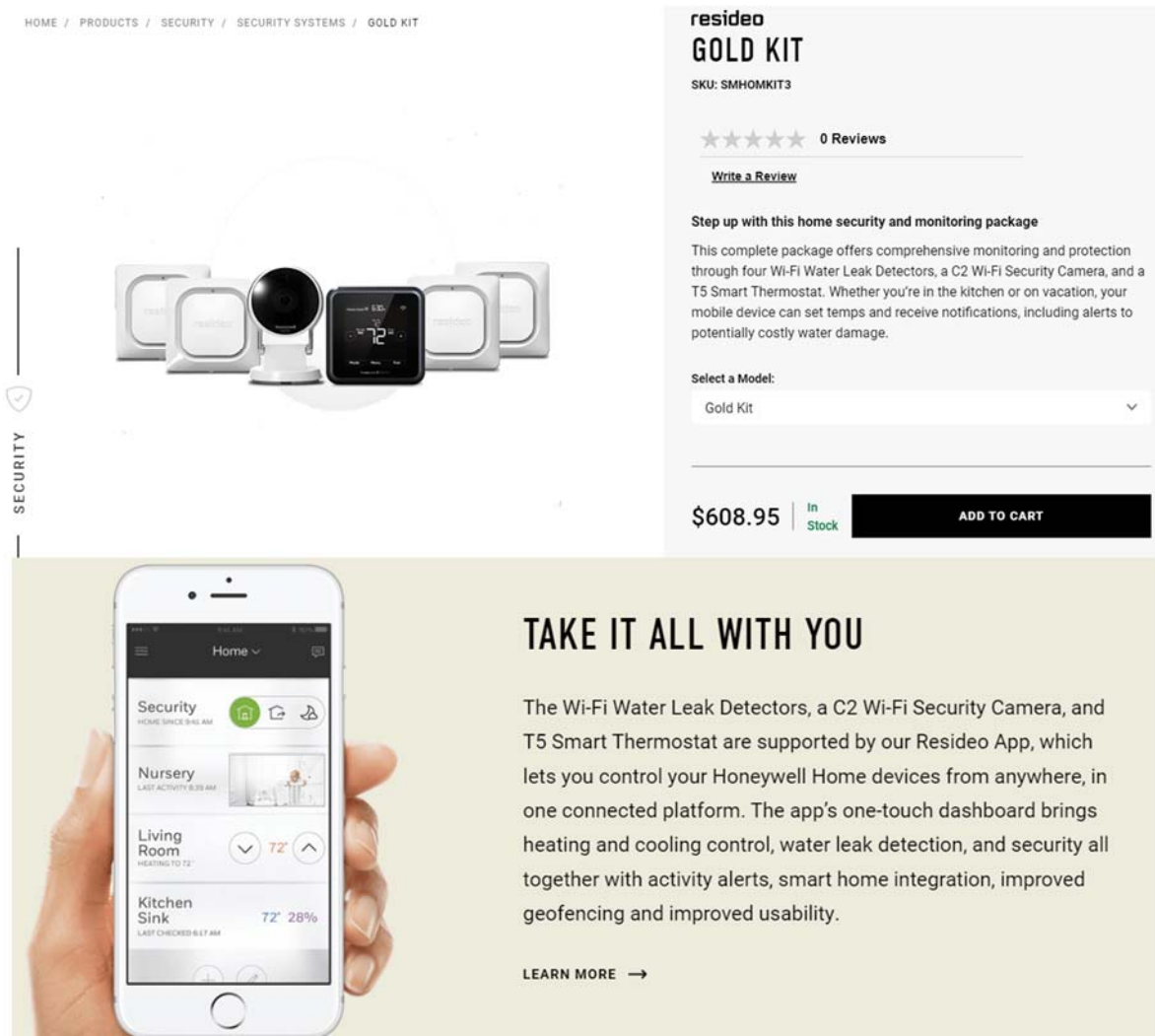
BRONZE KIT \$329.97
★★★★★ (0)
ADD TO CART

SILVER KIT \$489.95
★★★★★ (0)
ADD TO CART

PROA7 PROSERIES 7 INCH ALL-IN-PANEL **Requires a pro for pricing, installation and warranty.**
★★★★★ (0)
More options available
FIND A PRO

Security Systems, RESIDEO, <https://www.resideo.com/us/en/products/security/security-systems/> (last visited Oct. 5, 2022).

32. Resideo’s security kits, such as the “Gold Kit” shown below, include Wi-Fi enabled components—“Wi-Fi Water Leak Detectors, a C2 Wi-Fi Security Camera, and a T5 Smart Thermostat,” supported by the Resideo App.




Gold Kit, RESIDEO, <https://www.resideo.com/us/en/products/security/security-systems/gold-kit-smhomkit3/> (last visited Oct. 5, 2022).

33. Resideo’s Security Products include Wi-Fi enabled “Intrusion Panels & Systems,” “Keypads,” and “Controllers,” such as the L7000 Lynx Touch 7000, L5210 Lynx Touch, and Tuxedow Tuxedo Touch ® and Smart Controller, each shown below.

INTRUSION PANELS & SYSTEMS

Resideo's innovative line of control panels provides you with more the power, capacity and versatility to satisfy virtually any installation requirement from a single platform.



HOME / PRODUCTS / SECURITY / INTRUSION PANELS & SYSTEMS / ALL-IN-ONE SYSTEMS / LYNX™ TOUCH 7000


Honeywell Home L7000 LYNX TOUCH 7000

SKU: L7000

Low-cost Installs. High Customer Satisfaction.

All-in-One home and business control system featuring advanced automation functions and easy operation from one brilliant, 7" color touchscreen with graphic icons with intuitive prompts for easy operation. Seamlessly integrates with home security, lighting, thermostats, and more for control from home or away.

- On-premises video viewing
- Wi-Fi support



HOME / PRODUCTS / SECURITY / INTRUSION PANELS & SYSTEMS / ALL-IN-ONE SYSTEMS / LYNX TOUCH 5210


Honeywell Home L5210 LYNX TOUCH

SKU: L5210

Simple Home and Business Automation

All-in-One system brings value with a crystal clear, 4.3" color touchscreen with graphic icons and intuitive prompts for easy operation. This smart home security system with Wi-Fi® uses remote services to save install time and reduce monthly costs.

- On-premises video viewing
- Wi-Fi support



HOME / PRODUCTS / SECURITY / KEYPADS / GRAPHIC TOUCHSCREEN / TUXEDO TOUCH® SECURITY ..

resideo TUXEDOW TUXEDO TOUCH® SECURITY AND SMART CONTROLLER (HONEYWELL HOME)

SKU: TUXEDOW

Resideo's Tuxedo Touch® Controller is an innovative 7" color touchscreen keypad with smart control that helps dealers increase system add-on revenue, drive additional RMR and reduce attrition. Users can control thermostats, lights, locks, doors, garage doors and more with either 500 or 300 Z-Wave® series peripherals, as well as recording and viewing IP cameras directly on the display or through Resideo Total Connect.


Communication Type Z-Wave, WiFi

See *Intrusion Panels & Systems*, RESIDEO, <https://www.resideo.com/us/en/pro/products/security/intrusion-panels-systems/#first=12> (last visited Oct. 5, 2022); *Security Keypads*, RESIDEO, <https://www.resideo.com/us/en/pro/products/security/keypads/> (last visited Oct. 5, 2022).

19

PLAINTIFF’S ORIGINAL COMPLAINT
FOR PATENT INFRINGEMENT

34. Other Resideo “Security Products” that are Wi-Fi enabled are the LCP500-L Lyric® Controller Touchscreen Control Panel, the LKP500-EN Lyric® Keypad, the Prosixpir – Proseries Wireless Motion Detector, as shown below.




HOME / PRODUCTS / SECURITY / INTRUSION PANELS & SYSTEMS / ALL-IN-ONE SYSTEMS / LYRIC CONTROLLER

Honeywell Home

LCP500-L LYRIC® CONTROLLER TOUCHSCREEN CONTROL PANEL

SKU: LCP500-L

Serves as the central hub for security and lifestyle management including: lights, locks, thermostats and more for homes and businesses—controlled wirelessly from a dynamic, 7-inch display or remotely on smart devices. Lyric is Wi-Fi® enabled, features easy installation and delivers a great user experience right out of the box.



HOME / PRODUCTS / SECURITY / KEYPADS / WIRELESS KEYPADS / LYRIC KEYPAD FOR HONEYWELL


Honeywell Home

LKP500-EN LYRIC® KEYPAD FOR HONEYWELL HOME LYRIC CONTROLLER

SKU: LKP500-EN

Optimized for the Lyric Controller, the Lyric Keypad enables easy, on-premises security system control for the ultimate convenience and flexibility. Sleek and stylish, it blends with any décor and can be mounted on the wall or placed on tabletops, nightstands or virtually anywhere in the home.

WIFI Yes



HOME / PRODUCTS / SECURITY / PROSERIES / SECURITY AND SAFETY / MOTION SENSOR / PROSERIES WIRELESS MOTI...

Honeywell Home

PROSIXPIR - PROSERIES WIRELESS MOTION DETECTOR

SKU: PROSIXPIR

Motion Detection for the Whole Security System

Designed for systems that support SIX Two-Way Wireless Technology, these devices deliver faster installation, easier troubleshooting, remote diagnostics and increased RMR. The suite of next-generation devices includes motion, smoke and glassbreak detectors, door/window sensors, two-way wireless key and siren.





WIFI Yes

See All-in-one-systems, resideo pro, <https://www.resideo.com/us/en/pro/products/security/intrusion-panels-systems/all-in-one-systems/> (last visited Oct. 5, 2022); Security Keypads, RESIDEO PRO, <https://www.resideo.com/us/en/pro/products/security/keypads/> (last visited Oct. 5, 2022); Prosixpir – Proseries Wireless Motion Detector, RESIDEO PRO, <https://www.resideo.com/us/en/pro/products/security/proseries/security-and-safety/motion-sensor/prosixpir-proseries-wireless-motion-detector-prosixpir/> (last visited Oct. 5, 2022).

35. Other examples of Defendants’ infringing products include Resideo’s smart home “Water Management Products” such as water leak & freeze detectors and related products, as shown below.

SMART HOME WATER MANAGEMENT PRODUCTS

With smart water monitoring systems like WiFi water leak detectors and remote water shut off capabilities, shop Resideo to take control of how you support your water usage and protect your home. Shop online or connect with a Resideo Pro for a consultation, recommendations and installation.

 <p>WATER LEAK & FREEZE DETECTOR \$79.99 ★★★★★ (5431) <i>More options available</i> ADD TO CART</p>	 <p>T5 SMART THERMOSTAT AND LEAK PROTECTION KIT \$358.97 ★★★★★ (0) ADD TO CART</p>
 <p>WIFI COLOR THERMOSTAT AND LEAK PROTECTION KIT \$408.97 ★★★★★ (0) ADD TO CART</p>	 <p>WHOLE HOME COMFORT AND LEAK PROTECTION KIT \$439.96 ★★★★★ (0) OUT OF STOCK</p>

Smart Home Water Management Products, RESIDEO,
<https://www.resideo.com/us/en/products/water/#first=12> (last visited Oct. 5, 2022).

36. Resideo's Wi-Fi Leak & Freeze Detector is shown as Wi-Fi enabled and is supported by the Resideo App, as shown below.

HOME / PRODUCTS / WATER / SPOT LEAK DETECTION / WATER LEAK & FREEZE DE...

resideo
WIFI WATER LEAK & FREEZE DETECTOR
SKU: RCHW3610WF1001/U

★★★★☆ 4.2 | 5431 Reviews
363 out of 505 (72%) reviewers recommend this product

[Write a Review](#)

Always on duty
The Water Leak & Freeze Detector keeps you connected and aware of potentially costly water leaks in your home. Whether you're in the kitchen or on vacation you can receive notifications when a pipe freezes or a leak is detected.

Select a Model:
WiFi Water Leak & Freeze Detector

\$79.99 In Stock **ADD TO CART**

WORKS WITH YOUR WIFI

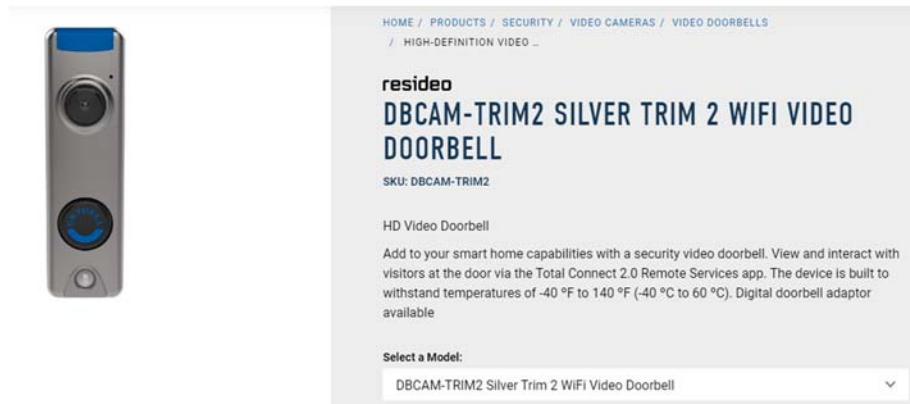
You already have what you need. This water leak sensor works with your WiFi — no need for an extra hub. Simply connect to your Resideo app, and you'll be able to access all alerts and updates. Plus, the app guides you through device setup, making installation quick and easy.

Wi-Fi Leak & Freeze Detector, RESIDEO, <https://www.resideo.com/us/en/products/water/spot-leak-detection/wifi-water-leak-freeze-detector-rchw3610wf1001-u/> (last visited Oct. 5, 2022).

37. Resideo also provides video cameras and video doorbells that are Wi-Fi (IEEE 802.11) compliant, e.g., the IPCAM-WIC2 HD Wi-Fi, IPCAM-WO2 HD Wi-Fi, and DBCAM-Trim2 Silver Trim 2 Wi-Fi Video Doorbell products shown below.



Security Connected Cameras, RESIDEO, <https://www.resideo.com/us/en/pro/products/security/video-cameras/connected-cameras/> (last visited Oct. 5, 2022).



DBCAM-Trim2 Silver Trim 2 WiFi Video Doorbell, RESIDEO, <https://www.resideo.com/us/en/pro/products/security/video-cameras/video-doorbells/dbcam-trim2-silver-trim-2-wifi-video-doorbell-dbcam-trim2/> (last visited Oct. 5, 2022).

38. The Accused Products utilize intrusion detection methods for a local or metropolitan area network to infringe at least the '678 and '572 patents. For example, the IEEE 802.11 authentication methods utilized by the Accused Products include a TKIP-based method, as explained below, that uses 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>

39. 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 and CCMP) 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>

40. In the TKIP method 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>

41. 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>

42. 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.

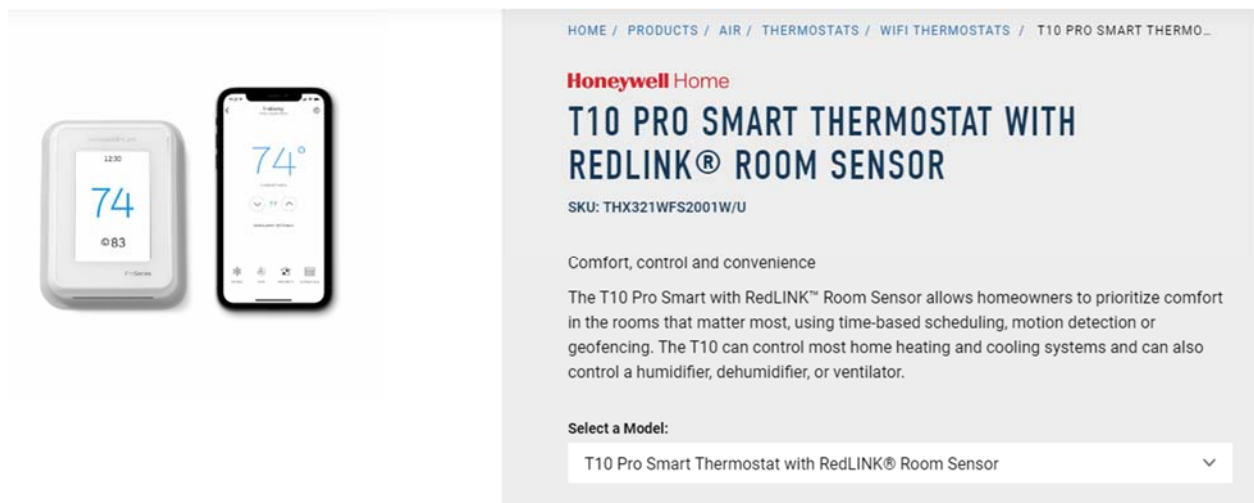
If a subsequent MIC failure occurs within 60 s of the most recent previous failure, then a STA whose IEEE 802.1X entity has acted as a Supplicant shall deauthenticate (as defined in 11.3.1.3) itself or deauthenticate all the STAs with a security association if its IEEE 802.1X entity acted as an Authenticator.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

43. The Asserted Patents cover Resideo's Wi-Fi compliant devices, which support WPA, WPA2 and WPA3 security mechanisms, as described below and in the following paragraphs.

The WPA mechanism is based on Temporal Key Integrity Protocol (TKIP), while the WPA2 and WPA3 are based on Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP).

44. Resideo configures its infringing smart home devices to not only connect to Wi-Fi compliant networks, but also to utilize authentication techniques such as WPA (TKIP) and WPA2 (CCMP) for secure connections to those wireless networks. As shown below, Resideo's T10 Pro Smart Thermostat is configured to connect to wireless networks via Wi-Fi.



T10 Pro Smart Thermostat with Redlink Room Sensor, RESIDEO PRO, <https://www.resideo.com/us/en/pro/products/air/thermostats/wifi-thermostats/t10-pro-smart-thermostat-with-redlinkr-room-sensor-thx321wfs2001w-u/#specifications> (last visited Oct. 5, 2022).

45. As shown below, Resideo’s T10 Pro Smart Thermostat product is not only certified by the Wi-Fi Alliance for 802.11 a, b, g, and h connectivity, but also is certified to utilize security measures such as “WPA2 – Personal 2021-01” and “WPA-Personal” for 802.11 secure connections.



Wi-Fi CERTIFIED™ Certificate



This certificate lists the features that have successfully completed Wi-Fi Alliance interoperability testing. Learn more: www.wi-fi.org/certification/programs

Certification ID: WFA121299

Product Info

Date of Certification	August 26, 2022
Company	Resideo
Product Name	T10+ Pro Smart Thermostat
Product Model Variant	THX321WF3003W
Model Number	THX321WF3003W
Category	Smart Home
Sub-category	Thermostat

Summary of Certifications

CLASSIFICATION	CERTIFICATION
Connectivity	2.4 GHz Spectrum Capabilities 5 GHz Spectrum Capabilities Wi-Fi CERTIFIED™ a Wi-Fi CERTIFIED™ b Wi-Fi CERTIFIED™ g Wi-Fi CERTIFIED™ n
Optimization	WMM®
Security	Protected Management Frames WPA2™-Personal 2021-01 WPA™-Personal

Product Finder, WI-FI ALLIANCE, <https://www.wi-fi.org/product-finder-results?subcategories=34> (listing certifications in the “Smart Home” category and providing a link to download Certification ID: WFA121299) (last accessed Oct. 5, 2022).

46. Moreover, Resideo indicates in its “Troubleshooting” page that at least its smart home security and camera device products use “one of the following security protocols” including “WPA TKIP PSK,” WPA2 AES PSK,” and “WPA2 MIXED PSK”:

MY WI-FI IS NOT WORKING ON MY SMART HOME SECURITY OR CAMERA DEVICE

Last updated 8/29/22

Advanced Troubleshooting

1. Connect to a 2.4 GHz network with its own Network Name (SSID).
2. Make sure the Wi-Fi router is set for DHCP, No Static Networks. Refer to your router support or Internet Service Provider for assistance.
3. Make sure Wi-Fi network is using one of the following security protocols. Other security protocols are not recommended.
 - OPEN
 - WEP PSK
 - WPA TKIP PSK
 - WPA2 AES PSK
 - WPA2 MIXED PSK

My Wi-Fi Is Not Working On My Smart Home Security Or Camera Device, RESIDEO, <https://www.honeywellhome.com/us/en/support/my-wi-fi-is-not-working-on-my-smart-home-security-or-camera-device/> (last visited Oct. 5, 2022).

47. As shown above, the Accused Products provide wireless connectivity utilizing the 802.11 protocols at one or both of 2.4 GHz and/or 5 GHz Wi-Fi speeds. This capability ascertains the presence of a MAC controller, a Wi-Fi antenna, and a transceiver in the device and provides a secure wireless LAN.

48. The Accused Products further utilize a cryptography circuit that implements the 802.11 protocols authentication techniques, including TKIP and CCMP. Shown below is a block diagram from the 802.11 protocol documentation showing the TKIP-based cryptography circuit (such as used with WPA) that is 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.

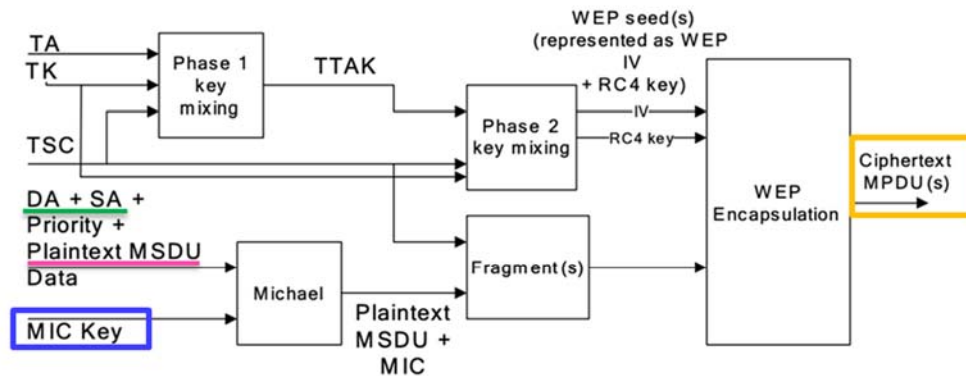


Figure 8-4—TKIP encapsulation block diagram

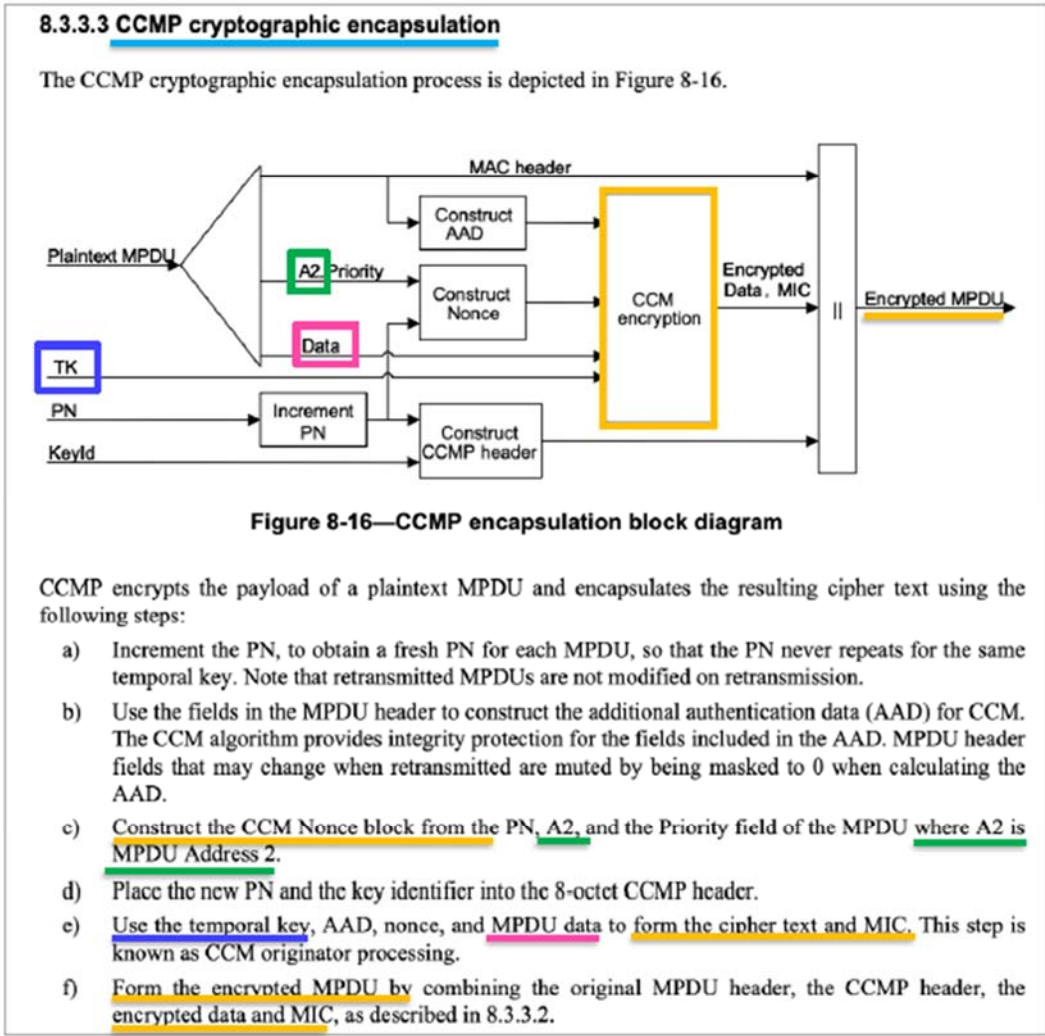
- a) TKIP MIC computation protects the MSDU Data field and corresponding SA, DA, and Priority fields. The computation of the MIC is performed on the ordered concatenation of the SA, DA, Priority, and MSDU Data fields. The MIC is appended to the MSDU Data field. TKIP discards any MIC padding prior to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

49. Shown below is a block diagram from the 802.11 protocol documentation showing the CCMP-based cryptography circuit (such as used with WPA2) that is utilized in the Accused Products. The circuit shown encrypts both address (A2 – MPDU address 2) and data information (plaintext MPDU) by adding encryptions bits (temporal key (TK)) to both the address and data. The

cryptography circuit of the Accused Products is also configured to decrypt the encrypted address and data information.

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



Page 229, <https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf>

COUNT I

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

50. Plaintiff incorporates paragraphs 1 through 49 herein by reference.

51. 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.

52. 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.

53. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '678 patent in this District and elsewhere in Texas and the United States.

54. On information and belief, Defendants design, develop, manufacture, import, distribute, offer to sell, sell, and use the Accused Products, including via the activities of Resideo and its subsidiaries, members, segments, companies, brands and/or related entities, such as Defendant Ademco and U.S.-based subsidiaries, members, segments, companies and/or brands of Defendants.

55. Defendants each directly infringe the '678 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '678 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs, installers, and/or consumers. Furthermore, on information and belief, Defendants design the Accused Products for U.S. consumers, make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners,

retailers, showrooms, resellers, dealers, installers, customers and other related service providers in the United States, or in the case that it delivers the Accused Products outside of the United States it does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the '678 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to “whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers ... constitute an infringing sale under § 271(a)”).

56. Furthermore, Defendant Resideo directly infringes the '678 patent through its direct involvement in the activities of its subsidiaries, and related entities, including Defendant Ademco, and other U.S.-based subsidiaries, members, segments, companies and/or brands of Defendant Resideo, including by designing the Accused Products for U.S. consumers and selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. On information and belief, U.S.-based subsidiaries, including at least Ademco, conduct activities that constitute direct infringement of the '678 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants. Defendant Resideo is vicariously liable for the infringing conduct of Defendant Ademco and other U.S.-based subsidiaries, members, segments, companies and/or brands of Resideo (under both the alter ego and agency theories). On information and belief, Defendants Resideo, Ademco, and other U.S. based subsidiaries members, segments, companies and/or brands of Resideo are essentially the same company, comprising members, segments, companies and/or brands of Resideo, including the “Products & Solutions” and “ADI Global Distribution” segments of Resideo. Moreover, Resideo, as the parent company,

along with its related entities, has the right and ability to control the infringing activities of those subsidiary entities such that Defendants Resideo and Ademco receive a direct financial benefit from that infringement.

57. For example, Defendants infringe claim 51 of the '678 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 such as smart Wi-Fi connected and programmable thermostats and related kits, Wi-Fi security cameras, water leak & freeze detectors, Wi-Fi outdoor and indoor video cameras, video doorbells, security control panels and related accessories, including motion detectors, smoke detectors, communications modules, and related accessories and software applications.

58. 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.

59. At a minimum, Defendants have known of the '678 patent at least as early as the filing date of this complaint. In addition, Defendants have known about their infringement of Harris Corporation's (“Harris”) patent portfolio, which includes the '678 patent, since at least its receipt

of a letter from Acacia Research Corporation to Resideo, dated June 22, 2020. The letter notifies Resideo that its products practice the Wi-Fi technologies covered by the Stingray patent portfolio.

60. On information and belief, since at least the above-mentioned date when Defendants were on notice of their infringement, Defendants have each actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, installers, OEMs, consumers, and other related service providers that import, distribute, purchase, offer for sale, sell, or use the Accused Products that include or are made using all of the limitations of one or more claims of the '678 patent to directly infringe one or more claims of the '678 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the date of notice provided above, Defendants each conduct 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 each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMS, installers, consumers, and other related service providers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing and certifying (with for example the Wi-Fi Alliance and the FCC) wireless networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g., Resideo Help & Support*, RESIDEO, <https://www.resideo.com/us/en/support/> (providing links where consumers may access instructions for using Resideo's products) (last visited Oct. 6, 2022).

Furthermore, Defendants market and offer smartphone and tablet interfaces as application software (i.e., apps) to provide access to the Accused Products, connect such products to wireless networks, including Wi-Fi networks, remote control of the Accused Products, and other services supporting use of the Accused Products. *See, e.g., Applications for Your Connected Products*, resideo, <https://www.resideo.com/us/en/apps/> (providing to consumers a description of and links for downloading “the right app that works with your Honeywell Home and Resideo products”) (last visited Oct. 6, 2022); *Access ADI Wherever You Go*, ADI, A RESIDEO COMPANY, <https://www.adiglobaldistribution.us/adi-app> (providing to consumers links for downloading “the ADI app for the easiest, fastest, access to products, account information and more”) (last visited Oct. 6, 2022). Such compatibility provides convenience and added functionality that induces consumers to use the Defendants’ products, including via the smartphone and tablet Wi-Fi apps and other interfaces utilizing Wi-Fi protocols in networks with other third-party devices. Thus, these activities further infringe or induce infringement of the ’678 patent.

61. On information and belief, despite having knowledge of the ’678 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ’678 patent, Defendants have 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, 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.

62. Plaintiff Stingray has been damaged as a result of Defendants’ 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)

63. Plaintiff incorporates paragraphs 1 through 62 herein by reference.

64. 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.

65. 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.

66. Defendants have and continue 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.

67. On information and belief, Defendants design, develop, manufacture, import, distribute, offer to sell, sell, and use the Accused Products, including via the activities of Resideo and its subsidiaries, members, segments, companies, brands and/or related entities, such as Defendant Ademco and U.S.-based subsidiaries, members, segments, companies and/or brands of Defendants.

68. Defendants each directly infringe the '572 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '572 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs,

installers, and/or consumers. Furthermore, on information and belief, Defendants design the Accused Products for U.S. consumers, make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, installers, customers and other related service providers in the United States, or in the case that it delivers the Accused Products outside of the United States it does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the '572 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to “whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers ... constitute an infringing sale under § 271(a)”).

69. Furthermore, Defendant Resideo directly infringes the '572 patent through its direct involvement in the activities of its subsidiaries, and related entities, including Defendant Ademco, and other U.S.-based subsidiaries, members, segments, companies and/or brands of Defendant Resideo, including by designing the Accused Products for U.S. consumers and selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. On information and belief, U.S.-based subsidiaries, including at least Ademco, conduct activities that constitute direct infringement of the '572 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants. Defendant Resideo is vicariously liable for the infringing conduct of Defendant Ademco and other U.S.-based subsidiaries, members, segments, companies and/or brands of Resideo (under both the alter ego and agency theories). On information and belief, Defendants Resideo, Ademco, and other U.S. based subsidiaries members,

segments, companies and/or brands of Resideo are essentially the same company, comprising members, segments, companies and/or brands of Resideo, including the “Products & Solutions” and “ADI Global Distribution” segments of Resideo. Moreover, Resideo, as the parent company, along with its related entities, has the right and ability to control the infringing activities of those subsidiary entities such that Defendants Resideo and Ademco receive a direct financial benefit from that infringement.

70. For example, Defendants infringe claim 1 of the '572 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 such as smart Wi-Fi connected and programmable thermostats and related kits, Wi-Fi security cameras, water leak & freeze detectors, Wi-Fi outdoor and indoor video cameras, video doorbells, security control panels and related accessories, including motion detectors, smoke detectors, communications modules, and related accessories and software applications.

71. 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.

72. At a minimum, Defendants have known of the '572 patent at least as early as the filing date of this complaint. In addition, Defendants have known about their infringement of Harris Corporation's ("Harris") patent portfolio, which includes the '572 patent, since at least its receipt of a letter from Acacia Research Corporation to Resideo, dated June 22, 2020. The letter notifies Resideo that its products practice the Wi-Fi technologies covered by the Stingray patent portfolio.

73. On information and belief, since at least the above-mentioned date when Defendants were on notice of their infringement, Defendants have each actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, installers, OEMs, consumers, and other related service providers that import, distribute, purchase, offer for sale, sell, or use the Accused Products that include or are made using all of the limitations of one or more claims of the '572 patent to directly infringe one or more claims of the '572 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the date of notice provided above, Defendants each 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 each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMS, installers, consumers, and other related service providers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing and certifying (with for example the Wi-Fi Alliance and the FCC) wireless networking features in the Accused Products, and/or providing technical support,

replacement parts, or services for these products to purchasers in the United States. *See, e.g., Resideo Help & Support*, RESIDEO, <https://www.resideo.com/us/en/support/> (providing links where consumers may access instructions for using Resideo’s products) (last visited Oct. 6, 2022). Furthermore, Defendants market and offer smartphone and tablet interfaces as application software (i.e., apps) to provide access to the Accused Products, connect such products to wireless networks, including Wi-Fi networks, remote control of the Accused Products, and other services supporting use of the Accused Products. *See, e.g., Applications for Your Connected Products*, resideo, <https://www.resideo.com/us/en/apps/> (providing to consumers a description of and links for downloading “the right app that works with your Honeywell Home and Resideo products”) (last visited Oct. 6, 2022); *Access ADI Wherever You Go*, ADI, A RESIDEO COMPANY, <https://www.adiglobaldistribution.us/adi-app> (providing to consumers links for downloading “the ADI app for the easiest, fastest, access to products, account information and more”) (last visited Oct. 6, 2022). Such compatibility provides convenience and added functionality that induces consumers to use the Defendants’ products, including via the smartphone and tablet Wi-Fi apps and other interfaces utilizing Wi-Fi protocols in networks with other third-party devices. Thus, these activities further infringe or induce infringement of the ’572 patent.

74. 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.

75. Plaintiff Stingray has been damaged as a result of Defendants' 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

76. 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.

77. 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

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

PRAYER FOR RELIEF

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

- A. A judgment that Defendants have infringed the Asserted Patents as alleged herein, directly and/or indirectly by way of inducing infringement of such patents;
- B. A judgment for an accounting of damages sustained by Plaintiff as a result of the acts of infringement by Defendants;

- C. 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;
- D. A judgment and order requiring Defendants to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;
- E. 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
- F. Such other and further relief as the Court deems just and equitable.

Dated: October 26, 2022

Respectfully submitted,

/s/ Jeffrey R. Bragalone

Jeffrey R. Bragalone (lead attorney)

Texas Bar No. 02855775

E-mail: jbragalone@bosfirm.com

Terry A. Saad

Texas Bar No. 24066015

E-mail: tsaad@bosfirm.com

Marcus Benavides

Texas Bar No. 24035574

E-mail: mbenavides@bosfirm.com

Brandon V. Zuniga

Texas Bar no. 24088720

E-mail: bzuniga@bosfirm.com

Paul C. Stevenson

Texas Bar No. 24117098

E-mail: pstevenson@bosfirm.com

BRAGALONE OLEJKO SAAD PC

901 Main Street

Suite 3800

Dallas, Texas 75202

Telephone: (214) 785-6670

Facsimile: (214) 785-6680

**ATTORNEYS FOR PLAINTIFF
STINGRAY IP SOLUTIONS LLC**