

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

STINGRAY IP SOLUTIONS LLC,

Plaintiff,

v.

Vivint, Inc.,

Defendant.

§  
§  
§  
§  
§  
§  
§  
§  
§  
§

CASE NO. \_\_\_\_\_

JURY TRIAL DEMANDED

**PLAINTIFF’S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT**

Plaintiff Stingray IP Solutions LLC (“Stingray”) files this Original Complaint in this Eastern District of Texas (the “District”) against Defendant Vivint, Inc. d/b/a Vivint (“Defendant” or “Vivint”) for infringement of U.S. Patent No. 7,224,678 (the “’678 patent”), U.S. Patent No. 7,440,572 (the “’572 patent”), U.S. Patent No. 7,441,126 (“the “’126 patent”), and U.S. Patent No. 7,616,961 (“the “’961 patent”) (these patents collectively referred to as the “Asserted Patents”).

**THE PARTIES**

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

2. On information and belief, Defendant Vivint, Inc. is a company organized under the laws of Utah, USA, with its principal place of business located at 4931 North 300 West, Provo, Utah, USA 84604. Vivint, Inc. may be served with process via its registered agents, including C T Corporation System, 1999 Bryan Street, Suite 900, Dallas, TX, USA 75201-3136.

3. On information and belief, Vivint, Inc. is a wholly owned subsidiary of Vivint Smart Home, Inc. (“VSH”). VIVINT SMART HOME, INC., *Form 10-K Annual Report For the Fiscal Year Ended December 31, 2022*, Ex. 21.1, (Feb. 24, 2023), available for download at

<https://www.sec.gov/Archives/edgar/data/1713952/000171395223000008/ck0001713952-20221231.htm> [hereinafter “*Vivint Annual Report*”]. The Vivint Annual Report asserts that “Vivint Smart Home, Inc., and its wholly owned subsidiaries, (collectively the “Company”), is one of the largest smart home companies in the United States” and “[t]he Company is engaged in the sale, installation, servicing and monitoring of smart home and security systems.” *Id.* at 80.

4. “[Vivint] provide[s] a fully integrated solution for consumers with [its] vertically integrated business model which includes hardware, software, sales, installation, support and professional monitoring.” *Id.* at 9. “This model” enabled Vivint “to deliver . . . a complete end-to-end smart home experience.” *Id.* For example, [Vivint] help[s] consumers create a customized solution for their home by integrating smart cameras (indoor, outdoor, doorbell), locks, lights, thermostats, garage door control, car protection and a host of safety and security sensors.” *Id.* at 9.

5. “Some of [Vivint’s] key products include: Vivint Smart Hub - a 7-inch touchscreen hub that seamlessly connects all smart home devices and makes it easy to control the home[,] Vivint Smart Home App – a single mobile app to control all of the smart home devices in a comprehensive Vivint smart home[,] Vivint Doorbell Camera Pro – an AI-powered doorbell camera with advanced analytics and Smart Deter technology to intelligently detect packages and actively help protect them from porch pirates and other potential threats[,] Vivint Outdoor Camera Pro – an AI-powered security camera that uses advanced analytics and Smart Deter technology to intelligently detect and deter lurkers around the home[,] Vivint Indoor Camera – an indoor camera with two-way talk and one-touch callout so families can easily connect and communicate[,] Vivint Smart Thermostat – a thermostat that provides a new level of intelligence for temperature control and energy savings by integrating with all the door, window and motion sensors in a Vivint smart home[,] Vivint Car Guard – a first-of-its-kind service that allows homeowners to manage the

security of both their home and car with a single app[, and] Vivint Spotlight Pro – an enhancement of the Vivint Outdoor Camera Pro which adds intelligent lighting including smart deter technology by adding person tracking, enhanced lighting deterrence behaviors, and elegant, intelligent everyday outdoor lighting.” *Id.* at 11-12.

6. “[Vivint’s] range of other devices, including smart locks, garage door control, door and window sensors, motion sensors, glass break detectors, key fobs, emergency pendants, smoke and carbon monoxide detectors and water sensors, extend the smart home experience to every part of the home, connecting users to their environments in new ways.” *Id.* at 12. “In July 2021, [Vivint] announced a partnership with Freedom Forever, one of the country’s leading solar installers” that “enables Freedom Forever to include a Vivint smart home system with each of its solar sales.” *Id.*

7. “For the years ended December 31, 2022, 2021 and 2020, the [Vivint Smart Home, Inc.] conducted business through one operating segment, Vivint.” *Id.* at 114. However, Vivint Smart Home, Inc., asserts that “[Vivint Smart Home, Inc.] is not a commercial entity, and [its subsidiary] Vivint, Inc., . . . is the entity that sells products.” *SB IP Holdings LLC v. Vivint Smart Home, Inc.*, No. 4:21-cv-00912-ALM, Dkt. No. 6, pp. 6-7 (E.D. Tex. January 18, 2022) (representations found in Defendant Vivint Smart Home, Inc.’s Brief in Support of its Motion to Dismiss).

8. On information and belief, Defendant Vivint, Inc. is the primary operating entity for parent Vivint Smart Home, Inc. and sells a large volume of products. For example, the Vivint Annual Report states that “Vivint Smart Home is a leading smart home platform company serving approximately 1.9 million subscribers as of December 31, 2022” and “on average, the subscribers on [Vivint’s] cloud-based home platform had approximately 15 security and smart home devices in each home.” *Vivint Annual Report* at 9. Consequently, “[Vivint’s] cloud-based home platform

[] manages more than 27 million in-home devices as of December 31, 2022.” *Id.* Vivint’s sales include “Direct-to-Home Sales.” *Id.* at 13.

9. For the years ending December 31, 2022, 2021, and 2020, Vivint operated primarily in the United States and Canada, however, in the United States alone, Vivint had revenue during these years of over \$1.659 billion, \$1.418 billion, and \$1.186 billion, respectively. *Id.* at 114. On June 8, 2022, the Company completed the sale of its Canada business, leaving operations primarily in the United States. *See id.*

10. Vivint’s “headquarters, and one of [its] two monitoring facilities, are located in Provo, Utah.” *Id.* at 44. “[Vivint] lease[s] the premises for a separate monitoring station located in Eagan, Minnesota” and “also ha[s] facility leases in Lehi, Utah; Lindon, Utah; Logan, Utah; Boston, Massachusetts; and various other locations throughout the United States for research and development, call center, warehousing, recruiting, and training purposes.” *Id.* Vivint “control[s] the design, interoperability and quality of [its] Products” and also implements “remote software or firmware updates” for its customers. *Id.* at 49, 51.

11. On information and belief, Vivint, Inc., along with its parents, subsidiaries, members, segments, companies, brands and/or related entities, for example, U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities, is engaged in “research and development” (including, for example, “Continuous innovation” at various “innovation centers” in the United States, *see id.* at 11), importation (*id.* at 27), “end-to-end distribution” (*id.* at 9), “sales” (*id.*), “installation” (*id.*), “support” (*id.*), “professional monitoring” (*id.*) and “adjacent products and services” (*id.*). Vivint’s “nationwide sales and service footprint covers the majority of U.S. zip codes.” *Id.* at 13. Vivint’s products are manufactured outside the U.S. and then imported into the United States or manufactured inside the U.S., 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.

12. On information and belief, Vivint maintains a corporate presence in the United States, including in Texas and in this District, via at least Vivint, Inc. d/b/a Vivint, which is a Utah company having multiple offices in this District, including at least offices located at 1115 W. Hickory Street, Suite 105, Denton, Texas 76201 in Denton County, Texas; 16440 Gateway Dr, Frisco, Texas 75035 in Collin County, Texas; 5212 Tennyson Pkwy Suite 150, Plano, TX 75024 in Collin County, Texas. *See, e.g., VIVINT, INC., Vivint Denton Service Area*, <https://www.vivint.com/locations/texas/denton> (last visited Sep. 7, 2023); *VIVINT, INC., Vivint Frisco Service Area*, <https://www.vivint.com/locations/texas/frisco> (last visited Sep. 7, 2023); *VIVINT, INC., Vivint Plano Service Area*, <https://www.vivint.com/locations/texas/plano> (last visited Sep. 7, 2023). On behalf and for the benefit of Vivint and its parents, subsidiaries, members, segments, companies, brands and/or related entities, Vivint coordinates the importation, distribution, marketing, offers for sale, sale, and use of Vivint's products in the U.S. For example, Vivint maintains distribution channels in the U.S. for Vivint's products, for example, via at least its own online stores, its own retail stores, distribution partners, retailers, reseller partners, dealers, and other related service providers. *See, e.g., Pick your package, then personalize it*, *VIVINT*, <https://www.vivint.com/shop/> (last visited Sep. 7, 2023) (including "Buy Now" options for a "Premium Plus Package," "Premium Package," and "Vivint Starter Kit" all including at least one component enabled with Wi-Fi connectivity); *Website Terms of Use*, *VIVINT, INC.*, <https://www.vivint.com/legal/terms-of-use> (last visited Sep. 7, 2023) (stating "[t]hese terms of use are entered into by and between you and Vivint, Inc. ('Vivint')" and "[m]inimum \$29.99/month services agreement required in conjunction with minimum \$599.99 equipment purchase"); *Select*

*a State for Vivint Service Locations in the U.S.*, VIVINT, INC., <https://www.vivint.com/locations> (last visited Sep. 7, 2023) (listing all U.S. states except for Maine); *Partner with Vivint—the best in home security: When you sell for Vivint, you’re building a career with the No. 1 provider of home security systems in the U.S.*, VIVINT, INC., <https://www.vivint.com/partners/vivint-dealers> (last visited Sep. 7, 2023) (answering “Frequently Asked Questions, including (i) “Can we sell anywhere? Yes. We service the vast majority of the US”; and (ii) “What does the Dealer payment structure look like? . . . Dealers are paid weekly[;] Smart home purchases are paid the Friday after installation[;] For solar, the installer funds Vivint within one to two weeks after installation. Dealers receive their payout the week after Vivint receives those funds.”); *Vivint Annual Report* at 12 (“In July 2021, [Vivint] announced a partnership with Freedom Forever, one of the country’s leading solar installers” that “enables Freedom Forever to include a Vivint smart home system with each of its solar sales.”)

13. As a result, via at least Vivint’s established distribution channels operated and maintained by at least Defendant Vivint, Inc. and/or its U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities, Vivint products are distributed, sold, advertised, and used nationwide, including being sold to consumers via physical and online Vivint stores operating in Texas and this District. Thus, Defendant does business in the U.S., the state of Texas, and in this District.

#### **JURISDICTION AND VENUE**

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

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

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

17. On information and belief, this Court has personal jurisdiction over Vivint, Inc., directly and/or indirectly via the activities of Vivint, Inc.'s partners, alter egos, intermediaries, agents, related entities, distributors, importers, customers, parents, subsidiaries, and/or consumers, including U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities.

18. On information and belief, Vivint, Inc. utilizes established distribution channels to distribute, market, offer for sale, sell, service, and/or warrant infringing products directly to consumers and other users, including offering such products and/or related services for sale. Vivint products and services have been sold from and/or in both brick-and-mortar stores and online retail

stores by entities within this District and in Texas. Alone and in concert with or via direction and control of or by at least these entities, Vivint, Inc. has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within the United States, giving rise to this action and/or has established minimum contacts with Texas. For example, Vivint, Inc. operates within a global network of manufacturing, sales and distribution of Vivint products that includes parents, subsidiaries and/or related entities of Vivint, Inc., retail stores, showrooms, dealers, resellers, professional installers, and/or distributors operating in Texas, including this District.

19. As another example, on information and belief, Vivint, Inc. maintains a place of business in this District through at least brick-and-mortar locations at 16440 Gateway Dr, Frisco, Texas 75035 in Collin County, Texas; *See, e.g., Property ID: 2869811 For Year 2023*, COLLIN CAD, <https://www.collincad.org/propertysearch?prop=2869811&year=2023> (showing that “Vivint, Inc.” owns property located in Collin County, TX); VIVINT, INC., *Vivint Frisco Service Area*, <https://www.vivint.com/locations/texas/frisco> (last visited Sep. 7, 2023) (listing an address at 16440 Gateway Dr, Frisco, Texas 75035 for “Vivint Frisco Service Area”).

20. On information and belief, as a part of Vivint’s global manufacturing and distribution network, Vivint, Inc. also purposefully places infringing Vivint products in established distribution channels in the stream of commerce, including in Texas, via distribution partners, retailers (e.g., national retailers), resellers, dealers, brand ambassadors, service providers, consumers, and/or other users. *See, e.g., Partner with Vivint—the best in home security: When you sell for Vivint, you’re building a career with the No. 1 provider of home security systems in the U.S.*, VIVINT, INC., <https://www.vivint.com/partners/vivint-dealers> (last visited Sep. 7, 2023) (answering “Frequently Asked Questions, including (i) “Can we sell anywhere? Yes. We service the vast majority of the US”; and (ii) “What does the Dealer payment structure look like? . . .



Dealers are paid weekly[;] Smart home purchases are paid the Friday after installation[;] For solar, the installer funds Vivint within one to two weeks after installation. Dealers receive their payout the week after Vivint receives those funds.”); *Vivint Annual Report* at 12 (“In July 2021, [Vivint] announced a partnership with Freedom Forever, one of the country’s leading solar installers” that “enables Freedom Forever to include a Vivint smart home system with each of its solar sales.”). Vivint, Inc. owns and operates at least one website that offers Vivint products and services to consumers in the United States, in Texas, and in this District. *See id.* Vivint, Inc. provides infringing Vivint product under the Vivint brand via its online and physical stores. *See, e.g., Pick your package, then personalize it*, VIVINT, <https://www.vivint.com/shop/> (last visited Sep. 7, 2023) (including “Buy Now” options for a “Premium Plus Package,” “Premium Package,” and “Vivint Starter Kit” all including at least one component enabled with Wi-Fi connectivity); *Website Terms of Use*, VIVINT, INC., <https://www.vivint.com/legal/terms-of-use> (last visited Sep. 7, 2023) (stating “[t]hese terms of use are entered into by and between you and Vivint, Inc. (‘Vivint’)” and “[m]inimum \$29.99/month services agreement required in conjunction with minimum \$599.99 equipment purchase”); *Select a State for Vivint Service Locations in the U.S.*, VIVINT, INC., <https://www.vivint.com/locations> (last visited Sep. 7, 2023) (listing all U.S. states except for Maine). For example, Vivint wireless doorbell cameras, outdoor security cameras, indoor security cameras, sensors, plugs, thermostats, access devices, and/or Smart Hub control panels are offered for sale in this District by at least Vivint’s local places of business and/or nationwide online retail stores, for example, at [vivint.com](http://vivint.com). *See id.* Therefore, Vivint, Inc., alone and in concert with its parents, subsidiaries, members, segments, companies, brands and/or related entities, has purposefully directed its activities at Texas, and should reasonably anticipate being brought into this Court, at least on this basis. Through its own conduct and/or through direction and control of

its parents, subsidiaries, members, segments, companies, brands and/or related entities, Vivint, Inc. has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over Vivint, Inc. would not offend traditional notions of fair play and substantial justice.

21. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and/or 1400(b). As alleged herein, Defendant Vivint, Inc. has committed acts of infringement in this District. As further alleged herein, Defendant Vivint, Inc., via its own operations and/or employees, has a regular and established place of business in this District, for example, at 1115 W. Hickory Street, Suite 105, Denton, Texas 76201 in Denton County, Texas; 16440 Gateway Dr, Frisco, Texas 75035 in Collin County, Texas; 5212 Tennyson Pkwy Suite 150, Plano, TX 75024 in Collin County, Texas, among other Vivint locations owned, leased and/or operated in this District. Accordingly, Vivint, Inc. may be sued in this district under 28 U.S.C. § 1400(b).

22. On information and belief, Defendant Vivint, Inc. 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**

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

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) 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.

26. 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.

27. 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.

28. On information and belief, a significant portion of the operating revenue of Defendant is derived from the manufacture, distribution, sale, servicing, installation and/or use of smart home and business products and components, including, for example, smart home, home security, business security, networking, solar energy, insurance and IoT products and components, which are manufactured in or imported into the United States, distributed to and/or by resellers, dealers, and third-party manufacturers, and/or sold to and used by U.S. consumers. For example, in the United States, Vivint's single operating segment reported revenue of \$1.659 billion for the year ending December 31, 2022. *Vivint Annual Report* at 114.

29. The Asserted Patents cover Defendant's home and business IoT and smart home products and components, software, services, and processes related to same that generally connect to other devices in a network or other networks using a wireless protocol, such as Zigbee (also known as "ZigBee") and/or Wi-Fi (also known as "WiFi"). *See, e.g., LIGHT BRIDGE, VIVINT, INC.*, <https://www.vivint.com/products/smart-light-bridge> (last visited Oct. 25, 2023) ("Zigbee 3.0 connectivity"); *SMART LIGHT BULBS, VIVINT, INC.*, <https://www.vivint.com/products/smart-light-bulbs> (last visited Oct. 25, 2023) ("Zigbee 3.0"); *SMART SWITCH, VIVINT, INC.*, <https://www.vivint.com/products/smart-light-switch> (last visited Oct. 25, 2023); *Certified Products Search, CONNECTIVITY STANDARDS ALLIANCE*, [https://csa-iot.org/csa-iot\\_products/?p\\_keywords=vivint&p\\_type%5B%5D=17&p\\_type%5B%5D=14&p\\_type%5B%5D=1053&p\\_certificate=&p\\_family=](https://csa-iot.org/csa-iot_products/?p_keywords=vivint&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_family=) (last visited Oct. 25, 2023) (listing three "Vivint Smart Lighting switch plates" as "Zigbee 3.0" certified); *Smart Home Installation Guide: What You Really Need, VIVINT, INC.*, <https://www.vivint.com/resources/article/smart-home-installation->

guide (last visited Sep. 8, 2023) (“All the devices in a smart home are connected through a Wi-Fi internet connection.”); *10 Simple Ways to Secure Your Home*, VIVINT, INC., <https://www.vivint.com/resources/article/10-simple-ways-tips-on-how-to-secure-your-home> (last visited Sep. 8, 2023) (stating that “securing your WiFi is just as important as securing doors and windows, especially if you have smart home devices” and “[y]ou can lock down your WiFi by . . . enabling WPA or WPA-2 encryption”). Defendant’s infringing Vivint products include, but are not limited to, devices and products enabled or compliant with Wi-Fi and/or Zigbee, including without limitation Vivint Wi-Fi modules (e.g. WIFI Module Model Number NM02), control panels (e.g., Smart Hubs); doorbell cameras; outdoor security cameras; indoor security cameras; smart thermostats; touchscreen panels; smartphone and/or tablet applications (e.g., Vivint Smart Home App); sensors; car tracking and/or anti-theft devices (e.g., Car Guard with Wi-Fi radio); spotlights; smart monitoring and/or access control devices (e.g., any and all Wi-Fi-enabled smart locks, garage door controllers, and sensors); smart lighting devices (e.g., light bridges, smart light bulbs, and smart lighting switch plates); Vivint packages (e.g., Vivint “Premium Plus Package,” “Premium Package,” and “Vivint Starter Kit” package) that include any of these products; and related accessories and software (all collectively referred to as the “Accused Products”). These Accused Products infringe the Asserted Patents by at least their manufacture, importation, distribution, offers for sale, sale, and use in the U.S.

30. The Asserted Patents cover Accused Products of Vivint that use the Zigbee protocol to communicate with other devices on a communication network, including those of third-party manufacturers. Examples of the Vivint’s Zigbee products include the Vivint Light Bridge, Vivint Smart Light Bulbs, and Vivint Smart Lighting switch plates, which are shown below:


LIGHT BRIDGE

# The light bridge that unlocks your lighting

The ultimate smart lighting hub, the Vivint Smart Lighting Bridge makes the magic—bringing your smart lights to life while extending the power of your smart home.

844.481.8630

[Request more information](#)

A dark grey, square-shaped smart lighting bridge device with a green LED indicator light on its top surface. Two cables are plugged into the back of the device.

INTERNET CONNECTION	Ethernet connection to wireless router	CONNECTIVITY	Zigbee 3.0 connectivity
---------------------	--	--------------	-------------------------

[Start Your Quote →](#)

LIGHT BRIDGE, VIVINT, INC., <https://www.vivint.com/products/smart-light-bridge> (last visited Oct. 25, 2023) (“Zigbee 3.0 connectivity”).

SMART LIGHT BULBS

# The reinvented light bulb—it’s wicked smart

Go beyond ordinary lighting. Illuminate your space with Smart Light Bulbs that bring intelligence to the way you see your home, control it, and protect it.

866.556.0413

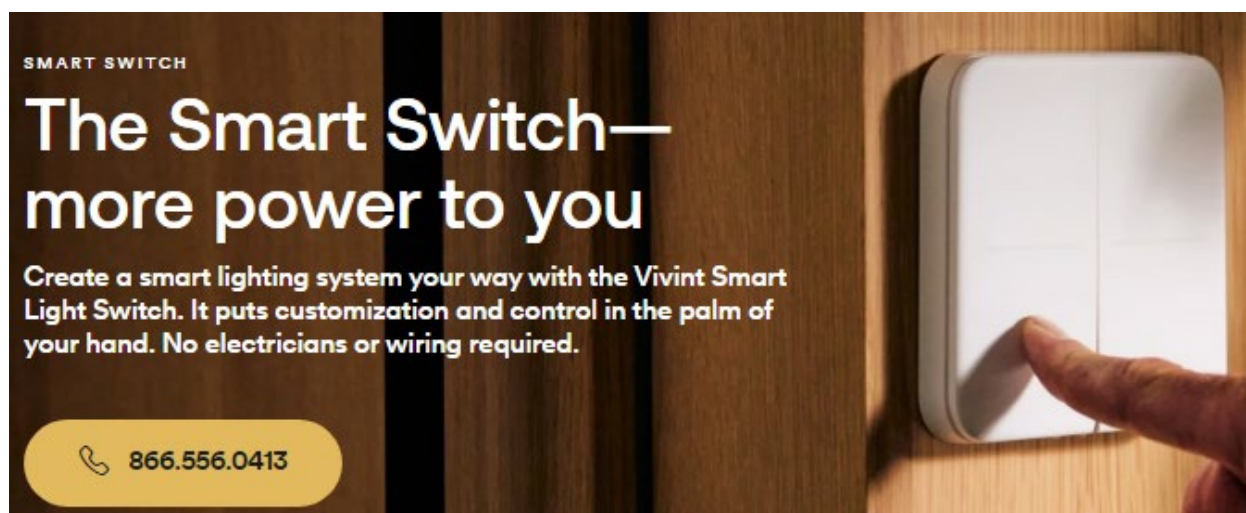
[Request more information](#)

Three ERIA Smart Light Bulbs are shown against a dark background. The central bulb is illuminated with a bright yellow light, while the two flanking bulbs are illuminated with a bright blue light. Each bulb has the brand name 'ERIA' and 'White tunable' printed on its base.

COMMUNICATION TYPE	Zigbee 3.0
--------------------	------------

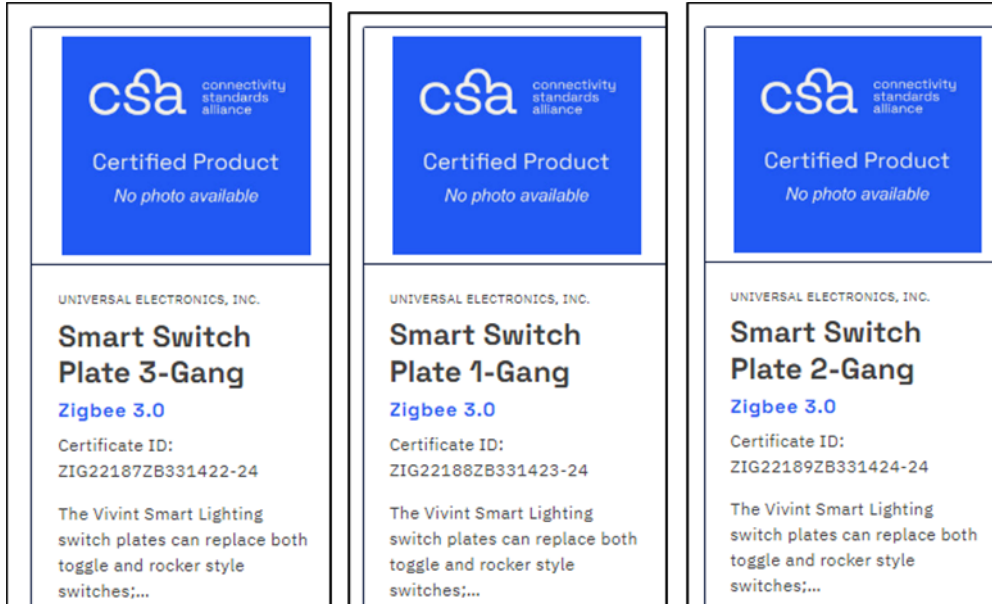
Start Your Quote →

*SMART LIGHT BULBS*, VIVINT, INC., <https://www.vivint.com/products/smart-light-bulbs> (last visited Oct. 25, 2023) (“Zigbee 3.0”).



NUMBER OF GANGS	1-, 2-, and 3-gang
-----------------	--------------------

*SMART SWITCH*, VIVINT, INC., <https://www.vivint.com/products/smart-light-switch> (last visited Oct. 25, 2023).



*Certified Products Search*, CONNECTIVITY STANDARDS ALLIANCE, [https://csa-iot.org/csa-](https://csa-iot.org/csa-iot_products/?p_keywords=vivint&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_family=)

[iot\\_products/?p\\_keywords=vivint&p\\_type%5B%5D=17&p\\_type%5B%5D=14&p\\_type%5B%5D=1053&p\\_certificate=&p\\_family=](https://csa-iot_products/?p_keywords=vivint&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_family=) (last visited Oct. 25, 2023) (listing three “Vivint Smart

Lighting switch plates” as “Zigbee 3.0” certified).

31. 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).

32. 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](http://ecee.colorado.edu/~liue/teaching/comm_standards/2015S_zigbee/802.15.4-2011.pdf)

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

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



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

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

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

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>

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

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



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

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

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.

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

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

35. 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.

36. The Asserted Patents also cover Accused Products of Vivint that utilize the Wi-Fi protocol. Examples of such products that include Defendant’s infringing Vivint products include, but are not limited to, devices and products enabled or compliant with Wi-Fi (IEEE 802.11), including without limitation Vivint Wi-Fi modules (e.g. WIFI Module Model Number NM02), control panels (e.g., Smart Hubs); doorbell cameras; outdoor security cameras; indoor security cameras; Vivint packages (e.g., Vivint “Premium Plus Package,” “Premium Package,” and “Vivint Starter Kit” package) that include any of these products; and related accessories and software. Vivint discusses at least some of these products on its website as follows:

## How do I turn my home into a smart home?

All the devices in a smart home are connected through a **Wi-Fi** internet connection. Create your own smart setup by choosing and installing smart devices that work together, fit the layout of your home, and meet your automation needs.

.....

## What’s included in a smart home system?

An effective smart home system can be as complex or as simple as you want it to be. For instance, if you live in an apartment, your setup might just consist of a doorbell camera to monitor your front doorway and a smart thermostat to remotely control the temperature in your home.

However, a larger family home might consist of a network of connected security cameras, smart lighting, smart locks, security sensors, a smart garage door opener, and several other smart gadgets, depending on your preferences.

The next few sections will cover some devices that many homeowners choose to include in their smart home systems.

## Smart control hub

.....

## Smart lighting

.....

## Smart thermostat

.....

## Smart door locks

.....

## Smart security sensors

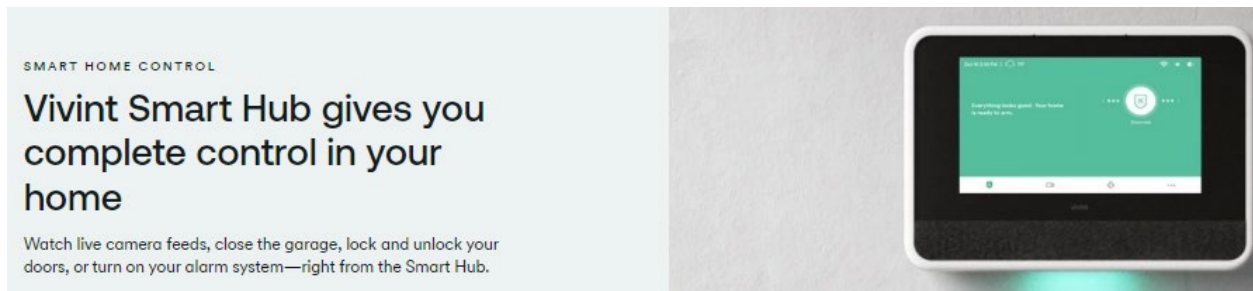
.....

## Smart garage door control

.....

## Smart security camera system

*Smart Home Installation Guide: What You Really Need*, VIVINT, <https://www.vivint.com/resources/article/smart-home-installation-guide> (Sep. 26, 2022) (last visited Sep. 20, 2023).



*Smart Home Technology*, VIVINT, <https://www.vivint.com/packages/home-automation> (last visited Sep. 20, 2023).

## Vivint Smart Hub - General Info and Specifications

.....



.....

## Details & Specifications

.....

Battery	<ul style="list-style-type: none"><li>• Minimum 3470 mAh, 3.7 V Lithium-ion Polymer</li><li>• Minimum 24 hour back-up</li></ul>
---------	---

.....

Communication Frequency (i.e. RF, Z-Wave, Wi-Fi)	<ul style="list-style-type: none"><li>• 802.11 b/g/n WLAN AP/Router; Verizon CDMA Cellular</li><li>• Z-Wave Plus; 345 MHz, NFC</li></ul>
---	--

Connectivity Requirements	<ul style="list-style-type: none"><li>• Dual-Band Wi-Fi module: 802.11 a/b/g/n/ac client and AP mode</li><li>• Ethernet port</li><li>• LTE cellular module</li></ul>
---------------------------	--

*Vivint Smart Hub - General Info and Specifications, VIVINT, <https://support.vivint.com/s/article/Products-Vivint-Smart-Hub-v2> (last visited Sep. 20, 2023).*



## Doorbell Camera Pro

[Tech Specs](#)

[Features](#)

[FAQs](#)

[Compare](#)

[Reviews](#)

[Get Started](#)

DOORBELL CAMERA PRO (GEN 2)

# Don't just record crime, prevent it

The Doorbell Camera Pro doesn't just notify you when packages arrive. It's the only video doorbell camera that proactively protects them.

ADD DOORBELL CAMERA PRO TO YOUR SYSTEM

 855.847.2045

Request more information →

## Specs

IMAGE SENSOR

1664x1664p  
with 2x HDR

MAXIMUM VIDEO RESOLUTION

1080p

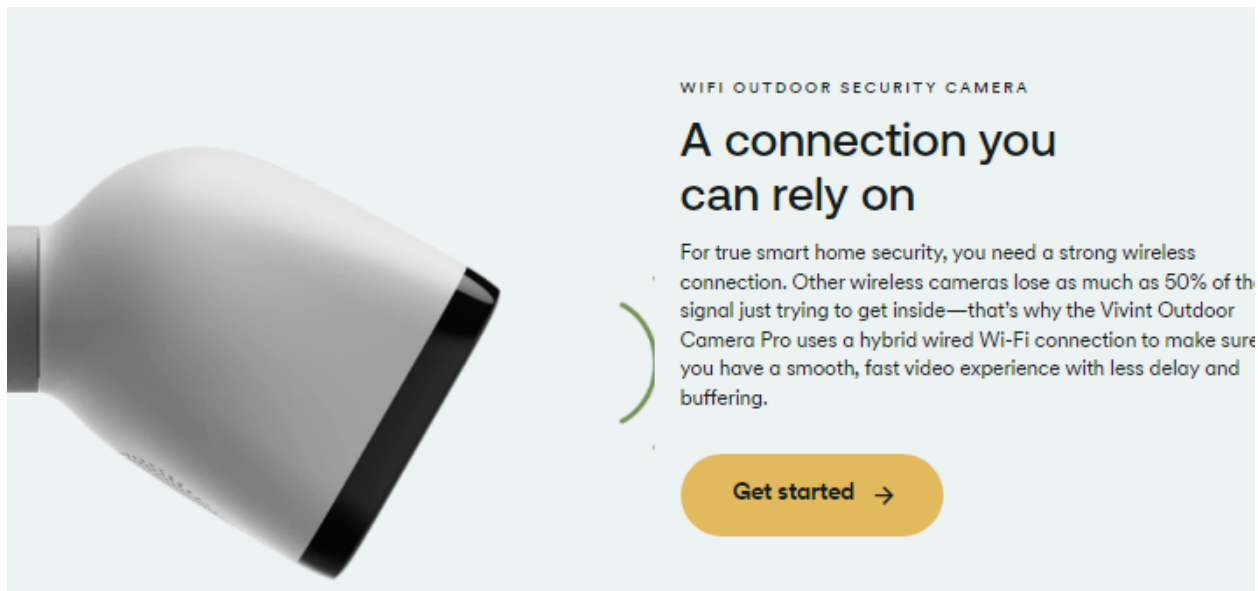
FIELD OF VIEW

180° x 180°

CONNECTIVITY

2.4/5GHz  
802.11 b/g/n/ac  
band Wi-Fi /  
Bluetooth &  
NFC

*Doorbell Camera Pro*, VIVINT, <https://www.vivint.com/products/doorbell-camera> (last visited Sep. 20, 2023).

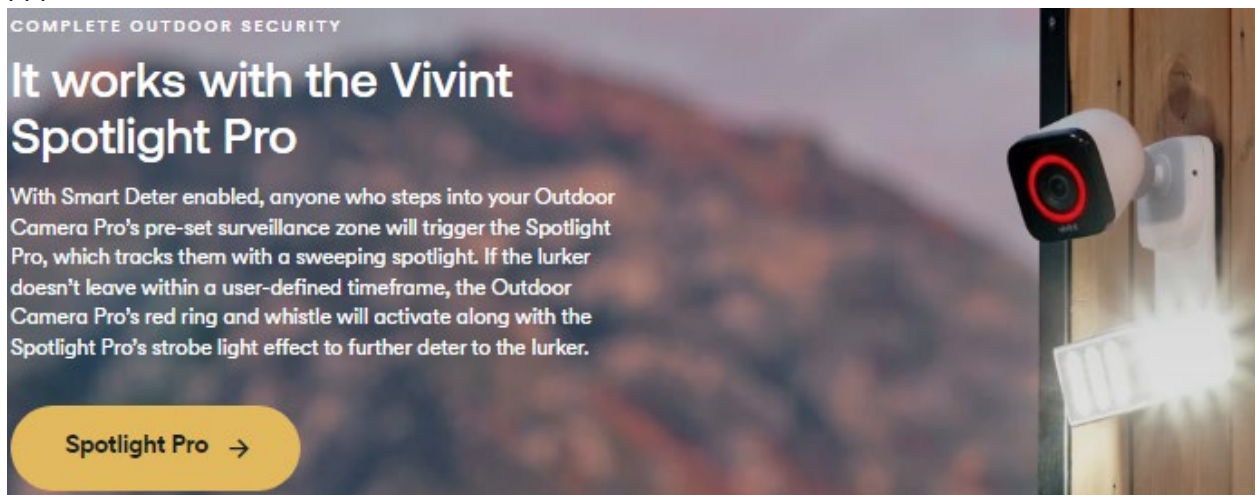


WIFI OUTDOOR SECURITY CAMERA

## A connection you can rely on

For true smart home security, you need a strong wireless connection. Other wireless cameras lose as much as 50% of the signal just trying to get inside—that's why the Vivint Outdoor Camera Pro uses a hybrid wired Wi-Fi connection to make sure you have a smooth, fast video experience with less delay and buffering.

Get started →



COMPLETE OUTDOOR SECURITY

## It works with the Vivint Spotlight Pro

With Smart Deter enabled, anyone who steps into your Outdoor Camera Pro's pre-set surveillance zone will trigger the Spotlight Pro, which tracks them with a sweeping spotlight. If the lurker doesn't leave within a user-defined timeframe, the Outdoor Camera Pro's red ring and whistle will activate along with the Spotlight Pro's strobe light effect to further deter to the lurker.

Spotlight Pro →

*Outdoor Camera Pro*, VIVINT, <https://www.vivint.com/products/outdoor-camera> (last visited Sep. 20, 2023).



## Introducing the Vivint Indoor Camera Pro

.....

- **Dual-band Wi-Fi connectivity.** Wi-Fi with dual-band Wi-Fi means better connectivity, especially in smart homes that have multiple devices connecting to your home's Wi-Fi connection.

*Meet the New Indoor Camera Pro, VIVINT, <https://www.vivint.com/resources/article/new-indoor-camera-pro> (last visited Sep. 20, 2023).*



## How do smart door locks work?

.....

Smart locks use a wireless protocol to function. Vivint smart locks [connect to your Wi-Fi internet](#), while some use Bluetooth or Z-Wave technology to function.

*Guide to Smart Keys and Smart Locks for Your Doors in 2023*, VIVINT, <https://www.vivint.com/resources/article/guide-to-wifi-and-your-smart-door-lock> (last visited Sep. 20, 2023).

★★★★☆ (31,556 reviews)



### Premium Plus Package

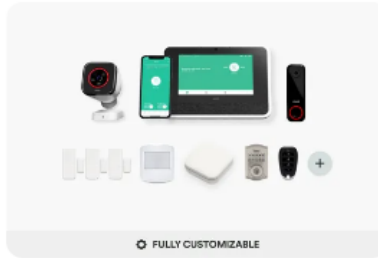
Equipment starting at  
**\$41/mo**  
as low as 0% financing for 60 months<sup>1</sup>

Buy Now

Edit Package

Includes:

- ✓ Vivint Smart Hub Control Panel
- ✓ Flood/Water Damage Sensor
- ✓ Break-In Security Sensors x4
- ✓ Doorbell Camera x1
- ✓ Outdoor Camera x2
- ✓ 90-second Smart Clips
- ✓ Smart Lock
- ✓ Vivint Key Fob
- ✓ Indoor Camera Pro
- ✓ Smart Thermostat
- ✓ Smart Garage Door Controller



### Premium Package

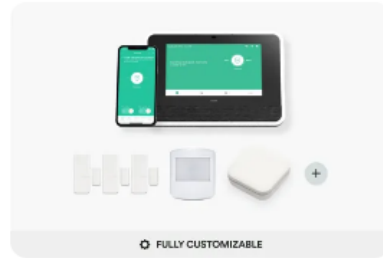
Equipment starting at  
**\$25/mo**  
as low as 0% financing for 60 months<sup>1</sup>

Buy Now

Edit Package

Includes:

- ✓ Vivint Smart Hub Control Panel
- ✓ Flood/Water Damage Sensor
- ✓ Break-In Security Sensors x4
- ✓ Doorbell Camera x1
- ✓ Outdoor Camera x1
- ✓ 90-second Smart Clips
- ✓ Smart Lock
- ✓ Vivint Key Fob
- ✗ Indoor Camera
- ✗ Smart Thermostat
- ✗ Smart Garage Door Controller



### Vivint Starter Kit

Equipment starting at  
**\$10/mo**  
as low as 0% financing for 60 months<sup>1</sup>

Buy Now

Edit Package

Includes:

- ✓ Vivint Smart Hub Control Panel
- ✓ Flood/Water Damage Sensor
- ✓ Break-In Security Sensors x4
- ✗ Doorbell Camera
- ✗ Outdoor Camera
- ✗ 90-second Smart Clips
- ✗ Smart Lock
- ✗ Vivint Key Fob
- ✗ Indoor Camera
- ✗ Smart Thermostat
- ✗ Smart Garage Door Controller

*Smarter Security, customized for you.*, VIVINT, <https://www.vivint.com/shop/packages> (last visited Sep. 20, 2023) (“Pick your package, then personalize it. Add products to create a system that fits your unique home.”).

37. The Accused Products utilize intrusion detection methods for a local or metropolitan area network to infringe at least the ’678, ’572, and ’126 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.

### 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>

38. 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>

39. 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>

40. 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>

41. 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>

42. The Asserted Patents also cover Vivint's Wi-Fi compliant devices, which support WPA, WPA2, and/or WPA3 security mechanisms, as described below and in the following paragraph. *See, e.g., 10 Simple Ways to Secure Your Home*, Vivint, Inc., <https://www.vivint.com/resources/article/10-simple-ways-tips-on-how-to-secure-your-home> (last

visited Sep. 8, 2023) (stating that “securing your WiFi is just as important as securing doors and windows, especially if you have smart home devices” and “[y]ou can lock down your WiFi by . . . enabling WPA or WPA-2 encryption”). Of the WPA, WPA2 and/or WPA3 security mechanism used by the Accused Products (e.g., Vivint’s smart home Wi-Fi devices), WPA is based on Temporal Key Integrity Protocol (TKIP), while WPA2 and WPA3 are based on Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). Shown below are exemplary IEEE 802.11 compliant smart control panels and smart home packages that include a smart control panel. The devices each have a housing.

## Vivint Smart Hub - General Info and Specifications

....



....

### Details & Specifications

....

<p>Communication Frequency (i.e. RF, Z-Wave, Wi-Fi)</p>	<ul style="list-style-type: none"> <li>• 802.11 b/g/n WLAN AP/Router; Verizon CDMA Cellular</li> <li>• Z-Wave Plus; 345 MHz, NFC</li> </ul>
<p>Connectivity Requirements</p>	<ul style="list-style-type: none"> <li>• Dual-Band Wi-Fi module: 802.11 a/b/g/n/ac client and AP mode</li> <li>• Ethernet port</li> <li>• LTE cellular module</li> </ul>

*Vivint Smart Hub - General Info and Specifications*, VIVINT, <https://support.vivint.com/s/article/Products-Vivint-Smart-Hub-v2> (last visited Sep. 20, 2023).

Package Name	Equipment Starting At	Financing
Premium Plus Package	\$41/mo	as low as 0% financing for 60 months <sup>1</sup>
Premium Package	\$25/mo	as low as 0% financing for 60 months <sup>1</sup>
Vivint Starter Kit	\$10/mo	as low as 0% financing for 60 months <sup>1</sup>

Package Name	Includes:
Premium Plus Package	<ul style="list-style-type: none"><li>✓ Vivint Smart Hub Control Panel</li><li>✓ Flood/Water Damage Sensor</li><li>✓ Break-In Security Sensors x4</li><li>✓ Doorbell Camera x1</li><li>✓ Outdoor Camera x2</li><li>✓ 90-second Smart Clips</li><li>✓ Smart Lock</li><li>✓ Vivint Key Fob</li><li>✓ Indoor Camera Pro</li><li>✓ Smart Thermostat</li><li>✓ Smart Garage Door Controller</li></ul>
Premium Package	<ul style="list-style-type: none"><li>✓ Vivint Smart Hub Control Panel</li><li>✓ Flood/Water Damage Sensor</li><li>✓ Break-In Security Sensors x4</li><li>✓ Doorbell Camera x1</li><li>✓ Outdoor Camera x1</li><li>✓ 90-second Smart Clips</li><li>✓ Smart Lock</li><li>✓ Vivint Key Fob</li><li>✗ Indoor Camera</li><li>✗ Smart Thermostat</li><li>✗ Smart Garage Door Controller</li></ul>
Vivint Starter Kit	<ul style="list-style-type: none"><li>✓ Vivint Smart Hub Control Panel</li><li>✓ Flood/Water Damage Sensor</li><li>✓ Break-In Security Sensors x4</li><li>✗ Doorbell Camera</li><li>✗ Outdoor Camera</li><li>✗ 90-second Smart Clips</li><li>✗ Smart Lock</li><li>✗ Vivint Key Fob</li><li>✗ Indoor Camera</li><li>✗ Smart Thermostat</li><li>✗ Smart Garage Door Controller</li></ul>

*Smarter Security, customized for you.*, VIVINT, <https://www.vivint.com/shop/packages> (last visited Sep. 20, 2023) (“Pick your package, then personalize it. Add products to create a system that fits your unique home.”).

## Panel (Vivint Smart Hub) - Connect To Wi-Fi Network

Low effort

Typically takes 5-7 minutes

Must be completed at home

.....

### Connect your panel to WiFi

Tap on your WiFi network name (SSID), then enter in your WiFi password. It could take up to 5 minutes for the panel to reconnect. If your network isn't showing up scroll down and tap **Refresh List**. If it still doesn't show up, tap **Other** and manually enter your network name and password then tap OK.



*Panel (Vivint Smart Hub) - Connect To Wi-Fi Network, VIVINT, <https://support.vivint.com/s/article/Smart-Hub-Connect-WiFi> (last visited Sep. 20, 2023).*

43. As shown above, the Accused Products provide configurable Wi-Fi settings. This capability ascertains the presence of a MAC controller and a Wi-Fi antenna and transceiver in the device and provides a secure wireless LAN.

44. The Accused Products further utilize a cryptography circuit that implements the 802.11 protocol's authentication techniques, including, for example, TKIP and/or 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.

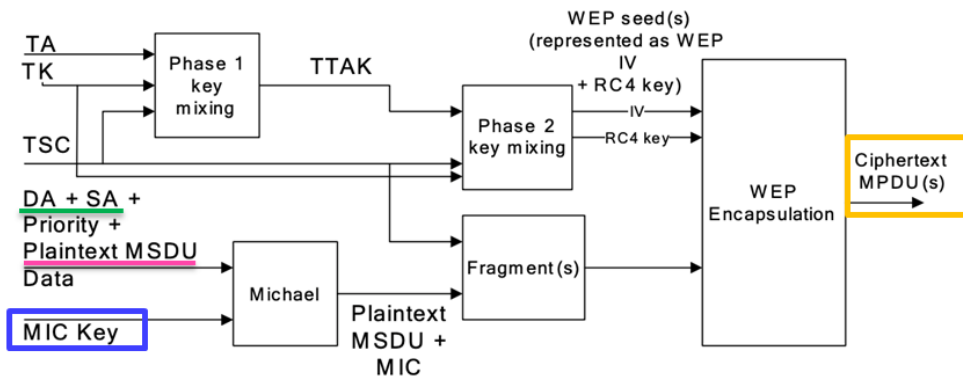


Figure 8-4—TKIP encapsulation block diagram

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

45. 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 encryption 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)

### 8.3.3.3 CCMP cryptographic encapsulation

The CCMP cryptographic encapsulation process is depicted in Figure 8-16.

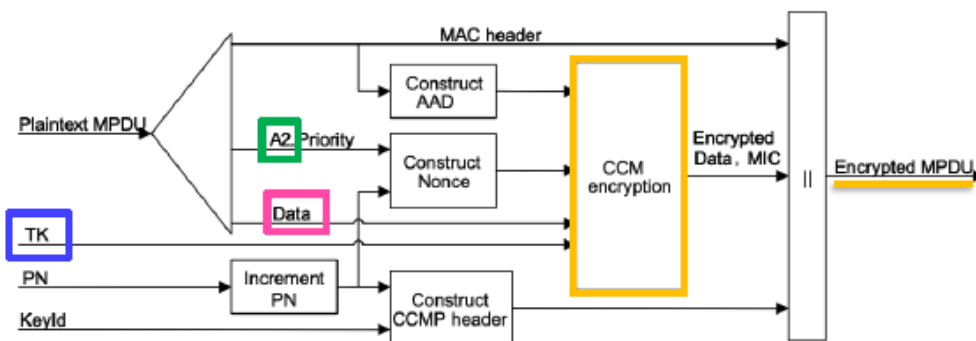


Figure 8-16—CCMP encapsulation block diagram

CCMP encrypts the payload of a plaintext MPDU and encapsulates the resulting cipher text using the following steps:

- Increment the PN, to obtain a fresh PN for each MPDU, so that the PN never repeats for the same temporal key. Note that retransmitted MPDUs are not modified on retransmission.
- Use the fields in the MPDU header to construct the additional authentication data (AAD) for CCM. The CCM algorithm provides integrity protection for the fields included in the AAD. MPDU header fields that may change when retransmitted are muted by being masked to 0 when calculating the AAD.
- Construct the CCM Nonce block from the PN, A2, and the Priority field of the MPDU where A2 is MPDU Address 2.
- Place the new PN and the key identifier into the 8-octet CCMP header.
- Use the temporal key, AAD, nonce, and MPDU data to form the cipher text and MIC. This step is known as CCM originator processing.
- Form the encrypted MPDU by combining the original MPDU header, the CCMP header, the encrypted data and MIC, as described in 8.3.3.2.

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

46. On information and belief, Defendant also infringes the '126 patent via products that utilize a volatile memory for storing cryptography information utilized in the cryptography circuit and a battery for maintaining the cryptography information in the volatile memory. As shown in Vivint's Smart Hub control panel specifications, the control panel utilizes 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.

## Vivint Smart Hub - General Info and Specifications

.....



.....

### Details & Specifications

.....

Battery	<ul style="list-style-type: none"> <li>• Minimum 3470 mAh, 3.7 V Lithium-ion Polymer</li> <li>• Minimum 24 hour back-up</li> </ul>
---------	--

.....

Communication Frequency (i.e. RF, Z-Wave, Wi-Fi)	<ul style="list-style-type: none"> <li>• 802.11 b/g/n WLAN AP/Router; Verizon CDMA Cellular</li> <li>• Z-Wave Plus; 345 MHz, NFC</li> </ul>
Connectivity Requirements	<ul style="list-style-type: none"> <li>• Dual-Band Wi-Fi module: 802.11 a/b/g/n/ac client and AP mode</li> <li>• Ethernet port</li> <li>• LTE cellular module</li> </ul>

*Vivint Smart Hub - General Info and Specifications*, VIVINT, <https://support.vivint.com/s/article/Products-Vivint-Smart-Hub-v2> (last visited Sep. 20, 2023).

### **COUNT I**

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

47. Plaintiff incorporates paragraphs 1 through 46 herein by reference.

48. 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.

49. 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.

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

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

52. Defendant directly infringes the '678 patent via 35 U.S.C. § 271(a) by making (including, e.g., via contract manufacturers), offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '678 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parents, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, Defendant designs the Accused Products for U.S. consumers, has made and/or sold and/or continues to make and/or 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/or related service providers in the United States, or in the case that Defendant delivers the Accused Products outside of the United States Defendant 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)”).

53. Furthermore, Vivint, Inc. directly infringes the '678 patent through its direct involvement in the activities of its subsidiaries and related entities, including U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities. Defendant designs the Accused Products for U.S. consumers, sells and offers for sale those Accused Products in the U.S. directly and to its related entities, and imports the Accused Products into the United States for sale and/or for its related entities. On information and belief, parents, subsidiaries, members, segments, companies, brands and/or related entities of Defendant, for example, U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities of Defendant, 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 Defendant. Defendant Vivint, Inc. is vicariously liable for the infringing conduct of Defendant's U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities (under both the alter ego and agency theories). On information and belief,

Defendant Vivint, Inc. and U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities are essentially the same company, comprising parents, subsidiaries, members, segments, companies, brands and/or related entities of Vivint. Moreover, Vivint, Inc., along with its related entities, has the right and ability to control the infringing activities of U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities such that Defendant receives a direct financial benefit from that infringement.

54. For example, Vivint infringes claim 51 of the '678 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to, Vivint Wi-Fi modules (e.g. WIFI Module Model Number NM02), control panels (e.g., Smart Hubs); doorbell cameras; outdoor security cameras; indoor security cameras; smart thermostats; touchscreen panels; smartphone and/or tablet applications (e.g., Vivint Smart Home App); Sensors; car tracking and/or anti-theft devices (e.g., Car Guard with Wi-Fi radio); spotlights; smart monitoring and/or access control devices (e.g., any and all Wi-Fi-enabled smart locks, garage door controllers, and sensors); Vivint packages (e.g., Vivint “Premium Plus Package,” “Premium Package,” and “Vivint Starter Kit” package) that include any of these products; and related accessories and software.

55. 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.

56. At a minimum, Vivint has known of the '678 patent at least as early as the filing date of this complaint. In addition, Vivint has known about its infringement of the L3Harris ("Harris") patent portfolio, which includes the '678 patent, since at least its receipt on July 21, 2020, of a communication from Acacia Research Group on behalf of Stingray IP Solutions LLC, offering a license to the patent portfolio including the '678 patent. Further, Vivint has known about its infringement of the Harris patent portfolio, which includes the '678 patent, since at least its receipt of a letter from Stingray, a subsidiary of Acacia Research Group LLC, to Jim Lundberg, Vice President & Deputy General Counsel of both Vivint, Inc. and Vivint Smart Home, Inc. dated January 20, 2022, requesting Vivint to discuss licensing the patent portfolio including the '678 patent. *See, e.g., EcoFactor, Inc. v. Vivint, Inc.*, No. 6:22-cv-00034-ADA, Dkt. 16-1 (W.D. Tex. May 2, 2022) (Declaration by Jim Lundberg indicating he is Vice President and Deputy General Counsel of Vivint, Inc.); *Jim Lundberg*, LINKEDIN, <https://www.linkedin.com/in/jim-lundberg-708a3a32> (last visited July 28, 2023) (indicating Jim Lundberg is Vice President and Deputy General Counsel of Vivint Smart Home, Inc). Then on at least twenty-four (24) additional occasions, Stingray provided Vivint with follow-up communications regarding the opportunity to license the Harris patent portfolio, including the '678 patent. However, Vivint provided no response to these communications and offers to license the Stingray patents. All statutory requirements to recover pre-suit damages have been satisfied.

57. On information and belief, since at least the above-mentioned date or dates when Vivint was on notice of its infringement, Defendant has actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers,

integrators, installers, OEMs, consumers, users and 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 referenced above, Defendant does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '678 patent. On information and belief, Defendant intends to cause, and has taken affirmative steps to induce, infringement by manufacturers, importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMs, installers, consumers, users, and/or related service providers through at least, *inter alia*, the following activities: 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, testing, certifying, and/or placing orders to manufacture the Accused Products in conformity with U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products; distributing or making available instructions or manuals for these products to consumers, installers, purchasers and/or prospective buyers; testing and/or certifying wireless networking features in the Accused Products (with, for example, the WiFi Alliance and/or the Connectivity Standards Alliance, i.e., for Zigbee certification); and/or providing technical support, product files, videos, replacement parts, and/or services for these products to purchasers in the United States. *See, e.g., VIVINT SERVICES*, VIVINT, <https://www.vivint.com/services> (last visited Sep. 15, 2023) (“The services we provide take all the guesswork out of creating your secure, smart home. We’ll customize your security system, install everything for you, and keep your home secure with 24/7 security monitoring....Our service

doesn't end when your system is installed. From troubleshooting to warranties and repairs, we can help. Just chat or call to connect with us....We also protect your business.”); *see also Vivint*, YOUTUBE.COM, <https://www.youtube.com/@vivint> (providing consumers with Vivint-produced how-to videos related to Vivint products) (last visited Sep. 15, 2023); *WiFi Module for Vivint Model Number: NM02*, available at <https://fccid.io/2AAAS-NM02/User-Manual/Users-Manual-rev-6025778.pdf> (last visited Oct. 25, 2023) (manual and product specification provided to the Federal Communications Commission (FCC) on behalf of Vivint for an “802.11 a/b/g/n/ ac Dual Band WiFi Module for Vivint”); *Certified Products Search*, CONNECTIVITY STANDARDS ALLIANCE, [https://csa-iot.org/csa-iot\\_products/?p\\_keywords=vivint&p\\_type%5B%5D=17&p\\_type%5B%5D=14&p\\_type%5B%5D=1053&p\\_certificate=&p\\_family=](https://csa-iot.org/csa-iot_products/?p_keywords=vivint&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_family=) (last visited Oct. 25, 2023) (showing Vivint's Zigbee products certified by the Connectivity Standards Alliance include at least five products: two Vivint Lighting Bridges and three Vivint Smart Lighting switch plates); *BB03 Vivint Zigbee Bridge Label Diagram*, VIVINT, available at <https://fccid.io/2AAAS-BB03/Label/FCC-ID-Label-and-Location-6197650> (last visited Oct. 25, 2023) (showing a label provided on behalf of Vivint to the FCC for Vivint's Zigbee Bridge model number BB03). Furthermore, Vivint markets and offers smartphone and tablet interfaces and its application software (e.g., apps) that, via Wi-Fi and/or Zigbee networks, provide access to the Accused Products, connect such products to wireless networks, including Wi-Fi and/or Zigbee networks, provide remote control for Vivint products, provide other services supporting use of the Accused Products and work with smart home platforms including at least Google Assistant, Amazon Alexa, and/or Apple products to control Vivint products with voice commands or connect with other connected products. *See Frequently asked smart control questions*, VIVINT, <https://www.vivint.com/products/smart-control> (last visited Sep. 15, 2023) (“Is

a smart home app necessary? If you want to get the most out of your smart home system, an app is essential. If you've installed Vivint security, our app gives you complete control over your entire system. With the Vivint app, you can: Manage all of the devices in your system from one platform. Monitor and control your system no matter where you are. Always know what's happening at home with notification and alerts.”); *What makes a smart home app great?*, VIVINT, <https://www.vivint.com/resources/article/vivint-smart-home-app-reviews> (last visited Sep. 15, 2023) (including reviews to support the assertion that “[t]he Vivint app . . . [is] the best smart home app on the market”); *Smart Home Devices That Work With Vivint*, VIVINT <https://www.vivint.com/resources/article/smart-home-devices-work-vivint> (last visited Sep. 15, 2023) (“Vivint integrates seamlessly with your favorite smart home devices, including Google Nest, Google Home, and Amazon Echo.”); *Smart Home App - Download*, VIVINT, <https://support.vivint.com/s/article/Smart-Home-App-Download> (last visited Sep. 15, 2023) (providing instructions to download the Vivint Smart Home App for “Apple Users” and “Android Users.”). Such compatibility provides convenience and added functionality that induces consumers to use Vivint products, including at least via the smartphone and tablet Wi-Fi apps, other interfaces utilizing Wi-Fi and/or Zigbee, and other protocols in networks (e.g., Wi-Fi and/or Zigbee networks) with other third-party devices, and thus further infringe the '678 patent.

58. On information and belief, despite having knowledge of the patent portfolio including the '678 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '678 patent and/or the patent portfolio, Vivint has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendant's infringing activities relative to the '678 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a



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

59. Plaintiff Stingray has been damaged as a result of Vivint'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 Vivint's 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)

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

61. 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.

62. 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.

63. Vivint 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.

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

65. Defendant directly infringes the ‘572 patent via 35 U.S.C. § 271(a) by making (including, e.g., via contract manufacturers), offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the ‘572 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parents, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, Defendant designs the Accused Products for U.S. consumers, has made and/or sold and/or continues to make and/or 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/or related service providers in the United States, or in the case that Defendant delivers the Accused Products outside of the United States Defendant 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)”).

66. Furthermore, Vivint, Inc. directly infringes the ‘572 patent through its direct involvement in the activities of its subsidiaries and related entities, including U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities. Defendant designs the Accused Products for U.S. consumers, sells and offers for sale those Accused Products in the U.S. directly and to its related entities, and imports the Accused Products into the United States for sale

and/or for its related entities. On information and belief, parents, subsidiaries, members, segments, companies, brands and/or related entities of Defendant, for example, U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities of Defendant, 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 Defendant. Defendant Vivint, Inc. is vicariously liable for the infringing conduct of Defendant's U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities (under both the alter ego and agency theories). On information and belief, Defendant Vivint, Inc. and U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities are essentially the same company, comprising parents, subsidiaries, members, segments, companies, brands and/or related entities of Vivint. Moreover, Vivint, Inc., along with its related entities, has the right and ability to control the infringing activities of U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities such that Defendant receives a direct financial benefit from that infringement.

67. For example, Vivint infringes claim 1 of the '572 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to, Vivint Wi-Fi modules (e.g. WIFI Module Model Number NM02), control panels (e.g., Smart Hubs); doorbell cameras; outdoor security cameras; indoor security cameras; smart thermostats; touchscreen panels; smartphone and/or tablet applications (e.g., Vivint Smart Home App); sensors; car tracking and/or anti-theft devices (e.g., Car Guard with Wi-Fi radio); spotlights; smart monitoring and/or access control devices (e.g., any and all Wi-Fi-enabled smart locks, garage door controllers, and sensors); Vivint packages (e.g., Vivint "Premium Plus Package," "Premium Package," and "Vivint Starter Kit" package) that include any of these products; and related accessories and software.

68. 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.

69. Vivint further infringes the ’572 patent via 35 U.S.C. § 271(g) by selling, offering to sell, and/or importing IoT and smart home devices, their components, and/or products containing same, that are made by a process covered by the ’572 patent. On information and belief, the infringing IoT and smart home devices, their components, and/or products containing same are not materially changed by subsequent processes, and they are neither trivial nor nonessential components of another product.

70. Vivint 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.

71. At a minimum, Vivint has known of the ’572 patent at least as early as the filing date of this complaint. In addition, Vivint has known about its infringement of the L3Harris (“Harris”) patent portfolio, which includes the ’572 patent, since at least its receipt on July 21,

2020, of a communication from Acacia Research Group on behalf of Stingray IP Solutions LLC, offering a license to the patent portfolio including the '572 patent. Further, Vivint has known about its infringement of the Harris patent portfolio, which includes the '572 patent, since at least its receipt of a letter from Stingray, a subsidiary of Acacia Research Group LLC, to Jim Lundberg, Vice President & Deputy General Counsel of both Vivint, Inc. and Vivint Smart Home, Inc. dated January 20, 2022, requesting Vivint to discuss licensing the patent portfolio including the '572 patent. *See, e.g., EcoFactor, Inc. v. Vivint, Inc.*, No. 6:22-cv-00034-ADA, Dkt. 16-1 (W.D. Tex. May 2, 2022) (Declaration by Jim Lundberg indicating he is Vice President and Deputy General Counsel of Vivint, Inc.); *Jim Lundberg*, LINKEDIN, <https://www.linkedin.com/in/jim-lundberg-708a3a32> (last visited July 28, 2023) (indicating Jim Lundberg is Vice President and Deputy General Counsel of Vivint Smart Home, Inc). Then on at least twenty-four (24) additional occasions, Stingray provided Vivint with follow-up communications regarding the opportunity to license the Harris patent portfolio, including the '572 patent. However, Vivint provided no response to these communications and offers to license the Stingray patents. All statutory requirements to recover pre-suit damages have been satisfied.

72. On information and belief, since at least the above-mentioned date or dates when Vivint was on notice of its infringement, Defendant has actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, installers, OEMs, consumers, and 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 referenced above, Defendant does so with knowledge, or with willful

blindness of the fact, that the induced acts constitute infringement of the ‘572 patent. On information and belief, Defendant intends to cause, and has taken affirmative steps to induce, infringement by manufacturers, importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMs, installers, consumers, users, and/or related service providers through at least, *inter alia*, the following activities: 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, testing, certifying, and/or placing orders to manufacture the Accused Products in conformity with U.S. laws and regulations including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products; distributing or making available instructions or manuals for these products to consumers, installers, purchasers and/or prospective buyers; testing and/or certifying wireless networking features in the Accused Products (with, for example, the WiFi Alliance and/or the Connectivity Standards Alliance, i.e., for Zigbee certification); and/or providing technical support, product files, videos, replacement parts, and/or services for these products to purchasers in the United States. *See, e.g., VIVINT SERVICES*, VIVINT, <https://www.vivint.com/services> (last visited Sep. 15, 2023) (“The services we provide take all the guesswork out of creating your secure, smart home. We’ll customize your security system, install everything for you, and keep your home secure with 24/7 security monitoring....Our service doesn’t end when your system is installed. From troubleshooting to warranties and repairs, we can help. Just chat or call to connect with us....We also protect your business.”); *see also Vivint*, YOUTUBE.COM, <https://www.youtube.com/@vivint> (providing consumers with Vivint-produced how-to videos related to Vivint products) (last visited Sep. 15, 2023); *WIFI Module for Vivint Model Number: NM02*, available at <https://fccid.io/2AAAS-NM02/User-Manual/Users-Manual-rev-6025778.pdf>

(last visited Oct. 25, 2023) (manual and product specification provided to the Federal Communications Commission (FCC) on behalf of Vivint for an “802.11 a/b/g/n/ ac Dual Band WiFi Module for Vivint”); *Certified Products Search*, CONNECTIVITY STANDARDS ALLIANCE, [https://csa-iot.org/csa-iot\\_products/?p\\_keywords=55vivint&p\\_type%5B%5D=17&p\\_type%5B%5D=14&p\\_type%5B%5D=1053&p\\_certificate=&p\\_family=](https://csa-iot.org/csa-iot_products/?p_keywords=55vivint&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_family=) (last visited Oct. 25, 2023) (showing Vivint’s Zigbee products certified by the Connectivity Standards Alliance include at least five products: two Vivint Lighting Bridges and three Vivint Smart Lighting switch plates); *BB03 Vivint Zigbee Bridge Label Diagram*, VIVINT, available at <https://fccid.io/2AAAS-BB03/Label/FCC-ID-Label-and-Location-6197650> (last visited Oct. 25, 2023) (showing a label provided on behalf of Vivint to the FCC for Vivint’s Zigbee Bridge model number BB03). Furthermore, Vivint markets and offers smartphone and tablet interfaces and its application software (e.g., apps) that, via Wi-Fi and/or Zigbee networks, provide access to the Accused Products, connect such products to wireless networks, including Wi-Fi and/or Zigbee networks, provide remote control for Vivint products, provide other services supporting use of the Accused Products and work with smart home platforms including at least Google Assistant, Amazon Alexa, and/or Apple products to control Vivint products with voice commands or connect with other connected products. *See Frequently asked smart control questions*, VIVINT, <https://www.vivint.com/products/smart-control> (last visited Sep. 15, 2023) (“Is a smart home app necessary? If you want to get the most out of your smart home system, an app is essential. If you’ve installed Vivint security, our app gives you complete control over your entire system. With the Vivint app, you can: Manage all of the devices in your system from one platform. Monitor and control your system no matter where you are. Always know what’s happening at home with notification and alerts.”); *What makes a smart home app great?*, VIVINT,

<https://www.vivint.com/resources/article/vivint-smart-home-app-reviews> (last visited Sep. 15, 2023) (including reviews to support the assertion that “[t]he Vivint app . . . [is] the best smart home app on the market”); *Smart Home Devices That Work With Vivint*, VIVINT, <https://www.vivint.com/resources/article/smart-home-devices-work-vivint> (last visited Sep. 15, 2023) (“Vivint integrates seamlessly with your favorite smart home devices, including Google Nest, Google Home, and Amazon Echo.”); *Smart Home App – Download*, VIVINT, <https://support.vivint.com/s/article/Smart-Home-App-Download> (last visited Sep. 15, 2023) (providing instructions to download the Vivint Smart Home App for “Apple Users” and “Android Users.”); *WiFi Module for Vivint Model Number: NM02*, available at <https://fccid.io/2AAAS-NM02/User-Manual/Users-Manual-rev-6025778.pdf> (last visited Oct. 25, 2023) (manual and product specification provided to the Federal Communications Commission (FCC) on behalf of Vivint for an “802.11 a/b/g/n/ ac Dual Band WiFi Module for Vivint”); *Certified Products Search*, CONNECTIVITY STANDARDS ALLIANCE, [https://csa-iot.org/csa-iot\\_products/?p\\_keywords=56vivint&p\\_type%5B%5D=17&p\\_type%5B%5D=14&p\\_type%5B%5D=1053&p\\_certificate=&p\\_family=](https://csa-iot.org/csa-iot_products/?p_keywords=56vivint&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_family=) (last visited Oct. 25, 2023) (showing Vivint’s Zigbee products certified by the Connectivity Standards Alliance include at least five products: two Vivint Lighting Bridges and three Vivint Smart Lighting switch plates). Such compatibility provides convenience and added functionality that induces consumers to use Vivint products, including via at least the smartphone and tablet Wi-Fi apps, other interfaces utilizing Wi-Fi and/or Zigbee, and other protocols in networks (e.g., Wi-Fi- and/or Zigbee networks) with other third-party devices, and thus further infringe the ‘572 patent.

73. On information and belief, despite having knowledge of the patent portfolio including the ‘572 patent and knowledge that it is directly and/or indirectly infringing one or more



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

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

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

76. 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.

77. 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.

78. Vivint 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.

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

80. Defendant directly infringes the '961 patent via 35 U.S.C. § 271(a) by making (including, e.g., via contract manufacturers), offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '961 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parents, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, Defendant designs the Accused Products for U.S. consumers, has made and/or sold and/or continues to make and/or 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/or related service providers in the United States, or in the case that Defendant delivers the Accused Products outside of the United States Defendant does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the '961 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to “whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers ... constitute an infringing sale under § 271(a)”).

81. Furthermore, Defendant Vivint, Inc. directly infringes the '961 patent through its direct involvement in the activities of its subsidiaries and related entities, including U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities. Defendant designs the Accused Products for U.S. consumers, sells and offers for sale those Accused Products in the U.S. directly and to its related entities, and imports the Accused Products into the United States for sale and/or for its related entities. On information and belief, parents, subsidiaries, members, segments, companies, brands and/or related entities of Defendant, for example, U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities of Defendant, conduct activities that constitute direct infringement of the '961 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendant. Defendant Vivint, Inc. is vicariously liable for the infringing conduct of Defendant's U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities (under both the alter ego and agency theories). On information and belief, Defendant Vivint, Inc. and U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities are essentially the same company, comprising parents, subsidiaries, members, segments, companies, brands and/or related entities of Vivint. Moreover, Vivint, Inc., along with its related entities, has the right and ability to control the infringing activities of U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities such that Defendant receives a direct financial benefit from that infringement.

82. For example, Vivint infringes claim 1 of the '961 patent via the Accused Products that utilize Zigbee protocols, including, but not limited to, smartphone and/or tablet applications (e.g., Vivint Smart Home App), Vivint smart lighting devices (e.g., light bridges, smart light bulbs,

and smart lighting switch plates); Vivint packages that include any of these products; and related accessories and software.

83. 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.

84. At a minimum, Vivint has known of the ’961 patent at least as early as the filing date of this complaint. In addition, Vivint has known about its infringement of the L3Harris (“Harris”) patent portfolio, which includes the ’961 patent, since at least its receipt on July 21, 2020, of a communication from Acacia Research Group on behalf of Stingray IP Solutions LLC, offering a license to the patent portfolio including the ’961 patent. Further, Vivint has known about its infringement of the Harris patent portfolio, which includes the ’961 patent, since at least its receipt of a letter from Stingray, a subsidiary of Acacia Research Group LLC, to Jim Lundberg,

Vice President & Deputy General Counsel of both Vivint, Inc. and Vivint Smart Home, Inc. dated January 20, 2022, requesting Vivint to discuss licensing the patent portfolio including the '961 patent. *See, e.g., EcoFactor, Inc. v. Vivint, Inc.*, No. 6:22-cv-00034-ADA, Dkt. 16-1 (W.D. Tex. May 2, 2022) (Declaration by Jim Lundberg indicating he is Vice President and Deputy General Counsel of Vivint, Inc.); *Jim Lundberg*, LINKEDIN, <https://www.linkedin.com/in/jim-lundberg-708a3a32> (last visited July 28, 2023) (indicating Jim Lundberg is Vice President and Deputy General Counsel of Vivint Smart Home, Inc). Then on at least twenty-four (24) additional occasions, Stingray provided Vivint with follow-up communications regarding the opportunity to license the Harris patent portfolio, including the '961 patent. However, Vivint provided no response to these communications and offers to license the Stingray patents. All statutory requirements to recover pre-suit damages have been satisfied.

85. On information and belief, since at least the above-mentioned date or dates when Vivint was on notice of its infringement, Defendant has actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, installers, OEMs, consumers, and 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 referenced above, Defendant does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '961 patent. On information and belief, Defendant intends to cause, and has taken affirmative steps to induce, infringement by manufacturers, importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMs, installers, consumers, users, and/or related service providers through at

least, *inter alia*, the following activities: 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, testing, certifying, and/or placing orders to manufacture the Accused Products in conformity with U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products; distributing or making available instructions or manuals for these products to consumers, installers, purchasers and/or prospective buyers; testing and/or certifying wireless networking features in the Accused Products (with, for example, the WiFi Alliance and/or the Connectivity Standards Alliance, i.e., for Zigbee certification); and/or providing technical support, product files, videos, replacement parts, and/or services for these products to purchasers in the United States. *See, e.g., VIVINT SERVICES*, VIVINT, <https://www.vivint.com/services> (last visited Sep. 15, 2023) (“The services we provide take all the guesswork out of creating your secure, smart home. We’ll customize your security system, install everything for you, and keep your home secure with 24/7 security monitoring....Our service doesn’t end when your system is installed. From troubleshooting to warranties and repairs, we can help. Just chat or call to connect with us....We also protect your business.”); *see also Vivint*, YOUTUBE.COM, <https://www.youtube.com/@vivint> (providing consumers with Vivint-produced how-to videos related to Vivint products) (last visited Sep. 15, 2023); *WiFi Module for Vivint Model Number: NM02*, available at <https://fccid.io/2AAAS-NM02/User-Manual/Users-Manual-rev-6025778.pdf> (last visited Oct. 25, 2023) (manual and product specification provided to the Federal Communications Commission (FCC) on behalf of Vivint for an “802.11 a/b/g/n/ ac Dual Band WiFi Module for Vivint”); *Certified Products Search*, CONNECTIVITY STANDARDS ALLIANCE, <https://csa-iot.org/csa->

iot\_products/?p\_keywords=vivint&p\_type%5B%5D=17&p\_type%5B%5D=14&p\_type%5B%5D=1053&p\_certificate=&p\_family= (last visited Oct. 25, 2023) (showing Vivint's Zigbee products certified by the Connectivity Standards Alliance include at least five products: two Vivint Lighting Bridges and three Vivint Smart Lighting switch plates); *BB03 Vivint Zigbee Bridge Label Diagram*, VIVINT, available at <https://fccid.io/2AAAS-BB03/Label/FCC-ID-Label-and-Location-6197650> (last visited Oct. 25, 2023) (showing a label provided on behalf of Vivint to the FCC for Vivint's Zigbee Bridge model number BB03). Furthermore, Vivint markets and offers smartphone and tablet interfaces and its application software (e.g., apps) that, via Wi-Fi and/or Zigbee networks, provide access to the Accused Products, connect such products to wireless networks, including Wi-Fi and/or Zigbee networks, provide remote control for Vivint products, provide other services supporting use of the Accused Products and work with smart home platforms including at least Google Assistant, Amazon Alexa, and/or Apple products to control Vivint products with voice commands or connect with other connected products. *See Frequently asked smart control questions*, VIVINT, <https://www.vivint.com/products/smart-control> (last visited Sep. 15, 2023) ("Is a smart home app necessary? If you want to get the most out of your smart home system, an app is essential. If you've installed Vivint security, our app gives you complete control over your entire system. With the Vivint app, you can: Manage all of the devices in your system from one platform. Monitor and control your system no matter where you are. Always know what's happening at home with notification and alerts."); *What makes a smart home app great?*, VIVINT, <https://www.vivint.com/resources/article/vivint-smart-home-app-reviews> (last visited Sep. 15, 2023) (including reviews to support the assertion that "[t]he Vivint app . . . [is] the best smart home app on the market"); *Smart Home Devices That Work With Vivint*, VIVINT <https://www.vivint.com/resources/article/smart-home-devices-work-vivint> (last visited Sep. 15,

2023) (“Vivint integrates seamlessly with your favorite smart home devices, including Google Nest, Google Home, and Amazon Echo.”); *Smart Home App – Download*, VIVINT, <https://support.vivint.com/s/article/Smart-Home-App-Download> (last visited Sep. 15, 2023) (providing instructions to download the Vivint Smart Home App for “Apple Users” and “Android Users.”). Such compatibility provides convenience and added functionality that induces consumers to use Vivint products, including via at least the smartphone and tablet Wi-Fi apps, other interfaces utilizing Wi-Fi and/or Zigbee, and other protocols in networks (e.g., Wi-Fi and/or Zigbee networks) with other third-party devices, and thus further infringe the ’961 patent.

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

87. Plaintiff Stingray has been damaged as a result of Vivint’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 Vivint’s 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)

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

89. 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.

90. 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 filed on January 16, 2001.

91. Vivint 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.

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

93. Defendant directly infringes the '126 patent via 35 U.S.C. § 271(a) by making (including, e.g., via contract manufacturers), offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '126 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parents, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, Defendant designs the Accused Products for

U.S. consumers, has made and/or sold and/or continues to make and/or 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/or related service providers in the United States, or in the case that Defendant delivers the Accused Products outside of the United States Defendant does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the '126 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to “whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers ... constitute an infringing sale under § 271(a)”).

94. Furthermore, Vivint, Inc. directly infringes the '126 patent through its direct involvement in the activities of its subsidiaries and related entities, including U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities. Defendant designs the Accused Products for U.S. consumers, sells and offers for sale those Accused Products in the U.S. directly and to its related entities, and imports the Accused Products into the United States for sale and/or for its related entities. On information and belief, parents, subsidiaries, members, segments, companies, brands and/or related entities of Defendant, for example, U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities of Defendant, conduct activities that constitute direct infringement of the '126 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 Defendant. Defendant Vivint, Inc. is vicariously liable for the infringing conduct of Defendant's U.S.-based parents, subsidiaries, members, segments, companies, brands

and/or related entities (under both the alter ego and agency theories). On information and belief, Defendant Vivint, Inc. and U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities are essentially the same company, comprising parents, subsidiaries, members, segments, companies, brands and/or related entities of Vivint. Moreover, Vivint, Inc., along with its related entities, has the right and ability to control the infringing activities of U.S.-based parents, subsidiaries, members, segments, companies, brands and/or related entities such that Defendant receives a direct financial benefit from that infringement.

95. For example, Vivint 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, Vivint Wi-Fi modules (e.g. WIFI Module Model Number NM02), control panels (e.g., Smart Hubs); Vivint packages (e.g., Vivint “Premium Plus Package,” “Premium Package,” and “Vivint Starter Kit” package) that include any of these products; and related accessories and software.

96. 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 the cryptography

information, and a battery for maintaining the cryptography information in said at least one volatile memory.

97. At a minimum, Vivint has known of the ‘126 patent at least as early as the filing date of this complaint. In addition, Vivint has known about its infringement of the L3Harris (“Harris”) patent portfolio, which includes the ‘126 patent, since at least its receipt on July 21, 2020, of a communication from Acacia Research Group on behalf of Stingray IP Solutions LLC, offering a license to the patent portfolio including the ‘126 patent. Further, Vivint has known about its infringement of the Harris patent portfolio, which includes the ‘126 patent, since at least its receipt of a letter from Stingray, a subsidiary of Acacia Research Group LLC, to Jim Lundberg, Vice President & Deputy General Counsel of both Vivint, Inc. and Vivint Smart Home, Inc. dated January 20, 2022, requesting Vivint to discuss licensing the patent portfolio including the ‘126 patent. *See, e.g., EcoFactor, Inc. v. Vivint, Inc.*, No. 6:22-cv-00034-ADA, Dkt. 16-1 (W.D. Tex. May 2, 2022) (Declaration by Jim Lundberg indicating he is Vice President and Deputy General Counsel of Vivint, Inc.); *Jim Lundberg*, LINKEDIN, <https://www.linkedin.com/in/jim-lundberg-708a3a32> (last visited July 28, 2023) (indicating Jim Lundberg is Vice President and Deputy General Counsel of Vivint Smart Home, Inc). Then on at least twenty-four (24) additional occasions, Stingray provided Vivint with follow-up communications regarding the opportunity to license the Harris patent portfolio, including the ‘126 patent. However, Vivint provided no response to these communications and offers to license the Stingray patents. All statutory requirements to recover pre-suit damages have been satisfied.

98. On information and belief, since at least the above-mentioned date or dates when Vivint was on notice of its infringement, Defendant has actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, installers,

OEMs, consumers, and 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 referenced above, Defendant does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the ‘126 patent. On information and belief, Defendant intends to cause, and has taken affirmative steps to induce, infringement by manufacturers, importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMs, installers, consumers, users, and/or related service providers through at least, *inter alia*, the following activities: 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, testing, certifying, and/or placing orders to manufacture the Accused Products in conformity with U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products; distributing or making available instructions or manuals for these products to consumers, installers, purchasers and/or prospective buyers; testing and/or certifying wireless networking features in the Accused Products (with, for example, the WiFi Alliance and/or the Connectivity Standards Alliance, i.e., for Zigbee certification); and/or providing technical support, product files, videos, replacement parts, and/or services for these products to purchasers in the United States. *See, e.g., VIVINT SERVICES*, VIVINT, <https://www.vivint.com/services> (last visited Sep. 15, 2023) (“The services we provide take all the guesswork out of creating your secure, smart home. We’ll customize your security system, install everything for you, and keep your home secure with 24/7 security monitoring....Our service doesn’t end when your system is installed.

From troubleshooting to warranties and repairs, we can help. Just chat or call to connect with us....We also protect your business.”); *see also Vivint*, YOUTUBE.COM, <https://www.youtube.com/@vivint> (providing consumers with Vivint-produced how-to videos related to Vivint products) (last visited Sep. 15, 2023); *WiFi Module for Vivint Model Number: NM02*, available at <https://fccid.io/2AAAS-NM02/User-Manual/Users-Manual-rev-6025778.pdf> (last visited Oct. 25, 2023) (manual and product specification provided to the Federal Communications Commission (FCC) on behalf of Vivint for an “802.11 a/b/g/n/ ac Dual Band WiFi Module for Vivint”); *Certified Products Search*, CONNECTIVITY STANDARDS ALLIANCE, [https://csa-iot.org/csa-iot\\_products/?p\\_keywords=vivint&p\\_type%5B%5D=17&p\\_type%5B%5D=14&p\\_type%5B%5D=1053&p\\_certificate=&p\\_family=](https://csa-iot.org/csa-iot_products/?p_keywords=vivint&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_family=) (last visited Oct. 25, 2023) (showing Vivint’s Zigbee products certified by the Connectivity Standards Alliance include at least five products: two Vivint Lighting Bridges and three Vivint Smart Lighting switch plates); *BB03 Vivint Zigbee Bridge Label Diagram*, VIVINT, available at <https://fccid.io/2AAAS-BB03/Label/FCC-ID-Label-and-Location-6197650> (last visited Oct. 25, 2023) (showing a label provided on behalf of Vivint to the FCC for Vivint’s Zigbee Bridge model number BB03). Furthermore, Vivint markets and offers smartphone and tablet interfaces and its application software (e.g., apps) that, via Wi-Fi and/or Zigbee networks, provide access to the Accused Products, connect such products to wireless networks, including Wi-Fi and/or Zigbee networks, provide remote control for Vivint products, provide other services supporting use of the Accused Products and work with smart home platforms including at least Google Assistant, Amazon Alexa, and/or Apple products to control Vivint products with voice commands or connect with other connected products. *See Frequently asked smart control questions*, VIVINT, <https://www.vivint.com/products/smart-control> (last visited Sep. 15, 2023) (“Is

a smart home app necessary? If you want to get the most out of your smart home system, an app is essential. If you've installed Vivint security, our app gives you complete control over your entire system. With the Vivint app, you can: Manage all of the devices in your system from one platform. Monitor and control your system no matter where you are. Always know what's happening at home with notification and alerts.”); *What makes a smart home app great?*, VIVINT, <https://www.vivint.com/resources/article/vivint-smart-home-app-reviews> (last visited Sep. 15, 2023) (including reviews to support the assertion that “[t]he Vivint app . . . [is] the best smart home app on the market”); *Smart Home Devices That Work With Vivint*, VIVINT <https://www.vivint.com/resources/article/smart-home-devices-work-vivint> (last visited Sep. 15, 2023) (“Vivint integrates seamlessly with your favorite smart home devices, including Google Nest, Google Home, and Amazon Echo.”); *Smart Home App – Download*, VIVINT, <https://support.vivint.com/s/article/Smart-Home-App-Download> (last visited Sep. 15, 2023) (providing instructions to download the Vivint Smart Home App for “Apple Users” and “Android Users.”). Such compatibility provides convenience and added functionality that induces consumers to use Vivint products, including via at least the smartphone and tablet Wi-Fi apps, other interfaces utilizing Wi-Fi and/or Zigbee, and other protocols in networks (e.g., Wi-Fi and/or Zigbee networks) with other third-party devices, and thus further infringe the ‘126 patent.

99. On information and belief, despite having knowledge of the patent portfolio including the ‘126 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ‘126 patent and/or the patent portfolio, Vivint has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendant’s infringing activities relative to the ‘126 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a

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

100. Plaintiff Stingray has been damaged as a result of Vivint'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 Vivint's 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**

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

102. 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**

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

### **PRAYER FOR RELIEF**

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

- a. A judgment that Defendant has 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 Defendant;
- c. A judgment and order requiring Defendant to pay Plaintiff damages under 35 U.S.C. § 284, including up to treble damages as provided by 35 U.S.C. § 284, and any royalties determined to be appropriate;
- d. A judgment and order requiring Defendant 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 Defendant 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, 2023

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

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**

1507 Bill Owens Parkway

Longview, Texas 75604

Telephone: (903) 757-6400

Facsimile: (903) 757-2323

**ATTORNEYS FOR PLAINTIFF  
STINGRAY IP SOLUTIONS LLC**