UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

Portus Singapore Pte Ltd., and
Portus Pty Ltd.,
 	
            Plaintiffs,
 	
          v.
 	
Amcrest Technologies LLC,
 	
                Defendant.
	
	CASE NO. 4:22-cv-01973
	
	Jury Trial Demanded

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiffs Portus Singapore Pte Ltd. and Portus Pty Ltd. ("Plaintiffs") file this complaint for

patent infringement against Defendant Amcrest Technologies LLC ("Defendant" or "Amcrest") and

in support alleges as follows:

NATURE OF THE ACTION

1.   This is a civil action arising under the Patent Laws of the United States, 35 U.S.C. §

271, *et seq.*

THE PARTIES

2.   Plaintiff Portus Singapore Pte Ltd. is a company organized under the laws of the

Republic of Singapore.

3.   Plaintiff Portus Pty Ltd. is a subsidiary of Portus Singapore Pte Ltd., and a company

organized under the laws of Australia.

4.   On information and belief, Amcrest Technologies LLC is a limited liability company

organized and existing under the laws of Texas with a place of business at 16727 Park Row, Houston,

Texas 77081. Defendant has a registered agent with Yusuf Ravat, 7941 Katy Fwy # 178, Houston, TX 77024, but this address is believed to be a UPS Store mailbox. Abdurahman Ravat is the founding member of Amcrest Technologies LLC, and he may be found, on information and belief, at 122 Paul Revere Dr., Houston, TX 77024.

5.   Amcrest makes, imports, offers to sell, sells, and uses the accused devices in the United States, including in the State of Texas generally and this judicial district in particular.

JURISDICTION AND VENUE

6.   This Court has jurisdiction over the subject matter of this action asserted herein under the Patent Laws of the United States, United States Code, Title 35. This is an action for patent infringement that arises under the patent laws of the United States, 35 U.S.C. § 271, *et seq*.

7.   This Court has original subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

8.   This Court has personal jurisdiction over Defendant. Defendant has sustained and systematic activities in this District and is committing infringing acts in Texas and this District. Defendant regularly conducts business in the State of Texas and within this District, including the sales of the accused products that are the subject of this patent infringement lawsuit. Upon information and belief, Defendant has employees in this District who are responsible for the accused products. Defendant engages in other persistent courses of conduct and derives substantial revenue from products and/or services provided in this District and in Texas, and has purposefully established substantial, systematic, and continuous contacts within this District and should reasonably expect to be sued in a court in this District.

9.   Defendant maintains an established place of business at 16727 Park Row, Houston, Texas 77081.

10.   Venue is proper in this district as to Amcrest pursuant to 28 U.S.C. § 1400(b).

11.   Infringement is occurring within the State of Texas and this District through Defendant's distribution and sales of "smart" devices under, for example, outdoor, indoor, and security cameras, as well smart home products (the "Accused Products," which are further defined below).

12.   Venue is further proper because Defendant has placed the Accused Products into the stream of commerce knowing or understanding that such products would be used in the United States, including in the Southern District of Texas. Defendant has manufactured, distributed, sold, and/or offered to sell the Accused Products to customers for use throughout this District.

13.   This Court has personal jurisdiction over Defendants at least because Defendant has made, used, offered to sell and sold the accused products within the District thus committing acts of infringement within the District, and placed infringing products into the stream of commerce knowing or understanding that such products would be used in the United States, including in the Southern District of Texas.

FACTUAL BACKGROUND

Plaintiff Portus

14.   Portus is the original creator of the smart home. Portus pioneered the technology for viewing your home when you are away, as well as understanding and managing household energy use, so its users could live in more enjoyable, affordable homes.

15.   With Portus' patented technology, users have the freedom to monitor and control their home from anywhere.

16.   With Portus' patented technology, Portus enables a home to be safer and more efficient through a connected environment.

17.   As well as helping households, Portus facilitated utilities by providing insight into their customers' energy use. The understanding of consumers' energy demands the technology gives is invaluable to a household's or company's planning capacity and carbon constraints.

18.   Further, Portus' technology facilitates utilities' demand management by providing insight into their customers' energy use. The understanding of consumers' energy demands the technology gives is invaluable to companies' planning capacity and carbon constraints.

19.   Initially founded in Australia, Portus moved to Singapore after winning equity funding through an investment arm of the Singapore government.

20.   Portus Singapore Pte Ltd. is the owner by assignment from the inventors, Charles Cameron Lindquist and Timothy John Lindquist, of all right, title, and interest in and to Portus is the owner, by assignment, of the two patents-in-suit: U.S. Patent Nos. 8,914,526 (the '526 Patent) attached as Exhibit A; and 9,961,097 (the '097 Patent) attached as Exhibit B.

21.   Portus Pty Ltd. is the exclusive licensee of the '526 and '097 Patents.

22.   Tim Lindquist, one of the Portus founders, is one of the inventors of the asserted patents and is recognized as an inventor of the Connected Home. Tim was proclaimed as a pioneer of the Smart Grid by Smart Grid Today.

The '526 Patent

23.   Portus Singapore Pte Ltd. is the owner by assignment from the inventors, Charles Cameron Lindquist and Timothy John Lindquist, of all right, title, and interest in and to United States Patent Number 8,914,526 (the "'526 Patent"), titled "Local and Remote Monitoring Using a Standard Web Browser" including the right to sue for all past infringement.

24.   Portus Pty Ltd. is the exclusive licensee of the '526 Patent.

25.   Attached to this Complaint as Exhibit A is a true and correct copy of the '526 Patent.

26.   The '526 Patent issued from United States Patent and Trademark Office application no. 09/868,417, which was based on a PCT application no. 99/01128, which was filed on December 17, 1999. That PCT application was based on Australian patent application (PP 7764) filed on December 17, 1998.

27.   The Patent Office issued the '526 Patent on December 16, 2014, after a full and fair examination.

28.   The '526 Patent is valid and enforceable.

29.   The '526 Patent abstract describes a home security and control system for monitoring and controlling an external environment such as a home environment comprising: an Internet browser connectable to an external network, or "Cloud"" a Cloud located external to the home environment and accessible via the Internet browser; a communications server located in the Cloud and adapted to interconnect on demand with one of a series of connection gateways located in predetermined home environments; and a connection gateway located in the home environment adapted to control and/or monitor the operation of at least one security device in the home environment; wherein upon accessing a predetermined address by the Internet browser on the Cloud, the communications server connects to a predetermined one of the connection gateways to control and/or monitor the operation of the security device.
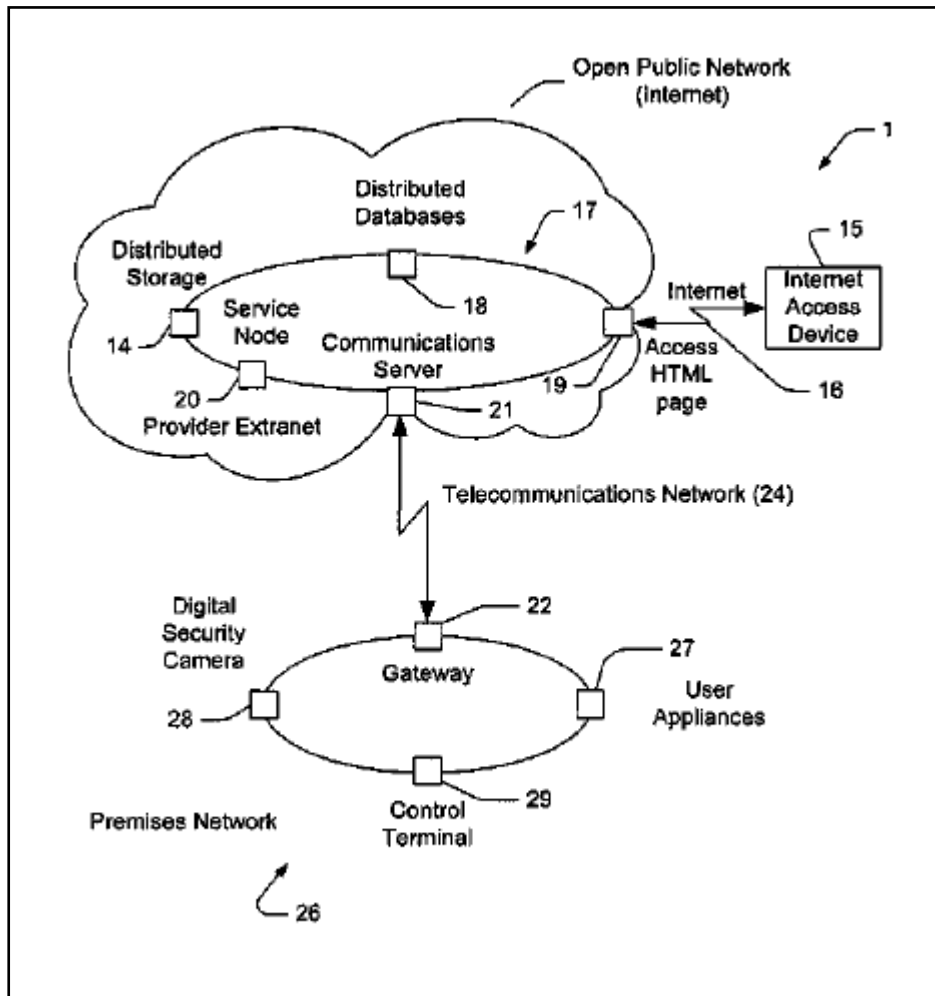
30.   The inventors of the '526 Patent, recognized that home automation and security

systems had become more advanced and that the "[u]sers often have a common need to control and

monitor such systems both locally and remotely." '526 Patent at 1:35-36. However, despite the

growing complexity of these systems, users "generally must resort to non-visual monitoring and

control mechanisms for remote operation [such as] by telephone through codes entered via a

telephone handset." *Id*. at 1:38-41.

31.   The '526 Patent provides several advantages over the prior art such as: a) allowing

remote control of a home security system through operation of a website rather than through the

cumbersome automated systems and choices provided via telephone; b) providing a geographically

independent standard interface for remote connection to a home security system that is universally

accessible and not platform or hardware dependent.

6

32.   A person of ordinary skill in the art at the time of the invention would have recognized that the steps (and combination of steps) claimed in the '526 Patent were, at the time of invention, unconventional and describe remote monitoring of home security and automation systems in a way that, at the time of the invention, was not routine.

33.   A person of ordinary skill in the art at the time of the invention would have understood that, at the time of the invention, there was no conventional manner in which to use a web browser remotely to monitor and control home automation and security systems. A skilled artisan, at the time of the invention, would have recognized the problem that such remote monitoring at the time of the invention could only be accomplished via cumbersome telephone-based input and automation systems.

34.   The '526 Patent provides technical solutions to this problem not solved in the prior art. The inventions disclosed in the '526 patent achieves that "when a customer connects to their home, their home effectively appears to them as a website, with all devices, security and otherwise, accessible for monitoring and control." '526 Patent at 2:49-52.

35.   A person skilled in the art at the time of the invention would have understood that the system of using an Internet browser; a Cloud external to the user premises and accessible via the Internet browser; a plurality of connection gateways that are part of the home network; and a communications server located in the Cloud and adapted to communicate on-demand with the connection gateways was not, at the time of the invention, conventional, well-understood, nor routine.

36.   A person of ordinary skill in the art at the time of the invention would have understood that the system described in claim 1 of the '526 Patent was not, at the time of the invention, conventional, well-understood, or routine.

37.   A person skilled in the art at the time of the invention would have understood that the claims recite steps and structural limitations operating in an unconventional manner to achieve an improved operation of home security and automation.

38.   These technological improvements provide greater cost savings and efficiencies in allowing remote monitoring of a home security and automation systems through a web browser.

39.   The novel use and arrangement of the specific system recited in the '526 claims were not well-understood, routine, nor conventional to a person skilled in the relevant field at the time of the inventions.

The '097 Patent

40.   Portus Singapore Pte Ltd. is the owner by assignment from the inventors, Charles Cameron Lindquist and Timothy John Lindquist, of all right, title, and interest in and to United States Patent Number 9,961,097 (the "'097 Patent"), titled "System for Remote Access of a User Premises" including the right to sue for all past infringement.

41.   Portus Pty Ltd. is the exclusive licensee of the '097 Patent.

42.   Exhibit B is a true and correct copy of the '097 Patent.

43.   The '097 Patent issued from application no. 14/536,784 filed on November 10, 2014.

44.   The Patent Office issued the '097 Patent on May 1, 2018, after a full and fair examination.

45.   The '097 Patent is valid and enforceable.

46.   The '097 Patent provides several advantages over the prior art such as: a) allowing remote control of a home security system through operation of a website rather than through the cumbersome automated systems and choices provided via telephone; b) providing a geographically independent standard interface for remote connection to a home security system that is universally accessible and not platform or hardware dependent.

47.   A person of ordinary skill in the art at the time of the invention would have recognized that the steps (and combination of steps) claimed in the '097 Patent were, at the time of invention, unconventional and describe remote monitoring of home security and automation systems in a way that, at the time of the invention, was not routine.

48.   A person of ordinary skill in the art at the time of the invention would have understood that, at the time of the invention, there was no conventional manner in which to use a web browser remotely to monitor and control home automation and security systems. A skilled artisan, at the time of the invention, would have recognized the problem that such remote monitoring at the time of the invention could only be accomplished via cumbersome telephone-based input and automation systems.

49.   The '097 Patent provides technical solutions to this problem not solved in the prior art. By using a web browser so that "when a customer connects to their home, their home effectively appears to them as a website, with all devices, security and otherwise, accessible for monitoring and control." '097 Patent at 2:64-67.

50.   A person skilled in the art at the time of the invention would have understood that the system of using an Internet browser; a Cloud external to the user premises and accessible via the Internet browser; a plurality of connection gateways that are part of the home network; and a communications server located in the Cloud and adapted to communicate on-demand with the connection gateways was not, at the time of the invention, conventional, well-understood, nor routine.

51.   A person of ordinary skill in the art at the time of the invention would have understood that the system described in claim 1 of the '097 Patent was not, at the time of the invention, conventional, well-understood, or routine.
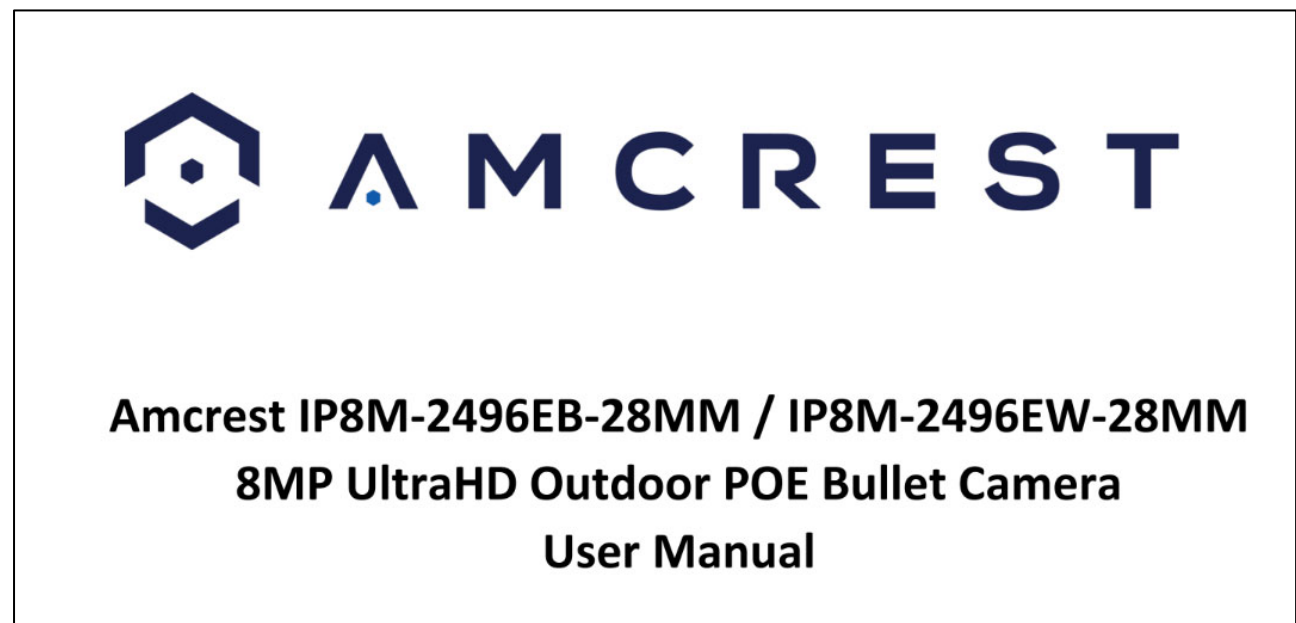
52.   A person skilled in the art at the time of the invention would have understood that the claims recite steps and structural limitations operating in an unconventional manner to achieve an improved operation of home security and automation.

53.   These technological improvements provide greater cost savings and efficiencies in allowing remote monitoring of a home security and automation systems through a web browser.

54.   The novel use and arrangement of the specific system recited in the '097 claims were not well-understood, routine, nor conventional to a person skilled in the relevant field at the time of the inventions.

<u>Defendant's Infringing Products</u>

55.   Amcrest provides smart home solutions through the Amcrest brand with products such as smart home products, IP cameras, including both wired and wireless outdoor cameras, indoor cameras, and security camera systems that are viewable through one of the Amcrest Apps or computer—or the "Accused Products." The Accused Products also include functionality whereby the Defendant is able to access and process the personal data of its users—users are required to agree to provide this information for the benefit of the Defendant in order to use the Accused Products.

Amcrest IP8M-2496EB-28MM / IP8M-2496EW-28MM
8MP UltraHD Outdoor POE Bullet Camera
User Manual

https://support.amcrest.com/hc/en-us/articles/360001554112-User-Manuals

AMCREST POE AI CAMERA User Guide

https://manuals.plus/amcrest/poe-ai-camera-manual.pdf

AMCREST

SmartHome

2MP Wi-Fi Pan/Tilt Camera

User Manual

https://support.amcrest.com/hc/en-us/articles/360040091111-User-Manual-ASH21-
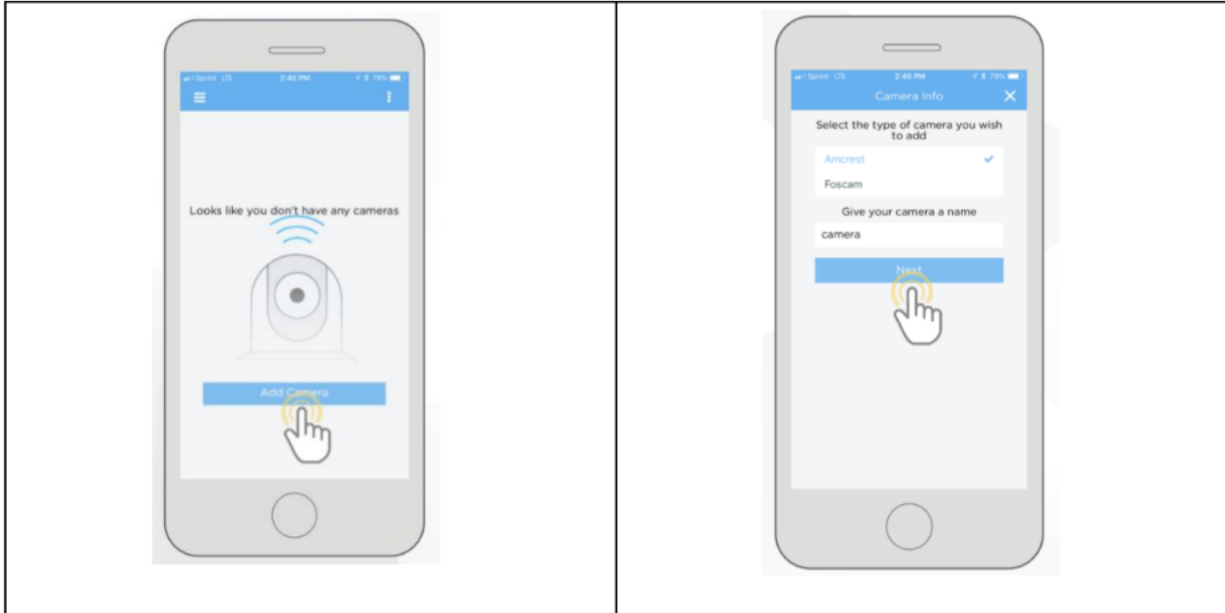
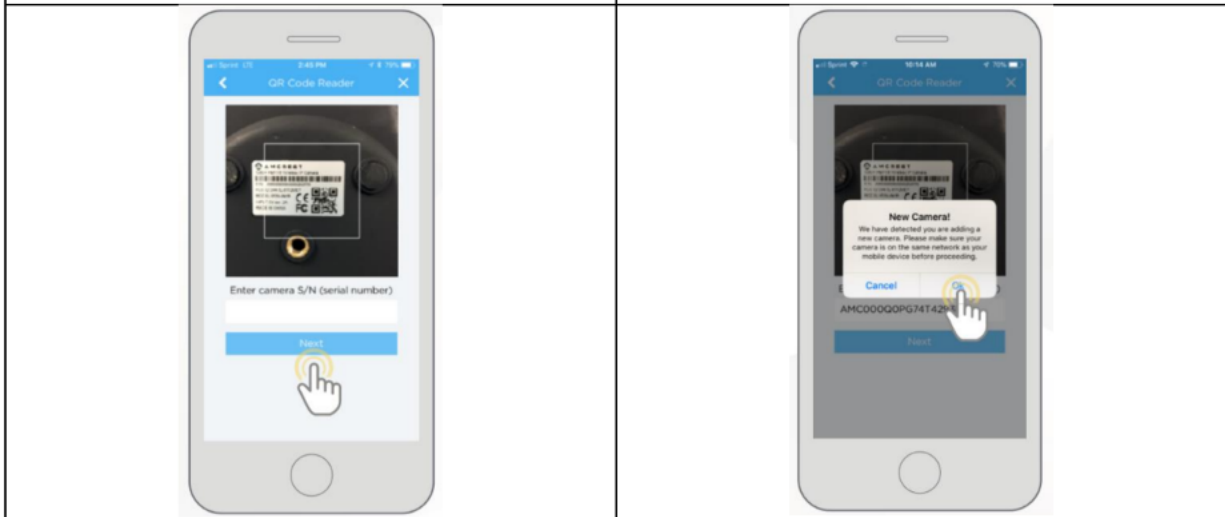1. Download and open the Amcrest Cloud app from the App Store or Play Store

Note: Connect your mobile device to the same network that your camera is on.

2. Register for an Amcrest Cloud account. To register click on **Sign Up** and fill out the form to complete registration.

3. Tap on **Add Camera**	4. Give your camera a name (Ex. Garage, Living Room, Kitchen, etc.) and tap **Next** to continue.
5. Scan the QR code on the back/side/bottom of the camera or manually enter the camera's serial number in the **Enter camera S/N (serial number** field. Press **Next** to continue.	6. If you are adding a new camera that does not have a set password the app will automatically detect that a new camera is being added. Tap **OK** to proceed.

AMCREST

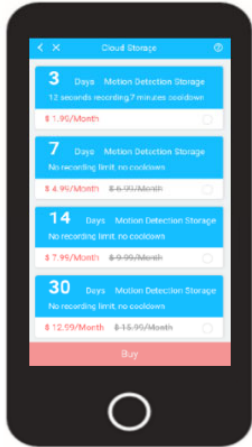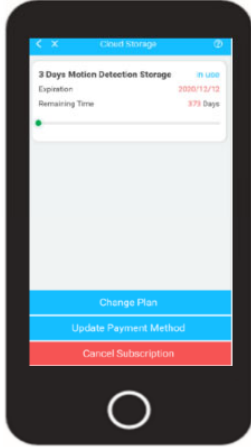https://support.amcrest.com/hc/en-us/articles/360001554112-User-Manuals
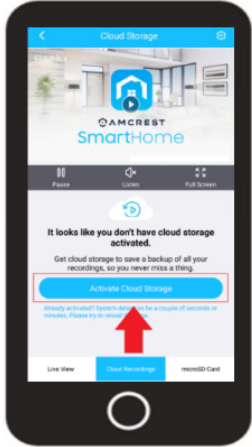
Amcrest Smart Home Cloud

The Amcrest Smart Home Cloud is an optional premium cloud storage service that offers a wide range of storage options for cloud users who wish to have secure cloud based options for their recordings. This is different from Amcrest Cloud service as the Amcrest Smart Home cloud is exclusive to Amcrest Smart Home devices and will not be compatible with other traditional or legacy Amcrest IP cameras or devices.

All cloud plans are available for purchase in the Amcrest Smart Home app once an account and device has been properly setup. An Amcrest Smart Home cloud subscription will be active for exactly 30 days starting from the minute you subscribed and are based off motion detection recordings only. To keep a cloud subscription active it is recommended to select "Auto Renewal" when checking out. For more information on how to activate an Amcrest Smart Home Cloud storage plan, please refer to the information provided below.

Access Your Account

Log into your Amcrest Smart Home app and select the device you wish to activate.

On the live view screen tap on **Cloud Recordings**.

Activate Cloud Storage

Tap on **Activate Cloud Storage**.

Choose Your Plan

Select a Cloud Storage plan from the list of cloud plans and tap **Buy.**

View Cloud Plan

Enter your billing information into the billing form. All plans will require a credit card to process the request.

After you have purchased your Amcrest Smart Home cloud plan you will be able to store and view your recordings all from the Cloud Recordings menu.

https://support.amcrest.com/hc/en-us/articles/360040091111-User-Manual-ASH21-

56.   Amcrest provided promotional and instructional videos promoting the Accused Products online on websites such as youtube.com.

https://www.youtube.com/watch?v=d6nLDdSOfOk

Amcrest Surveillance Pro - Setup Remote Access for Amcrest IP Cameras
https://www.youtube.com/watch?v=_v5K3Me8bhY

57.   The Amcrest System provides smartphone applications, and internet web portals, for

monitoring home security and camera systems (collectively, the "Amcrest System Apps").

Quick and Easy Setup

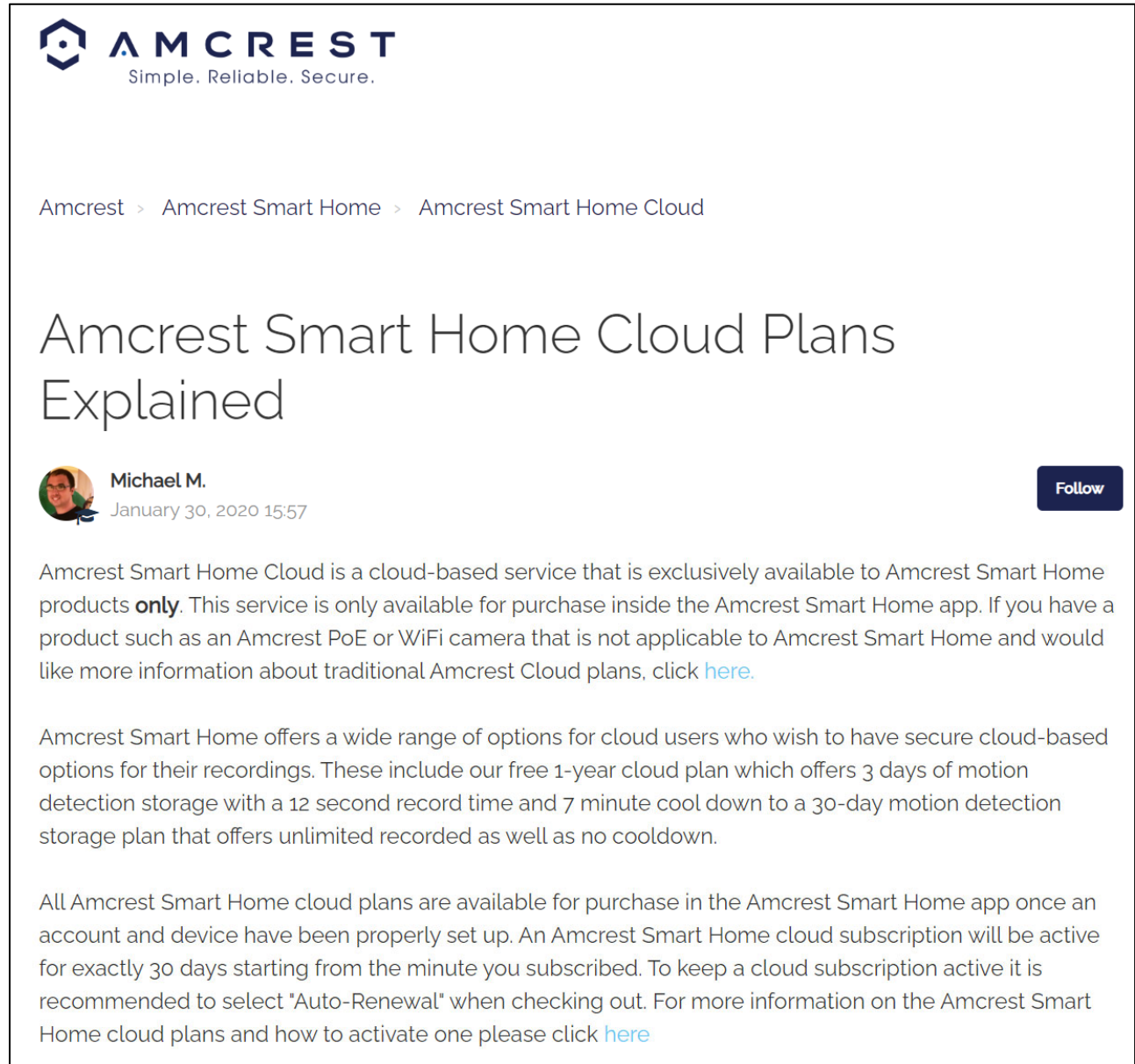Quickly add cameras with our easy setup process to immediately start recording and reviewing footage on the cloud.

https://amcrest.com/cloud/#NewPlans

17

AMCREST
Simple. Reliable. Secure.

Amcrest > Amcrest Smart Home > Amcrest Smart Home Cloud

Amcrest Smart Home Cloud Plans Explained

Michael M.
January 30, 2020 15:57

Follow

Amcrest Smart Home Cloud is a cloud-based service that is exclusively available to Amcrest Smart Home products **only**. This service is only available for purchase inside the Amcrest Smart Home app. If you have a product such as an Amcrest PoE or WiFi camera that is not applicable to Amcrest Smart Home and would like more information about traditional Amcrest Cloud plans, click here.

Amcrest Smart Home offers a wide range of options for cloud users who wish to have secure cloud-based options for their recordings. These include our free 1-year cloud plan which offers 3 days of motion detection storage with a 12 second record time and 7 minute cool down to a 30-day motion detection storage plan that offers unlimited recorded as well as no cooldown.

All Amcrest Smart Home cloud plans are available for purchase in the Amcrest Smart Home app once an account and device have been properly set up. An Amcrest Smart Home cloud subscription will be active for exactly 30 days starting from the minute you subscribed. To keep a cloud subscription active it is recommended to select "Auto-Renewal" when checking out. For more information on the Amcrest Smart Home cloud plans and how to activate one please click here

https://support.amcrest.com/hc/en-us/articles/360038973932-Amcrest-Smart-Home-Cloud-Plans-Explained

58.   The Amcrest System includes various Amcrest servers that form networks (e.g., a first network) located external to a user's premises (business or home) and are accessible via a smartphone app or Internet browser. Amcrest offers two cloud-based services called the "Amcrest Cloud" or "Amcrest Smart Home Cloud." In reference to the Accused Products and the networks formed by the Amcrest System, these cloud products shall jointly be referred to as the "Amcrest Cloud." The Amcrest Cloud includes a plurality of communications servers with hardware processing circuitry

18

(second hardware processing circuitry) (referred to interchangeably as "Amcrest Communication Servers" or "Amcrest Servers").

59.   The Amcrest System includes a plurality of devices, such as Amcrest wired and wireless camera devices, smart hubs, and alarm hubs, which serve as "Connection Gateways". At least a subset (a plurality) of the Amcrest Connection Gateways are located in a user (home/office) premises and are part of a local (home/office) network in such premises (referred to as "Amcrest Home Network"). The Amcrest Servers are configured to connect to the Amcrest Connection Gateways.

60.   The Amcrest Communications Servers are adapted to interconnect on-demand with the Amcrest Connection Gateways. The Amcrest Connection Gateways are accessible by the Amcrest Communications Servers. The Amcrest Communications Servers are accessible via the Amcrest System Apps.

61.   When a Amcrest System App is used to access the Amcrest Cloud to monitor or control devices in the Amcrest Home Network, authorization data is provided by the Amcrest System App. See, e.g.:

https://www.amcrestcloud.com/secure-login
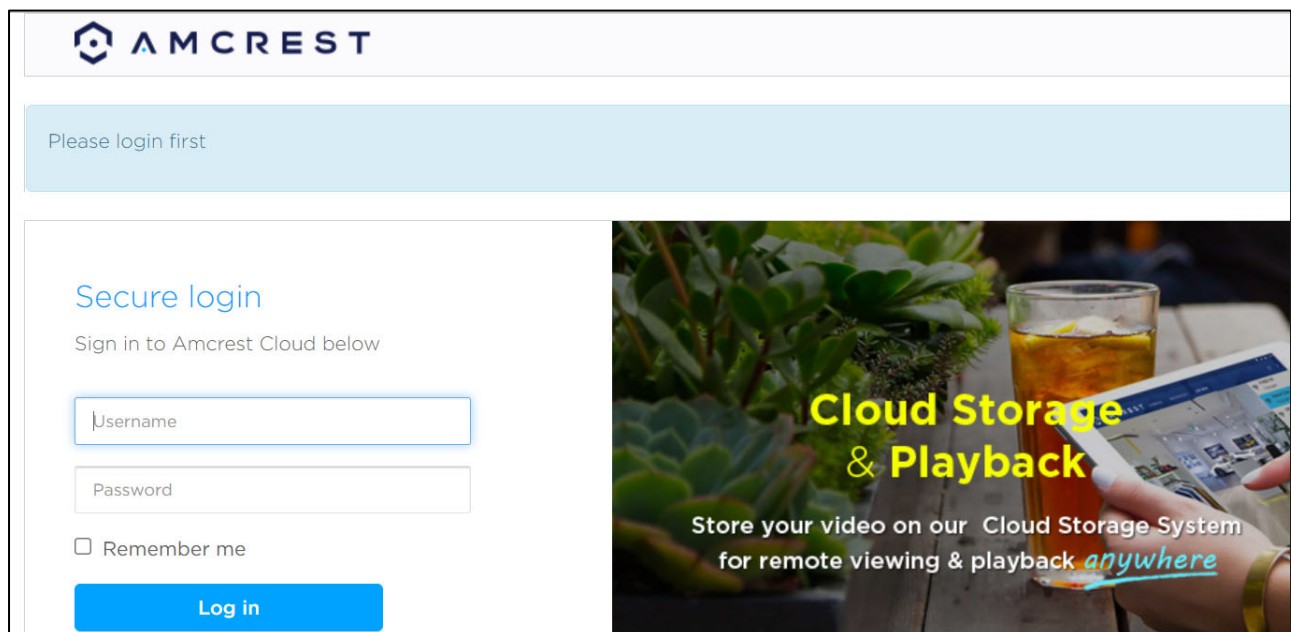
COUNT I – DIRECT PATENT INFRINGEMENT OF THE '526 Patent

62.   Portus re-alleges the foregoing paragraphs as if fully set forth herein.

63.   Defendant's infringing Accused Products and other remote security and automation control systems with the same or similar features and functionality that satisfy each element of one or more asserted claims.

64.   Defendant has directly infringed the '526 Patent in violation of 35 U.S.C. § 271(a) by one or more of the following: (1) making the Accused Products which embody the patented inventions of at least claim 57 of the '526 Patent, by combining all elements of the Accused Products as described above, in a manner that meets each limitation of at least claim 57 of the '526 Patent; and (2) putting into service and operating the Accused Products when all elements of such system are combined as described above, thus meeting each limitation of at least claim 57 of the '526 Patent.

65.   The Accused Products satisfy various elements of the claims of the '526 Patent, including certain devices that are Connection Gateways or networked components of the respective home network, or both.

66.   For example, through the Amcrest Accused Products, Defendants infringe claim 57 of the '526 Patent. The Amcrest Accused Products form a system for remote access of user premises networks in respective user premises, the system comprising:

a.   a first network (a) located external to said user premises (e.g., *the Amcrest Cloud, which is located external to the user premises*), (b) including a first arrangement of processing circuitry comprising at least one hardware processor programmed to control network access (e.g., *the Amcrest servers have processors programmed to control network access through a username and password*), and (c) including a hardware user access browser device that comprises a processor running an access browser (e.g., *Amcrest servers and Cloud are accessible by a user through the Amcrest System Apps*); and

b.   a plurality of second arrangements of processing circuitry each comprising at least one hardware processor programmed to control network access, each of at least a subset of which is located in a respective one of the user premises and part of the respective user premises network of the respective user premises (e.g., *the Amcrest System includes a plurality of connection gateways, such as smart home products, IP cameras, including both wired and wireless outdoor cameras, indoor cameras, and security camera systems*);

20

c.   wherein:

d.   said first circuitry arrangement is adapted by its programming to initiate an establishment of network connections to said second circuitry arrangements (e.g., *the Amcrest Servers are configured to connect to the Amcrest Connection Gateways*);

e.   the user access browser located on the first network is usable, by input of Uniform Resource Locators (URL), for locating and examining information on said first network and said user premises networks (e.g., *the Amcrest System is configured to be responsive to the input of a URL, when the Amcrest Cloud and Amcrest Communications Servers are accessed as a result of the input of the URL at the Amcrest System Apps, the Amcrest Communications Server provides Amcrest System Apps information like images or videos*);

f.   each of the at least the subset of second circuitry arrangements is accessible by the first circuitry arrangement (e.g., *the Amcrest Communications Servers are configured to connect to the Amcrest Connection Gateways*);

g.   responsive to user-input of a URL in accordance with which said user access browser accesses a predetermined location on said first network to which address the URL corresponds, said first circuitry arrangement subsequently, by execution of its programming (e.g., *the Amcrest System is configured to be responsive to the input of a URL, at the Amcrest System Apps, to access an address on the Amcrest Cloud, such that the Amcrest System Apps provide authorization data*):

h.   determines which one of said user premises networks in which one of said second circuitry arrangements is located authorization data indicates authority to at least one of monitor and control (e.g., *when a Amcrest System App is used to access the Amcrest Cloud to monitor or control devices in the Amcrest Home Network, authorization data is provided by the Amcrest System App*): and

i.   initiates an establishment of a network connection to said one of said second circuitry arrangements to create a new communications session for a temporary interconnection between said first network and said determined one of said user premises networks to at least one of control and monitor operation of at least one of the one or more devices of said user premises network, by which communications session the first network (e.g., *the Amcrest Communications Server creates a new communications session between itself and the Amcrest Connection Gateway in a user's home network that was determined to be indicated by the authorization data. In normal operation of the Amcrest System, the new communications session is used to at least monitor or control at least one service or networked component in user's home network*):

j.   obtains information contained within the user premises network from the second circuitry arrangement of the determined user premises network (*e.g., after the new communications session is created, the Amcrest Cloud obtains/receives information contained within the determined a user's home network from the Amcrest Connection Gateway (e.g., from one of the networked components)*); and

k.   using a web server, serves to the user access browser the information from the second circuitry arrangement of the determined user premises network (e.g., *the system provides such information to the Amcrest System Apps*);

21

l. the communications session provides a seamless access to information stored on said determined one of said user premises networks from said user access browser (e.g, *the system saves such information in the Amcrest System Apps for subsequent review by a user without requiring the user to provide the authentication data*); and

m. the at least one of control and monitoring of the at least one device using the first circuitry arrangement is possible only by interaction with information served by said one of said second circuitry arrangements (e.g., *the Amcrest devices may only be remotely controlled and monitored by providing information from the device to the Amcrest Cloud*).

67.   Defendants various Accused Products infringed based on similar functionality as described above.

68.   Defendant conditions use of the remote access features of the Accused Products and its customers' receipt of a benefit upon performance of the limitations of the asserted claims in the Asserted Patents, and Defendant establishes the manner or timing of that performance. Defendant requires that a user agree to terms and conditions that allow Defendant to track content, use, and performance information of user and the Accused Products. For example, users must agree to Amcrest's terms and conditions that "your acceptance of this Agreement constitutes your acceptance and agreement to be bound by Amcrest's Privacy Policy." These Terms and Conditions are available at https://amcrest.com/terms. Amcrest's Privacy Policy further defines the personal information that the user must agree to allow Amcrest to obtain and use: "For specific purposes, in case you provide your name, gender, category and number of credentials, date of birth, country, email address, telephone number, contact address, postal code, services, or information desired and other similar personal information that are required for registration or reading of e-information by voluntary filing in forms, you will be deemed having understood and accepted the use of your personal information and agree that the respective Amcrest app or apps may use your personal information for specific purposes. Also, to improve technology as well as service, Amcrest apps may collect, use, and provide your non-privacy information to third parties, which helps to provide you with a better user experience. Also, to improve technology as well as service, Amcrest apps may collect, use, and provide your non-privacy information to third parties, such as lock time, alarm number, Amcrest

device type, Amcrest device name and Amcrest device ID, which help to provide you with a better user experience. This app collects location data to enable Wi-Fi network detection in the background." The Amcrest privacy policy is available at https://amcrest.com/privacy-policy.

69.   The Accused Products, when combined and used as described above, satisfy each and every element of each asserted claim of the '526 Patent either literally or under the doctrine of equivalents.

70.   Defendant's infringing activities are and have been without authority or license under the '526 Patent.

71.   The preceding discussion of claim 57 in the '526 Patent serves as an example only. The Accused Products infringe other claims in the '526 Patent upon same or similar grounds. Portus reserves its right to identify additional claims and additional infringing products as supported by discovery in the case.

72.   As a result of Defendant's unlawful infringement of the '526 Patent, Portus has suffered and will continue to suffer damage. Portus is entitled to recover from Defendant the damages suffered by Portus as a result of Defendant's unlawful acts of infringement.

73.   On information and belief and at a minimum, Defendant has been aware that the claims in the application that became the '526 Patent were allowed before the filing of this complaint.

74.   On information and belief, given Defendant's prior knowledge of the '526 Patent and their own infringement of the same, Defendant has induced their users' and contributed to their users' direct infringement of one or more claims of the '526 Patent through the Defendant's advertisements, instructions, advice, and guidance as provided by user manuals and instructions, the Defendant's websites, and Defendant's support and help services.

75.   Moreover, on information and belief, its infringement has been willful and egregious. Because of Defendant's willful and egregious infringement, Portus is entitled to enhanced damages, in the form of treble damages, under 35 U.S.C. § 284.

76.   To the extent Defendant did not learn of the '526 Patent and its infringement before the filing of this complaint by virtue of its monitoring of prior art and published patents and communications from Portus and its agents, Defendant was willfully blind to its infringement of the '526 Patent.

77.   Furthermore, because Defendant's infringement of the '526 Patent is willful, this action is "exceptional" within the meaning of 35 U.S.C. § 285, entitling Portus to its attorneys' fees and expenses.

COUNT II – DIRECT PATENT INFRINGEMENT OF THE '097 PATENT

78.   Plaintiffs reallege and incorporate by reference the allegations set forth above, as if set forth verbatim herein.

79.   Defendant's infringing Accused Products and other remote security and camera systems with the same or similar features and functionality that satisfy each element of one or more asserted claims.

80.   Defendant has directly infringed the '097 Patent in violation of 35 U.S.C. § 271(a) by one or more of the following: (1) making the Accused Products which embody the patented inventions of at least claim 1 of the '097 Patent, by combining all elements of the Accused Products as described above, in a manner that meets each limitation of at least claim 1 of the '097 Patent; and (2) putting into service and by operating the Accused Products when all elements of such system are combined as described above, thus meeting each limitation of at least claim 1 of the '097 Patent.

81.   For example, through the Amcrest Accused Products, Defendants infringe claim 1 of

the '097 Patent. The Amcrest Accused Products form a system for remote access of a user premises

comprising:

a. a first hardware processing circuitry running an access browser module (*e.g., the Accused Products utilizes an access browser hardware device including a processor to access the internet through the Amcrest System Apps*);

b. a second hardware processing circuitry located in a first network (*e.g., the Accused Products include a second processor in the Amcrest Cloud that is located external to the user premises*); and

c. a connection gateway that is located in, and is part of a local network of, the user premises (*the Accused Products include a plurality of connection gateways, e.g., Amcrest connection gateways, such as the Amcrest cameras) each comprising at least one hardware processor and each of at least a subset of which is located in a respective one of the user premises and is part of the respective home network of the respective user (e.g., connected to the home network via Ethernet*));

d. wherein:

e. the second hardware processing circuitry is external to the user premises, is accessible via the access browser module, and is configured to communicate on-demand with the connection gateway (*e.g., the Accused Product includes a communications server (e.g., Amcrest Communications or Cloud servers) comprising at least one hardware processor and located in said Amcrest Cloud and adapted to interconnect on-demand with said connection gateways (e.g., users are able to access their devices through the Amcrest System Apps*));

f. the connection gateway is integrated with or communicatively coupled to one or more networked components of the local network of the user premises (*e.g., the connection gateways are accessible by the Amcrest Cloud and are integrated with networked components (e.g., a user's Amcrest devices) of the respective home network*); and

g. the system is configured such that user-input of a Uniform Resource Locator (URL), in accordance with which the first hardware processing circuitry, using the access browser module, accesses an address on the first network, begins a sequence in which the second hardware processing circuitry responsively serves to the first hardware processing circuitry, via the access browser module, information regarding at least one of the one or more networked components of the local network, which information the second hardware processing circuitry obtains from the connection gateway without a direct communicative coupling between the second hardware processing circuitry and the at least one networked component of the local network (*e.g., the Defendants' web application is responsive to user-input of a Uniform Resource Locator (URL) (e.g., when accessing Amcrest System Apps) in accordance with which said app accesses a predetermined address on said Amcrest Cloud to which the URL corresponds, in which accessing said app provides information (e.g., videos) contained within the home network from the connection gateway of the determined home network and Amcrest's Cloud servers are not directly communicatively coupleable to a user's*

Amcrest devices (e.g., certain Amcrest devices only communicate through connection gateways); in which accessing said app provides authorization data to the Amcrest Cloud (e.g., a login and password));

h.   wherein the sequence includes the first hardware processing circuitry transmitting to the second hardware processing circuitry authentication data indicating authority to access the at least one networked component of the local network, the transmission of the authentication data being required for the serving of the information to the first hardware processing circuitry (*e.g., the connection gateways for the Accused Products require that the user first provide authentication data in which accessing said app provides authorization data to the Amcrest Cloud to access the networked components)*, and wherein:

i.   the user premises is one of a plurality of user premises (*e.g., Defendants' Accused Products serve multiple users and multiple premise*s);

j.   the connection gateway is one of a plurality of connection gateways, each of which is located in, and is part of a respective local network of, a respective one of the plurality of user premises, and to each of which the second hardware processing circuitry is configured to connect(*e.g., Defendants' Accused Products serve multiple users and multiple premises, which each include at least one connection gateway located in and connects to a respective local network of the premises*); and

k.   the sequence further including the second hardware processing circuitry determining which one of the local networks the authentication data indicates authority to access (*e.g., Defendants' server is configured to use the user's login credentials to determine which home network is the user's home network and is further configured to provide authorization data to allow the user to access devices in the user's home network*);

l.   the sequence further including the second hardware processing circuitry establishing a new communication session between the first hardware processing circuitry and the connection gateway of the respective local network that the authentication data indicates authority to access upon verification of the authentication data (*e.g., Defendants' servers create a new communications session between the Amcrest Cloud and one of the Amcrest Connection Gateways to monitor operation of the Amcrest devices contained within the home network, which is determined based on the authentication*); and

m.   wherein the second hardware processing circuitry receives, via the connection gateway, selected information from at least one of the networked components of the local network of the user premises, and stores the selected information in the first network for subsequent review by a user associated with the user premises, without requiring the user to provide the authentication data (*e.g., in the Accused Products, information from the Amcrest devices, such as a user's login information, is stored in the first network, via for example in a user's mobile application, which may then be reviewed by a user associated with the user premises without requiring the user to provide the authentication data (e.g., a user in the first network may by automatically logged in to the Accused Products without having to subsequently enter their login information*)); and

n.   wherein the authority to access the at least one networked component of the local network by transmitting the authentication data also provides authority to access and review the

previously stored selected information in the first network via the access browser module (*e.g., the Amcrest user app and Amcrest Cloud servers communicate such that authority is provided to access a Amcrest device in a local network and review the previously stored selected information via authentication data*).

82.   Defendant's other Accused Products infringe based on similar functionality as the Amcrest Accused Products.

83.   Defendant conditions use of the remote access features of the Accused Products and its customers' receipt of a benefit upon performance of the limitations of the asserted claims in the Asserted Patents, and Defendant establishes the manner or timing of that performance. Defendant requires that a user agree to terms and conditions that allow Defendant to track content, use, and performance information of user and the Accused Products. For example, users must agree to Amcrest's terms and conditions that "your acceptance of this Agreement constitutes your acceptance and agreement to be bound by Amcrest's Privacy Policy." These Terms and Conditions are available at https://amcrest.com/terms. Amcrest's Privacy Policy further defines the personal information that the user must agree to allow Amcrest to obtain and use: "For specific purposes, in case you provide your name, gender, category and number of credentials, date of birth, country, email address, telephone number, contact address, postal code, services, or information desired and other similar personal information that are required for registration or reading of e-information by voluntary filing in forms, you will be deemed having understood and accepted the use of your personal information and agree that the respective Amcrest app or apps may use your personal information for specific purposes. Also, to improve technology as well as service, Amcrest apps may collect, use, and provide your non-privacy information to third parties, which helps to provide you with a better user experience. Also, to improve technology as well as service, Amcrest apps may collect, use, and provide your non-privacy information to third parties, such as lock time, alarm number, Amcrest device type, Amcrest device name and Amcrest device ID, which help to provide you with a better

user experience. This app collects location data to enable Wi-Fi network detection in the background." The Amcrest privacy policy is available at https://amcrest.com/privacy-policy.

84.   The Accused Products satisfy each and every element of each asserted claim of the '097 Patent either literally or under the doctrine of equivalents.

85.   Defendant's infringing activities are and have been without authority or license under the '097 Patent.

86.   The preceding discussion of claim 1 in the '097 Patent serves as an example only. The Accused Products infringe other claims in the '097 Patent upon same or similar grounds. Portus reserves its right to identify additional claims and additional infringing products as supported by discovery in the case.

87.   As a result of Defendant's unlawful infringement of the '097 Patent, Portus has suffered and will continue to suffer damage. Portus is entitled to recover from Defendant the damages suffered by Portus as a result of Defendant's unlawful acts of infringement.

88.   On information and belief and at a minimum, Defendant has been aware that the claims in the application that became the '097 Patent were allowed before the filing of this complaint.

89.   On information and belief, given Defendant's prior knowledge of the '097 Patent and their own infringement of the same, Defendant has induced their users' and contributed to their users' direct infringement of one or more claims of the '097 Patent through the Defendant's advertisements, instructions, advice, and guidance as provided by user manuals and instructions, the Defendant's websites, and Defendant's support and help services.

90.   Moreover, on information and belief, Defendants' infringement has been willful and egregious. Because of Defendants' willful and egregious infringement, Portus is entitled to enhanced damages, in the form of treble damages, under 35 U.S.C. § 284.

91.   To the extent Defendant did not learn of the '097 Patent and its infringement before the filing of this complaint by virtue of its monitoring of prior art and published patents and communications from Portus and its agents, Defendant was willfully blind to its infringement of the '097 Patent.

92.   Furthermore, because Defendant's infringement of the '097 Patent is willful, this action is "exceptional" within the meaning of 35 U.S.C. § 285, entitling Portus to its attorneys' fees and expenses.

JURY DEMAND

93.   Portus hereby demands a trial by jury.

PRAYER

WHEREFORE, Portus prays for judgment in its favor and against Defendants as follows:

a. A judgment that Defendant has infringed, either literally or under the doctrine of equivalents, one or more claims of the Asserted Patents;

b. An award of damages adequate to compensate for the infringements, but in no event less than a reasonable royalty made for use of the inventions of the Asserted Patents, together with interest and costs as determined by the Court;

c. An award of enhanced damages under 35 U.S.C. § 284, in the form of treble damages;

d. An award of on-going royalties for any continuing or future infringement of the claims of the Asserted Patents;

e. An award of Plaintiff's reasonable attorneys' fees, costs, and expenses pursuant to 35 U.S.C. §§ 284 and 285 or as otherwise permitted by law;

f. Such other and further relief at law or in equity as the Court determines is just and proper.

Dated: June 16, 2022   CLAYTON, MCKAY & BAILEY, PC

By: */s/ Manoj S. Gandhi*
Manoj S. Gandhi
manoj@cmblaw.com
Texas Bar No. 24055518
1919 Decatur St.
Houston, TX 77007
Phone: (832) 782-4964

Brannon C. McKay (*pro hac to be filed*)
brannon@cmblaw.com
800 Battery Ave. SE, Suite 100
Atlanta, GA 30338
Telephone: (404) 353-1628

J. Josh Clayton
josh@cmblaw.com
Texas Bar No. 24050426
2310 N. Henderson Ave., #312
Dallas, Texas 75206
Telephone: (713) 410-6217

ATTORNEYS FOR PLAINTIFFS