IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

PORTUS SINGAPORE PTE LTD AND PORTUS PTY LTD. Plaintiffs, v. **VIVINT, INC.,** Defendant.	**Civil Action No. 3:19-cv-310-K** **JURY TRIAL DEMANDED**

AMENDED COMPLAINT

This is an action for patent infringement in which Plaintiffs Portus Singapore Pte Ltd. and Portus Pty Ltd. (collectively, "Plaintiffs") accuse Defendant, Vivint, Inc. ("Defendant"), of infringing U.S. Patent Nos. 8,914,526 (the "'526 Patent") and 9,961,097 (the "'097 Patent") (collectively, the "Asserted Patents") alleging as follows:

PARTIES

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

2. Plaintiff Portus Pty Ltd. is a subsidiary of Portus Singapore Pte Ltd., and a company organized under the laws of Australia.

3. Upon information and belief, Defendant Vivint, Inc., is a corporation organized and existing under the laws of the State of Utah, with its principal place of business at 4931 North 300 West, Provo, UT 84604. Defendant may be served via its registered agent for service of process: Nathan Wilcox, 4931 North 300 West, Provo, UT 84604.

JURISDICTION AND VENUE

4. This is an action for infringement of the Asserted Patents arising under 35 U.S.C. §§ 271(a)-(b), 281, and 284 - 85. This Court has subject matter jurisdiction over this action under 28 U.S.C. §1331 and §1338(a).

5. Venue is proper in this district under 28 U.S.C. § 1400(b). Defendant has a regular and established place of business at 12850 Hillcrest Rd #207, Dallas, TX 75230 and has committed acts of patent infringement in this district.

6. Upon information and belief, Defendant 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 forum, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

U.S. PATENT NO. 8,914,526

7. On December 16, 2014, United States Patent No. 8,914,526 was duly and legally issued by the United States Patent and Trademark Office for an invention entitled "Local and Remote Monitoring Using a Standard Web Browser." A true and correct copy of the '526 Patent is attached hereto as Exhibit A.

8. Charles Cameron Lindquist and Timothy John Lindquist are the inventors of the '526 Patent.

9. Portus Singapore Pte Ltd., is the owner by assignment of the '526 Patent with all rights in and to that patent.

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

11. Upon information and belief, to the extent any marking was required by 35 U.S.C. § 287, Plaintiffs have complied with such requirements.

12. Defendant directly or through intermediaries, makes, uses, imports, sells, and/or offers for sale products and or/systems (*i.e.*, Vivint SmartHome with Vivint Smart Hub (the "Accused Instrumentality")) that infringe one or more claims of the '526 Patent. When placed into operation, the Accused Instrumentality infringes claims 1, 3, 4, 5, 12, 17, 18, 22, 23, 25, 44, 45, 46, 49, 50, 54, 58 and 59 of the '526 Patent. Additionally, Defendant induces the infringement of claims 1, 3, 4, 5, 12, 17, 18, 22, 23, 25, 44, 45, 46, 49, 50, 54, 58 and 59 of the '526 Patent by its customers using the Accused Instrumentalities.

U.S. PATENT NO. 9,961,097

13. On May 1, 2018, United States Patent No. 9,961,097 was duly and legally issued by the United States Patent and Trademark Office for an invention entitled "System for Remote Access of a User Premises." A true and correct copy of the '097 Patent is attached hereto as Exhibit B.

14. Charles Cameron Lindquist and Timothy John Lindquist are the inventors of the '097 Patent.

15. Portus Singapore Pte Ltd., is the owner by assignment of the '097 Patent with all rights in and to that patent.

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

17. Upon information and belief, to the extent any marking was required by 35 U.S.C. § 287, Plaintiffs have complied with such requirements.

18. Defendant directly or through intermediaries, makes, uses, imports, sells, and/or offers for sale products and or/systems, *i.e.*, the Accused Instrumentality, that infringe one or more

claims of the ‘097 Patent. When placed into operation, the Accused Instrumentality infringes claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 15, 16, 17, 18, 19, 20, 21, and 22 of the ’097 Patent. Additionally, Defendant induces the infringement of claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 15, 16, 17, 18, 19, 20, 21, and 22 of the ’097 Patent by its customers using the Accused Instrumentalities.

COUNT I
DIRECT INFRINGEMENT OF U.S. PATENT NO. 8,914,526

19. Upon information and belief, Defendant has been and is now infringing claims 1, 3, 4, 5, 12, 17, 18, 22, 23, 25, 44, 45, 46, 49, 50, 54, 58 and 59 of the ’526 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, directly or through intermediaries, making, using, selling, and/or offering for sale the Accused Instrumentality to the injury of Plaintiffs. Defendant is directly infringing, literally infringing, and/or infringing the ’526 Patent under the doctrine of equivalents. Defendant is thus liable for direct infringement of the ’526 Patent pursuant to 35 U.S.C. § 271(a).

20. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 1 of the ’526 Patent. It is a system for remote access of home networks in respective user premises comprising: an Internet browser hardware device including a processor running an Internet browser (*e.g.*, a smartphone, tablet, or computer with an internet browser is used by Defendant, its resellers, or end users); an extranet located external to said user premises and accessible via said Internet browser (*e.g.*, it includes a server which is located outside of the user premises); a plurality of connection gateways each comprising a hardware processor (*e.g.*, Smart Hub), 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 premises (*e.g.*, individual Smart Hubs are located at the premises of different users); and at least one communications server that each comprises a hardware processor located in said extranet and

adapted to interconnect on demand with said connection gateways (*e.g.*, a server adapted to connect to Smart Hubs when a user logs into their account); wherein: each of the at least the subset of the plurality of connection gateways is accessible by the at least one communications server and is communicatively coupled to one or more networked components of the respective home network in which the respective connection gateway is located (*e.g.*, each Smart Hub is connected to one or more networked components such as motion, window, and door sensors), the at least one communications server not being communicatively coupleable to the one or more networked components of the respective home network (*e.g.*, the server connects to the Smart Hub which connects to the networked components through the home network); and responsive to user input of a Uniform Resource Locator (URL) in accordance with which said Internet browser accesses a predetermined address on said extranet to which address the URL corresponds, in which accessing said Internet browser provides authorization data, one of said at least one communications server subsequently (*e.g.*, when a enters the URL of the server, it accesses the server's IP address corresponding to the URL): determines which one of said home networks in which one of said connection gateways is located said authorization data indicates authority to at least one of control and monitor (*e.g.*, when a user logs in using the username and password, it determines which Vivint device to access); and creates a new communications session between said communications server and said one of said connection gateways located in said determined one of said home networks to at least one of control and monitor operation of at least one service in said home network, by which communications session the extranet (*e.g.*, when a user enters their username and password, the server connects to the Smart Hub/Vivint devices): obtains information contained within the home network from the connection gateway of the determined home network (*e.g.*, it obtains information from the networked devices such as motion, window, and door sensors and

video cameras); and serves a webpage to the Internet browser via which the information from the connection gateway of the determined home network is provided to said Internet browser (*e.g.*, the server sends a webpage to the user's web browser which contains information from the Smart Hub). *See* Ex. A-1 Figs. 1-24 for factual support.

21. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 3 of the '526 Patent. They meet the limitations of claim 1 and further, wherein at least one of said networked components is a monitoring service located within said determined one of said home networks, and the operation of the at least one service includes operation of the monitoring device (*e.g.*, it includes window, door, and motion detection sensors which are located inside the premises and which are monitored). *See* Ex. A-1 Figs. 1-24 for factual support.

22. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 4 of the '526 Patent. They meet the limitations of claim 1 and further, wherein said communications server utilizes a telecommunications network to interconnect with said connection gateway (*e.g.*, the server connects to the Smart Hub over the internet, which is a telecommunications network). *See* Ex. A-1 Figs. 1-24 for factual support.

23. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 5 of the '526 Patent. They meet the limitations of claim 1 and further, wherein authentication to access said extranet is required only once per Internet browser session (*e.g.*, the user need only log in once). *See* Ex. A-1 Figs. 1-24 for factual support.

24. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 12 of the '526 Patent. They meet the limitations of

claim 1 and further, wherein the connection gateway acts as a hub and Internet connection mechanism for said networked components, including information appliances (*e.g.*, the Vivint Smart Hub acts as a hub and internet connection for the connected devices, such as door and windows sensors). *See* Ex. A-1 Figs. 1-24 for factual support.

25. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 17 of the ’526 Patent. They meet the limitations of claim 13 and further, wherein the control terminal is of reduced handheld size, so that it can operate as a universal premises remote control (*e.g.*, the Vivint Smart Home app provides remote access to Vivint connected devices). *See* Ex. A-1 Figs. 1-24 for factual support.

26. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 18 of the ’526 Patent. They meet the limitations of claim 13 and further, wherein the control terminal includes a digital camera, microphone and speaker, and video conferencing software, thus allowing the control terminal to be used as a videophone, through a standard browser interface (*e.g.*, the Vivint Smart Hub allows communication with family visitors, or monitoring agents through the panel). *See* Ex. A-1 Figs. 1-24 for factual support.

27. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 22 of the ’526 Patent. They meet the limitations of claim 1 and further, wherein at least one of said networked components comprises a digital security camera embodying an image capture and compression method and an interconnection to said connection gateway (*e.g.*, the Vivint Smart Hub connects to one or more video cameras which include an image capture and compression method which is connected to the Vivint Smart Hub). *See* Ex. A-1 Figs. 1-24 for factual support.

28. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 23 of the '526 Patent. They meet the limitations of claim 22 and further, wherein: said camera includes motion detection and image significance algorithms which run in said camera, and a filter so that only detected motion input is compressed and sent through said connection gateway to said extranet (*e.g.*, the Vivint doorbell and outdoor camera detects motion and is sent to the Vivint Smart Home app); and the system is configured to generate and send to the extranet an alert in response to a detected motion. (*e.g.*, a door, window, or outdoor sensor is activated by motion alert). *See* Ex. A-1 Figs. 1-24 for factual support.

29. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 25 of the '526 Patent. They meet the limitations of claim 1 and further, wherein: said system further comprises a device activating a security condition upon the occurrence of a predetermined event in said user premises in which said determined home network is located (*e.g.*, a motion, door, or windows sensor activates a sequence); and upon the occurrence of said predetermined event, said device notifies said connection gateway located in said determined one of said home networks and transfers event information on said predetermined event to said connection gateway located in said determined one of said home networks and said connection gateway located in said determined one of said home networks establishes an interconnection with said communications server and transfers said event information via said communications server for storage on the extranet for later interrogation by a user of said system and initiates predetermined alert notification actions (*e.g.*, the Vivint doorbell camera, indoor camera, and outdoor camera captures video of the alert event and stores it for later review by the user). *See* Ex. A-1 Figs. 1-24 for factual support.

30. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 44 of the ’526 Patent. They meet the limitations of claim 1 and further, wherein the at least one service includes a security monitoring service (*e.g.*, the Vivint Smart Home system provides home security monitor such as door and windows sensors). *See* Ex. A-1 Figs. 1-24 for factual support.

31. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 45 of the ’526 Patent. They meet the limitations of claim 1 and further, wherein the at least one service includes a video surveillance service (*e.g.*, the Vivint Smart Home app and Smart Hub provides video monitoring services). *See* Ex. A-1 Figs. 1-24 for factual support.

32. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 46 of the ’526 Patent. They meet the limitations of claim 1 and further, wherein the at least one service includes an automation and control service (*e.g.*, the video capture is automated). *See* Ex. A-1 Figs. 1-24 for factual support.

33. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 49 of the ’526 Patent. They meet the limitations of claim 1 and further, where the a least one service implements monitoring or control of a plurality of devices connected to at least one network interconnected with connection gateway (*e.g.*, the Vivint Smart Hub provides monitoring and control for multiple devices such as window and door sensors). *See* Ex. A-1 Figs. 1-24 for factual support.

34. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 50 of the ’526 Patent. They meet the limitations of claim 1 and further, where the Internet browser is on at least one of a mobile phone with web

browsing capability, a WebPhone, and Portable Digital Assistant (PDA) (*e.g.*, the Vivint Smart Hub website can be accessed from a smart phone). *See* Ex. A-1 Figs. 1-24 for factual support.

35. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 54 of the '526 Patent. They meet the limitations of claim 1 and further, wherein the extranet serves a webpage to the Internet browser, which webpage is user-interactable for input of instructions in accordance with which the one of said communications server communicates with the connection gateway of the determined home network, in accordance with which communication the connection gateway controls one or more of the networked components of the respective home network in which the respective connection gateway is located (*e.g.*, the server serves a webpage which includes controls allowing the networked devices to be controlled, such as a doorbell camera). *See* Ex. A-1 Figs. 1-24 for factual support.

36. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 58 of the '526 Patent. The Accused Instrumentality provides a system for remote access of user premises networks in respective user premises comprising: an Internet browser hardware device comprising a processor running an Internet browser (*e.g.*, a smartphone, tablet, or computer with an internet browser is used by Defendant, its resellers, or end users); a network located external to said user premises and accessible via said Internet browser (*e.g.*, it includes a server which is located outside of the user premises); a plurality of connection gateways, each comprising a hardware processor (*e.g.*, Smart Hub) and each of at least a subset of which is located in a respective one of the user premises (*e.g.*, individual Smart Hubs are located at the premises of different users) and is part of the respective user premises network of the respective user premises; and at least one communications server comprising a

hardware processor (*e.g.*, Smart Hub), located in said network and adapted to interconnect on-demand with said connection gateways (*e.g.*, a server adapted to connect to Smart Hubs when a user logs into their account); wherein: each of the at least the subset of the plurality of connection gateways is accessible by the at least one communications server and is communicatively coupled to one or more networked components of the respective user premises network in which the respective connection gateway is located (*e.g.*, each Smart Hub is connected to one or more networked components such as motion, window, and door sensors), the at least one communications server not being communicatively coupleable to the one or more networked components of the respective user premises network (*e.g.*, the server connects to the Smart Hub which connects to the networked components through the home network); and responsive to user-input of a Uniform Resource Locator (URL) in accordance with which said Internet browser accesses a predetermined address on said network to which address the URL corresponds, in which accessing said Internet browser provides authorization data, one of said at least one communications server subsequently (*e.g.*, when a enters the URL of the server, it accesses the server's IP address corresponding to the URL): determines which one of said user premises networks in which one of said connection gateways is located said authorization data indicates authority to at least one of control and monitor (*e.g.*, when a user logs in using the username and password, it determines which Vivint device to access); and creates a new communications session between said communications server and said one of said connection gateways located in said determined one of said user premises networks to at least one of control and monitor operation of at least one service in said user premises network, by which communications session the network located external to said user premises (e.g., when a user enters their username and password, the server connects to the Smart Hub/Vivint devices): obtains information contained within the user

premises network from the connection gateway of the determined user premises network (*e.g.*, it obtains information from the networked devices such as motion, window, and door sensors and video cameras); and uses a web server to serve to the Internet browser information from the connection gateway of the determined user premises network (*e.g.*, the server sends a webpage to the user's web browser which contains information from the Smart Hub). *See* Ex. A-1 Figs. 1-24 for factual support.

37. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 59 of the '526 Patent. The Accused Instrumentalities provide a system for remote access of home networks in respective user premises comprising: a mobile device comprising a hardware processor that provides a user interface (*e.g.*, the Smart Hub operates in conjunction with a mobile device, such as an android and iOS smartphone, running the Smart Home App which provides an interface); a plurality of connection gateways, each comprising at least one hardware processor (*e.g.*, Smart Hub) 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 premises (*e.g.*, individual smart hubs are located at the premises of different users); and an extranet (*e.g.*, Vivint Secure Servers) comprising at least one hardware device (*e.g.*, the server computer) and that is (a) located external to said user premises, (b) accessible via said mobile device via a wireless network and an Internet protocol connection, and (c) adapted to interconnect on-demand with said connection gateways (*e.g.*, Vivint Smart Hub); wherein: each of the at least the subset of the plurality of connection gateways is accessible by the extranet and is communicatively coupled to one or more networked components of the respective home network in which the respective connection gateway is located (*e.g.*, each smart hub is connected to one or more networked components such as window and door sensors), the extranet not being directly

communicatively coupleable to the one or more networked components of the respective home network (*e.g.*, the server connects to the smart hub which connects to the networked components through the home network); and responsive to user input, using the user interface, of a Uniform Resource Locator (URL) in accordance with which said mobile device accesses a predetermined address on said extranet to which address the URL corresponds, in which accessing said mobile device provides authorization data, said extranet subsequently (*e.g.*, when a user enters the URL of the server, it accesses the server's IP address corresponding to the URL): determines which one of said home networks in which one of said connection gateways is located said authorization data indicates authority to at least one of control and monitor (*e.g.*, when a user logs in using the username and password, it determines which Vivint smart hub device to access); creates a new communications session between said extranet and said one of said connection gateways located in said determined one of said home networks to at least one of control and monitor operation of at least one of the networked components in said home network (*e.g.*, when a user enters their username and password, the server connects to the smart hub); obtains information contained within the home network from the connection gateway of the determined home network (*e.g.*, it obtains information from the networked devices such as window and door sensors and video cameras); and using a web server, serves to the mobile device (e.g., mobile device running the Vivint Smart Home application or browser) the information from the connection gateway of the determined home network, for a display in the user interface that is based on the information (*e.g.*, Live, Motion, Light, & Temperature). *See* Ex. A-1 Figs. 1-24 for factual support.

38. As a result of Defendant's direct infringement of the '526 Patent, Plaintiffs have suffered monetary damages and are entitled to a money judgment in an amount adequate to compensate for Defendant's infringement, but in no event less than a reasonable royalty for the

use made of the invention by Defendant, together with interest and costs as fixed by the court, and Plaintiffs will continue to suffer damages in the future unless Defendant's infringing activities are enjoined by this Court.

39. Unless a permanent injunction is issued enjoining Defendant and its agents, servants, employees, representatives, affiliates, and all others acting on in active concert therewith from infringing the '526 Patent, Plaintiffs will be greatly and irreparably harmed.

COUNT II
DIRECT INFRINGEMENT OF U.S. PATENT NO. 9,961,097

40. Upon information and belief, Defendant has been and is now infringing claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 15, 16, 17, 18, 19, 20, 21, and 22 of the '097 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, directly or through intermediaries, making, using, selling, and/or offering for sale the Accused Instrumentality to the injury of Plaintiffs. Defendant is directly infringing, literally infringing, and/or infringing the '097 Patent under the doctrine of equivalents. Defendant is thus liable for direct infringement of the '097 Patent pursuant to 35 U.S.C. § 271(a).

41. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 1 of the '097 Patent. The Accused Instrumentality provides a system for remote access of a user premises comprising: a first hardware processing circuitry running an access browser module (*e.g.*, a smartphone, tablet, or computer with an internet browser is used by Defendant, its resellers, or end users); a second hardware processing circuitry (*e.g.*, a server) located in a first network; and a connection gateway that is located in, and is part of a local network of, the user premises (*e.g.*, the Smart Hub is a connection gateway connected to a network at the user premises); wherein: the second hardware processing circuitry is external to the user premises (*e.g.*, the server), is accessible via the access browser module (*e.g.*,

a user can log into the server via a web browser), and is configured to communicate on-demand with the connection gateway (*e.g.*, the server connects to and communicates with the Smart Hub upon user request); 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 Smart Hub functions as a gateway connecting various devices such as door and window sensors which are part of the local network); and the system is configured such that user-input of a Uniform Resource Locator (URL) (*e.g.*, the Vivint web page), in accordance with which the first hardware processing circuitry (*e.g.*, a smartphone, tablet, or computer), using the access browser module, accesses an address on the first network (*e.g.*, a server), begins a sequence in which the second hardware processing circuitry (*e.g.*, the server) responsively serves to the first hardware processing circuitry (*e.g.*, the smartphone, tablet, or computer), via the access browser module, information regarding at least one of the one or more networked components of the local network (*e.g.*, it provides information to the smartphone, tablet, or computer via the browser regarding the connected devices, such as door and windows sensors), which information the second hardware processing circuitry (*e.g.*, the server) 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 server receives the information related to the connected devices via the hub, and is not directly connected to the networked devices), wherein the sequence includes the first hardware processing circuitry (*e.g.*, the smartphone, tablet, or computer) transmitting to the second hardware processing circuitry (*e.g.*, the server) authentication data indicating authority to access the at least one networked component of the local network (*e.g.*, it provides information to the smartphone, tablet, or computer via the browser regarding the connected devices, such as door and windows sensors), the transmission of the authentication data

being required for the serving of the information to the first hardware processing circuitry, and wherein: the user premises is one of a plurality of user premises (*e.g.*, the system includes multiple smart hub's which are located at different user premises); 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 (*e.g.*, it includes multiple Smart Hubs which function as connection gateways and are installed a different user premises), and to each of which the second hardware processing circuitry is configured to connect (*e.g.*, the server is configured to connect to the multiple Smart Hubs); and the sequence further including the second hardware processing circuitry (*e.g.*, the server) determining which one of the local networks the authentication data indicates authority to access (*e.g.*, the server determine which Smart Hub device to access based on the user's login information), the sequence further including the second hardware processing circuitry (*e.g.*, the server) establishing a new communication session between the first hardware processing circuitry and the connection gateway (*e.g.*, the Smart Hub) of the respective local network that the authentication data indicates authority to access upon verification of the authentication data (*e.g.*, when a user enters their username and password, the server connects to the Smart Hub), and wherein the second hardware processing circuitry (*e.g.*, the server) receives, via the connection gateway (*e.g.*, the Smart Hub), selected information from at least one of the networked components of the local network of the user premises (*e.g.*, video information is received at the server from a networked video camera via the Vivint video devices), 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.*, the server receives and stores video from networked video cameras even while the user is not logged into the server), and wherein the authority to access the at least one networked component of the local network

(*e.g.*, a door and windows sensor or video camera) 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.*, when the user logs in to the server, they are granted access to the stored video on the server as well as access to the local devices). *See* Ex. B-1 Figs. 1-12 for factual support.

42. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 2 of the ’097 Patent. They meet the limitations of claim 1 and further, wherein the access browser module is an Internet browser (*e.g.*, smartphone, tablet, or computer). *See* Ex. B-1 Figs. 1-12 for factual support.

43. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 3 of the ’097 Patent. They meet the limitations of claim 1 and further, wherein the first network is an extranet (*e.g.*, Vivint Secure Servers). *See* Ex. B-1 Figs. 1-12 for factual support.

44. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 4 of the ’097 Patent. They meet the limitations of claim 1 and further, wherein the second hardware processing circuitry (*e.g.*, a server) is configured to interconnect on-demand with the connection gateway (*e.g.*, the server connects to the Smart Hub when a user logs in). *See* Ex. B-1 Figs. 1-12 for factual support.

45. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 5 of the ’097 Patent. They meet the limitations of claim 1 and further, wherein the second hardware processing circuitry (*e.g.*, a server) is not communicatively coupleable to the at least one networked component of the local network (*e.g.*,

the networked components are connected to the Smart Hub, not the server). *See* Ex. B-1 Figs. 1-12 for factual support.

46. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 6 of the '097 Patent. They meet the limitations of claim 1 and further, wherein the second hardware processing circuitry (*e.g.*, a server) stores information identifying a plurality of users (*e.g.*, user accounts), information identifying respective ones of the plurality of user premises which respective ones of the users (*e.g.*, the account identifies the specific Vivint devices, and thus the correct user premises) are permitted to access, and, for each of the connection gateways, respective connection information for communicating with the respective connection gateway. *See* Ex. B-1 Figs. 1-12 for factual support.

47. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 7 of the '097 Patent. They meet the limitations of claim 1 and further, wherein the second hardware processing circuitry (*e.g.*, a server) performs dynamic webpage generation in the sequence, which begins in response to the user-input of the URL, the dynamic webpage generation being personalized according to the authentication data (e.g., the user's webpage is personalized). *See* Ex. B-1 Figs. 1-12 for factual support.

48. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 8 of the '097 Patent. They meet the limitations of claim 1 and further, wherein the second hardware processing circuitry (*e.g.*, a server) obtains the information from the connection gateway (*e.g.*, the Smart Hub) via the new communications session (*e.g.*, an internet connection such as a TCP/IP connection). *See* Ex. B-1 Figs. 1-12 for factual support.

49. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 9 of the ’097 Patent. They meet the limitations of claim 1 and further, wherein the URL identifies the address. *See* Ex. B-1 Figs. 1-12 for factual support.

50. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 10 of the ’097 Patent. They meet the limitations of claim 1 and further, wherein the second hardware processing circuitry (*e.g.*, a server) includes a plurality of components distributed in the first network (*e.g.*, it includes multiple servers and storage devices connected in the first network). *See* Ex. B-1 Figs. 1-12 for factual support.

51. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 11 of the ’097 Patent. They meet the limitations of claim 1 and further, wherein the first hardware processing circuitry is external to the user premises (*e.g.*, the user’s smartphone, tablet, or computer is external to the user premises). *See* Ex. B-1 Figs. 1-12 for factual support.

52. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 15 of the ’097 Patent. They meet the limitations of claim 1 and further, wherein the first hardware processing circuitry is embodied in a mobile device (*e.g.*, a smartphone, tablet, or laptop computer). *See* Ex. B-1 Figs. 1-12 for factual support.

53. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 16 of the ’097 Patent. They meet the limitations of claim 1 and further, wherein the information is presented as a webpage by the access browser module. *See* Ex. B-1 Figs. 1-12 for factual support.

54. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 17 of the ’097 Patent. They meet the limitations of claim 1 and further, wherein the accessing includes at least one of controlling and monitoring one or more of the networked components (*e.g.*, it can monitor a video camera). *See* Ex. B-1 Figs. 1-12 for factual support.

55. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 18 of the ’097 Patent. They meet the limitations of claim 1 and further, wherein the selected information is event information captured by one of the networked components as a result of the occurrence of a predetermined event detected by one of the networked components (*e.g.*, events generated by a sensor are captured such as when motion is detected). *See* Ex. B-1 Figs. 1-12 for factual support.

56. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 19 of the ’097 Patent. The Accused Instrumentalities provide the system for remote access of a user premises comprising: a first hardware processing circuitry including a user interface (*e.g.*, a web browser operating on a device including hardware running a browser, such as a smartphone, tablet, or computer); a second hardware processing circuitry (*e.g.*, a server) located in a first network; and a connection gateway that is located in, and is part of a local network of, the user premises (*e.g.*, the Smart Hub is a connection gateway connected to a network at the user premises); wherein: the second hardware processing circuitry is external to the user premises (*e.g.*, the server), is accessible by the first hardware processing circuitry (*e.g.*, a user can log into the server via a web browser use a smartphone, tablet, or computer), and is configured to communicate on-demand with the connection gateway (*e.g.*, the server connects to and communicates with the smart hub upon user request); 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 Smart Hub functions as a gateway connecting various devices such as door and window sensors which are part of the local network); and the system is configured such that user-input of a Uniform Resource Locator (URL) using the user interface (*e.g.*, inputting the web address into a browser), in accordance with which the first hardware processing circuitry accesses an address on the first network (*e.g.*, the smartphone, tablet, or computer accesses the website), begins a sequence in which the second hardware processing circuitry responsively serves to the first hardware processing circuitry, for display using the user interface, information regarding at least one of the one or more networked components of the local network (*e.g.*, the server serves a webpage with information regarding the networked components such as windows and door sensors), 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 information from the connected devices comes from the Smart Hub device and is transferred to the server), 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 (*e.g.*, the smartphone, tablet, or computer transmits login information to the server which grants access to networked components such as windows and door sensors or video cameras), the transmission of the authentication data being required for the serving of the information to the first hardware processing circuitry (*e.g.*, no data will be transmitted until the user is authenticated), and wherein: the user premises is one of a plurality of user premises (*e.g.*, the system includes multiple Smart Hub's which are located at different user premises); 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 (*e.g.*, it includes multiple smart hubs which function as connection gateways and are installed a different user premises), and to each of which the second hardware processing circuitry is configured to connect (*e.g.*, the server is configured to connect to the multiple Smart Hubs); and the sequence further including the second hardware processing circuitry (*e.g.*, the server) determining which one of the local networks the authentication data indicates authority to access (*e.g.*, the server determine which smart hub device to access based on the user's login information), 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.*, when a user enters their username and password, the server connects to the smart hub), and wherein the second hardware processing circuitry (*e.g.*, the server) receives, via the connection gateway (*e.g.*, the Smart Hub), selected information from at least one of the networked components of the local network of the user premises (*e.g.*, video information is received at the server from a networked video camera via the Smart Hub), 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.*, the server receives and stores video from networked video cameras even while the user is not logged into the server), and wherein the authority to access the at least one networked component of the local network (*e.g.*, a door and windows sensor or video camera) by transmitting the authentication data also provides authority to access and review the previously stored selected information in the first network via the user interface (*e.g.*, when the user logs in to the server, they are granted access to

the stored video on the server as well as access to the local devices). *See* Ex. B-1 Figs. 1-12 for factual support.

57. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 20 of the ’097 Patent. They meet the limitations of claim 19 and further, wherein the accessing includes at least one of controlling and monitoring one or more of the networked components (*e.g.*, it can monitor a video camera). *See* Ex. B-1 Figs. 1-12 for factual support.

58. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 21 of the ’097 Patent. The Accused Instrumentalities provide system of claim 19 wherein the selected information is event information captured by one of the networked components as a result of the occurrence of a predetermined event detected by one of the networked components (*e.g.*, events generated by a sensor are captured such as when motion is detected). *See* Ex. B-1 Figs. 1-12 for factual support.

59. When Defendant, its resellers, or end-user customers, use the Accused Instrumentality, they directly infringe claim 22 of the ’097 Patent. They meet the limitations of claim 19 and further, wherein the first network is an extranet (*e.g.*, Vivint Secure Servers). *See* Ex. B-1 Figs. 1-12 for factual support.

60. As a result of Defendant’s direct infringement of the ’097 Patent, Plaintiffs have suffered monetary damages and are entitled to a money judgment in an amount adequate to compensate for Defendant’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendant, together with interest and costs as fixed by the court, and Plaintiffs will continue to suffer damages in the future unless Defendant’s infringing activities are enjoined by this Court.

61. Unless a permanent injunction is issued enjoining Defendant and its agents, servants, employees, representatives, affiliates, and all others acting on in active concert therewith from infringing the ’097 Patent, Plaintiffs will be greatly and irreparably harmed.

COUNT III
INDUCED INFRINGEMENT OF THE ASSERTED PATENTS

62. Upon information and belief, Defendant has been and is now inducing the infringement by its resellers and end-use customers of claims 1, 3, 4, 5, 12, 17, 18, 22, 23, 25, 44, 45, 46, 49, 50, 54, 58 and 59 of the ’526 Patent and claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 15, 16, 17, 18, 19, 20, 21, and 22 of the ’097 Patent in the State of Texas, in this Judicial District, and elsewhere in the United States, by, among other things, directly or through intermediaries, making, using, importing, selling and/or offering for sale the Accused Instrumentalities to the injury of Plaintiffs since at least February 6, 2019, the date of the filing of the Original Complaint. Defendant’s resellers and end-use customers are directly infringing, literally infringing, and/or infringing the Asserted Patents under the doctrine of equivalents. Defendant is thus liable for infringement of the Asserted Patents pursuant to 35 U.S.C. § 271(b).

63. As shown above, Defendant has and continues to indirectly infringe the Asserted Patents by inducing the infringement by its end-users and resellers of claims 1, 3, 4, 5, 12, 17, 18, 22, 23, 25, 44, 45, 46, 49, 50, 54, 58 and 59 of the ’526 Patent and claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 15, 16, 17, 18, 19, 20, 21, and 22 of the ’097 Patent in accordance with 35 U.S.C. 271(b).

64. As shown above, Defendant, its resellers, distributors, and end-users of the Accused Instrumentalities have engaged in and currently engage in activities that constitute direct infringement of claims 1, 3, 4, 5, 12, 17, 18, 22, 23, 25, 44, 45, 46, 49, 50, 54, 58 and 59 of the ’526 Patent and claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 15, 16, 17, 18, 19, 20, 21, and 22 of the ’097 Patent.

65. As shown above, the operation and use by Defendant, its resellers, or end-user customers of the Accused Instrumentality constitutes a direct infringement of claims

66. Defendant's affirmative act of selling and/or offering for sale the Accused Instrumentality and providing instruction manuals, advertisement of the infringing features, and support for the Accused Instrumentality have induced and continues to induce Defendant's resellers and end users to use the Accused Instrumentality in their normal and customary way to infringe claims 1, 3, 4, 5, 12, 17, 18, 22, 23, 25, 44, 45, 46, 49, 50, 54, 58 and 59 of the '526 Patent and claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 15, 16, 17, 18, 19, 20, 21, and 22 of the '097 Patent.

67. Through its making, selling, and/or offering for sale the Accused Instrumentality, Defendant specifically intends that its resellers and end-users directly infringe claims 1, 3, 4, 5, 12, 17, 18, 22, 23, 25, 44, 45, 46, 49, 50, 54, 58and 59 of the '526 Patent and claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 15, 16, 17, 18, 19, 20, 21, and 22 of the '097 Patent. Defendant has had knowledge of the Asserted Patents since at least February 6, 2019, the date of the filing of the original complaint, and actually induces others, such as resellers and end-use customers, to directly infringe by using, selling, supplying, and or distributing the Accused Instrumentality within the United States. Defendant is aware since at least February 6, 2019. that such actions would induce actual infringement. Furthermore, Defendant remains aware that these normal and customary activities would infringe the Asserted Patents.

68. For example, in connection with the sale and/or offering for sale of the Accused Instrumentality, Defendant provides manuals and support to resellers and end-use customers regarding the user and operation of the Accused Instrumentality. Specifically, Defendant provides support, *see e.g.*, https://support.vivint.com/s/. When end-users follow such instructions and support, they directly infringe the Asserted Patents. Defendant knows or should have known, since

at least February 6, 2019, that by providing such instructs and support, resellers and end-use customers follow these instructions and support and directly infringe the Asserted Patents.

69. Accordingly, Defendant has performed and continues to perform acts that constitute indirect infringement, and would induce actual infringement, with the knowledge of the Asserted Patents and with the knowledge or willful blindness to the fact that the induced acts would constitute infringement.

DEMAND FOR JURY TRIAL

Plaintiffs, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully requests that this Court enter:

1. A judgment in favor of Plaintiffs that Defendant has infringed the Asserted Patents;

2. A judgment in favor of Plaintiffs that Defendant has induced its resellers and end-users to infringe the Asserted Patents;

3. A permanent injunction enjoining Defendant and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in active concert therewith from infringement, inducing the infringement of, or contributing to the infringement of the Asserted Patents, or such other equitable relief the Court determines is warranted;

4. A judgment and order requiring Defendant pay to Plaintiffs their damages, costs, expenses, and prejudgment and post-judgment interest for Defendant's infringement of the Asserted Patents as provided under 35 U.S.C. § 284, and an accounting of ongoing post-judgment infringement; and

5. Any and all other relief, at law or equity, to which Plaintiffs may show themselves to be entitled.

DATED May 29, 2019.

Respectfully submitted,

By: */s/ Stevenson Moore*
Timothy T. Wang
Texas Bar No. 24067927
twang@nilawfirm.com
Stevenson Moore V
Texas Bar No. 24076572
smoore@nilawfirm.com

NI, WANG & MASSAND, PLLC
8140 Walnut Hill Ln., Ste. 500
Dallas, TX 75231
Tel: (972) 331-4600
Fax: (972) 314-0900

ATTORNEYS FOR PLAINTIFFS PORTUS SINGAPORE PTE LTD. AND PORTUS PTY LTD.

CERTIFICATE OF SERVICE

On May 29, 2019, I filed the foregoing document with the clerk of court for the U.S. District Court, Northern District of Texas. I hereby certify that I have served the document on all counsel of record by a manner authorized by Rule 5(b)(2) of the Federal Rules of Civil Procedure.

/s/ Stevenson Moore
Stevenson Moore