IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS

SHERMAN DIVISION

VIRGINIA INNOVATION SCIENCES, INC., Plaintiff, v. VECTOR SECURITY, INC., Defendant.	**Civil Action No. _____** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Virginia Innovation Sciences, Inc. ("VIS" or "Plaintiff"), for its Complaint against Defendant Vector Security, Inc., ("Vector" or "Defendant") alleges the following:

NATURE OF THE ACTION

1. This is an action for patent infringement arising under the Patent Laws of the United States, 35 U.S.C. § 1 *et seq*.

THE PARTIES

2. Plaintiff is a corporation organized under the laws of the State of Virginia with a place of business at 6301 Edsall Road #517, Alexandria, Virginia 22312.

3. Upon information and belief, Vector is a corporation organized and existing under the laws of Pennsylvania, with a place of business at 2000 Ericsson Drive, Warrendale, PA 15086, and can be served through its registered agent, The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington DE 19801. Upon information and belief, Vector sells and offers to sell products and services throughout the United States, including in this judicial district, and introduces products and services that into the stream of commerce and that

incorporate infringing technology knowing that they would be sold in this judicial district and elsewhere in the United States.

JURISDICTION AND VENUE

4. This is an action for patent infringement arising under the Patent Laws of the United States, Title 35 of the United States Code.

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

6. Venue is proper in this judicial district under 28 U.S.C. §1400(b). On information and belief, Vector has committed acts of infringement in this District and has a regular and established place of business within this District, including, without limitation, a branch location at 3416 E. Denman Ave., Lufkin, TX 75901.

7. On information and belief, Defendant is subject to this Court's general and specific personal jurisdiction because it has sufficient minimum contacts within the State of Texas and this District, pursuant to due process and/or the Texas Long Arm Statute because Defendant purposefully availed itself of the privileges of conducting business in the State of Texas and in this District, because Defendant regularly conducts and solicits business within the State of Texas and within this District, and because Plaintiff's causes of action arise directly from each of Defendant's business contacts and other activities in the State of Texas and this District.

COUNT I – INFRINGEMENT OF U.S. PATENT NO. 9,912,983

8. The allegations set forth in the foregoing paragraphs 1 through 7 are incorporated into this First Claim for Relief.

9. On March 6, 2018, U.S. Patent No. 9,912,983 ("the '983 patent"), entitled "METHOD AND SYSTEM FOR EFFICIENT COMMUNICATION," was duly and legally

issued by the United States Patent and Trademark Office. A true and correct copy of the ’983 patent is attached as Exhibit 1.

10. The inventions of the ’983 patent resolve technical problems related to the use of a wireless hub used in a detection system. For example, the ’983 patent overcomes limitations in the prior art relating to providing alerts as to the status of an item over the internet or other next-generation wireless communication network.

11. In contrast, the inventions allow a user to efficiently set up a system comprising a hub system connected with one or more sensors capable of sensing a status of an item, such that the hub system can be informed of an updated status of the item and notify servers and/or user terminals accordingly. Furthermore, the inventions of the ’983 patent enable a user to pair a variety of sensors with a hub system through short-range communications.

12. The claims of the ’983 patent recite an invention that is not merely the routine or conventional use of a wireless hub system. Instead, the invention relies on using a network interface and a short-range wireless transmission channel separately to both detect the status of an item being sensed by a sensor and transmit information about the status to a user device. The ’983 patent claims thus specify how signals are received and transmitted over both channels to promptly notify servers and/or user terminals of the status.

13. The technology claimed in the ’983 patent does not preempt all ways of using wireless hub based detection or monitoring systems, nor preempt the use of all wireless hub based detection or monitoring systems, nor preempt any other well-known or prior art technology.

14. Accordingly, each claim of the ’983 patent recites a combination of elements sufficient to ensure that the claim in practice amounts to significantly more than a patent on an ineligible concept.

15. Plaintiff is the assignee and owner of the right, title and interest in and to the ’983 patent, including the right to assert all causes of action arising under said patents and the right to any remedies for infringement of them.

16. Upon information and belief, Defendant has and continues to directly infringe, individually or jointly with Amazon.com, Inc., at least claims 117, 118, 119, 121, 122, 22, 24, 25, 62, and 65 of the ’983 patent (the “Asserted Claims”) by making, using, selling, importing and/or providing and causing to be used a wireless hub system, including but not limited to the Vector Security Home Security System, the Vector Security Home Security Video System, the Vector Security Voice Control with Amazon’s Echo Dot, and the Vector Security Mobile App (the “Accused Instrumentalities”).

17. In particular, claim 117 of the ’983 patent recites a wireless hub system configured to receive, through a wireless transmission channel, a signal transmitted in response to a detection of an updated status of an item having a unique identifier, identify the item, and communicate, through a network communication channel, information about the updated status to a user device in accordance with a configuration setting.

18. Claim 118 depends from claim 117 and further recites that the configuration setting specifies when and how to notify the user of the updated status.

19. Claim 119 depends from claim 117 and further recites that the signal from the item status sensing device is transmitted in response to an automatic detection, by a sensor included in the item status sensing device, of the updated status.

20. Claim 121 depends from claim 117 and further recites that the user device is a cellular phone.

21. Claim 122 depends from claim 117 and further recites that the wireless hub system is further configured to communicate a video from a video camera to a user terminal through a cellular network.

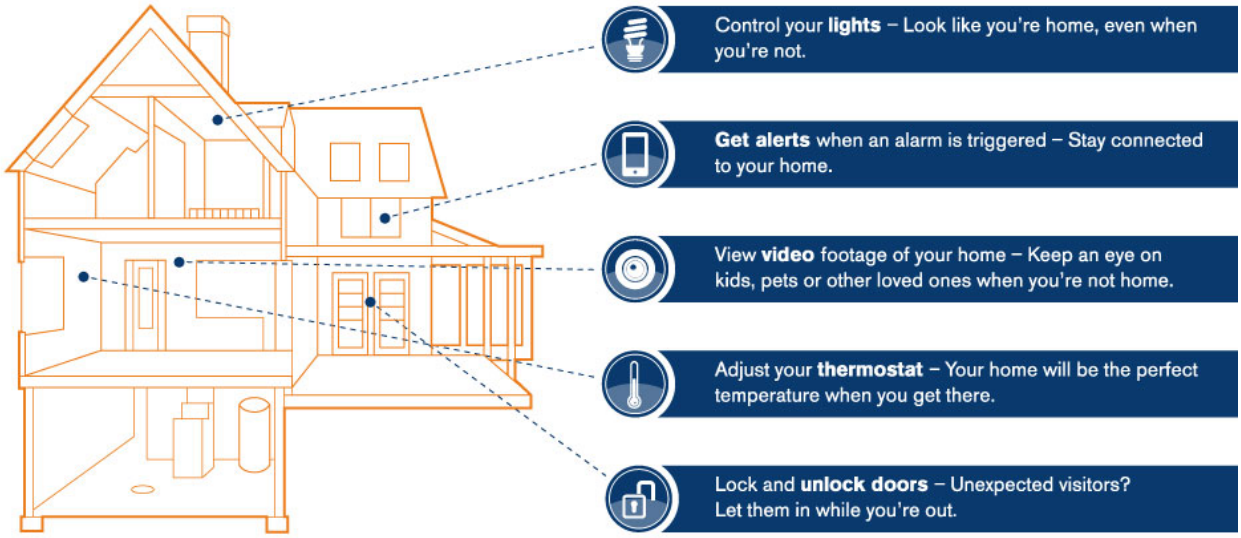
22. Claim 22 recites a wireless hub system configured to receive a wireless signal through a wireless communication network, a decoder to decompress the wireless signal, and a network interface configured to communicate information for managing an item status of an item in connection with an updated status of the item.

23. Claim 25 depends from claim 22 and further recites that the wireless hub is configured to communicate a video from a video camera to a user's terminal at least in part through a cellular network.

24. Claim 62 recites a wireless hub system configured to receive a wireless signal through a wireless communication network, a decoder to decompress the wireless signal, and a network interface configured to communicate information for managing an item status of an item in connection with an updated status of the item and corresponding to a unique identifier associated with the item.

25. Claim 65 depends from claim 62 and further recites that the wireless hub system is further configured to communicate a video from a video camera to a user's terminal through a cellular network or Internet.

26. The Accused Instrumentalities infringe the Asserted Claims. By way of example, the Vector Security System comprises a wireless control panel and one or more wireless sensors. *See, e.g.*:



(https://www.vectorsecurity.com/store/solutionOverview.)

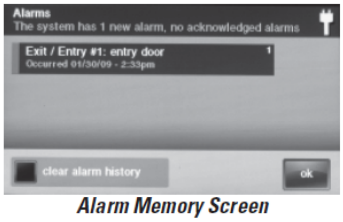
27. The wireless control panel in the Accused Instrumentalities includes a memory to store information (identifiers) for each of one or more wireless sensors (e.g., lights, entry sensors, etc.). *See, e.g.*:

Alarm Memory

If an alarm has occurred while the system was armed, the Disarm Screen will show the time and date of the alarm and the sensor(s) that triggered the alarm.

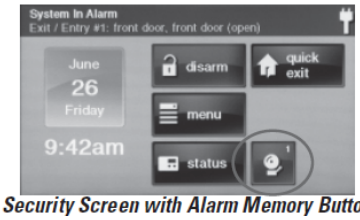
After the system is disarmed, the Alarm Memory screen will be displayed. The Alarm Memory Screen shows the sensor(s) that have caused the alarm. If more than one sensor has been triggered, the display will show the order that alarms occurred. **The alarm memory will automatically clear the next time the system is armed.** You can also check the **CLEAR ALARM HISTORY** button and press **OK** to manually clear the alarm memory (24-hour sensors that are still violated will remain in alarm memory).

Disarm Screen Showing Alarms



Alarm Memory Screen

Anytime there are events stored in alarm memory, the Security Screen will display the button. The number on the button is the number of sensors that triggered during the alarm. Press the button to view the Alarm Memory Screen.



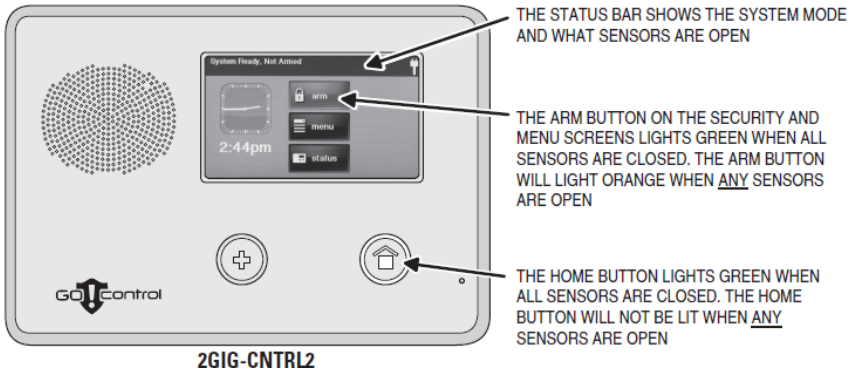
Security Screen with Alarm Memory Button

(https://www.vectorsecurity.com/UserFiles/File/PDF/Learning%20Center/2%20GIG%20Wireless%20Security%20System%20User%20Manual.pdf at 15.)

Viewing Each Sensor's Status

The Control Panel will also show you which sensor-protected doors and windows are open. Your installer has programmed descriptive names for each sensor-protected door and window. The Control Panel's color display will show the names of which door and windows are open.

- The top area of the display on the Home, Security, and Menu Screens will list any sensors that are currently open.
- Pressing the **STATUS** button will also display a list of all open sensors along with general system status and alerts.



2GIG-CNTRL2

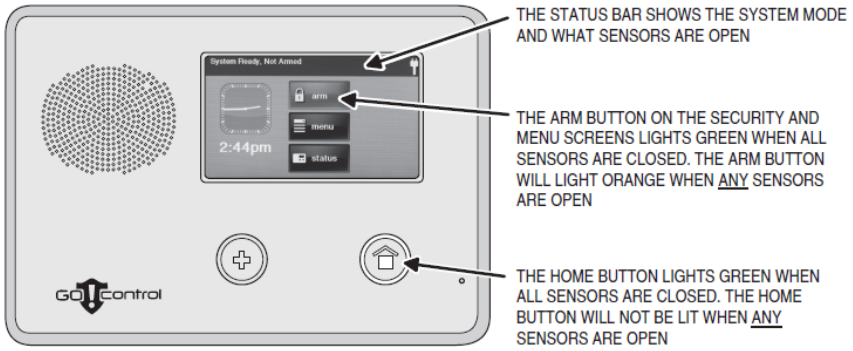
(https://www.vectorsecurity.com/UserFiles/File/PDF/Learning%20Center/2%20GIG%20Wireless%20Security%20System%20User%20Manual.pdf at 8.)

28. The control panel can identify an "item" (e.g., smoke, motion, etc.) associated with each of the sensors. *See, e.g.*:

Viewing Each Sensor's Status

The Control Panel will also show you which sensor-protected doors and windows are open. Your installer has programmed descriptive names for each sensor-protected door and window. The Control Panel's color display will show the names of which door and windows are open.

- The top area of the display on the Home, Security, and Menu Screens will list any sensors that are currently open.
- Pressing the **STATUS** button will also display a list of all open sensors along with general system status and alerts.

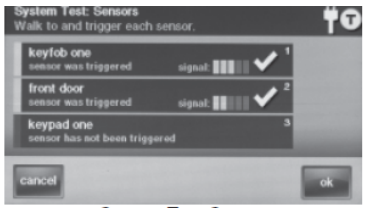


2GIG-CNTRL2

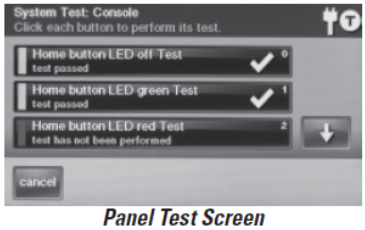
(https://www.vectorsecurity.com/UserFiles/File/PDF/Learning%20Center/2%20GIG%20Wireless%20Security%20System%20User%20Manual.pdf at 8.)

Sensor Test

When each sensor is tested, the Control Panel will beep and announce the sensor's name, a green bar will light on the display, and 1-5 signal bars will light to show the strength of that sensor's wireless signal.



Sensor Test Screen



Panel Test Screen

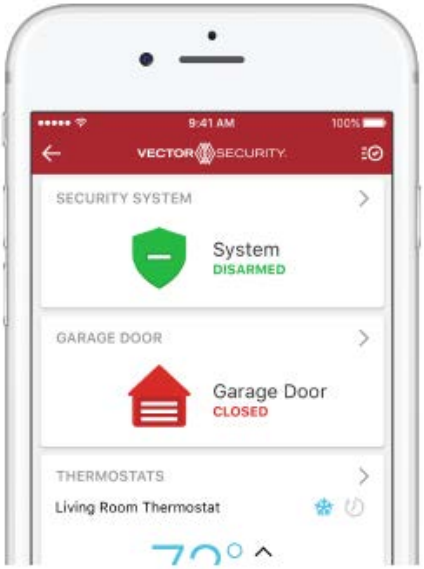
6. A list of all sensors will be displayed. Use the ↑ and ↓ arrows to scroll through the list.
7. Go to each sensor listed, and trigger it.
   - For door or window sensors, open and close the door or window.
   - For motion detectors, stay out of the protected area for five minutes, then walk through the area.
   - For portable sensors and wireless keypads, press a button.
   - For smoke, CO, or glass break detectors, press the detector's test button.
   - When the green bar is displayed for a sensor, it has tested OK.
8. Press **OK** when all sensors have been tested. A confirmation screen will be displayed.

(https://www.vectorsecurity.com/UserFiles/File/PDF/Learning%20Center/2%20GIG%20Wireless%20Security%20System%20User%20Manual.pdf at 31.)

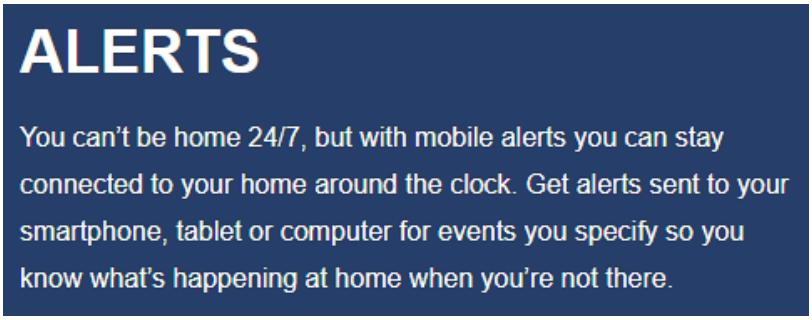
29. When the Vector Security System detects a triggering event, the control panel transmits a signal to a central monitoring station and/or to a user device such as a phone or tablet device. The control panel includes a network interface configured to provide a communication through a network communication channel (e.g., a network channel between the wireless control panel and the central monitoring station or user device). *See, e.g.*:

> *The heart of the system is the Control Panel. It receives the wireless radio signals from remote system "sensors" that monitor doors, windows, motion detectors, smoke detectors, carbon monoxide detectors, and panic buttons. The Control Panel processes these signals and controls the alarm siren. The system can communicate to an alarm monitoring "Central Station" over the regular telephone network and optionally over the cellular telephone network to report violations, alarms, and system status.*

(https://www.vectorsecurity.com/UserFiles/File/PDF/Learning%20Center/2%20GIG%20Wireless%20Security%20System%20User%20Manual.pdf at ii.)

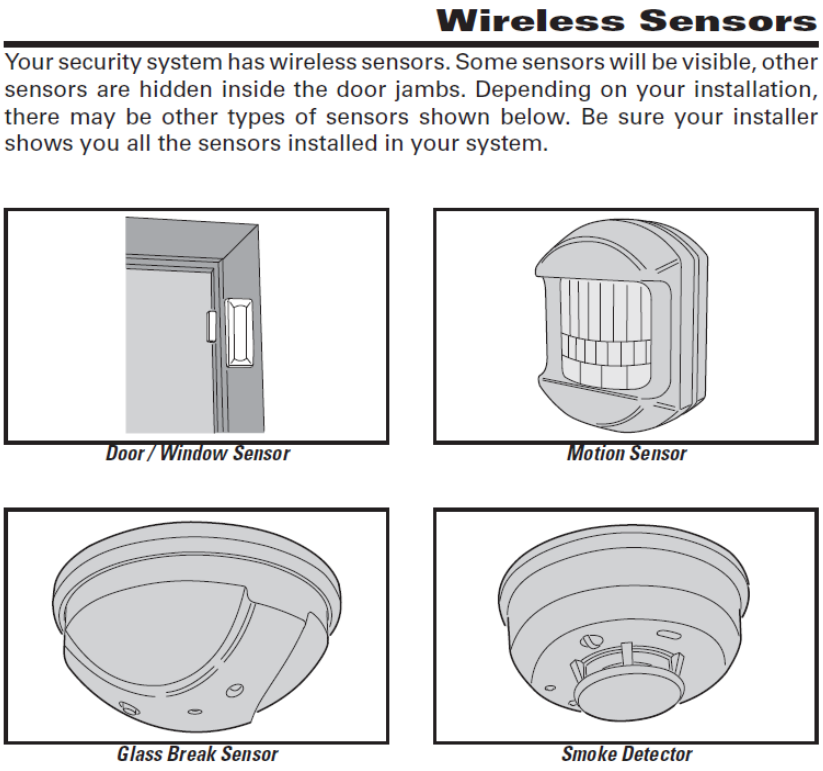


(https://www.vectorsecurity.com/products/video/app.)



(https://www.vectorsecurity.com/products/automation.)

30. Upon information and belief, the wireless control panel in each Accused Instrumentality is configured to receive a signal from a sensor (e.g., an item sensing device) through a short-range wireless transmission channel, including, for example, a radio frequency (RF) channel. *See, e.g.*:

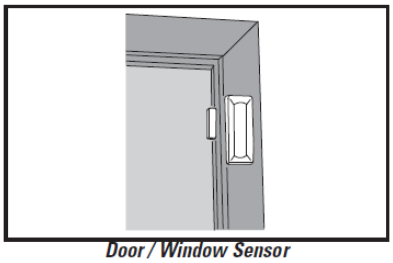


(https://www.vectorsecurity.com/UserFiles/File/PDF/Learning%20Center/2%20GIG%20Wireless%20Security%20System%20User%20Manual.pdf at 5.)

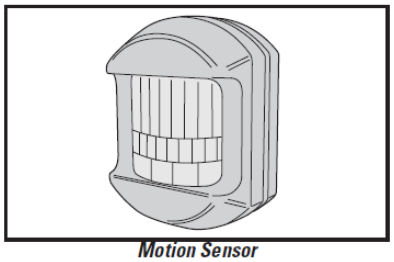
31. A sensor is activated when the sensor detects that the status of the item being monitored (e.g., motion, doors, windows) has changed. The activated sensor indicates the updated status of the item to the wireless control panel by transmitting a signal to the wireless control panel. A pathway is established for transmission of the signal between the sensor and the wireless control panel. *See, e.g.*:

Wireless Sensors

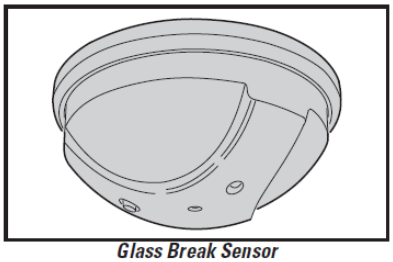
Your security system has wireless sensors. Some sensors will be visible, other sensors are hidden inside the door jambs. Depending on your installation, there may be other types of sensors shown below. Be sure your installer shows you all the sensors installed in your system.



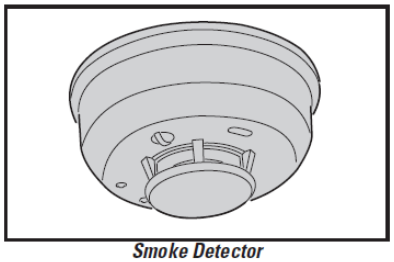
Door / Window Sensor



Motion Sensor



Glass Break Sensor



Smoke Detector

(https://www.vectorsecurity.com/UserFiles/File/PDF/Learning%20Center/2%20GIG%20Wireless%20Security%20System%20User%20Manual.pdf at 5.)

Sensor Status

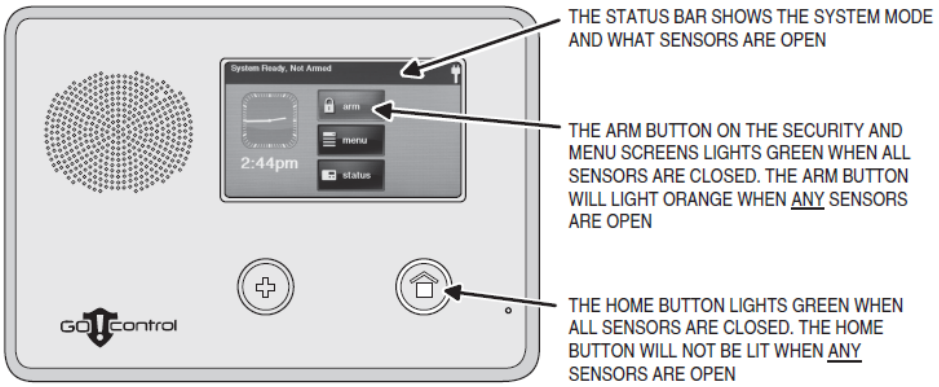
The security system constantly monitors all of the sensors attached to the protected doors and windows in your home or business. The Control Panel knows if each protected door or window is open or closed. The open or closed condition of the protected doors and windows is called the *"sensor status"*.

For maximum security, all the doors and windows on the premises should be closed when leaving the building. In some cases, such as when using the security system for protection when staying at home, it may be desirable to leave some protected doors or windows open. The system uses ***"bypasses"*** to resolve the open door or window conditions. Before the system can be armed, all protected doors and windows must be closed or bypassed. **Bypasses and their two types are explained in detail on the next page.**

Viewing Each Sensor's Status

The Control Panel will also show you which sensor-protected doors and windows are open. Your installer has programmed descriptive names for each sensor-protected door and window. The Control Panel's color display will show the names of which door and windows are open.

- The top area of the display on the Home, Security, and Menu Screens will list any sensors that are currently open.
- Pressing the **STATUS** button will also display a list of all open sensors along with general system status and alerts.



2GIG-CNTRL2

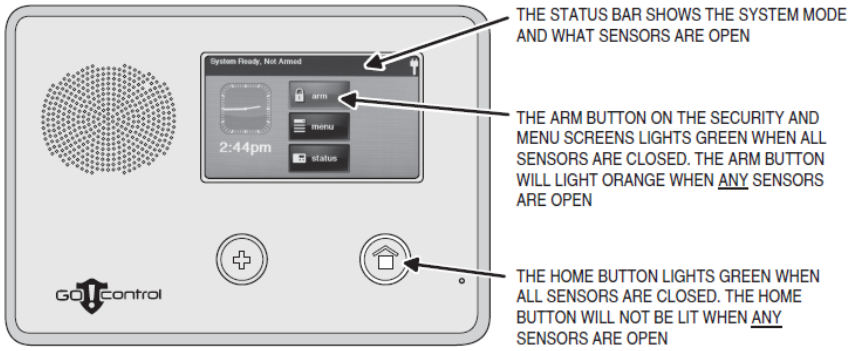
(https://www.vectorsecurity.com/UserFiles/File/PDF/Learning%20Center/2%20GIG%20Wireless%20Security%20System%20User%20Manual.pdf at 8.)

32. Each sensor in an Accused Instrumentality has an associated identifier (e.g., a name/type) that enables the wireless control panel to identify which of the sensors has been activated. For example, during a sensor test, the name/type of each sensor is displayed at the wireless control panel. Thus, the signal received during the sensor test includes the identifier (corresponding to the name/type) of the sensor. *See, e.g.*:

Viewing Each Sensor's Status

The Control Panel will also show you which sensor-protected doors and windows are open. Your installer has programmed descriptive names for each sensor-protected door and window. The Control Panel's color display will show the names of which door and windows are open.

- The top area of the display on the Home, Security, and Menu Screens will list any sensors that are currently open.
- Pressing the **STATUS** button will also display a list of all open sensors along with general system status and alerts.

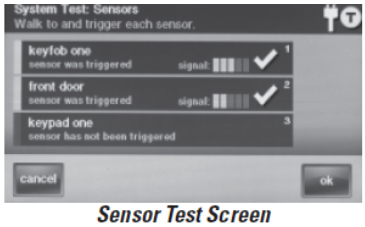


2GIG-CNTRL2

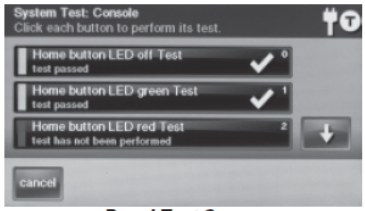
(https://www.vectorsecurity.com/UserFiles/File/PDF/Learning%20Center/2%20GIG%20Wireless%20Security%20System%20User%20Manual.pdf at 8.)

Sensor Test

When each sensor is tested, the Control Panel will beep and announce the sensor's name, a green bar will light on the display, and 1-5 signal bars will light to show the strength of that sensor's wireless signal.



Sensor Test Screen



Panel Test Screen

6. A list of all sensors will be displayed. Use the ↑ and ↓ arrows to scroll through the list.
7. Go to each sensor listed, and trigger it.
   - For door or window sensors, open and close the door or window.
   - For motion detectors, stay out of the protected area for five minutes, then walk through the area.
   - For portable sensors and wireless keypads, press a button.
   - For smoke, CO, or glass break detectors, press the detector's test button.
   - When the green bar is displayed for a sensor, it has tested OK.
8. Press **OK** when all sensors have been tested. A confirmation screen will be displayed.

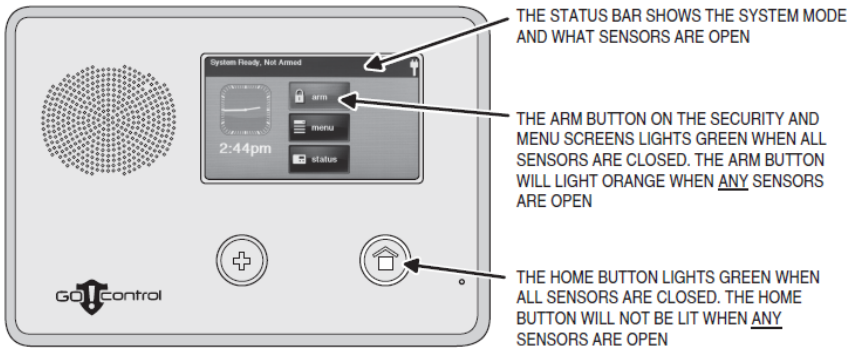
(https://www.vectorsecurity.com/UserFiles/File/PDF/Learning%20Center/2%20GIG%20Wireless%20Security%20System%20User%20Manual.pdf at 31.)

33. The Vector Security System is configured to identify each of the sensors connected to it and the "item" they correspond to (e.g., motion, windows, doors). When a sensor transmits information to the control panel, the control panel recognizes the transmitting sensor. *See, e.g.*:

Viewing Each Sensor's Status

The Control Panel will also show you which sensor-protected doors and windows are open. Your installer has programmed descriptive names for each sensor-protected door and window. The Control Panel's color display will show the names of which door and windows are open.

- The top area of the display on the Home, Security, and Menu Screens will list any sensors that are currently open.
- Pressing the **STATUS** button will also display a list of all open sensors along with general system status and alerts.



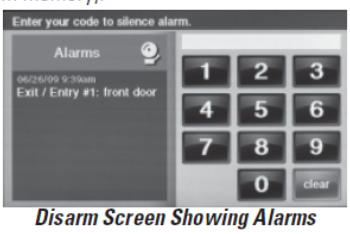
2GIG-CNTRL2

(https://www.vectorsecurity.com/UserFiles/File/PDF/Learning%20Center/2%20GIG%20Wireless%20Security%20System%20User%20Manual.pdf at 8.)

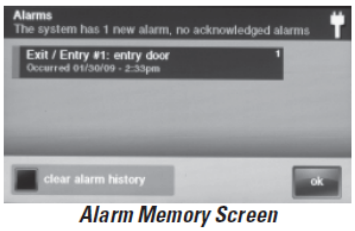
Alarm Memory

If an alarm has occurred while the system was armed, the Disarm Screen will show the time and date of the alarm and the sensor(s) that triggered the alarm.

After the system is disarmed, the Alarm Memory screen will be displayed. The Alarm Memory Screen shows the sensor(s) that have caused the alarm. If more than one sensor has been triggered, the display will show the order that alarms occurred. **The alarm memory will automatically clear the next time the system is armed.** You can also check the **CLEAR ALARM HISTORY** button and press **OK** to manually clear the alarm memory (24-hour sensors that are still violated will remain in alarm memory).

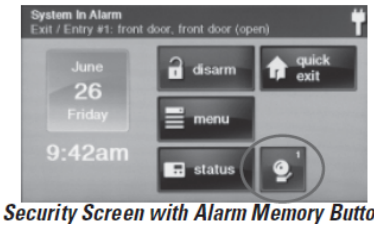


Disarm Screen Showing Alarms



Alarm Memory Screen

Anytime there are events stored in alarm memory, the Security Screen will display the button. The number on the button is the number of sensors that triggered during the alarm. Press the button to view the Alarm Memory Screen.

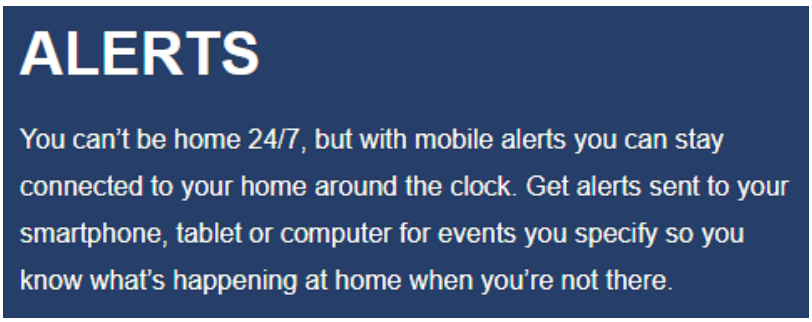


Security Screen with Alarm Memory Button

(https://www.vectorsecurity.com/UserFiles/File/PDF/Learning%20Center/2%20GIG%20Wireless%20Security%20System%20User%20Manual.pdf at 15.)

34. The control panel in the Vector Security System is configured to provide information about an updated status (e.g., an alert) to a user device (e.g., a phone or tablet) through the Vector Security Mobile App. *See, e.g.*:

(https://www.vectorsecurity.com/products/video/app.)



(https://www.vectorsecurity.com/products/automation.)

35. The Accused Instrumentalities are further configured to notify a user of the updated status by sending an alert to the user device according to a configuration setting that specifies when or how to communicate the information to the user. *See, e.g.*:

(https://www.vectorsecurity.com/products/video/app.)

> *Regardless of what's happening around your home, you'll know when it happens. With alerts for locks, cameras, lights, thermostat, and garage door sent directly to your smartphone, you'll never be left to wonder.*
>
> ***Locks***

Alerts sent to your mobile device let you know if you forgot to lock your door. No need for second-guessing or driving back home to check.

Video Cameras

Get alerted to events you specify, like when your kids come home from school, or when your pet sitter or household workers arrive. Set triggers so you can be alerted right away if something is amiss.

Garage Door

You're two blocks from home and wondering whether you closed the garage door behind you. There's no need to drive back when you have a smart garage door opener. Alerts sent to your phone will let you know if you've left it open or if someone has tampered with it.

Lights

Look like you're home, even when you're not by setting your lights on a schedule. Get alerts sent to your smartphone or tablet if a motion light goes off.

Thermostat

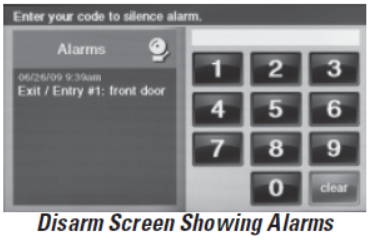
Always come home to a house that's the perfect temperature while staying energy efficient. Set your thermostat based on your schedule and preference, and get alerts if temperatures are too warm or too cold.

(https://www.vectorsecurity.com/products/mobile-alerts.)

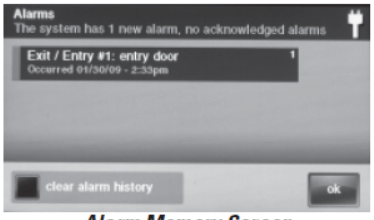
Alarm Memory

If an alarm has occurred while the system was armed, the Disarm Screen will show the time and date of the alarm and the sensor(s) that triggered the alarm.

After the system is disarmed, the Alarm Memory screen will be displayed. The Alarm Memory Screen shows the sensor(s) that have caused the alarm. If more than one sensor has been triggered, the display will show the order that alarms occurred. **The alarm memory will automatically clear the next time the system is armed.** You can also check the **CLEAR ALARM HISTORY** button and press **OK** to manually clear the alarm memory (24-hour sensors that are still violated will remain in alarm memory).

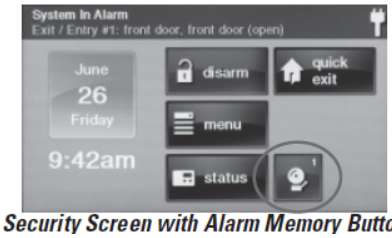


Disarm Screen Showing Alarms



Alarm Memory Screen

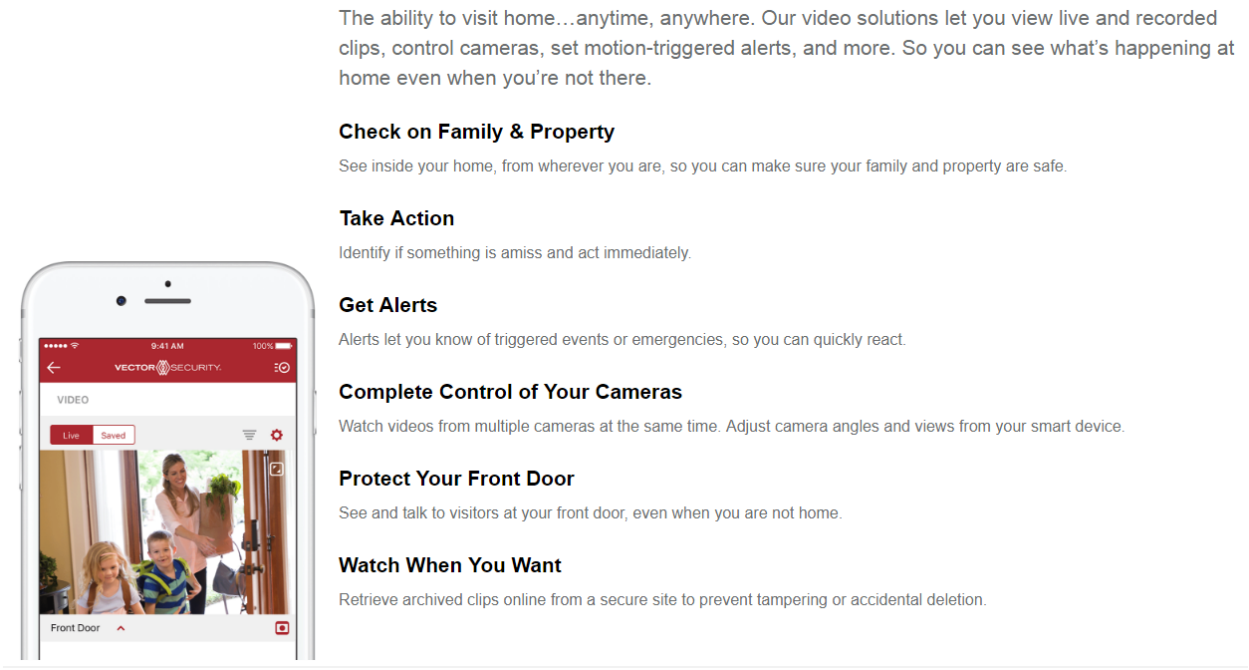
Anytime there are events stored in alarm memory, the Security Screen will display the button. The number on the button is the number of sensors that triggered during the alarm. Press the button to view the Alarm Memory Screen.



Security Screen with Alarm Memory Button

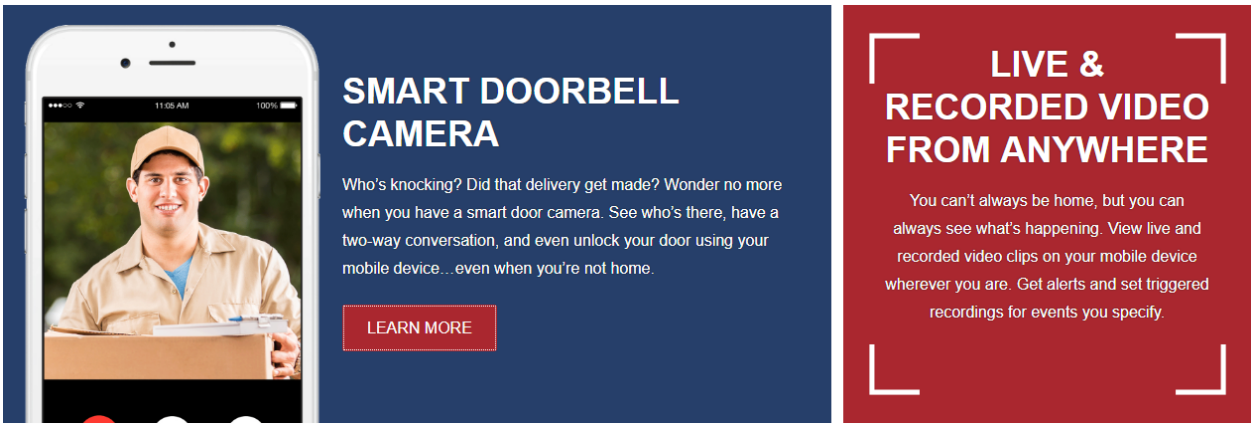
(https://www.vectorsecurity.com/UserFiles/File/PDF/Learning%20Center/2%20GIG%20Wireless%20Security%20System%20User%20Manual.pdf at 15.)

36. The Accused Instrumentalities further include a video-enabled home security system. (https://www.vectorsecurity.com/products/video-systems; https://www.vectorsecurity.com/products/video-systems/video-security-in-smart-homes.) The video home security system is capable of capturing live video from the home and either pushing it to a smart device or recording it for later viewing. On information and belief, the video home security system includes a decoder for decompressing a compressed video signal received over a wireless communication network. See, e.g.:



(https://www.vectorsecurity.com/products/video-systems/smart-home-layout-video.)

37. The Accused Instrumentalities are configured to communicate video from a video camera to a user's smart device through a cellular network and/or the Internet. See, e.g.:



(https://www.vectorsecurity.com/products/video-systems.)

38. Defendant has and continues to jointly infringe one or more of the Asserted Claims by the collective conduct of Vector Security and Amazon.com, Inc. ("Amazon") in making, using, offering to sell, selling, and importing the aforementioned Vector Security Voice Control with Amazon Echo Dot. (*See, e.g.*, https://www.vectorsecurity.com/products/voice-

control.) In particular, Vector Security and Amazon have effectively formed a joint enterprise such that the infringing acts are attributable to Vector Security, who provides a home security system with a wireless hub, and Amazon, who provides the Echo Dot device and Alexa voice application.

39. On information and belief, the Accused Instrumentalities are used, marketed, provided to, and/or used by or for each of Defendant's partners, clients, customers and end users across the country and in this District.

40. Defendant was made aware of the '983 patent and its infringement thereof at least as early as the filing of this Complaint.

41. Upon information and belief, since at least the time Defendant received notice, Defendant has induced and continues to induce others to infringe at least one claim of the '983 patent under 35 U.S.C. § 271(b) by, among other things, and with specific intent or willful blindness, actively aiding and abetting others to infringe, including but not limited to Defendant's partners, clients, customers, and end users, whose use of the Accused Instrumentalities constitutes direct infringement of at least one claim of the '983 patent.

42. In particular, Defendant's actions that aid and abet others such as its partners, customers, clients, and end users to infringe include advertising and distributing the Accused Instrumentalities and providing instruction materials, training, and services regarding the Accused Instrumentalities. On information and belief, Defendant has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because Defendant has had actual knowledge of the '983 patent and knowledge that its acts were inducing infringement of the '983 patent since at least the date Defendant received notice that such activities infringed the '983 patent.

43. Upon information and belief, Defendant is liable as a contributory infringer of the ’983 patent under 35 U.S.C. § 271(c) by offering to sell, selling and importing into the United States wireless hub systems to be especially made or adapted for use in an infringement of the ’983 patent. The Accused Instrumentalities are a material component for use in practicing the ’983 patent and are specifically made and are not a staple article of commerce suitable for substantial non-infringing use.

44. Since at least the filing of this Complaint, Defendant’s infringement has been willful.

45. Plaintiff has been harmed by Defendant’s infringing activities.

JURY DEMAND

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff demands a trial by jury on all issues triable as such.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment for itself and against Defendant as follows:

A. An adjudication that Defendant has infringed the ’983 patent;

B. An award of damages to be paid by Defendant adequate to compensate Plaintiff for Defendant’s past infringement of the ’983 patent and any continuing or future infringement through the date such judgment is entered, including interest, costs, expenses and an accounting of all infringing acts including, but not limited to, those acts not presented at trial;

C. A declaration that this case is exceptional under 35 U.S.C. § 285, and an award of Plaintiff’s reasonable attorneys’ fees; and

D. An award to Plaintiff of such further relief at law or in equity as the Court deems just and proper.

Dated: July 5, 2018

DEVLIN LAW FIRM LLC

/s/ Timothy Devlin

Timothy Devlin (#4241)
tdevlin@devlinlawfirm.com
1306 N. Broom St., 1st Floor
Wilmington, Delaware 19806

Telephone: (302) 449-9010
Facsimile: (302) 353-4251

Attorneys for Plaintiff
Virginia Innovation Sciences, Inc.