

THE PARTIES

2. Brazos is a limited liability corporation organized and existing under the laws of Delaware, with its principal place of business at 606 Austin Avenue, Suite 6, Waco, Texas 76701.

3. On information and belief, Defendant Huawei Technologies Co., Ltd. is a Chinese corporation that does business in Texas, directly or through intermediaries, with a principal place of business at Bantian, Longgang District, Shenzhen 518129, People's Republic of China.

4. Upon information and belief, Defendant Huawei Technologies USA Inc. is a corporation organized and existing under the laws of Texas that maintains an established place of business at 2391 NE Interstate 410 Loop, San Antonio, Texas 78217. Huawei Technologies USA, Inc. is authorized to do business in Texas and may be served via its registered agent, CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201-3136.

5. Defendants operate under and identify with the trade name "Huawei." Each of the Defendants may be referred to individually as a "Huawei Defendant" and, collectively, Defendants may be referred to below as "Huawei" or as the "Huawei Defendants."

JURISDICTION AND VENUE

6. This is an action for patent infringement which arises under the Patent Laws of the United States, in particular, 35 U.S.C. §§271, 281, 284, and 285.

7. This Court has jurisdiction over the subject matter of this action under 28 U.S.C. §§ 1331 and 1338(a).

8. This Court has specific and general personal jurisdiction over each Huawei Defendant pursuant to due process and/or the Texas Long Arm Statute, because each Huawei Defendant has committed acts giving rise to this action within Texas and within this judicial district. The Court's exercise of jurisdiction over each Huawei Defendant would not offend

traditional notions of fair play and substantial justice because Huawei has established minimum contacts with the forum. For example, on information and belief, Huawei Defendants have committed acts of infringement in this judicial district, by among other things, selling and offering for sale products that infringe the asserted patent, directly or through intermediaries, as alleged herein.

9. Venue in the Western District of Texas is proper pursuant to 28 U.S.C. §§1391 and 1400(b) because Defendants have committed acts of infringement in this judicial district and have regular and established places of business in this judicial district and in Texas. As non-limiting examples, on information and belief, Defendants have sold or offered to sell the Accused Products in this judicial district and have employees or agents that operate Huawei equipment in this judicial district, including at 189 CR 265, Georgetown, TX 78626, 1150 S. Bell Blvd., Cedar Park, TX 78613, 1399 S A W Grimes Blvd., Round Rock, TX 78664, 12335 IH 35, Jarrell, TX 76537, 1050 Rabbit Hill Rd., Unit #E, Georgetown, TX 78626, 1602 A W Grimes Blvd., Round Rock, TX 78664, 4120 IH 35 N, Georgetown, TX 78626, 900 CR 272, Leander, TX 78641, 1950 Crystal Falls Pkwy., Leander, TX 78641, 1101 N. Industrial Blvd., Round Rock, TX 78681, 506 McNeil Rd., Round Rock, TX 78681, 3210 Chisholm Trail Rd., Round Rock, TX 78681, 112 Roundville Ln., Round Rock, TX 78664, 202 Central Dr. W, Georgetown, TX 78628, 3595 E. Hwy. 29, Georgetown, TX 78626, 1402 W Welch St., Taylor, TX 76574, 3801 Oak Ridge Dr., Round Rock, TX 78681, 1957 Red Bud Ln. #B, Round Rock, TX 78664, 6603 S Lakewood Dr., Georgetown, TX 78633, 500 W Front, Hutto, TX 78634.

COUNT ONE - INFRINGEMENT OF
U.S. PATENT NO. 7,933,211

10. Brazos re-alleges and incorporates by reference the preceding paragraphs of this Complaint.

11. On April 26, 2011, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,933,211 (“the ’211 Patent”), entitled “Method and system for providing prioritized failure announcements.” A true and correct copy of the ’211 Patent is attached as Exhibit A to this Complaint.

12. Brazos is the owner of all rights, title, and interest in and to the ’211 Patent, including the right to assert all causes of action arising under the ’211 Patent and the right to any remedies for the infringement of the ’211 Patent.

13. Huawei makes, uses, sells, offers for sale, imports, and/or distributes in the United States, including within this judicial district, products such as, but not limited to, Huawei Cloud Stack (collectively, the “Accused Products”).

14. Huawei Cloud Stack is an on-premise cloud infrastructure for government and enterprise customers. Huawei Cloud Stack includes FusionSphere Virtualization layer, FusionSphere OpenStack cloud platform layer, and ManageOne unified management layer.

15. With ManageOne, the overview and maintenance administrators can monitor all the network resources. ManageOne provides alarm monitoring to monitor system resources and detect and handle faults.

HUAWEI CLOUD Stack

HUAWEI CLOUD Stack is cloud infrastructure on the premises of government and enterprise customers, offering seamless service experience on cloud and on-premises. HUAWEI CLOUD Stack comes in multiple editions to meet a range of diversified needs, such as moving legacy applications and workloads to the cloud, big data analytics and AI training, and building large-scale city clouds and industry clouds.

Huawei CLOUD Stack — Huawei's full-stack hybrid cloud — includes the: FusionSphere Virtualization layer, FusionSphere OpenStack cloud platform layer, service components offering different capabilities as the cloud service layer, ManageOne unified management layer, FusionBridge connecting to the public cloud to implement hybrid cloud deployment, and the cloud data center that provides customers with service awareness, business intelligence, unified management, and unified services.

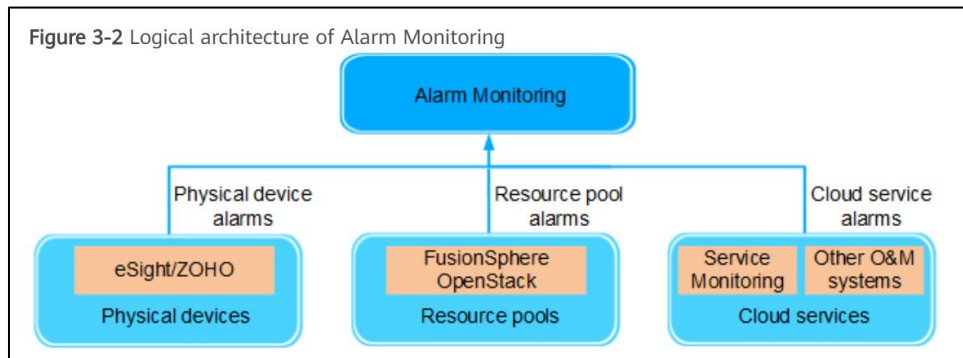
Source: <https://e.huawei.com/us/solutions/cloud-computing/huawei-cloud-stack>.

ManageOne Maintenance Portal provides all-round and hierarchical monitoring functions. O&M personnel can monitor resources, alarms, performance, capacity usage, and other information of the entire network, and learn the health status of network elements (NEs) and ICT resources in real time, which reduces IT costs, increases O&M efficiency, and improves user experience.

Source: https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000.

3.2 Alarm Monitoring

Alarm Monitoring on ManageOne Maintenance Portal centrally monitors the alarms of system services and third-party systems, facilitating quick locating and handling of network faults and ensuring normal services. Alarm Monitoring is dedicated to monitoring and O&M of ever-evolving complex networks. Alarm Monitoring can be used to monitor faults on traditional networks and next-generation networks, which reduces fault recovery durations and improves network O&M efficiency.



Source:

https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000

16. The alarms in the ManageOne system are based on various parameters (at least two priority indicators) such as Alarm Location, Alarm Severity, Alarm Source, and Alarm Type. The Alarm Location indicates the information that assists in fault locating. An Alarm Severity indicator provides the severity, importance, and urgency of a fault. Values include “Critical,” “Major,” “Minor,” and “Warning.” By using these attributes, these alarms can be classified.

Table 3-25 Parameters in the alarm list

Parameter	Description
Alarm ID	Indicates an alarm ID. Each alarm is uniquely identified by an alarm ID.
Alarm Serial Number	Indicates the alarm SN. When an alarm is generated, it may be modified multiple times. For example, its severity may change or it may be cleared. The SN uniquely identifies an alarm. When alarms are merged, the original alarms are moved to the historical-alarm list. The Current Alarms page record the new alarm and its new SN.
List Serial Number	Indicates the serial number assigned to an alarm after the alarm is merged. It is different from the alarm serial number.
Alarm Matched Rule Name	Indicates the name of the rule that an alarm matches.
VDC ID	Indicates the VDC ID. Each VDC is uniquely identified by a VDC ID and a VDC name.
VDC Name	Indicates the VDC name.
Occurrences	Indicates the number of occurrences times or merged times for an alarm triggered by a fault. This parameter helps users to increase concerns on the alarm and handle it in time. This parameter is not displayed on the Masked Alarms and Historical Alarms pages.
Alarm source	Indicates the device or NE that generates an alarm. For example: Operations Support System (OSS)

Location Info	Indicates the information that assists in fault locating. Based on the information, you can quickly locate the location where the alarm is generated.
---------------	---

Severity	Indicates the alarm severities, which include critical, major, minor, and warning.
----------	--



Alarm Source Type	Indicates the type of the NE where an alarm is generated.
Type	For details about alarm types, see Concepts .



Operation	<p>Indicates the operations that users can perform on the alarm.</p> <ul style="list-style-type: none"> • Acknowledge alarms. • Clear alarms. • Check alarm records. • Set Masking Rule: For details, see 3.2.5.6 Configuring Masking Rules. • Set Identification Rule: For details, see 3.2.5.9 Configuring Identification Rules. • Set Notification Rule: For details, see 3.2.5.8 Configuring Notification Rules. • Set Severity and Type Redefinition Rule: For details, see 3.2.5.10 Configuring Severity and Type Redefinition Rules. • Set Name Redefinition Rule: For details, see 3.2.5.11 Configuring Name Redefinition Rules. • Set Intermittent/Toggling Rule: For details, see 3.2.5.14 Configuring an Intermittent or Toggling Rule. • Set Alarm Aggregation Rule: For details, see 3.2.5.15 Configuring Aggregation Rules.
Location Info	<p>Indicates the information that assists in fault locating. Based on the information, you can quickly locate the location where the alarm is generated.</p>

Source:

https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000.

Table 3-5 Alarm severities

Alarm Severity	Default Color	Description	Handling Policy
Critical		Services are affected. Corrective measures must be taken immediately.	The fault must be rectified immediately. Otherwise, services may be interrupted or the system may break down.
Major		Services are affected. If the fault is not rectified in a timely manner, serious consequences may occur.	Major alarms need to be handled in time. Otherwise, important services will be affected.

Alarm Severity	Default Color	Description	Handling Policy
Minor		Minor impact on services. Problems of this severity may result in serious faults, and therefore corrective actions are required.	You need to find out the cause of the alarm and rectify the fault.
Warning		Potential or imminent fault that affects services is detected, but services are not affected.	Warning alarms are handled based on network and NE running status.

Source:

https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000.

Table 3-9 Alarm and event types

Type	Description
Communication alarm	Alarms caused by failures of the communications in an NE, between NEs, between an NE and a management system, or between management systems. For example, device communication interruption alarm.
Quality of service alarm	Alarms caused by service quality deterioration. For example, device congestion alarm.
Processing error alarm	Alarms caused by software or processing errors. For example, version mismatch alarm.
Equipment alarm	Alarms caused by physical resource faults. For example, board fault alarm.
Environmental alarm	Alarms generated when the environment where the device resides is faulty. For example, temperature alarm generated when the hardware temperature is too high.
Integrity alarm	Alarms generated when requested operations are denied. For example, alarms caused by unauthorized modification, addition, and deletion of user information.
Operation alarm	Alarms generated when the required services cannot run properly due to problems such as service unavailability, faults, or incorrect invocation. For example, alarms caused by service rejection, service exit, and procedural errors.
Physical resource alarm	Alarms generated when physical resources are damaged. For example, alarms caused by cable damage and intrusion into an equipment room.

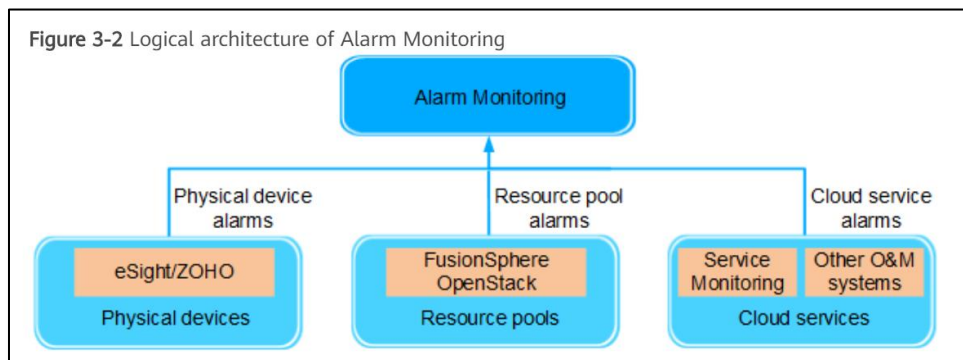
Type	Description
Security alarm	Alarms generated when security issues are detected by a security service or mechanism. For example, alarms caused by authentication failures, confidential disclosures, and unauthorized accesses.
Time domain alarm	Alarms generated when an event occurs at improper time. For example, alarms caused by information delay, invalid key, or resource access at unauthorized time.
Property change	Events generated when MO attributes change. For example, events caused by addition, reduction, and change of attributes.
Object creation	Events generated when an MO instance is created.
Object delete	Events generated when an MO instance is deleted.
Relationship change	Events generated when MO relationship attributes change.
State change	Events generated when MO status attributes change.
Route change	Events generated when routes change.
Protection switching	Alarms or events caused by the switchover.
Over limit	Alarms or events reported when the performance counter reaches the threshold.
File transfer status	Alarms or events reported when the file transfer succeeds or fails.
Backup status	Events generated when MO backup status changes.
Heart beat	Events generated when heartbeat notifications are sent.

Source:

https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000

17. ManageOne features alarm monitoring to detect and fix alarms. In this architecture, faults/errors (fault condition or failure) are detected at the physical devices or resource pools (network elements). These network elements then generate the alarms on detecting the fault condition.

3.2 Alarm Monitoring



Source:

https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000.

Alarm and Event

If the system or MOs detect an exception or a significant status change, an alarm or event will be displayed on the GUI of alarm management. MOs refer to the objects or NEs connected to alarm management. **Table 3-4** describes the definitions of the alarm and event.

Source:

https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000.

18. Using the alarm attributes, errors can be classified and prioritized based on its severity and location. As an example, ManageOne provides a Masking Rules feature to mask unimportant alarms or events. If two masking rules are configured for the same alarm, the rule with higher priority takes effect (i.e. determining a fault correction priority).

3.2.5.6 Configuring Masking Rules

You can set an alarm masking rule to mask alarms or events that you are not concerned about. New alarms or events meeting the masking rules will not be displayed on the **Current Alarms** and **Event Logs** pages. The system provides preset masking rules for users to mask unimportant alarms or events. If preset masking rules cannot meet requirements, administrators can create masking rules as required.

Source:

https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000.

Procedure

Step 1 Choose **Alarms > Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Masking Rules**.

Step 3 On the **Masking Rules** page, click **Create** and select **Alarm Masking Rules**.

Step 4 In the **Basic Information** area, set the rule name, description, and whether to enable the rule.

Step 5 In the **Conditions** area, set the alarm severities, alarm sources, and alarms for the rule to take effect. Set advanced conditions to filter the alarms for the rule to take effect based on alarm parameters.

NOTE

- By default, **Designated alarms** is deselected, indicating that the rule takes effect for all alarms.
- **All alarm sources** is available only when the user can manage all resources.
- In the **Alarm sources** area, you can select **All alarm sources** to mask the alarms that meet the conditions and are generated by the system and all MOs. Therefore, exercise caution when you set the alarm source.

Step 6 In the **Time Filter** area, set when the rule is effective. You can set the effective time and effective cycle.

NOTE

If all options of **Time Filter** are not selected, the rule is effective at any time.

Step 7 In the **Action** area, set **Masked alarms** to **Discard** or **Show in Masked Alarms**.

NOTE

- When an event masking rule is being created, masked events can only be discarded.
- If **Discard** is selected, the alarm will not be displayed. Therefore, exercise caution when performing this operation.

Step 8 Set the priority of this rule. When an alarm meets two alarm masking rules, the rule with a higher priority takes effect.



Source:

https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000.

19. The Accused Product allows an administrator to monitor alarms and view “Top 10 Alarms” and “Top 10 Alarm Sources.” All the alarms occurring at that instant are prioritized, and the top priority alarms are shown under “Top 10 Alarms.”

3.2.2 Monitoring and Viewing Alarms or Events

O&M personnel can monitor and view alarms or events in Alarm Management in real time to learn about the alarms or events on the system in real time and take corresponding measures.

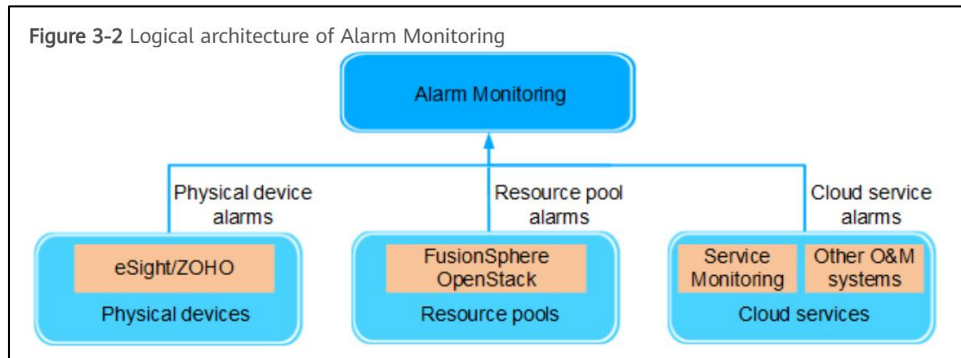
Monitoring alarms using alarm indicators	The alarm indicators in the upper right corner of the Current Alarms page show the number of critical alarms, number of major alarms, number of minor alarms, and number of warning alarms.
Monitoring alarms using the statistics panel	Click  in the upper right corner of the Current Alarms page to view the alarm statistics charts. The statistical result is obtained based on the filtered alarms. By default, the Top 10 Alarms , Duration , Top 10 Alarm Sources , and Severity statistical charts are displayed on the statistics panel. If you want to view the Status statistical chart or adjust the display sequence of the charts, click  on the upper right of the statistics panel. In the upper right of each chart, select the chart to be displayed from the drop-down menu. On the statistics panel, you can click any statistical result to quickly filter the alarms that meet the condition. If you close the statistics panel, the filter criteria selected on the panel are automatically deselected.

Source:

https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000

20. ManageOne can prioritize alarms after detecting fault conditions. When an alarm is generated at a network element, the alarm is transmitted to the ManageOne panel/dashboard (network management function) for the admin to take action (transmit an announcement notification). This alarm includes both visual and audio notifications indicating said detected fault condition (or failure) on the ManagOne panel/dashboard and contains details about the alarm.

3.2 Alarm Monitoring





Source:

https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000.

3.2.2 Monitoring and Viewing Alarms or Events

O&M personnel can monitor and view alarms or events in Alarm Management in real time to learn about the alarms or events on the system in real time and take corresponding measures.

Monitoring alarms using alarm indicators	The alarm indicators in the upper right corner of the Current Alarms page show the number of critical alarms, number of major alarms, number of minor alarms, and number of warning alarms.
Monitoring alarms using the statistics panel	Click  in the upper right corner of the Current Alarms page to view the alarm statistics charts. The statistical result is obtained based on the filtered alarms. By default, the Top 10 Alarms , Duration , Top 10 Alarm Sources , and Severity statistical charts are displayed on the statistics panel. If you want to view the Status statistical chart or adjust the display sequence of the charts, click  on the upper right of the statistics panel. In the upper right of each chart, select the chart to be displayed from the drop-down menu. On the statistics panel, you can click any statistical result to quickly filter the alarms that meet the condition. If you close the statistics panel, the filter criteria selected on the panel are automatically deselected.

Source:

https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000.

3.2.3 Handling Alarms

You can use Alarm Monitoring to handle alarms to facilitate troubleshooting. For example, you can specify an alarm handler and acknowledge or clear alarms.

Prerequisites

You have the rights for **Alarm Operation**, **Clear Alarm**, **Set Redefinition Rules**, and **Synchronize Alarms**.

Context

Alarm Monitoring comprises the following major alarm operations: acknowledging alarms, clearing alarms, changing alarm severities, and setting alarms to the invalid or maintenance state. **Table 3-12** describes alarm acknowledgment and clearance operations. **Figure 3-3** shows the relationships between alarm statuses.

Source:

https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000.

3.2.5.3 Setting Alarm Sounds

You can set different alarm sounds for alarm at different severities or specify alarm sound for different alarm names to facilitate alarm monitoring. When an alarm is generated, the sound box on your PC produces a corresponding sound.

Source:

https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000

21. In view of preceding paragraphs, each and every element of at least claim 1 of the '211 Patent is found in the Accused Products.
22. Huawei has and continues to directly infringe at least one claim of the '211 Patent, literally or under the doctrine of equivalents, by making, using, selling, offering for sale, importing, and/or distributing the Accused Products in the United States, including within this judicial district, without the authority of Brazos.
23. Huawei has received notice and actual or constructive knowledge of the '211 Patent since at least the date of service of this Complaint.

24. Since at least the date of service of this Complaint, through its actions, Huawei has actively induced product makers, distributors, retailers, and/or end users of the Accused Products to infringe the '211 Patent throughout the United States, including within this judicial district, by, among other things, advertising and promoting the use of the Accused Products in various websites, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the Accused Products. Examples of such advertising, promoting, and/or instructing include the documents at:

- <https://e.huawei.com/us/solutions/cloud-computing/huawei-cloud-stack>
- https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100105316&partNo=k001&mid=SUPE_DOC&t=1593336499000

25. Since at least the date of service of this Complaint, through its actions, Huawei has contributed to the infringement of the '211 Patent by having others sell, offer for sale, or use the Accused Products throughout the United States, including within this judicial district, with knowledge that the Accused Products infringe the '211 Patent. The Accused Products are especially made or adapted for infringing the '211 Patent and have no substantial non-infringing use. For example, in view of the preceding paragraphs, the Accused Products contain functionality which is material to at least one claim of the '211 Patent.

JURY DEMAND

Brazos hereby demands a jury on all issues so triable.

REQUEST FOR RELIEF

WHEREFORE, Brazos respectfully requests that the Court:

- (A) Enter judgment that Huawei infringes one or more claims of the '211 Patent literally and/or under the doctrine of equivalents;

- (B) Enter judgment that Huawei has induced infringement and continues to induce infringement of one or more claims of the '211 Patent;
- (C) Enter judgment that Huawei has contributed to and continues to contribute to the infringement of one or more claims of the '211 Patent;
- (D) Award Brazos damages, to be paid by Huawei in an amount adequate to compensate Brazos for such damages, together with pre-judgment and post-judgment interest for the infringement by Huawei of the '211 Patent through the date such judgment is entered in accordance with 35 U.S.C. §284, and increase such award by up to three times the amount found or assessed in accordance with 35 U.S.C. §284;
- (E) Declare this case exceptional pursuant to 35 U.S.C. §285; and Award Brazos its costs, disbursements, attorneys' fees, and such further and additional relief as is deemed appropriate by this Court.

Dated: September 29, 2020

Respectfully submitted,

/s/ James L. Etheridge
James L. Etheridge
Texas State Bar No. 24059147
Ryan S. Loveless
Texas State Bar No. 24036997
Travis L. Richins
Texas State Bar No. 24061296
Brett A. Mangrum
Texas State Bar No. 24065671
Jeffrey Huang
ETHERIDGE LAW GROUP, PLLC
2600 E. Southlake Blvd., Suite 120 / 324
Southlake, Texas 76092
Telephone: (817) 470-7249
Facsimile: (817) 887-5950
Jim@EtheridgeLaw.com
Ryan@EtheridgeLaw.com

Travis@EtheridgeLaw.com
Brett@EtheridgeLaw.com
JeffH@EtheridgeLaw.com

COUNSEL FOR PLAINTIFF