**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

WSOU INVESTMENTS, LLC d/b/a BRAZOS LICENSING AND DEVELOPMENT,	§ § § §	
Plaintiff,	§ §	CIVIL ACTION NO. 6:20-cv-331
	§	**JURY TRIAL DEMANDED**
v.	§ §	
MICROSOFT CORPORATION,	§ § §	
Defendant.	§ §	

**ORIGINAL COMPLAINT FOR PATENT
INFRINGEMENT**

Plaintiff WSOU Investments, LLC d/b/a Brazos Licensing and Development ("Brazos" or "Plaintiff"), by and through its attorneys, files this Complaint for Patent Infringement against Microsoft Corporation ("Microsoft" or "Defendant") and alleges:

NATURE OF THE ACTION

1.   This is a civil action for patent infringement arising under the Patent Laws of the United States, 35 U.S.C. §§ 1, et seq., including §§ 271, 281, 284, and 285.

THE PARTIES

2.   Brazos is a limited liability corporation organized and existing under the laws of Delaware, with its principal place of business at 605 Austin Ave, Suite 6, Waco, Texas 76701.

3.   On information and belief, Defendant Microsoft Corporation is incorporated under the laws of Washington State with its principal place of business at 1 Microsoft Way, Redmond, Washington 98052. Microsoft may be served with process through its registered agent Corporation Service Company, 211 East 7th Street, Suite 620, Austin, Texas 78701.

9

4.   On information and belief, Microsoft has been registered to do business in the state of Texas under Texas SOS file number 0010404606 since about March 1987.

5.   On information and belief, Microsoft has had regular and established places of business in this judicial district since at least 2002.

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 Microsoft pursuant to due process and/or the Texas Long Arm Statute because Microsoft has committed acts giving rise to this action within Texas and within this judicial district. The Court's exercise of jurisdiction over Microsoft would not offend traditional notions of fair play and substantial justice because Microsoft has established minimum contacts with the forum. For example, on information and belief, Microsoft has 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/or 1400(b).

10.   This district was deemed to be a proper venue for patent cases against Microsoft in actions bearing docket numbers: 6-19-cv-00572 (*Zeroclick, LLC v. Microsoft Corporation*); 6-19-cv-00687 (*Exafer, Ltd. v. Microsoft Corporation.*); 6-19-cv-00399 (*Neodron Ltd. v. Microsoft Corporation*).

11.   On information and belief, Microsoft maintains a variety of regular and established business locations in the judicial district, including its Corporate Sales Office Locations, Retail Store Locations, and Datacenter Locations.

12.   On information and belief, Microsoft operates multiple corporate sales offices in the judicial district, and these offices constitute regular and established places of business.

13.   On information and belief, Microsoft employs hundreds of employees within its corporate sales offices located in the judicial district.

14.   On information and belief, Microsoft has an established place of business in this judicial district known as "Corporate Sales Office: Austin" located at 10900 Stonelake Boulevard, Suite 225, Austin, TX, USA 78759 and "Microsoft Retail Store: The Domain" located at 3309 Esperanza Crossing, Suite 104 Austin, TX 78758.

https://www.microsoft.com/en-us/about/officelocator?Location=78759

9

15.   On information and belief, Microsoft's "Corporate Sales Office: Austin" and "Microsoft Retail Store: The Domain" locations were respectively assessed by the Travis County Appraisal District in 2019 to have market values of over $2.3 million dollars and $2.7 million dollars.

http://propaccess.traviscad.org/clientdb/SearchResults.aspx

16.   On information and belief, Microsoft has another established place of business in this judicial district known as "Corporate Sales Office: San Antonio" located at Concord Park II, 401 East Sonterra Boulevard, Suite 300, San Antonio, Texas 78258.

Source: Google Maps

17.   On information and belief, Microsoft owns and operates multiple datacenters in the judicial district, including without limitation data centers located at 5150 Rogers Road, San Antonio, Texas 78251; 5200 Rogers Road, San Antonio, Texas 78251; 3823 Weisman Boulevard, San Antonio, Texas 78251; and 15000 Lambda Drive, San Antonio, Texas 782245.

18.   On information and belief, Microsoft utilizes its datacenter locations in this judicial district as regular and established places of business. As a non-limiting example, the data centers in San Antonio are referred to within Microsoft as "US Gov Texas."

19.   On information and belief, thousands of customers who rely on the infringing datacenter infrastructure that Microsoft's engineering and operations teams have built, reside in this judicial district.

COUNT ONE - INFRINGEMENT OF
U.S. PATENT NO. 7,366,160

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

21.   On April 29, 2008, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,366,160 ("the '160 Patent"), entitled "Method of Determining Service Trends." A true and correct copy of the '160 Patent is attached as Exhibit A to this Complaint.

22.   Brazos is the owner of all rights, title, and interest in and to the '160 Patent, including the right to assert all causes of action arising under the '160 Patent and the right to any remedies for the infringement of the '160 Patent.

23.   Microsoft 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, Microsoft's Azure Monitor(s) (collectively, the "Accused Products").

24.   Microsoft's Azure Monitor monitors network resources with tools for various network services. Azure Monitor determines the service trend of the performance metrics and generates alerts when a metric crosses the threshold.

25.   Azure Monitor helps in analyzing network resources. Azure Monitor collects data from multiple sources like CRM and, Office Apps into a common data platform where it can be analyzed for trends and anomalies.

Azure Monitor overview

Azure Monitor is a service in Azure that provides performance and availability monitoring for applications and services in Azure, other cloud environments, or on-premises. Azure Monitor collects data from multiple sources into a common data platform where it can be analyzed for trends and anomalies. Rich features in Azure Monitor assist you in quickly identifying and responding to critical situations that may affect your application.

https://opdhsblobprod01.blob.core.windows.net/contents/4a6d75bb3af747de838e6ccc97c5d
978/03a9959eadb93d2c2131be1f3b2ea464?sv=2015-04-
05&sr=b&sig=EV%2B2JDmkvfnTTZdyWVb4IyvBaP24ZtM2CUTBrBtINe4%3D&st=202
0-01-27T08%3A49%3A56Z&se=2020-01-28T08%3A59%3A56Z&sp=r ("Azure Network
Monitor"), Page 30.

26.   The below figure shows the Microsoft Azure Monitor Architecture. Azure Monitor provides insights about data, visualizes information, and generates alerts.
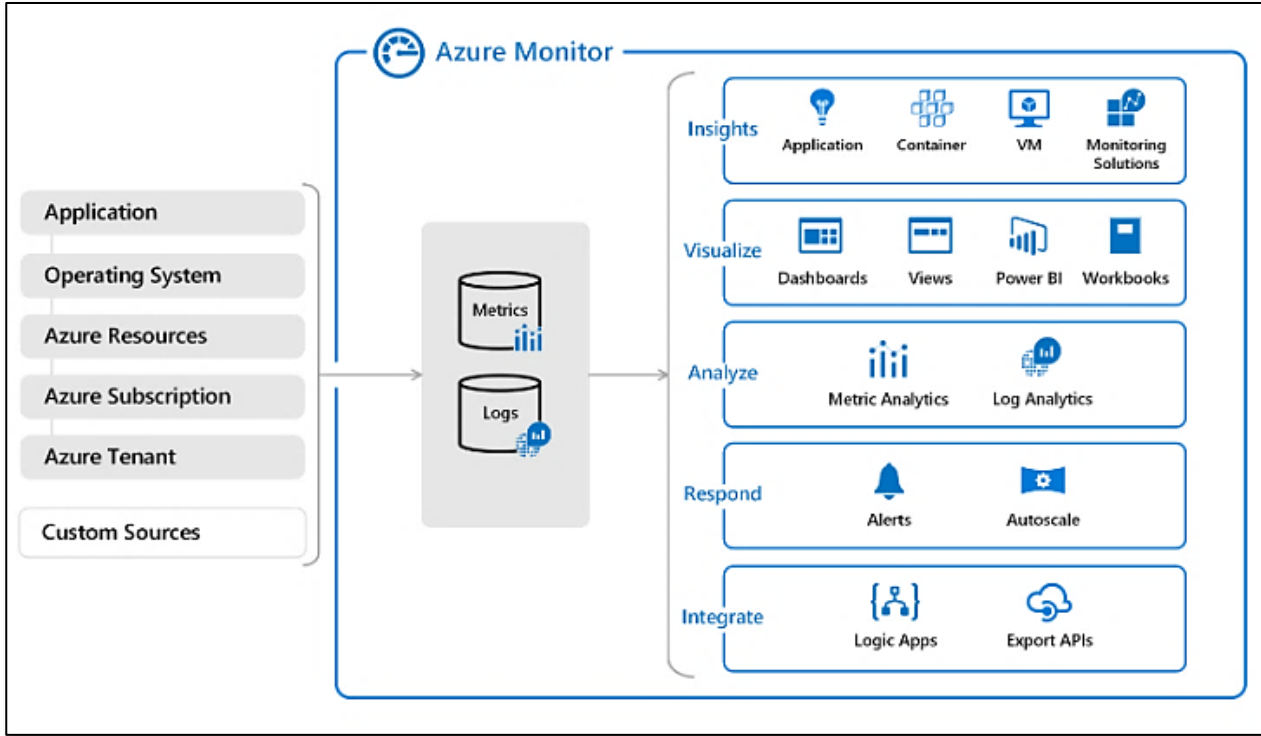
Azure Network Monitor, Page 20.

27.　　　Azure Monitor for Networks is a service of Azure Monitor. Azure Monitor for

network provides a visualization of health and metrics for all deployed resources.

Azure Monitor for Networks

Azure Monitor for Network provides a comprehensive view of health and metrics for all deployed network resource without any configuration. The advanced search capability helps identify resource dependencies, enabling scenarios such as identifying resources that are hosting your website by simply searching for hosted website name.

Azure Network Monitor, Page 1800.

28.　　　Metrics are values that describe aspects of a system. Metrics are collected at

regular intervals and can be aggregated using a variety of algorithms to determine the service

indicator trends.

Metrics are numerical values that describe some aspect of a system at a particular point in time. They are collected at regular intervals and are identified with a timestamp, a name, a value, and one or more defining labels. Metrics can be aggregated using a variety of algorithms, compared to other metrics, and analyzed for trends over time.

Azure Network Monitor, Page 197.

29.   The Smart Metric Pattern Recognition feature of Azure Monitor determines the trend in the metric. Pattern Recognition uses ML technology to automatically detect metric patterns and adapt to metric changes over time. Pattern Recognition provides the trends and alerts based on deviations of the metric from the pattern and helps prevent noisy or wide thresholds.

Smart Metric Pattern Recognition – Using our ML technology, we're able to automatically detect metric patterns and adapt to metric changes over time, which may often include seasonality (hourly / daily / weekly). Adapting to the metrics' behavior over time and alerting based on deviations from its pattern relieves the burden of knowing the "right" threshold for each metric. The ML algorithm used in Dynamic Thresholds is designed to prevent noisy (low precision) or wide (low recall) thresholds that don't have an expected pattern.

Azure Network Monitor, Page 2253.

30.   Azure Monitor has a Network Performance Monitor. The Network Performance Monitor has different types of categories. One of the categories is a service connectivity monitor.

31.   The Service connectivity Monitor in Network Performance Monitoring determines the connectivity to applications and network services which include, for example, Office 365 and Dynamic CRM. The service connectivity monitor also determines the response time and network latency (i.e. network parameters) during connection to the endpoint in a network.

8

> **Service Connectivity Monitor**
>
> Monitor the network connectivity to your applications and network services from multiple branch offices or locations. Applications and network services include Office 365, Dynamics CRM, internal line-of-business applications, and SQL databases.
> Use built-in tests to monitor network connectivity to Office 365 and Dynamics 365 endpoints.
> Determine the response time, network latency, and packet loss experienced when connecting to the endpoint.

Azure Network Monitor, Page 1844.

32.   The Network performance monitor selects the chosen metric from loss, latency, response time, or bandwidth utilization. (i.e. two or more parameters of a network representative and variable in time) for predicting trends or generating alerts in case of this system.

> **Network Performance Monitor dashboard**
>
> - **Top Network Health Events**: This page provides a list of the most recent health events and alerts in the system and the time since the events have been active. A health event or alert is generated whenever the value of the chosen metric (loss, latency, response time, or bandwidth utilization) for the monitoring rule exceeds the threshold.

Azure Network Monitor, Page 1834.

33.   The Network performance Monitor collects loss and latency information (i.e. network parameters). Data collection happens at regular intervals.

9

Data collection details

To collect loss and latency information, Network Performance Monitor uses TCP SYN-SYNACK-ACK handshake packets when you choose TCP as the protocol. Network Performance Monitor uses ICMP ECHO ICMP ECHO REPLY when you choose ICMP as the protocol. Trace route is also used to get topology information.

all the various routes in the network that must be tested. Using this data, the agents can deduce the network latency and packet loss figures. The tests are repeated every five seconds. Data is aggregated for about three minutes by the agents before it's uploaded to the Log Analytics workspace in Azure Monitor.
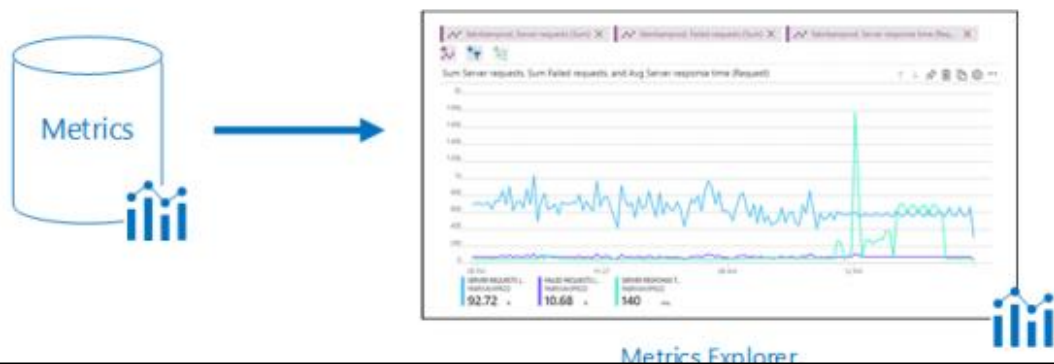
Azure Network Monitor, Page 1833.

34.   The Network Performance Monitor monitors resources through Key Performance indictor (KPIs) (i.e. service indictor). KPIs are key health/performance metrics.

Use Quality Gates to integrate monitoring into your pre-deployment or post-deployment. This ensures that you are meeting the key health/performance metrics (KPIs) as your applications move from dev to production and any differences in the infrastructure environment or scale is not negatively impacting your KPIs.

Azure Network Monitor, Page 184.

35.   To look at performance metrics, one can click on any of the graphs in the metrics explorer in the Azure Portal. Azure Portal helps to chart the values of multiple metrics over time.

portal. Have a look at any virtual machine for example, and you'll see several charts displaying performance metrics. Click on any of the graphs to open the data in metrics explorer in the Azure portal, which allows you to chart the values of multiple metrics over time. You can view the charts interactively or pin them to a dashboard to view them with other visualizations.

10

Azure Network Monitor, Page 214.

36.   Metrics (i.e. service indicator) are values that describe aspects of a system. Metrics can be collected at regular intervals (i.e. two or more times) and can be aggregated using a variety of algorithms.

Metrics are numerical values that describe some aspect of a system at a particular point in time. They are collected at regular intervals and are identified with a timestamp, a name, a value, and one or more defining labels. Metrics can be aggregated using a variety of algorithms, compared to other metrics, and analyzed for trends over time.

Azure Network Monitor, Page 197.

37.   As an example, metrics like Average Bandwidth is a function of Bandwidth (i.e. network parameter). Similarly, metrics like SucessE2ELatency are also a function of Latency (i.e. network parameter).

METRIC	METRIC DISPLAY NAME	UNIT	AGGREGATION TYPE	DESCRIPTION	DIMENSIONS
SuccessE2ELatency	Success E2E Latency	Milliseconds	Average	The end-to-end latency of successful requests made to a storage service or the specified API operation, in milliseconds. This value includes the required processing time within Azure Storage to read the request, send the response, and receive acknowledgment of the response.	GeoType,ApiName,Authentication

SuccessServerLatency	Success Server Latency	Milliseconds	Average	The latency used by Azure Storage to process a successful request, in milliseconds. This value does not include the network latency specified in SuccessE2ELatency.	GeoType,ApiName,Authentication

Azure Network Monitor, Page 2794.

METRIC	METRIC DISPLAY NAME	UNIT	AGGREGATION TYPE	DESCRIPTION	DIMENSIONS
AverageBandwidth	Gateway S2S Bandwidth	BytesPerSecond	Average	Average site-to-site bandwidth of a gateway in bytes per second	None

Azure Network Monitor, Page 2868.

38.   Azure Monitor determines a trend of a metric (i.e. service indicator). The trend of a metric is a function of metric values.

Trend charts

At each level that you drill down, you can see the trend of the applicable metric. It can be loss, latency, response time, or bandwidth utilization. To change the time interval for the trend, use the time control at the top of the chart.
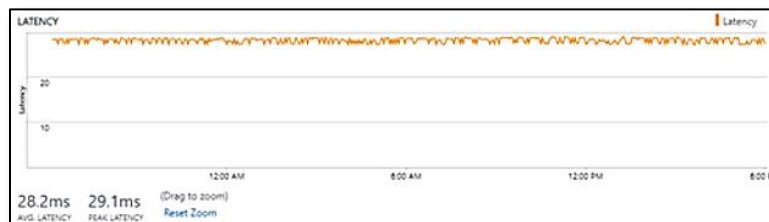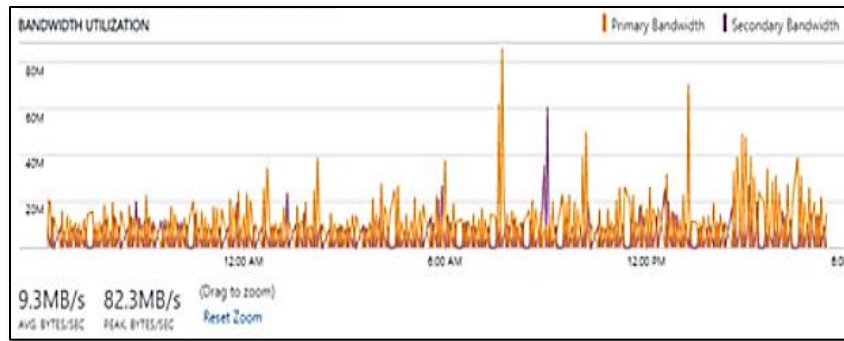
Azure Network Monitor, Page 1835.

39.   The trends of metrics like Bandwidth and Latency are shown below.

Trends of loss, latency, and throughput

The bandwidth utilization, latency, and loss charts are interactive. You can zoom in to any section of these charts by using mouse controls. You also can see the bandwidth, latency, and loss data for other intervals. In the upper left under the **Actions** button, select**Date/Time**.

Azure Network Monitor, Page 1854.

Azure Network Monitor, Page 1854.

40.   Azure Monitor proactively provides notifications about critical conditions and potentially attempts to take corrective actions. The Alerts are based on real-time values.

Alerts

Alerts in Azure Monitor proactively notify you of critical conditions and potentially attempt to take corrective action. Alert rules based on metrics provide near real time alerting based on numeric values, while rules based on logs allow for complex logic across data from multiple sources.
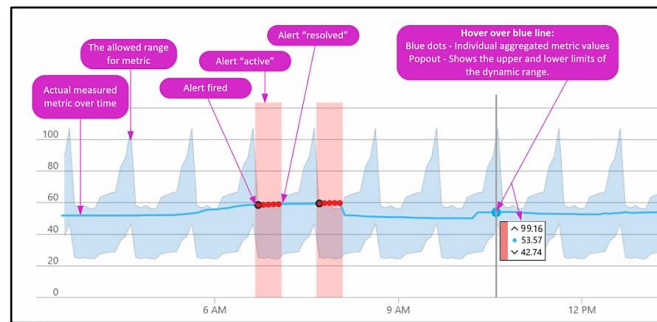
Azure Network Monitor, Page 24.

41.   The real-time alerts are predicted and calculated using Smart Metric Pattern Recognition. Smart Metric Pattern Recognition is Azure Monitor's Machine learning technology, which automatically detects metric patterns and adapts to metric changes over time. Alerts are based on deviations from a pattern. The algorithm is designed to prevent noisy or wide thresholds that don't have an expected pattern.

> **Smart Metric Pattern Recognition** – Using our ML technology, we're able to automatically detect metric patterns and adapt to metric changes over time, which may often include seasonality (hourly / daily / weekly). Adapting to the metrics' behavior over time and alerting based on deviations from its pattern relieves the burden of knowing the "right" threshold for each metric. The ML algorithm used in Dynamic Thresholds is designed to prevent noisy (low precision) or wide (low recall) thresholds that don't have an expected pattern.

Azure Network Monitor, Page 1854.

42.   An Alarm is triggered when deviation from these thresholds indicates an anomaly in the metric behavior (i.e. trend of the indicator crosses the defined threshold).

> The thresholds are selected in such a way that a deviation from these thresholds indicates an anomaly in the metric behavior.

Azure Network Monitor, Page 2257.

43.   In view of preceding paragraphs, each and every element of at least claim 1 of the '160 Patent is found in the Accused Products.

44.   Microsoft has and continues to directly infringe at least one claim of the '160 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.

45.   Microsoft has received notice and actual or constructive knowledge of the '160 Patent since at least the date of service of this Complaint.

46.   Since at least the date of service of this Complaint, through its actions, Microsoft has actively induced product makers, distributors, retailers, and/or end users of the Accused

14

Products to infringe the '160 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://opdhsblobprod01.blob.core.windows.net/contents/4a6d75bb3af747de838e6ccc97c5d978/03a9959eadb93d2c2131be1f3b2ea464?sv=2015-04-05&sr=b&sig=EV%2B2JDmkvfnTTZdyWVb4IyvBaP24ZtM2CUTBrBtINe4%3D&st=2020-01-27T08%3A49%3A56Z&se=2020-01-28T08%3A59%3A56Z&sp=r

47.   Since at least the date of service of this Complaint, through its actions, Microsoft has contributed to the infringement of the '160 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 '160 Patent. The Accused Products are especially made or adapted for infringing the '160 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 '160 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 Microsoft infringes one or more claims of the '160 Patent literally and/or under the doctrine of equivalents;

(B)   Enter judgment that Microsoft has induced infringement and continues to induce infringement of one or more claims of the '160 Patent;

(C)   Enter judgment that Microsoft has contributed to and continues to contribute to the infringement of one or more claims of the '160 Patent;

(D)   Award Brazos damages, to be paid by Microsoft in an amount adequate to compensate Brazos for such damages, together with pre-judgment and post-judgment interest for the infringement by Microsoft of the '160 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

(F)   Award Brazos its costs, disbursements, attorneys' fees, and such further and additional relief as is deemed appropriate by this Court.

Dated: April 27, 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

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

COUNSEL FOR PLAINTIFF

16