

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TEXAS  
MARSHALL DIVISION**

K.MIZRA LLC	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 2:21-cv-00247-JRG
	)	
CA, INC.,	)	(Lead Case)
	)	
Defendant.	)	

---

K.MIZRA LLC	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 2:21-cv-00248-JRG
	)	
FORESCOUT, INC.,	)	(Member Case)
	)	
Defendant.	)	

---

K.MIZRA LLC	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 2:21-cv-00249-JRG
	)	
FORTINET, INC.,	)	(Member Case)
	)	
Defendant.	)	

---

**FIRST AMENDED COMPLAINT**

Plaintiff K.Mizra LLC (“K.Mizra”) files this Amended Complaint against Defendant CA Inc. (“CA”).

**NATURE OF THE CASE**

1. This is an action for the infringement of U.S. Patent No. 8,965,892 (the “’892 patent

or “the Patent-in-Suit”).

2. Defendant CA has been making, selling, using and offering for sale email security products and related services such as the Symantec Messaging Gateway software, appliances, and various other network equipment, software, and related services incorporating its email security technology that infringes the ’892 patent in violation of 35 U.S.C. § 271 (collectively, “the Accused Instrumentalities”).

3. Plaintiff K.Mizra seeks appropriate damages and prejudgment and post-judgment interest for CA’s infringement of the Patents-in-Suit.

### **THE PARTIES**

4. Plaintiff K.Mizra is a Delaware limited liability company with its principal place of business at 777 Brickell Ave, #500-96031, Miami, FL 33131. K.Mizra is the assignee and owner of the Patent-in-Suit.

5. K.Mizra recently relocated its office from California to Florida in the summer of 2021.

6. Defendant CA is a Delaware Corporation that maintains a regular and established place of business in Texas, for example, at its campus at 5465 Legacy Drive, Plano, TX 75024. CA is registered to conduct business in the state of Texas and has appointed the Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company, located at 211 E. 7th St., Suite 620, Austin, TX 78701, as its agent for service of process.

7. CA is a subsidiary of Broadcom, Inc. (“Broadcom”) In 2019, CA acquired Symantec’s Enterprise Security business which developed, marketed, and sold the Symantec Messaging Gateway.

8. By maintaining facilities in Plano, CA has regular and established place of business

in the Eastern District of Texas.

9. K.Mizra sent letters to CA's parent Broadcom in January 2021 and then again in February 2021 about taking a license to K.Mizra's patent portfolio. Prior to K.Mizra filing this lawsuit with its Original Complaint, neither Broadcom nor CA responded to any of K.Mizra's correspondence regarding taking a license to K.Mizra's patents.

10. CA has been on notice of its infringement of the '892 patent at least as of the date of service of the Original Complaint on July 8, 2021.

11. Notwithstanding its receipt of notice that the Accused Instrumentalities infringe the '892 patent, including notice provided as of the service of the Original Complaint on July 8, 2021, CA continues to sell the Accused Instrumentalities in flagrant disregard of K.Mizra's rights under the '892 patent.

### **JURISDICTION AND VENUE**

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

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

14. This Court has personal jurisdiction over CA because, *inter alia*, CA has a continuous presence in, and systematic contact with, this District and has registered to conduct business in the state of Texas.

15. CA has committed and continues to commit acts of infringement of K.Mizra's Patent-in-Suit in violation of the United States Patent Laws, and has made, used, sold, offered for sale, marketed and/or imported infringing products into this District. CA's infringement has caused substantial injury to K.Mizra, including within this District.

16. Venue is proper in this District pursuant to 28 U.S.C. §§ 1400 and 1391 because CA has committed acts of infringement in this District and maintains a regular and established place of business in this District.

### **THE PATENT-IN-SUIT**

17. The '892 patent is titled "Identity-Based Filtering" and was issued by the United States Patent Office to inventor Aaron T. Emigh on February 24, 2015. The earliest application related to the '892 patent was filed on January 4, 2007. A true and correct copy of the '892 patent is attached as Exhibit A.

18. K.Mizra is the owner of all right, title and interest in and to the '892 patent with the full and exclusive right to bring suit to enforce the '892 patent.

19. The '892 patent is valid and enforceable under the United States Patent Laws.

20. The claims of the '892 patent are directed to technological solutions that address specific challenges rooted in computing technology involving the filtering of electronic content. With the proliferation of electronic documents and content on the internet such as PDFs, webpages, and electronic mail that are accessible via a network address or that traverse a computer network, there is a myriad of undesirable content that a computer user may encounter. *See* Exhibit A at 1:19-22. The inventors of the '892 patent understood the shortcomings of the traditional approaches to filtering unwanted content that were solely based on including or excluding certain addresses or uniform resource locators (URLs) associated with the document. The '892 patent explains that prior to its invention, "[a] variety of approaches to content filtering have been employed to avoid undesirable content. Examples of such approaches include blacklisting and whitelisting URLs and sites. However, these approaches fail to discriminate between specific content owners or creators within a site. In some cases, particular participants in a site or service may have more desirable, or

less desirable, content than other participants, and present approaches are unable to take advantage of this, leading to either inclusion of objectionable content, or exclusion of desirable content.” *Id.* at 1:23-32.

21. The technological invention of the ’892 patent improves upon these conventional techniques for computerized filtering of electronic documents over the internet by extracting and resolving certain data inherent in the electronic document to correlate and determine the reputations of the author or sender of the document and the group in which he or she may be a member of. For example, the ’892 patent describes “extracting an identity from a document and/or metadata” and analyzing content with “content analyzing technologies” such as Bayesian filtering or Support Vector Machines. *See, e.g., id.* at 2:24-36. The ’892 patent also discusses further steps of correlating identity, detecting affiliation, and determining reputation associated with electronic documents over a computer network. *Id.* at 1:38-63. The enhanced filtration techniques taught by the ’892 patent can be carried out “programmatically via an API or by retrieving one or more pages from the network and analyzing them.” *See, e.g., id.* at 6:5-67.

22. The ’892 patent claims a way to solve technological problems that existed within the field of electronic documents and computer technology. It provides a technological solution to a problem specific to technology related to electronic documents by improving computer functionality for filtering electronic documents. Faced with the shortcomings of plain filtering techniques such as white-listing or black-listing that existed at the time of the invention, the inventors of the ’892 patent developed a far more advanced approach with specific steps for determining and correlating group-related reputation and identity reputation. By utilizing such improvements to electronic content filtering technology, data security companies such as Cisco are able to take advantage of more optimally tailored filtering to block unwanted documents such

as electronic mail on computer networks without sacrificing the over-exclusion of desired content.

23. The way in which the claims of the '892 patent address the technological problem is not merely a nominal application of a generic computer to practice the invention. Instead, the claims of the '892 patent implement particular improvements to computerized data filtering technology in order to overcome the problems specifically arising in the field of electronic content filtering.

24. The claims of the '892 patent recite subject matter that is not merely the routine or conventional use of filtering undesired electronic documents that existed in the prior art. Instead, the claimed inventions are directed to particularized implementations of determining the reputation associated with electronic documents. The '892 patent claims specify improved computer functionality for extracting certain information and data inherent in the electronic documents for purposes of resolving the reputations associated with the document, author of the document, and groups of which the author may be a member.

**FIRST CAUSE OF ACTION**  
**(PATENT INFRINGEMENT UNDER 35 U.S.C. § 271 of '892 PATENT)**

25. K.Mizra re-alleges and incorporates by reference all of the foregoing paragraphs.

26. On information and belief, CA has directly and indirectly infringed and continues to infringe, either literally or under the doctrine of equivalents, one or more claims, including at least claim 15 of the '892 patent in violation of 35 U.S.C. §§ 271 et seq., by making, using, importing, selling, offering for sale, and/or importing in this District and into the United States certain products, including but not limited to those, relating to the Accused Instrumentalities.

27. On information and belief, CA has been and currently is infringing the '892 patent by the manufacture, use, sale, offer to sell and/or importation of its products, including at least the Accused Instrumentalities under 35 U.S.C. § 271.

28. For example, Claim 15 of the '892 patent recites the following:

[preamble] A non-transitory computer program product for determining a reputation associated with an electronic document accessible via a network address, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

[A] determining an identity relating to a person, wherein the identity is associated with the electronic document;

[B] determining that the person is a member of a group, wherein the group is associated with a group-related service and wherein the group is associated with a group reputation;

[C] determining an identity reputation, wherein the identity reputation is associated with the identity and wherein the identity reputation is based at least in part on the group reputation; and

[D] determining a document reputation, wherein determining the document reputation uses the identity reputation.

29. On information and belief, and based on publicly available information, at least the Accused Instrumentalities satisfy each and every limitation of at least claim 15 of the '892 patent.

30. The preamble of claim 15 recites a “non-transitory computer program product for determining a reputation associated with an electronic document accessible via a network address.” Regarding the preamble of claim 15, to the extent the preamble is determined to be limiting, the Accused Instrumentalities provide the features described in the preamble. For example, “Messaging Gateway combines multilayer protection technologies that effectively detect, block, and quarantine suspicious email:

## Messaging Security Solution

Symantec's on-premises email security solution begins with Messaging Gateway which provides essential inbound and outbound messaging security including, powerful protection against the latest messaging threats including ransomware, spear phishing, and business email compromise. It catches more than 99 percent of spam with a less than 1 in 1 million false positives, and effectively responds to new messaging threats with real-time automatic antispam and antimalware updates.

**Messaging Gateway** combines multilayer protection technologies that effectively detect, block, and quarantine suspicious email:

- Stops BEC attacks using advanced heuristics, BEC scam analysis, email sender authentication protocols (DMARC\*, DKIM, and SPF), and domain intelligence to block typo squatting and identity spoofing.
- Prevents spam and directory harvesting attacks using a combination of Symantec global and local sender reputation databases, heuristics, and customer-specific spam rules that restrict up to 90 percent of unwanted email before it reaches your network.
- Advanced content filtering controls prevent unwanted email such as newsletters and other marketing content from reaching users.

See Exhibit B, Symantec Messaging Gateway (available at

<https://docs.broadcom.com/doc/messaging-gateway-atp-data-protection-en>, last visited on May 28, 2021).

31. Specifically, Messaging Gateway uses the Symantec global and local sender reputation database:



## **Block email threats with the high effectiveness and accuracy**

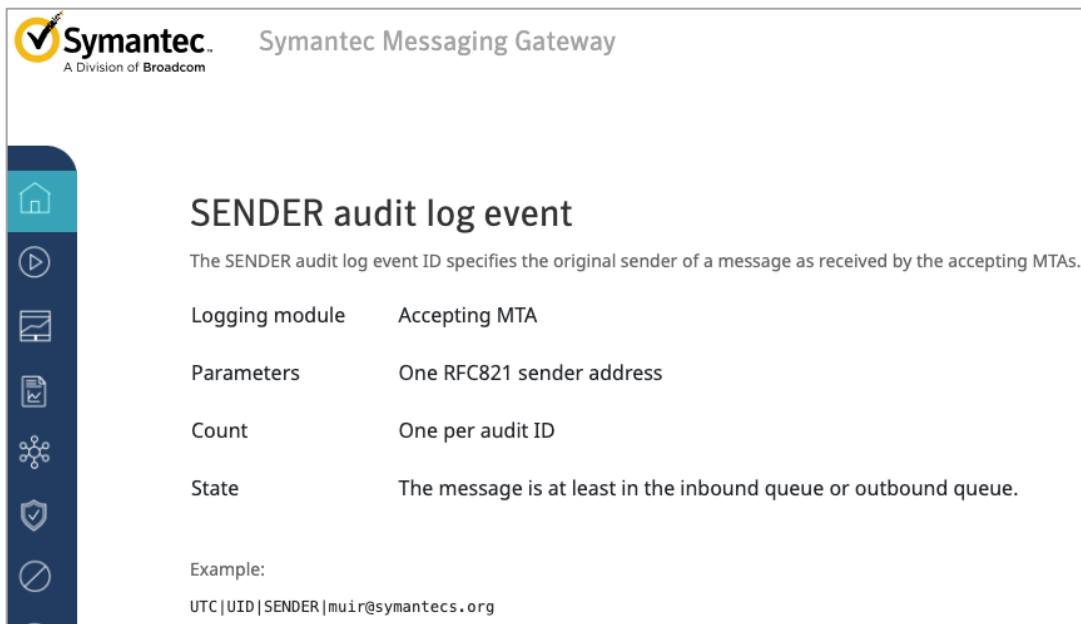
Prevent insidious email threats such as business email compromise, ransomware, and spam.

- Defeat business email compromise using advanced heuristics, BEC scam analysis, sender authentication enforcement & controls, and domain intelligence to help block typo squatting and identity spoofing.
- Protect your brand reputation by using automation to solve the practical issues of enforcing sender authentication (DMARC, DKIM and SPF) with Symantec Email Fraud Protection.
- Contain the latest file-based attacks such as ransomware using machine learning, predictive file analysis, and virtual machine aware sandboxing to reveal malicious behavior and safely detonate suspicious files.
- Spam filtering blocks attacks using global and local sender reputation, and heuristics to restrict up to 99 percent of unwanted email before it reaches your network.
- Defend against malicious links with URL reputation filtering which includes advanced phishing variant detection that sniffs out phishing links that are similar to known phishing attacks.

See Symantec Messaging Gateway Product Overview (available at <https://www.broadcom.com/products/cyber-security/network/messaging/gateway>, last visited May 28, 2021).

32. Thus, to the extent the preamble of claim 15 is limiting, the Accused Instrumentalities meet it.

33. Limitation A of claim 15 requires “determining an identity relating to a person, wherein the identity is associated with the electronic document.” The ’892 Accused Instrumentalities also meet all the requirements of limitation A of claim 15. For example, the Messaging Gateway’s SENDER audit logs show that the email sender identity is determined.



The screenshot shows the Symantec Messaging Gateway help page for the SENDER audit log event. The page includes the Symantec logo and a navigation sidebar. The main content area contains the following information:

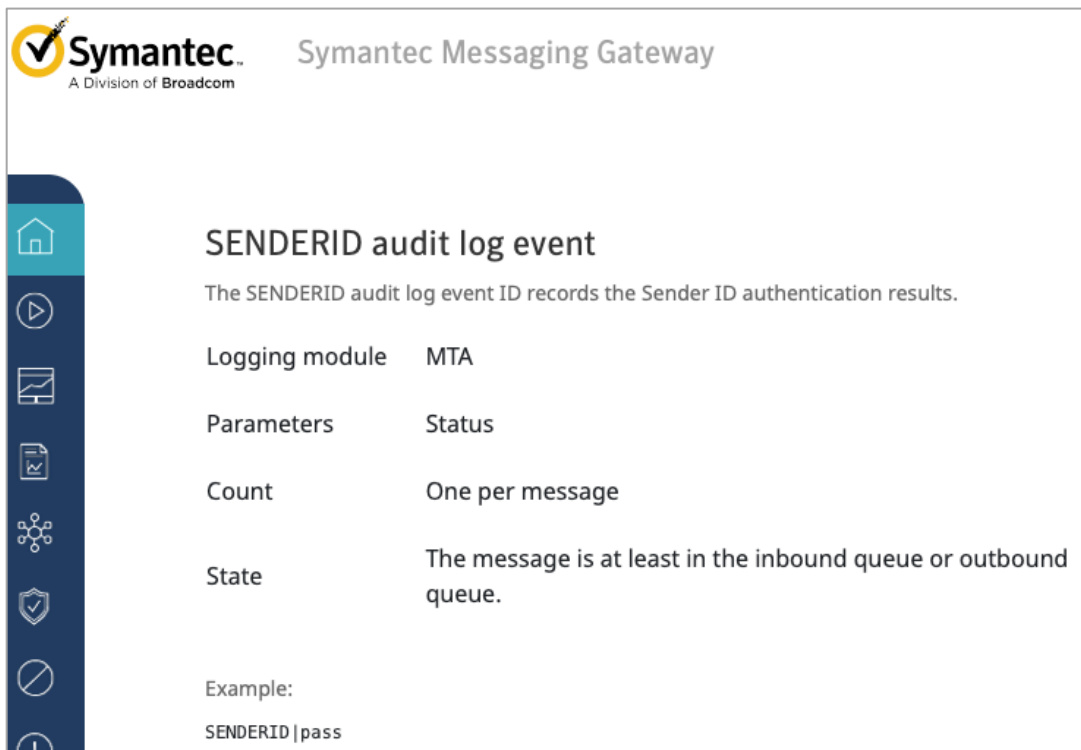
**SENDER audit log event**

The SENDER audit log event ID specifies the original sender of a message as received by the accepting MTAs.

Logging module	Accepting MTA
Parameters	One RFC821 sender address
Count	One per audit ID
State	The message is at least in the inbound queue or outbound queue.

Example:  
UTC|UID|SENDER|muir@symantecs.org

See Exhibit C, Symantec Messaging Gateway SENDER audit log event (available at [https://help.symantec.com/cs/SMG\\_10\\_7\\_0/SMG/v6046903\\_v132085995/SENDER-audit-log-event?locale=EN\\_US](https://help.symantec.com/cs/SMG_10_7_0/SMG/v6046903_v132085995/SENDER-audit-log-event?locale=EN_US), last visited May 28, 2021).



The screenshot shows the Symantec Messaging Gateway help page for the SENDERID audit log event. The page includes the Symantec logo and a navigation sidebar. The main content area contains the following information:

**SENDERID audit log event**

The SENDERID audit log event ID records the Sender ID authentication results.

Logging module	MTA
Parameters	Status
Count	One per message
State	The message is at least in the inbound queue or outbound queue.

Example:  
SENDERID|pass

See Exhibit D, Symantec Messaging Gateway SENDERID audit log event (available at

[https://help.symantec.com/cs/SMG\\_10\\_7\\_0/SMG/v126380661\\_v132085995/SENDERID-audit-log-event?locale=EN\\_US](https://help.symantec.com/cs/SMG_10_7_0/SMG/v126380661_v132085995/SENDERID-audit-log-event?locale=EN_US), last visited May 28, 2021).

34. Therefore, the '892 Accused Instrumentalities meet limitation A of claim 15.

35. Limitation B of claim 15 requires “determining that the person is a member of a group, wherein the group is associated with a group-related service and wherein the group is associated with a group reputation.” The Accused Instrumentalities also meet all the requirements of limitation B of claim 15. For example, Messaging Gateway determines whether a sender is a good sender or a bad sender based on the sender’s membership to at least one of the following groups: Local Good/Bad Sender Domains, Local Good/Bad Sender IPs, Third Party Good/Bad Senders, or Symantec Global Good/Bad Senders.

<b>Bad Sender</b>	A sender from whom you do not want to accept email messages. A Bad Sender is a member of at least one of the following groups: Local Bad Sender Domains, Local Bad Sender IPs, Third Party Bad Senders, or Symantec Global Bad Senders.
-------------------	---

<b>Good Sender</b>	A sender from whom you want to accept email messages. A Good Sender is a member of at least one of the following groups: Local Good Sender Domains, Local Good Sender IPs, Third Party Good Senders, or Symantec Global Good Senders.
--------------------	---

See [https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/email-security/messaging-gateway/generated-pdfs/smg\\_administration\\_guide\\_10\\_7\\_3.pdf](https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/email-security/messaging-gateway/generated-pdfs/smg_administration_guide_10_7_3.pdf) at 894, 897, last visited May 28, 2021.

36. Therefore, the Accused Instrumentalities meet limitation B of claim 15.

37. Limitation C of claim 15 requires “determining an identity reputation, wherein the identity reputation is associated with the identity and wherein the identity reputation is based at least in part on the group reputation.” The Accused Instrumentalities also meet all the requirements of limitation C of claim 15. For example, Messaging Gateway determines the reputation of the

sender as good or bad based on its membership to certain groups and the reputation of those groups.

Symantec Messaging Gateway lets you customize spam detection in the following ways:

Define good senders	Symantec Messaging Gateway treats mail coming from an address or connection in the Local Good Sender Domains and Local Good Sender IPs groups as legitimate mail. The good sender groups reduce the small risk that messages sent from trusted senders will be treated as spam or filtered in any way. By default messages from these senders are delivered normally.
Define bad senders	Symantec Messaging Gateway supports a number of actions for mail from a sender or connection in the Local Bad Sender Domains and Local Bad Sender IPs groups. By default, messages from senders in the Local Bad Sender Domains group are deleted. By default, SMTP connections from senders in the Local Bad Sender IPs and Third Party Bad Senders groups are rejected. However, you can instead choose other actions.

See [https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/email-security/messaging-gateway/generated-pdfs/smg\\_administration\\_guide\\_10\\_7\\_3.pdf](https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/email-security/messaging-gateway/generated-pdfs/smg_administration_guide_10_7_3.pdf) at 151, last visited May 28, 2021.

38. Therefore, the Accused Instrumentalities meet limitation C of claim 15.

39. Limitation D of claim 15 requires “determining a document reputation, wherein determining the document reputation uses the identity reputation.” The ’892 Accused Instrumentalities also meet all the requirements of limitation D of claim 15. For example, Messaging Gateway determines whether an email is legitimate based on the reputation of the sender as good or bad.

Symantec Messaging Gateway lets you customize spam detection in the following ways:

- |                     |  |
|---------------------|--|
| Define good senders | Symantec Messaging Gateway treats mail coming from an address or connection in the Local Good Sender Domains and Local Good Sender IPs groups as legitimate mail. The good sender groups reduce the small risk that messages sent from trusted senders will be treated as spam or filtered in any way. By default messages from these senders are delivered normally.  |
| Define bad senders  | Symantec Messaging Gateway supports a number of actions for mail from a sender or connection in the Local Bad Sender Domains and Local Bad Sender IPs groups. By default, messages from senders in the Local Bad Sender Domains group are deleted. By default, SMTP connections from senders in the Local Bad Sender IPs and Third Party Bad Senders groups are rejected. However, you can instead choose other actions. |

See [https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/email-security/messaging-gateway/generated-pdfs/smg\\_administration\\_guide\\_10\\_7\\_3.pdf](https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/email-security/messaging-gateway/generated-pdfs/smg_administration_guide_10_7_3.pdf) at 151, last visited May 28, 2021.

40. Therefore, the '892 Accused Instrumentalities meet limitation D of claim 15.

41. Accordingly, on information and belief, the Accused Instrumentalities meet all the limitations of, and therefore infringes, at least claims 15 of the '892 patent.

42. CA indirectly infringes the claims of the '892 patent within the United States by inducing infringement under 35 U.S.C. § 271(b). For example, since learning of the '892 patent and by failing to cease offering the Accused Instrumentalities for sale, CA has knowingly and intentionally induced users of the Accused Instrumentalities to directly infringe one or more claims of the '892 patent, inter alia, by (1) instructing users on how to use the Accused Instrumentalities in a manner that infringes the '892 Patent as described in the foregoing paragraphs; (2) providing customer support and training online and through its customer support call center on how to use them in an infringing manner; (3) directing its customers to additional online sources with instructions on how to infringe the '892 Patent (*see, e.g.,*

<https://support.broadcom.com/security/product-page.html?productName=Messaging%20Gateway>; <https://techdocs.broadcom.com>, last visited on September 15, 2021). CA also posts information on publicly available websites such as channels on YouTube, which explain how to use the Accused Instrumentalities in an infringing manner (*see, e.g.*, <https://www.youtube.com/users/symatecsup>); and touting these infringing uses of the Accused Instrumentalities in advertisements, white papers, and product literature, including but not limited to those listed on or available from Broadcom's website.

43. CA indirectly infringes the claims of the '892 patent by contributing to the direct infringement by end users under 35 U.S.C. § 271(c), for example, by providing the Accused Instrumentalities, which, as evidenced by Broadcom's websites and advertisements (*see, e.g.*, <https://www.broadcom.com/products/cyber-security/network/messaging/gateway>, last visited on September 15, 2021), is especially made for use in a manner that infringes one or more claims of the '892 patent as described herein and have no substantial non-infringing uses.

44. As a result of CA's infringement of the '892 patent, K.Mizra has suffered and continues to suffer substantial injury and is entitled to recover all damages caused by CA's infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for CA's wrongful conduct.

#### **PRAYER FOR RELIEF**

WHEREFORE, K.Mizra respectfully requests judgment against CA as follows:

A. That the Court enter judgment for K.Mizra on all causes of action asserted in this Complaint;

B. That the Court enter judgment in favor of K.Mizra and against CA for monetary damages to compensate it for CA's infringement of the Patents-in-Suit pursuant to 35 U.S.C. § 284, including costs and prejudgment interest as allowed by law;

C. That the Court enter judgment in favor of K.Mizra and against CA for accounting and/or supplemental damages for all damages occurring after any discovery cutoff and through the Court's entry of final judgment;

D. That the Court adjudge CA's infringement of the Patent-in-Suit to be willful dated from the filing of this Complaint.

E. That the Court enter judgment that this case is exceptional under 35 U.S.C. § 285 and enter an award to K.Mizra of its costs and attorneys' fees; and

F. That the Court award K.Mizra all further relief as the Court deems just and proper.

**JURY DEMAND**

K.Mizra requests that all claims and causes of action raised in this Complaint against CA be tried by a jury to the fullest extent possible.

Date: October 4, 2021

Respectfully submitted,

/s/ Cristofer Leffler

Cristofer I. Leffler, WA Bar No. 35020

**LEAD COUNSEL**

Cliff Win, Jr., CA Bar No. 270517

Folio Law Group PLLC

1200 Westlake Ave. N., Suite 809

Seattle, WA 98109

Tel: (206) 880-1802

Email: cris.leffler@foliolaw.com

Email: cliff.win@foliolaw.com

Joseph M. Abraham, TX Bar No. 24088879

Law Office of Joseph M. Abraham, PLLC

13492 Research Blvd., Suite 120, No. 177

Austin, TX 78750

Tel: (737) 234-0201

Email: joe@joeabrahamlaw.com

*Of Counsel:*

Andrea L. Fair

Texas Bar No. 24078488

Claire Abernathy Henry

Texas Bar No. 24053063

WARD, SMITH & HILL, PLLC

1507 Bill Owens Pkwy.

Longview, TX 75604

Tel: (903) 757-6400

Fax: (903) 757-2323

Email: andrea@wsfirm.com

Email: claire@wsfirm.com

*Counsel for Plaintiff K.Mizra LLC*