**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF DELAWARE**

| | |
|---|---|
| THREATMODELER SOFTWARE INC.,<br><br>Plaintiff,<br><br>v.<br><br>IRIUSRISK, INC.,<br><br>Defendant. | Civil Action No. _____<br><br>**DEMAND FOR JURY TRIAL** |

**PLAINTIFF THREATMODELER SOFTWARE INC.'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT AGAINST IRIUSRISK, INC.**

Plaintiff ThreatModeler Software Inc. ("ThreatModeler"), by and through its attorneys, hereby alleges this Complaint against Defendant IriusRisk, Inc. ("IriusRisk" or "Defendant") for patent infringement.

## PARTIES

1. Plaintiff ThreatModeler is a corporation organized and existing under the laws of the State of Delaware and having a principal place of business at 101 Hudson St., Suite 2100, Jersey City, New Jersey 07302.

2. Upon information and belief, Defendant IriusRisk, Inc. is a Delaware corporation having a principal place of business in Wilmington, Delaware. IriusRisk's registration to conduct business filed with the Georgia Secretary of State identifies its state of incorporation as Delaware, and identifies its principal place of business as Orange Street located in Wilmington, Delaware. IriusRisk can be served in the State of Delaware through its registered agent, the National Registered Agents, Inc., located at 1209 Orange Street, Wilmington, Delaware, 19801.

3. ThreatModeler is the sole and exclusive owner of U.S. Patent No. 10,699,008, titled "Threat model chaining and attack simulation systems and related methods" (the "'008 Patent") and U.S. Patent No. 10,713,366, titled "Systems and methods for automated threat

model generation from third party diagram files" (the "'366 Patent"). True and correct copies of the '008 Patent and the '366 Patent are attached as Exhibits A and B, respectively.

4. Defendant IriusRisk made, used, sold, offered for sale, and/or imported in the United States, including in this judicial district, products that directly and indirectly infringe at least claims 1 and 3 of the '008 Patent, and claims 1, 2, 4, 7, 8, 9, 11, 13, 16, 17, and 20 of the '366 Patent, either literally or under the doctrine of equivalents. These products include but are not limited to IriusRisk's Threat Modeler Platform including its Infrastructure as a Code (IaC) functionality, further including its interoperability with Amazon Web Services (AWS) and Hashicorp Terriform, and its Open Threat Model (collectively, the "Accused Products").

## JURISDICTION AND VENUE

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

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

7. Defendant IriusRisk is a company organized under the laws of the State of Delaware and is subject to this Court's specific and general personal jurisdiction.

8. Defendant IriusRisk has committed and induced acts of infringement within the state of Delaware, as alleged herein, and has derived substantial revenues from its infringing acts occurring within Delaware.

9. Defendant IriusRisk uses and offers to its customers and users, within the state and District of Delaware, the Accused Products. Defendant IriusRisk also solicits customers and potential customers within the state and District of Delaware via its internet presence, and on information and belief, offers to provide and actually provides demonstrations of its Accused Products to customers, potential customers, and users within the state and District of Delaware.

10. In addition to its office in the state of Delaware, Defendant IriusRisk has an office in Atlanta, Georgia. As alleged in paragraph 2 of this Complaint, IriusRisk's registration to conduct business with the Secretary of State in Georgia identifies its state of incorporation as

Delaware, and identifies its principal place of business as Orange Street located in Wilmington, Delaware.

11. For these reasons, personal jurisdiction exists and venue is proper in this District and Court under 28 U.S.C. § 1400(b).

**THREATMODELER'S INNOVATIONS AND PATENTS**

12. ThreatModeler is a cybersecurity company that has developed automated threat modeling solutions for fortifying an enterprise's software development lifecycle. ThreatModeler's solutions identify, predict and define threats in order to educate security and development teams to incorporate countermeasures during any phase of the software development lifecycle, including early in software and system development.

13. The cybersecurity applications for ThreatModeler's threat model solutions include but are not limited to medical fields, finance, and retail. For example, ThreatModeler has created the only threat modeling platform designed to build threat models for medical devices using ThreatModeler's medical device library according to FDA guidelines.

14. ThreatModeler's threat model solutions allow for nesting and chaining of a threat model as an architectural component within another threat model. Through nesting, ThreatModeler allows more robust threat modeling, and more comprehensive compiling of threats and identification of weaknesses and countermeasures from application interactions, shared components, and 3rd party elements.

15. ThreatModeler has collected numerous awards for its ThreatModeler platform, including being named "Most Innovative" by Cyber Defense Magazine's InfoSec Awards in 2018. ThreatModeler was awarded Cyber Defense Magazine's InfoSec Award in 2018, 2019, and 2021. ThreatModeler was awarded CyberSecurity Excellence Awards in 2017, 2018, 2019, and 2020. ThreatModeler was awarded the Big Innovation Award in 2021, and was a Digital Revolution Awards winner in 2021.

16. On May 16, 2022, ThreatModeler was named an SC Magazine Awards Finalist for Best Threat Intelligence Technology. SC Magazine reported that "Cybercrime is big

business, and techniques of bad actors are growing increasingly sophisticated. That leaves security teams thirsting for near realtime intelligence about the threat landscape." *See* https://www.scmagazine.com/news/threat-intelligence/finalists-best-threat-intelligence-technology. In recognizing ThreatModeler's technical achievements, SC Magazine reported: "ThreatModeler is a collaborative platform where security experts or non-security professionals alike can build threat models within a few hours or minutes instead of weeks through a completely automated process. The latest evolution of ThreatModeler's technology delivers real-time threat modeling capabilities, enabling developers to understand the full scope of their intended IT infrastructure." *Id*.

17. ThreatModeler has been granted multiple U.S. patents for various inventions including threat modeling functionality, systems, and methods.

18. In 2017, ThreatModeler filed four provisional patent applications directed to threat modeling methods and systems. ThreatModeler filed U.S. Provisional Application No. 62/530,295 on July 10, 2017. ThreatModeler filed U.S. Provisional Application No. 62/527,671 on June 30, 2017. ThreatModeler filed U.S. Provisional Application No. 62/520,954 on June 16, 2017. And ThreatModeler filed U.S. Provisional Application No. 62/507,691 on May 17, 2017. Collectively, these four U.S. provisional applications are referred to hereinafter as the "Provisional Applications."

19. ThreatModeler's '008 Patent was filed on Dec. 20, 2018 as U.S. Patent Application No. 16/228,738, as a continuation-in-part of U.S. Patent Application No. 15/922,856, filed on March 15, 2018 (which issued as U.S. Patent No. 10,200,399), which in turn is a continuation-in-part application of U.S. Patent Application Ser. No. 15/888,021, filed on February 3, 2018 (which issued as U.S. Patent No. 10,255,439). The '008 Patent also claims priority from and the benefit of the Provisional Applications. *See* Ex. A.

20. ThreatModeler's '366 Patent was filed on Aug. 15, 2019 as U.S. Patent Application No. 16/542,263, as a continuation-in-part of U.S. Patent Application No. 16/228,738, filed on December 20, 2018 (which issued as the '008 Patent), which is a

continuation-in-part of U.S. Patent Application No. 15/922,856, filed on March 15, 2018 (which issued as U.S. Patent No. 10,200,399), which in turn is a continuation-in-part of U.S. Patent Application No. 15/888,021, filed on February 3, 2018 (which issued as U.S. Patent No. 10,255,439). The '366 Patent also claims priority from and benefit of the Provisional Applications. *See* Ex. B.

**OVERVIEW OF U.S. PATENT NO. 10,699,008**

21. The '008 Patent is titled: "Threat model chaining and attack simulation systems and related methods." The '008 Patent discloses and claims innovative solutions for grouping components within a threat model in order to allow threat model chaining. The solutions developed, patented, and commercialized by ThreatModeler allow a user to build more complex threat models that use an existing component group's threat model as a feature.

22. The '008 Patent discloses an exemplary process for creating a component group within a threat model: "The 'group' and 'ungroup' selectors allow the user to create a group containing multiple components or to delete a group (but not the included components). As seen in FIG. 10 for example, there is a 'WINDOWS 7' group which includes file system, PDF client, SKYPE, OUTLOOK 2010, MCAFEE HIPS, MCAFEE AV VSE, IE11, BIT LOCKER, MCAFEE DLP, and OFFICE 2010 components. There is also a Laptop group containing the WINDOWS 7 group and further containing WiFi port, USB port, ethernet port, HDMI port, and BLUETHOOTH port components. Finally, there is an Office Network group which includes the Laptop group and also includes file server, SHAREPOINT, printer, WiFi access point, IRONPORT, email server, BLUECOAT proxy, and SSO (single sign on) components. Then there are other components (external email gateway, AKAMAI DNS) which are not part of any group. A group may be formed from any one or more components, and the AZURE group is seen containing only a single component: ONEDRIVE." *See* '008 Patent, col. 19, ll. 50-67.

23. The '008 Patent also discloses exemplary technical advantages of grouping components within a threat model: "Each grouping of components, however, could be diagrammed separately as an independent threat model and then saved as a component so that it

may be imported into another threat model/diagram. When a user adds any of these component groups to a blank or existing diagram/threat model the threat model of the component group is added to (and/or nested within) the threat model of the existing diagram/threat model. In this way the user can modify a threat model by incorporating previously defined threat models. This ability is generally termed 'threat model chaining' herein and is a useful mechanism for allowing a user to diagram complex systems/processes without having to repeatedly build common elements among the systems/processes." *See* '008 Patent, col. 20, ll. 23-36.

24. The '008 Patent provides further explanation of these exemplary technical advantages: "By non-limiting example, referring to FIG. 10, the WINDOWS 7 component group could be defined as a component, then the user could, in another diagram (or the same diagram), select and add a WINDOWS 7 component to the diagram to import into the diagram and associated threat model the threats associated with the WINDOWS 7 threat model. That same could be done for the LAPTOP component group. Accordingly, a component group and associated threats added to a diagram may in turn already include other nested/chained threat models therein, so for example if a user defined a laptop component group such as that in FIG. 10 as a 'WINDOWS LAPTOP' component then, when a user later adds a WINDOWS LAPTOP element to a diagram/threat model by selecting a WINDOWS LAPTOP component from the toolbox and dragging it onto the diagram, the threats associated with the laptop itself, as well as the nested/chained threats associated with the included WINDOWS 7 threat model, are automatically included in the threat model for the then displayed diagram." *See* '008 Patent, col. 20, ll. 41-58.

25. The '008 Patent describes the resulting benefit to a threat model that includes chained component groups: "[I]t is pointed out (as has been discussed to some extent above) that each individual component (or grouped set of components) of a threat model could, itself, be associated with its own threat model through the database. Because of this, the overall threat model that is shown (for instance in FIG. 13) in implementations could be called a threat model portfolio as it includes all sub-threat models and nested threat models. For example, an overall

threat model A could include components B, C, and D. Component B could be a single component, component C could be a previously modeled group of components having its own threat model, and component D could be a previously modeled group of components having its own threat model that also includes therein a nested threat model for a component group E. Accordingly, the threat model A would include all threat models associated with components and component groups B, C, D, and E, including all nested threat models. As described above, this 'threat model chaining' may allow for quick and simple building of process/system models without having to recreate commonly included system/process elements." *See* '008 Patent, col. 24, ll. 10-30.

26. The '008 Patent describes the industry benefit of these innovations. "It may be pointed out that increased interconnectivity of a computing system with other systems (such as the Internet, third party systems, end user systems, etc.) may increase economic value and efficiency though these may also increase organizational risk due to the increase in adversarial actors and a constantly evolving threat landscape. The threat modeling chaining and attack simulation systems and methods described herein allow organizations to manage threats at a comprehensive organizational level notwithstanding an ever-changing threat landscape." *See* '008 Patent, col. 22, ll. 52-61.

27. The patented chaining feature disclosed and claimed in the '008 Patent enables more robust threat modeling for complex systems, including for example the complex ecosystem of medical devices. This chaining features is key to understanding how security risks become security issues, and how to apply countermeasures for counteracting security risks.

## ASSERTED CLAIMS OF THE '008 PATENT

28. The asserted claims of the '008 Patent include claims 1 and 3.

## OVERVIEW OF U.S. PATENT NO. 10,713,366

29. The '366 Patent is titled: "Systems and methods for automated threat model generation from third party diagram files." The '366 Patent discloses and claims innovative solutions for importing a third party data file, correlating the third party data file contents with

threat model components stored in a database, and generating a threat model and threat report based on the third party data file. The solutions developed, patented, and commercialized by ThreatModeler allow a user to apply threat modeling advantages to cloud-based environments with unique or proprietary file formats, or to introduce threat modeling processes earlier in the software development lifecycle.

30. The '366 Patent describes this innovation, including an interface for importing a third party software file into a threat model: "The IMPORT selector allows a user to use a preexisting data file from a third party software program to generate a threat model. By non-limiting example, in implementations a user may import a MICROSOFT VISIO file in VSD and/or VSDX format, a file in PDF format, an XML file, a GLIFFY file, TMT file, JSON file, PNG file, JPEG file, or a number of other file formats. In the representative example shown in FIG. 25, the system is configured only to import VSD and VSDX file formats. The VISIO file imported by the user would be a VISIO diagram file on which the user has previously diagrammed a system, application, or process and now wishes to generate a threat model using that same diagram." *See* '366 Patent, col. 36, ll. 48-61.

31. As explained in the '366 Patent, "Generating the threat model may include using the system to determine threats, threat sources, threat risk levels, threat statuses, security requirements, compensating controls, threat mitigations, and so forth—associated with the system/method or the like that was diagrammed in the third party software and imported to generate the threat model—and displaying these to the end user." *See* '366 Patent, col. 39, ll. 47-53.

32. The patented technology for importing third party architecture files into a threat model, as disclosed and claimed in the '366 Patent, enables ThreatModeler's solution to be integrated with a cloud-based environment and provides threat modeling services that are synchronized with the cloud environment and validate security configurations in that environment.

## ASSERTED CLAIMS OF THE '366 PATENT

33. The asserted claims of the '366 Patent include claims 1, 2, 4, 7, 8, 9, 11, 13, 16, 17, and 20.

## IRIUSRISK'S NOTICE OF ASSERTED PATENTS AND ACTIONS

34. IriusRisk has been placed on constructive notice of the Asserted Patents at least by ThreatModeler's marking of its covered products (including ThreatModeler®) in compliance with 35 U.S.C. § 287(a). *See* https://threatmodeler.com/intellectual-property, https://threatmodeler.com/patents.

35. Plaintiff ThreatModeler and Defendant IriusRisk are competitors in the limited field of providing threat modeling services and solutions, and often submit competiting proposals for providing threat modeling services solutions to potential customers and users. Plaintiff ThreatModeler's threat model platform (herein referred to as the "ThreatModeler Platform") has received numerous industry accolades, including those recounted in paragraphs 15-16 of this Complaint, and those awards are widely published in industry trade magazines and websites. On information and belief, Defendant IriusRisk monitors and is aware of these same industry trade magazines and websites, and is and has been aware of ThreatModeler's industry awards and accolades. On information and belief, as a direct competitor of ThreatModeler, Defendant IriusRisk also monitors and is aware of ThreatModeler's website, including the announcements of issued patents and new ThreatModeler Platform product announced there. *See, e.g.*, https://threatmodeler.com/threatmodeler-announces-new-patent-for-iac-assist (posted June 7, 2022), https://threatmodeler.com/threatmodeler-launches-iac-assist-and-cloudmodeler-to-reduce-threat-drift-from-code-to-cloud (posted Nov. 29, 2021). Further, following the issuance of ThreatModeler's U.S. Patents and the incorporation of its patented features into its ThreatModeler Platform, Defendant IriusRisk has added similar features to its own Accused Products. For example, ThreatModeler's U.S. Patent No. 11,314,872 directed to and entitled "Systems and Methods for Automated Threat Modeling When Deploying Infrastructure as a Code" ("IaC") issued on April 26, 2022. The issuance of this patent was reported on by industry

journalists, including by Global Security Mag on or about June 9, 2022. *See* https://www.globalsecuritymag.com/ThreatModeler-Announces-New-Patent,20220609,126371.html. Approximately two months after the issuance of ThreatModeler's IaC patent, on or about June 17, 2022, and after ThreatModeler and Global Security Mag publicized the issuance of ThreatModeler's IaC patent, Defendant IriusRisk added a new link to its Threat Modeling Platform dropdown menu on its company home page, labeled "Infrastructure as Code" and linked to a site labeled "Infrastructure as Code (IaC)." *See* https://www.iriusrisk.com/?hsLang=en (second menu item in Threat Modeling Platform dropdown menu); https://www.iriusrisk.com/iac-hub. In its IaC site, Defendant IriusRisk described features substantially similar to those disclosed in ThreatModeler's IaC patent, stating that "Infrastructure as Code (IaC) has significant benefits in alleviating challenges with cloud-based services and enables provisioning of infrastructure to be automated, repeatable and consistent. Your IaC already describes a significant part of your architecture which is a great way to start your threat modeling. IriusRisk can automatically generate a data flow diagram and even the entire threat model without logging in to the UI." *Id*. On information and belief, Defendant IriusRisk has been monitoring ThreatModeler's website and granted U.S. patents, including the Asserted Patents, and was aware of ThreatModeler's granted U.S. patents prior to the filing of this Complaint.

36. IriusRisk has actual notice of the Asserted Patents no later than the date of service of this Complaint.

37. In order for a user to use and benefit from IriusRisk's Accused Products, the user must agree to and comply with the terms and conditions of a license provided by IriusRisk, and must operate the Accused Products in the manner provided by IriusRisk. Each user using the Accused Products pursuant to license from IriusRisk, and in communication with one or more IriusRisk-controlled servers, benefits from IriusRisk's providing of the Accused Products, the manner of which usage is designed and controlled by IriusRisk and conditioned on compliance with the user's license.

**COUNT I –INFRINGEMENT OF U.S. PATENT NO. 10,699,008**

38. ThreatModeler incorporates herein by reference the allegations stated in paragraphs 1-37 of this Complaint.

39. On June 30, 2020, the United States Patent and Trademark Office duly and legally issued the ’008 Patent. ThreatModeler is the owner by assignment of all right, title and interest in and to the ’008 Patent, including the right to sue, enforce and recover damages for all past, present, and future infringements of the patent.

40. Defendant IriusRisk has directly infringed, either literally or through the doctrine of equivalents, at least claims 1 and 3 of the ‘008 Patent, by making, using, offering to sell, selling and/or importing products in the United States and in this judicial district, including but not limited to the Accused Products, thereby constituting infringement under 35 U.S.C. § 271(a). *See* Ex. C, Infringement Claim Chart for U.S. Patent No. 10,699,008 (Claims 1 and 3). Defendant IriusRisk’s direct infringement includes, without limitation, IriusRisk’s testing of the Accused Products, and recorded and live demonstrations of the Accused Products to its customers, potential customers, and users. Additionally, the asserted claims of the ’008 Patent are directly infringed by IriusRisk because all of the user-side steps of the asserted method claims are attributable to IriusRisk.

41. To the extent any fact finder concludes that Defendant IriusRisk’s Accused Products do not literally satisfy any element of at least claims 1 and 3 of the ‘008 Patent, those elements are met under the Doctrine of Equivalents.

42. Defendant actively, knowingly, and intentionally has induced infringement of the ’008 Patent under 35 U.S.C. § 271(b) and (c) through a range of activities.

43. IriusRisk has induced infringement by IriusRisk’s customers and users by controlling the design and development of, offering for sale, and selling the services of the Accused Products with the knowledge and specific intent to encourage its customers and users to use the Accused Products in their intended manner, which infringes the ’008 Patent. IriusRisk has also induced infringement of the ’008 Patent by disseminating promotional, marketing,

educational, demonstrative, and tutorial materials relating to the Accused Products with the knowledge and specific intent that its customers and users will use the Accused Products to perform threat modeling in an infringing manner. On information and belief, IriusRisk has engaged in the above activities with knowledge of the '008 Patent and with the specific intent to encourage and cause direct infringement by its customers and users. Further, IriusRisk continues to engage in the above activities with actual knowledge of the '008 Patent and with the specific intent to encourage and cause direct infringement by its customers and users.

44. With knowledge of the '008 Patent, Defendant's continuing infringement of claims 1 and 3 has been intentional and willful.

45. Defendant's acts of willful infringement have caused damage to ThreatModeler, and ThreatModeler is entitled to recover from Defendant the damages sustained as a result of Defendant's wrongful acts in an amount subject to proof at trial, but in any event not less than a reasonable royalty.

**COUNT II –INFRINGEMENT OF U.S. PATENT NO. 10,713,366**

46. ThreatModeler incorporates herein by reference the allegations stated in paragraphs 1-45 of this Complaint.

47. On July 14, 2020, the United States Patent and Trademark Office duly and legally issued the '366 Patent. ThreatModeler is the owner by assignment of all right, title and interest in and to the '366 Patent, including the right to sue, enforce and recover damages for all past, present, and future infringements of the patent.

48. Defendant IriusRisk has directly infringed, either literally or through the doctrine of equivalents, at least claims 1, 2, 4, 7, 8, 9, 11, 13, 16, 17, and 20 of the '366 Patent, by making, using, offering to sell, selling and/or importing products in the United States and in this judicial district, including but not limited to the Accused Products, thereby constituting infringement under 35 U.S.C. § 271(a). *See* Ex. D, Infringement Claim Chart for U.S. Patent No. 10,713,366 (Claims 1, 2, 4, 7, 8, 9, 11, 13, 16, 17, and 20). Defendant IriusRisk's direct infringement includes, without limitation, IriusRisk's testing of the Accused Products, and

recorded and live demonstrations of the Accused Products to its customers, potential customers, and users. Additionally, the asserted claims of the ’366 Patent are directly infringed by IriusRisk because all of the user-side steps of the asserted method claims and user-side use of the asserted system claims are attributable to IriusRisk.

49. To the extent any fact finder concludes that Defendant IriusRisk’s Accused Products do not literally satisfy any element of at least claims 1, 2, 4, 7, 8, 9, 11, 13, 16, 17, and 20 of the ‘366 Patent, those elements are met under the Doctrine of Equivalents.

50. Defendant actively, knowingly, and intentionally has induced infringement of the ’366 Patent under 35 U.S.C. § 271(b) and (c) through a range of activities.

51. IriusRisk has induced infringement by IriusRisk’s customers and users by controlling the design and development of, offering for sale, and selling the services of the Accused Products with the knowledge and specific intent to encourage its customers and users to use the Accused Products in their intended manner, which infringes the ’366 Patent. IriusRisk has also induced infringement of the ’366 Patent by disseminating promotional, marketing, educational, demonstrative, and tutorial materials relating to the Accused Products with the knowledge and specific intent that its customers and users will use the Accused Products to perform threat modeling in an infringing manner. On information and belief, IriusRisk has engaged in the above activities with knowledge of the ’366 Patent and with the specific intent to encourage and cause direct infringement by its customers and users. Further, IriusRisk continues to engage in the above activities with actual knowledge of the ’366 Patent and with the specific intent to encourage and cause direct infringement by its customers and users.

52. With knowledge of the ’366 Patent, Defendant’s continuing infringement of claims 1, 2, 4, 7, 8, 9, 11, 13, 16, 17, and 20 has been intentional and willful.

53. Defendant’s acts of willful infringement have caused damage to ThreatModeler, and ThreatModeler is entitled to recover from Defendant the damages sustained as a result of Defendant’s wrongful acts in an amount subject to proof at trial, but in any event not less than a reasonable royalty.

## PRAYER FOR RELIEF

WHEREFORE, ThreatModeler prays that it have judgment against Defendant for the following:

(1) Adjudging that Defendant has directly infringed and induced infringement of at least claims 1 and 3 of the '008 Patent, and claims 1, 2, 4, 7, 8, 9, 11, 13, 16, 17, and 20 of the '366 Patent under 35 U.S.C. §§ 271(a), either literally or under the Doctrine of Equivalents.

(2) Adjudging that Defendant's infringement of the '008 Patent and the '366 Patent has been willful.

(3) Awarding ThreatModeler damages for Defendant's infringement adequate to compensate ThreatModeler for the infringement, but in any event, not less than a reasonable royalty;

(4) Awarding treble damages pursuant to 35 U.S.C. § 284;

(5) Declaration this case exceptional and awarding attorneys' fees pursuant to 35 U.S.C. § 285, or as otherwise permitted by law, and such other and further relief, at law or in equity, to which ThreatModeler is justly entitled.

## DEMAND FOR JURY TRIAL

ThreatModeler hereby demands a jury trial on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

*Of Counsel:*

DAVIDSON BERQUIST JACKSON & GOWDEY, LLP

Wayne M. Helge
James T. Wilson
8300 Greensboro Drive, Suite 500
McLean, VA 22102
Tel: (571) 765-7700
whelge@dbjg.com

RATNERPRESTIA

*/s/ Jeffrey B. Bove*
Jeffrey B. Bove (# 998)
Rex A. Donnelly (# 3492)
Karen R. Poppel (# 5373)
Nemours Building
1007 North Orange Street, Suite 205
Wilmington, DE 19801

jwilson@dbjg.com

Tel: (302) 778-2500
jbove@ratnerprestia.com
rdonnelly@ratnerprestia.com
kpoppel@ratnerprestia.com

*Attorneys for Plaintiff*
*ThreatModeler Software Inc.*

DATED: July 8, 2022

5759695