UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

BITSIGHT TECHNOLOGIES, INC., Plaintiff, v. NORMSHIELD INC. d/b/a BLACK KITE INC., Defendant.	Civil Action No. JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT, FALSE ADVERTISING, AND DECEPTIVE TRADE PRACTICES

Plaintiff BitSight Technologies, Inc. ("Plaintiff" or "BitSight") brings this action for patent infringement, violations of the Lanham Act including false advertising, and deceptive trade practices in violation of Massachusetts General Laws ("Mass. Gen. Laws") ch. 93A and ch. 266 against Defendant NormShield Inc. d/b/a Black Kite Inc. ("Defendant" or "Black Kite") as follows:

NATURE OF THIS ACTION

1. This is an action for infringement of U.S. Patent Nos. 9,438,615 (the "'615 patent"); 9,680,858 (the "'858 patent"); 9,973,524 (the "'524 patent"); 10,805,331 (the "'331 patent"); and 11,652,834 (the "'834 patent"); (collectively, the "Asserted Patents") arising under the patent laws of the United States, Title 35, United States Code, including 35 U.S.C. § 271; false advertising arising under the Trademark Act of 1946, 15 U.S.C. § 1051 *et seq.* (the "Lanham Act"); and violations of Mass. Gen. Laws ch. 93A and ch. 266.

2. BitSight is a pioneering innovator in the cyber risk management solutions industry. Founded in 2011, BitSight invented the security ratings industry by developing a universal system

and metric to interpret cyber risk, which allows BitSight to offer quicker, more affordable, and more practical answers to customers' cyber risk management needs. BitSight has transformed how companies manage exposure, performance, and risk for themselves and all entities in their digital ecosystems, as enterprises of all sizes and industries rely on BitSight to expand distributed ecosystems without fear of expanded attack surfaces. In particular, BitSight leverages its groundbreaking technology to help its customers accelerate digital transformation and add vendors and partners confidently without increasing cyber security risk.

3. Specifically, BitSight developed a system for determining a composite security rating of an organization based on security data collected from external sources on the internet, without access to that organization's internal documents and systems, that reasonably approximates an internal audit score of cybersecurity preparedness.

4. BitSight has secured patent protection for its foundational technology starting with the filing of the applications that led to the '331 patent in 2010 and 2011. In recognition of BitSight's inventions, the United States Patent and Trademark Office ("USPTO") has granted the company fifty patents, including the Asserted Patents.

5. In 2016—five years after BitSight's incorporation—Black Kite was founded as NormShield. Black Kite competes in the market for cyber risk management solutions. Since its inception, Black Kite has lagged behind BitSight—with its technology, its customer base, and the overall quality of its offerings. Instead of developing its own technology, Black Kite took a shortcut—its cyber risk management platform utilizes BitSight's foundational patented technology, including the Asserted Patents, without authorization.

6. Black Kite has not been content just to infringe BitSight's patents. Instead, Black Kite also has made and continues to make false and misleading statements in commerce about

BitSight and its offerings.

7. BitSight brings this action to protect its intellectual property, to stop Black Kite's unauthorized use of BitSight's patents, and to stop Black Kite's false and misleading statements regarding BitSight.

THE PARTIES

8. BitSight is a Delaware Corporation with its principal place of business at 111 Huntington Ave, Floor 4, Boston, MA 02199.

9. Black Kite is a Delaware Corporation with its principal place of business at 800 Boylston St, Suite 2905, Boston, Massachusetts 02199.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over BitSight's federal claims pursuant to 28 U.S.C. § 1331 and to 28 U.S.C. § 1338(a). This Court has supplemental jurisdiction over BitSight's state law claims pursuant to 28 U.S.C. § 1367(a).

11. This Court has personal jurisdiction over Black Kite at least because its principal place of business is in Massachusetts, it is a resident of and/or has regularly conducted business activities in this District, and it has committed acts of infringement, false advertising, and deceptive trade practices in this District.

12. Venue is proper in this judicial District for all claims under 28 U.S.C. §§ 1391(b)-(d) and 1400(b) because Black Kite is a corporate defendant that resides in this District.

BACKGROUND

A. BitSight's Revolutionary Business

13. Historically, companies wanting to reduce the cyber security risk of doing business with a third party, such as a vendor or partner, would perform or commission a cyber security

assessment of the third party to determine whether that third party maintained good security practices.

14. Generally, these assessments were slow, expensive, and impractical given the high volume of information and security systems that needed to be characterized. Perhaps most importantly, the assessments were also applied haphazardly, and failed to consistently predict the actual performance of a company's security program.

15. BitSight developed its revolutionary technology to help bridge this gap. Specifically, BitSight developed a system for determining a composite security rating—a universal metric to interpret cyber risk—derived by amassing security data collected externally from third-party computer systems online, resulting in a proprietary data set of security related events, assets, and effects.

16. BitSight derives security data from externally observable characteristics of a third-party computer system, meaning that BitSight can assess an entity's security risk without access to the third-party's internal documents and systems. BitSight's composite security ratings reasonably approximate an internal audit score of cybersecurity preparedness.

17. The BitSight platform can also optionally process additional, user-provided information concerning the relevant entity and its IP assets.

18. Similar to a credit score, BitSight Security Ratings range in value from 250 to 900, with higher Ratings representing better cybersecurity risk profiles (e.g., a lower risk), although currently the space below 300 and above 820 is reserved for future use.

19. BitSight's breakthrough approach to acquiring external data allows it to quickly and accurately identify security risks.

20. This data set and BitSight's associated analytics capabilities provide organizations with unique visibility into potential cyber risks, leading to better, smarter risk decisions. Specifically, BitSight has collected over 44 trillion raw events, continues to collect over 400 billion events daily, and collects data on 40 million organizations worldwide. Currently, every BitSight rating is based upon over 12 months of historical data where such data exists.

21. BitSight's data and analytics platform has been independently verified by AIR Worldwide and IHS Markit, confirming that BitSight's data analytics correlate with a security program's risk of adverse incidents. BitSight's innovative platform enables cybersecurity managers to better prioritize mitigation decisions with visibility into where the greatest risks lie. In addition, according to a Marsh McLennan Cyber Risk Analytics Center study, cybersecurity performance as measured by BitSight is statistically significant and correlated with the likelihood of cybersecurity incidents. The study concluded that poor performance in certain areas, including the BitSight Security Rating and BitSight's 13 risk vectors, reflects an increase in an organization's risk of experiencing a cybersecurity incident, while strong performance implies a lower risk of incident.

22. BitSight utilizes its groundbreaking technology and data models in several product offerings. For example, BitSight incorporates its technology into its Third-Party Risk Management ("TPRM") solutions, which include, among other features, continuous monitoring of third-party security controls to align with a company's risk tolerance and organizational objectives. BitSight also incorporates its technology into its BitSight's Security Performance Management ("SPM") solution that builds on BitSight's original, core offering by leveraging both externally collected data as well as a company's internal data to assess risk.

23. As a result of its leading technology, varied offerings, and nuanced approach, BitSight has successfully helped customers of varying sophistication and maturity improve their cyber security programs and more effectively protect against malware, ransomware, and other types of cyber attacks. BitSight now services 38% of Fortune 500 companies as part of its over 3,000 global customers. Over 50% of the world's cyber insurance premiums are underwritten by BitSight customers.

24. To protect its pioneering and innovative technology, BitSight has developed a robust portfolio of over fifty issued U.S. patents.

B. The Asserted Patents

25. BitSight's methods and systems underlying its approach to locating, collecting, analyzing, and communicating cyber risk management data are protected by numerous issued U.S. patents, including the Asserted Patents: U.S. Patent Nos. 9,438,615 (the "'615 Patent"); 9,680,858 (the "'858 patent"), 9,973,524 (the "'524 patent"); 10,805,331 (the "'331 Patent"); and 11,652,834 (the "'834 Patent").

1. The '331 and '524 Patents

26. The '331 patent was duly and legally issued on October 13, 2020 by the USPTO. U.S. Application No. 13/240,572, which issued as the '331 patent, was filed September 22, 2011. Stephen Wayne Boyer, Nagarjuna Venna, and Megumi Ando are the named inventors of the '331 patent. A true and correct copy of the '331 patent is attached as Exhibit 1.

27. The '524 patent was duly and legally issued on May 15, 2018 by the USPTO. U.S. Application No. 14/944,484, which issued as the '524 patent, was filed November 18, 2015 as a continuation of Application No. 13/240,572, which issued as the '331 patent. Stephen Boyer, Nagarjuna Venna, and Megumi Ando are the named inventors of the '524 patent. A true and

correct copy of the ’524 patent is attached as Exhibit 2.

28. BitSight is the owner and assignee of the ’331 and ’524 patents, and holds the sole and exclusive right to sue and recover damages for infringement thereof, including past infringement.

29. The claims of the ’331 and ’524 patents are valid and enforceable.

30. The ’331 and ’524 patents generally relate to “systems for determining the security of information systems and, in particular, for evaluating the security of third-party computer systems.” Ex. 1 (’331 patent), 1:23-25; Ex. 2 (’524 patent), 1:26-28.

31. Prior to the invention of the ’331 and ’524 patents, “[w]hen a company want[ed] to reduce its cyber security risk of doing business with another company’s computer systems, it [had to] either perform[], or hire[] an outside firm to perform, a cyber security risk assessment of the other company to determine if it is following good security practices.” Ex. 1 (’331 patent), 1:26-30; Ex. 2 (’524 patent), 1:29-33. However, such audits were “slow, expensive and impractical given the high volume of service provider security systems that need to be characterized by the company.” Ex. 1 (’331 patent), 1:38-40; Ex. 2 (’524 patent), 1:41-43. In addition, the “audits [were] not entirely predictive of the performance of the security systems.” Ex. 1 (’331 patent), 1:40-42; Ex. 2 (’524 patent), 1:43-45. Because of these shortcomings, there was a need in the art to develop a method and system to assess third-party security risk efficiently and accurately.

32. To address this need, the shared specification of ’331 and ’524 patent discloses a method and system “for creating a composite security rating from security characterization data of a third party computer system” that is “derived from externally observable characteristics of the third party computer system.” Ex. 1 (’331 patent), 1:46-56; Ex. 2 (’524 patent), 1:49-59. Specifically, the specification discloses that “[a] diverse set of network sensors and services around

the Internet collect and observe information about the third party entity computer systems. The system **10** then gathers, processes, and stores the data collected about entities from the sensors and service providers using custom developed data source specification collection processors." Ex. 1 ('331 patent), 7:27-34; Ex. 2 ('524 patent), 7:30-38. "Unlike internal audit systems, the system **10** is not relying upon a correlation between practices and outcomes. Instead, evidence of actual security outcomes is collected through the data sources partners." Ex. 1 ('331 patent), 7:3-6; Ex. 2 ('524 patent), 7:6-9.

33. The specification discloses numerous advantages of its improved method of assessing third-party security risk using externally collected data from the internet. For example, the specification discloses that "[a]dvantageously, the composite security rating has a relatively high likelihood of corresponding to an internal audit score despite use of externally observable security characteristics." Ex. 1 ('331 patent), 1:50-53; Ex. 2 ('524 patent), 1:53-56. Further, "[i]n some cases the system **10** revealed problems with the entities not revealed by internal evaluations." Ex 1 ('331 patent), 7:9-10, Ex. 2 ('524 patent), 7:12-13. Other advantages include that "[t]he system **10** can be entirely, or to a large extent, automated and need not have the permission of the entity being rated" and yields reports that "will allow risk management professionals to monitor, assess and mitigate partner risk by up-to-date ratings due to its persistent monitoring of the third party computer systems." Ex. 1 ('331 patent), 6:59-67; Ex. 2 ('524 patent), 6:62-7:3.

34. Like the specification, the claims of the '331 and '524 patents recite particular improvements in assessing third-party security risk using only external data. For example, claim 1 of the '331 patent recites "collecting information about two or more organizations" "from two or more sources," "at least some of [which is] collected automatically by computer using sensors on the Internet" including "information not controlled by the organization [that is] collected

without permission of the organization" and that is "indicative of compromises, vulnerabilities or configurations of technology systems of the organizations[,] indicative of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations . . . [and] indicative of durations of events associated with compromises or vulnerabilities or configurations." The claim goes on to recite "processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization." *See, e.g.*, Ex. 1 ('331 patent), cl. 1.

35. As another example, claim 29 of the '331 patent recites "collecting information about an organization that has computer systems, network resources, and employees, the organization posing risks to itself or to other parties through business relationships of the organization with the other parties" which includes "(a) information collected automatically by computer on the Internet without permission of the organization, and (b) information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability, the resiliencies being inversely proportional to the duration of detected malicious activity." The claim goes on to recite "processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk based on a business relationship with the organization, the composite rating comprising a measure of the resiliencies of the organization to recover from a security breach, and in connection with assessing the degree of risk, delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies." *See* Ex. 1 ('331 patent), cl. 29.

36. Similarly, the '524 patent claims recite "automatically [using] sensors on the Internet to collect externally observable cyber-security characterizations of the technical assets that maps technical assets to respective companies or other entities with which the assets are associated," "automatically deriving observations about the technical assets from the collected cyber-security characterizations, wherein the derived observations comprise (i) a number of technical assets that have been reported to be malicious and (ii) a duration of detected malicious activity associated with the technical assets," and "automatically generating a cyber-security rating for each of the entities using the entity map and the derived observations." *See, e.g.*, Ex. 2 ('524 patent), cl. 1.

37. The '331 and '524 patents do not simply claim automation of the manual process of performing a cyber security risk assessment. Instead, the '331 and '524 patents claim significant and specific technological improvements over the prior art by identifying, collecting, assessing, and applying models to external data collected automatically on the internet to arrive at a composite rating that captures a third-party organization's security risk. The claimed inventions of the '331 and '524 patents enable a computer to automatically perform a task that computers did not perform prior to BitSight's claimed inventions.

38. Therefore, a person of ordinary skill in the art would recognize that the inventions claimed in the '331 and '524 patents are not directed to abstract ideas.

39. During prosecution of the application leading to the '331 patent, the patent applicant overcame a rejection under 35 U.S.C. § 101.

40. In a Non-Final Rejection, dated June 3, 2015, the Examiner rejected pending claims, including then-pending independent claims 1 and 136 pursuant to 35 U.S.C. § 101. The Examiner took the position that the independent claims were "directed towards the abstract idea

gathering information regarding an entity and computing a rating score given the information gathered" and that while "[t]he claims also recite the additional element including computer systems interacting with the internet to gather information about an organization and processing the information to form a rating. . . . these additional elements are not sufficient to amount to significantly more than the judicial exception because the limitations are merely data gathering and instructions to implement the abstract idea on a computer which require no more than a generic computer to perform generic computer functions that are well-understood, routine and conventional activities previously known to the industry." The Examiner also wrote that "the claims do not recite an improvement to another technology or technical field, an improvement to the functioning of a computer itself, or meaningful limitations beyond generally linking the use of an abstract idea to a particular technological environment."

41. In a response dated September 2, 2015, the patent applicant explained that "[i]t is true that claim 1, for example, recites the collection of certain information 'automatically by computer using sensors on the Internet,' yet the examiner appears to have disregarded the substantial other features of the claim that amount to 'significantly more' than the identified abstract idea." The applicant further explained that "[t]he features of the claims do recite an improvement to one or more technologies or technical fields, for example, the technology of deriving information about an organization from sources that include the Internet, without permission of the organization, and then using the information for determining how to interact with the organization" and that "[t]his is a challenging technology and a wide range of applications have been proposed and used."

42. In an Office Action dated October 26, 2015, the Examiner withdrew the rejection of the pending claims of the '331 patent under § 101, stating "Applicant's arguments/amendments

filed 9/2/2015 in regards to 35 U.S.C. 101 . . . have been considered and are persuasive therefore the previously filed 35 U.S.C. 101 . . . rejections have been withdrawn."

43. The Examiner made no further rejections to the '331 patent based on § 101.

44. During prosecution of the application leading to the '524 patent, the patent applicant also overcame a rejection under 35 U.S.C. § 101.

45. In a Non-Final Rejection, dated March 11, 2016, the Examiner rejected then-pending independent claims 1-18 pursuant to 35 U.S.C. § 101. The Examiner took the position that independent claim 1 was "directed to collecting characterization of entities and generating a score based on the collected data" and does not "including additional elements that are sufficient to amount to significantly more than the judicial exception because they are 'and idea of itself.'" The Examiner also wrote that while "additional language teaches mapping technical assets, collecting eternally [sic] observable characterization and generated a security score based on the security characterizations," "these additional elements are not sufficient to amount to significantly more than the judicial exception because the limitations are merely instructions to implement the abstract idea on a computer and require no more than a generic computer to perform generic computer functions that are well-understood, routine and conventional activities previously known to the industry." The Examiner also wrote that "the claims do not recite an improvement to another technology or technical field, an improvement to the functioning of a computer itself, or meaningful limitations beyond generally linking the use of an abstract idea to a particular technological environment."

46. In a response dated October 5, 2016, the patent applicant explained that "the claims, as amended, provide a specific technique for generating and maintaining an entity map that allows for more efficient observations of network activity attributed to entities within the map." The

applicant further explained that "claim 1 does not merely recite a known method along with the requirement to perform the steps of the method on a computer. Rather, claim 1 recites a method for maintaining an entity map that is not well-understood, routine, or conventional."

47. In response, in a Non-Final Rejection dated January 17, 2017, the Examiner withdrew the rejection of the pending claims of the '331 patent under § 101, stating "Applicant's arguments/amendments directed towards the 35 U.S.C. § 101 rejection are persuasive therefore the rejection has been withdrawn."

48. The Examiner made no further rejections to the '524 patent based on § 101.

2. The '615 and '834 Patents

49. The '615 patent was duly and legally issued on September 6, 2016 by the USPTO. U.S. Application No. 14/021,585, which issued as the '615 patent, was filed September 9, 2013. Philip John Steuart Gladstone, Alan Joseph Kirby, John Matthew Truelove, David Feinzeig, Nagarjuna Venna, and Stephen Boyer are the named inventors of the '615 patent. A true and correct copy of the '615 patent is attached as Exhibit 3.

50. The '834 patent was duly and legally issued on May 16, 2023 by the USPTO. U.S. Application No. 17/025,930, which issued as the '834 patent, was filed September 18, 2020. Philip John Steuart Gladstone, Alan Joseph Kirby, John Matthew Truelove, David Feinzeig, Nagarjuna Venna, and Stephen Boyer are the named inventors of the '834 patent. A true and correct copy of the '834 patent is attached as Exhibit 4.

51. The '834 patent is a continuation of Application No. 16/405,121, filed May 7, 2019, which is a continuation of Application No. 15/216,955, filed on July 22, 2016, which is a continuation of Application No. 14/021,585, filed September 9, 2013, now the '615 patent.

52. BitSight is the owner and assignee of the '615 and '834 patents, and holds the sole

and exclusive right to sue and recover damages for infringement thereof, including past infringement.

53. The claims of the ’615 and ’834 patents are valid and enforceable.

54. Prior to the invention of the ’615 and ’834 patents, it was difficult to accurately capture a third party’s security risk relying solely on publicly available information. One reason for this challenge is that a single entity can be associated with many different domain names, servers, and IP addresses, such that it often may not be clear, absent time-consuming investigation, which organization owns the assets. As a result, it was difficult and time-consuming, and often impossible, to identify all (or even sample subsets of) assets—e.g., domain names, servers, and IP addresses—associated with an entity in order to assess the entity’s cyber security risks. Because each asset has the potential to pose an individual security risk, failing to account for a material portion of them could lead to an incomplete and/or inaccurate assessment of an entity’s security risk. *See* Ex. 3 (’615 patent), 2:57-3:40; Ex. 4 (’834 patent), 3:8-58.

55. In addition, attempts to capture a third party’s security risk often did not incorporate information individual users possessed that was relevant to the entities and their assets and that, if leveraged, could have improved the results of the identification effort. *See* Ex. 3 (’615 patent), 2:57-3:40; Ex. 4 (’834 patent), 3:8-58.

56. The specification and claims of the ’615 and ’834 patents describe particular improvements to the prior art method of identifying and “mapping” technical and non-technical assets to an entity.

57. For example, claim 84 of the ’615 patent describes a more efficient and improved method for identifying and mapping an entity’s assets that accounts for both publicly available information as well as a user’s non-technical information, including:

a. "generating a map between (a) technical assets that contribute to security characteristics of respective entities and (b) the identities of the entities that are associated with the respective technical assets, at least part of the generating of the map being done automatically";

b. "generating graphs of relationships among entities based on their associations with technical assets;" and

c. "enabling a user to assist in the generating of the map by presenting to the user through a user interface (a) data about the technical assets of entities and (b) an interactive tool for associating the technical assets with the identities of the entities."

Ex. 3 ('615 patent), cl. 84.

58. Similarly, claim 1 of the '834 patent describes an improved and specifically ordered method "for mapping Internet Protocol (IP) addresses to an entity" that includes:

a. "receiving a first domain name for the entity;"

b. "sending, to a domain name system (DNS) server, a first passive DNS query to identify first name servers for the first domain name;"

c. "receiving, from the DNS server, a list of the first name servers for the first domain name;"

d. "sending, for each of the first name servers, a second passive DNS query to identify second domain names for which the first name server is authoritative;"

e. "receiving, for each of the first name servers, a list of the second domain names for which the first name server is authoritative;"

f. "sending, for each of the second domain names, a third passive DNS query to identify host names for the hosts of the second domain name and IP addresses for the host names;"

g. "receiving a list of the host names and the IP addresses for the host names;" and

h. "mapping each IP address to an attribute for the entity."

Ex. 4 ('834 patent), cl. 1.

59. The specification of the '615 and '834 patents discloses "the following advantages" of its improved methods: "By understanding the nature and degree of security risks associated with other entities, an entity can evaluate, analyze, and reduce its own risk . . . . [and] analysis of traces of online activities of users may represent security policies or vulnerabilities of the entities that employ the users"; "analysis of traces of online activities may identify information associated with multiple entities more quickly, more accurately, and more privately than gathering data directly from the multiple entities"; "technical data may be retrieved and mapped to an entity in a manner not previously available"; and "the security risks of an entity may be analyzed or determined without involvement of the entity." Ex. 3 ('615 patent), 2:57-3:8; Ex. 4 ('834 patent), 3:8-26.

60. The '615 and '834 patents therefore do not simply claim automation of the manual process of associating internet assets with an entity. Instead, the '615 and '834 patents claim significant and specific technological improvements over the prior art including detailed, ordered methods for associating technical assets with an entity. The claimed inventions of the '615 and '834 patents enable a computer to automatically perform a task that computers did not perform prior to BitSight's claimed inventions.

61. Therefore, a person of ordinary skill in the art would recognize that the inventions claimed in the '615 and '834 patent are not directed to abstract ideas.

3. The '858 Patent

62. The '858 patent was duly and legally issued on June 13, 2017 by the USPTO. U.S. Application No. 15/134,845, which issued as the '858 patent, was filed April 21, 2016. Stephen

Boyer, Nagarjuna Venna, Philip John Steuart Gladstone, and Nicholas Whalen are the named inventors of the '858 patent. A true and correct copy of the '858 patent is attached as Exhibit 5.

63. The '858 patent is a continuation-in-part of Application No. 14/021,585, filed Sep. 9, 2013.

64. BitSight is the owner and assignee of the '858 patent, and holds the sole and exclusive right to sue and recover damages for infringement thereof, including past infringement.

65. The claims of the '858 patent are valid and enforceable.

66. Prior to the invention of the '858 patent, there was a need for an effective and efficient way of receiving and managing user annotations to create a full cyber security profile for an entity.

67. To address this need, the '858 patent specification discloses an improved process for collecting and presenting information concerning the security risks posed by entities. Specifically, the '858 patent specification describes "an annotation facility operated by computer [that] enables users to add, alter, or remove annotations indicative of security risks associated with respective security subjects or entities to which the security subjects belong." Ex. 5 ('858 patent), 2:19-22. "The annotations describe characteristics of the security subjects. The characteristics include at least one of a type, a location, a time period, a relationship with other security subjects, a relationship with an entity, or a combination of any two or more of them. The annotations include groupings of security subjects. The groupings include subnets." *Id.*, 2:42-49. "The managing [of] the annotations includes storing the annotations in a database in association with the security subjects or the entities or both." *Id.*, 1:64-67. To ensure reliability, users' permissions to annotate are managed based on their relationships with the target entities. *See id.*, 1:53-58.

68. Advantageously, "[t]he annotations platform can provide automated or human (or both) curation, screening, editing, and monitoring features to improve the quality, completeness, and utility of proposed annotations or actual annotations, and to filter out junk." *Id*., 4:30-34.

69. The claims of the '858 patent recite an improved cyber security risk evaluation method incorporating management of user annotations. For example, claim 1 of the '858 patent recites a computer-implemented method comprising:

a. "by a computer, acquiring and storing information indicative of security risks associated with security subjects and with entities to which the security subjects belong,"

b. "by the computer, analyzing the stored information to derive security indicators for the entities,"

c. "by the computer, presenting security information including the security indicators for the entities and security information for the security subjects, the security information for the security subjects including human-supplied annotations entered via an input device by an individual with specialized knowledge of the security subjects, and"

d. "by the computer, managing the annotations based on communications from a user, wherein the annotations comprise tags based at least in part on the individual's specialized knowledge of the security subjects wherein managing the annotations comprises curating, screening, editing, or monitoring the annotations and managing permissions to view or create annotations."

Ex. 5 ('858 patent), cl. 1.

70. The '858 patent claims a significant and specific technological improvement over the prior art by creating a framework for a cyber security program to receive and display user-input annotations, which is necessary to create a full cyber security profile for an entity.

71. Therefore, a person of ordinary skill in the art would recognize that the inventions claimed in the '858 patent are not directed to an abstract idea.

72. During prosecution, the '858 patent overcame an initial rejection under 35 U.S.C. § 101.

73. In a Non-Final Rejection, dated July 19, 2016, the Examiner rejected then-pending claims 1-30 pursuant to 35 U.S.C. § 101. The Examiner took the position that the claims were "directed to the abstract idea of vulnerability assessment" and "does/do not include additional elements that are sufficient to amount to significantly more than the judicial exception because the additional element(s) or combination of elements in the claim(s) other than the abstract idea per se amount(s) to no more than: mere instructions to implement the idea on a computer, and recitation of generic computer structure that serves to perform generic computer functions that are well-understood, routine, and conventional activities previously known to the pertinent industry." The Examiner further stated "these additional claim element(s) do not provide meaningful limitation(s) to transform the abstract idea into a patent eligible application of the abstract idea such that the claim(s) amounts to significantly more than the abstract idea itself.

74. In a Final Rejection dated January 26, 2017, the Examiner again rejected pending claims pursuant to 35 U.S.C. § 101 and wrote: "the Examiner upholds that the claimed invention is directed to an abstract idea and does not possess 'significantly more' that would render the claims statutory. The claim amendments do not root the claimed invention within computer technology due to the input being provided 'manually' and 'based at least in part on the user's knowledge of the security subjects' would constitute implementation via mental process(es) and manual actions of users. None of the limitations, considered as an ordered combination, provide eligibility, because the claims simply instruct the practitioner to implement the abstract idea with

routine, conventional activity. The mere recitation of the elements identified by the Examiner to be generic computer components (e.g., 'computer') does not add any meaningful limitation beyond generally linking the abstract method to a general purpose computer and that '[s]imply appending conventional steps, specified at a high level of generality, was not "enough" [in Mayo] to supply an "inventive concept."'" (cleaned up).

75. In a response dated March 23, 2017, the patent applicant amended the proposed claims, including independent claim 1, and explained: "Applicant's claimed technique seeks to provide solutions to industry problems in a technical manner. For instance, functionality to receive and manage annotations is necessary to create a full cyber-security profile for an entity. At a technical level, Applicant's claims recite a method and system that address this problem by creating the framework for a cyber-security program to receive and display user-input annotations."

76. In an April 27, 2017 Notice of Allowance, the Examiner stated that "[t]he amendments to the claims give cause for the previous 35 U.S.C. 101 rejection to be hereby withdrawn."

77. The Examiner made no further rejections based on § 101.

C. Black Kite's Patent Infringement

78. Black Kite purports to offer a platform that can provide to its customers a risk score that reflects a "true understanding of their cyber ecosystem risk" (the "Black Kite Platform"). *See* Exhibit 11, Black Kite, *About Black Kite*, https://blackkite.com/about/.

79. Black Kite claims that the Black Kite Platform makes it simple for businesses to quantify and monitor cyber risk across thousands of third parties, such as a company's vendors, in a non-invasive manner. *See* Exhibit 12, Black Kite, *Third Party Risk Intelligence*,

https://blackkite.com/platform/.

80. Black Kite states that it aims to calculate the likelihood and potential financial impact to a client company if one of its third-party vendors, partners, or suppliers were to experience a breach. *See id.*

81. Like BitSight, Black Kite states that it relies on publicly accessible, external data for its assessments. *See id.*

82. Black Kite states that it relies on "information from VirusTotal, Passive DNS servers, web search engines, and other Internet-wide scanners, as well as Black Kite's proprietary databases." *See id.*

83. Black Kite further states that "Black Kite's Risk Assessment gathers data from all these sources and performs contextualization and analysis to convert data into risk intelligence." *See id.*

84. Like BitSight, Black Kite notes that "[t]o generate the cyber risk rating, [it] only needs the company domain" because it "searches the databases to find all IP address ranges and domain names that belong to the company." *See id.*

85. Like BitSight, Black Kite provides a means for its users to engage with its platform and provide information relevant to the assessment through use of an alleged universal questionnaire. *See id.* Also like BitSight, Black Kite then communicates its findings by arriving at a score, which it calls a "Cyber Risk Score," which is a "letter-grade." *See id.*

86. On information and belief, the Black Kite Platform operates and is used in a manner that infringes the system and methods covered by the Asserted Patents. This infringement is detailed in the claim charts attached as Exhibits 6-10.

87. Through the making, using, selling, and/or offering for sale of the Black Kite Platform within the United States, Black Kite has directly infringed and continues to directly infringe, either literally or under the doctrine of equivalents, the Asserted Patents.

88. Black Kite has been on notice of its infringement of each of the Asserted Patents since at least as early as the filing of this Complaint.

89. Black Kite has known of its infringement of the Asserted Patents at least as early as April 27, 2020 when it cited the '524 patent to the USPTO during the prosecution of the application which led to Black Kite's U.S. Patent No. 10,949,543.

D. Black Kite's False Advertising

90. Black Kite has made false and misleading statements in commerce about BitSight and about Black Kite's own capabilities. These statements have been made publicly, for example on Black Kite's website, including in its "Black Kite Competitive Comparison," where Black Kite details "Black Kite vs. The Competition" and purports to compare its offerings to those of its competitors, including BitSight. *See* Exhibit 13, Black Kite, *Intel Beyond a Scorecard*, https://blackkite.com/competitors/ (hereinafter the "Black Kite Comparison").

91. On information and belief, Black Kite and its employees have also made false and misleading statements directly to BitSight's actual and potential customers.

92. Black Kite has stated in commerce that Black Kite has 290 controls and that BitSight has 40 controls. *See id*.

93. This statement is false, or at minimum deceptively misleading. Black Kite has artificially inflated the number of its "controls." Black Kite has included in its purported count of controls data that does not qualify "controls," as that term is understood by the industry and defined by the National Institute of Standards and Technology's ("NIST"), which defines a "control" as

"[a] safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements." Black Kite has included as "controls" items such as "domain names registered," "assets registered and used by the organization," and "external library vulnerabilities," *inter alia*. *See, e.g.*, Exhibit 14, Black Kite, *How Does Black Kite Calculate Cybersecurity Ratings?* (Mar. 9, 2023), https://blackkite.com/blog/cybersecurity-ratings/. None of the above are "controls."

94. Black Kite has stated in commerce that Black Kite has extensive integrations with RSA Archer, Splunk, OneTrust, and ServiceNow while BitSight only has "partial" integrations. *See* Exhibit 13 (Black Kite Comparison).

95. This statement is false, or at a minimum deceptively misleading. BitSight has a number of extensive, pre-built integrations, including with ServiceNow VRM, ServiceNow ITSM, Archer, ProcessUnity, Splunk, PowerBI and more. BitSight publicizes these integrations at https://www.BitSight.com/tprm-integrations (Exhibit 15).

96. Black Kite has stated in commerce that Black Kite offers extensive digital footprint discovery while BitSight only offers "partial" digital footprint recovery. *See* Exhibit 13 (Black Kite Comparison).

97. This statement is false, or at a minimum deceptively misleading. BitSight has continuously used both automated and human-curated processes in its digital footprint capability since the company was founded in 2011. Not only is this statement false, it is egregiously so. On information and belief, BitSight is the only vendor that has labeled asset data for hundreds of thousands of companies to use in innovative AI and machine learning models, which contributes to its industry-leading digital footprint discovery—far beyond anything that Black Kite offers.

98. Black Kite has stated in commerce that BitSight's grading methodology is "Proprietary and Non-Standard" while Black Kite's grading methodology is "Standards-based." *See id.*

99. This statement is false, or at a minimum deceptively misleading. First, BitSight bases its rating on likelihood of Security Incident, which it discloses transparently and is available for its customers to review at any time. Moreover, the implication of Black Kite's statement that BitSight's methodology is "non-standard" suggests that BitSight's approach is of poor, or at best of unverifiable quality. BitSight's approach has been independently verified five different times by external companies assessing data showing correlation to real business. For its part, Black Kite has, on information and belief, never publicly discussed even a single independent verification of its approach and ratings.

100. Black Kite has stated in commerce that it takes "days" to add a new vendor using BitSight but with Black Kite this can be done "instant[ly]." *See id.*

101. This statement is false, or at a minimum deceptively misleading. Black Kite misrepresents its own offering as well as BitSight's. Black Kite's license model is inflexible; adding a new vendor requires manually requesting this with a customer service agent. Meanwhile, BitSight allows its customers to do this via self-service, which is easier and quicker. Moreover, even Black Kite acknowledges, in a fine print disclaimer hidden well below its false statement, that when using BitSight's offering, adding a new vendor can be done in an "[i]nstant if pre-evaluated." Black Kite's failure to prominently disclaim this distorts its statement, implying yet another falsehood.

102. Black Kite has stated in commerce that Black Kite has a ransomware likelihood indicator but BitSight does not. *See id.*

103. This statement is false, or at a minimum deceptively misleading. Black Kite states that BitSight does not offer "Ransomware Susceptibility Index®." This is the name of Black Kite's branded ransomware likelihood indicator. BitSight does not offer the "Ransomware Susceptibility Index®," but it does offer a ransomware likelihood indicator. Black Kite's statement misleadingly suggests BitSight does not.

104. Black Kite has stated in commerce that Black Kite has custom questionnaire mapping but BitSight does not. *See id.*

105. This statement is false, or at a minimum deceptively misleading. Not only does BitSight map its findings to any set of questions and control sets, but it is also one of the core tenets of BitSight's Security Performance Management offering.

106. Black Kite has stated in commerce that Black Kite's offerings can have questionnaires and other security attestations added but BitSight's cannot. *See id.*

107. This statement is false, or at a minimum deceptively misleading.

108. The above statements are exemplary of the false and deceptively misleading statements that Black Kite is making and has made in commerce.

109. Each of the above Black Kite false and misleading statements actually deceives or has the tendency to deceive a substantial segment of Black Kite's audience, which consists of BitSight's actual and potential customers.

110. Each of the above Black Kite false and misleading statements is material in that it is likely to influence consumers' purchasing decisions.

111. The false and misleading statements concern key aspects of both BitSight's and Black Kite's respective offerings that speak to the quality and value of each's offerings. To this point, Black Kite uses these statements as an introduction and support for the following statement,

available at https://blackkite.com/competitors/ (Exhibit 13), wherein Black Kite claims to offer a superior product to BitSight and other competitors: "Although each Black Kite competitor has a different approach, Black Kite prides itself on having the highest quality data, collecting data on more than 35 million companies and leveraging 290 controls. SRS providers are not created equal, each having its own strengths in usability, analytics, compliance, and technical depth. Our data and threat intelligence is transparent, accurate, trustworthy, and mapped to industry standards. Black Kite is the only SRS to deliver the highest quality intelligence built to help organizations make better risk decisions for their business goals. Our data is cross verified, continuously updated, and vast, pulling from the Black Kite engineered, largest data lake in the world."

112. In addition, these statements concern alleged qualities of the Black Kite Platform that Black Kite refers to as "Essential features." *See id.*

113. Further confirming that Black Kite recognizes the materiality of its false and misleading statements, Black Kite has also made these false statements the focal points of its point-of-purchase advertising. On information and belief, the above false and misleading statements were communicated directly to BitSight's actual and potential customers by Black Kite salespersons.

114. On information and belief, Black Kite has actually deceived a number of customers who have either switched from BitSight to Black Kite and/or elected to purchase cyber risk management solutions from Black Kite instead of BitSight.

115. On information and belief, Black Kite's false advertising is willful and knowing because Black Kite is fully aware of its own offerings yet chooses to actively mislead consumers about them. Meanwhile, Black Kite's false and misleading statements about BitSight and its offerings are directly contradicted by publicly available information.

116. Black Kite's false and deceptive advertising took place primarily and substantially in Massachusetts. Black Kite is headquartered in Massachusetts. BitSight is, and always has been headquartered in Massachusetts. Black Kite's unfair and deceptive acts occurred in Massachusetts. Moreover, the harm to BitSight arising out of Black Kite's tortious conduct has been and will continue to be felt principally in Massachusetts.

COUNT 1: INFRINGEMENT OF U.S. PATENT NO. 10,805,331

117. BitSight incorporates the foregoing paragraphs of the Complaint by reference as if fully set forth herein.

118. The Black Kite Platform consists of all products, components, and services that are made, used, performed, offered for sale, and/or sold within the United States by or on behalf of Black Kite in connection with Black Kite's cyber risk management solutions.

119. Black Kite directly infringes the '331 patent in violation of 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by making, using, offering to sell, and/or selling within the United States, without authority, the Black Kite Platform. Exhibit 6 provides an infringement claim chart detailing how the Black Kite Platform directly infringes at least claims 1 and 29 of the '331 patent.

120. BitSight has suffered and will continue to suffer damages as a result of Black Kite's infringement of the '331 patent.

121. On information and belief, despite Black Kite's knowledge of the '331 patent, Black Kite has proceeded with its infringing activity, and with specific intent to cause (or willful blindness to causing) infringement of the '331 patent by developing, utilizing, selling, and offering to sell the Black Kite Platform.

122. Black Kite's infringement of the '331 patent has been and continues to be willful and deliberate, and this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

123. Unless Black Kite is enjoined from infringing the '331 patent, BitSight will suffer irreparable injury for which damages are an inadequate remedy.

COUNT 2: INFRINGEMENT OF U.S. PATENT NO. 9,973,524

124. BitSight incorporates the foregoing paragraphs of the Complaint by reference as if fully set forth herein.

125. The Black Kite Platform consists of all products, components, and services that are made, used, performed, offered for sale, and/or sold within the United States by or on behalf of Black Kite in connection with Black Kite's cyber risk management solutions.

126. Black Kite directly infringes the '524 patent in violation of 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by making, using, offering to sell, and/or selling within the United States, without authority, the Black Kite Platform. Exhibit 7 provides an infringement claim chart detailing how the Black Kite Platform directly infringes at least claim 1 of the '524 patent.

127. BitSight has suffered and will continue to suffer damages as a result of Black Kite's infringement of the '524 patent.

128. On information and belief, despite Black Kite's knowledge of the '524 patent, Black Kite has proceeded with its infringing activity, and with specific intent to cause (or willful blindness to causing) infringement of the '524 patent by developing, utilizing, selling, and offering to sell the Black Kite Platform.

129. Black Kite's infringement of the '524 patent has been and continues to be willful and deliberate, and this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

130. Unless Black Kite is enjoined from infringing the '524 patent, BitSight will suffer irreparable injury for which damages are an inadequate remedy.

COUNT 3: INFRINGEMENT OF U.S. PATENT NO. 9,438,615

131. BitSight incorporates the foregoing paragraphs of the Complaint by reference as if fully set forth herein.

132. The Black Kite Platform consists of all products, components, and services that are made, used, performed, offered for sale, and/or sold within the United States by or on behalf of Black Kite in connection with Black Kite's cyber risk management solutions.

133. Black Kite directly infringes the '615 patent in violation of 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by making, using, offering to sell, and/or selling within the United States, without authority, the Black Kite Platform. Exhibit 8 provides an infringement claim chart detailing how the Black Kite Platform directly infringes at least claim 84 of the '615 patent.

134. BitSight has suffered and will continue to suffer damages as a result of Black Kite's infringement of the '615 patent.

135. On information and belief, despite Black Kite's knowledge of the '615 patent, Black Kite has proceeded with its infringing activity, and with specific intent to cause (or willful blindness to causing) infringement of the '615 patent by developing, utilizing, selling, and offering to sell the Black Kite Platform.

136. Black Kite's infringement of the '615 patent has been and continues to be willful and deliberate, and this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

137. Unless Black Kite is enjoined from infringing the '615 patent, BitSight will suffer irreparable injury for which damages are an inadequate remedy.

COUNT 4: INFRINGEMENT OF U.S. PATENT NO. 11,652,834

138. BitSight incorporates the foregoing paragraphs of the Complaint by reference as if fully set forth herein.

139. The Black Kite Platform consists of all products, components, and services that are made, used, performed, offered for sale, and/or sold within the United States by or on behalf of Black Kite in connection with Black Kite's cyber risk management solutions.

140. Black Kite directly infringes the '834 patent in violation of 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by making, using, offering to sell, and/or selling within the United States, without authority, the Black Kite Platform. Exhibit 9 provides an infringement claim chart detailing how the Black Kite Platform directly infringes at least claim 1 of the '834 patent.

141. BitSight has suffered and will continue to suffer damages as a result of Black Kite's infringement of the '834 patent.

142. On information and belief, despite Black Kite's knowledge of the '834 patent, Black Kite proceeded with its infringing activity, and with specific intent to cause (or willful blindness to causing) infringement of the '834 patent by developing, utilizing, selling, and offering to sell the Black Kite Platform.

143. Black Kite's infringement of the '834 patent has been and continues to be willful and deliberate, and this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

144. Unless Black Kite is enjoined from infringing the '834 patent, BitSight will suffer irreparable injury for which damages are an inadequate remedy.

COUNT 5: INFRINGEMENT OF U.S. PATENT NO. 9,680,858

145. BitSight incorporates the foregoing paragraphs of the Complaint by reference as if fully set forth herein.

146. The Black Kite Platform consists of all products, components, and services that are made, used, performed, offered for sale, and/or sold within the United States by or on behalf of Black Kite in connection with Black Kite's cyber risk management solutions.

147. Black Kite directly infringes the '858 patent in violation of 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by making, using, offering to sell, and/or selling within the United States, without authority, the Black Kite Platform. Exhibit 10 provides an infringement claim chart detailing how the Black Kite Platform directly infringes at least claim 1 of the '858 patent.

148. BitSight has suffered and will continue to suffer damages as a result of Black Kite's infringement of the '858 patent.

149. On information and belief, despite Black Kite's knowledge of the '858 patent, Black Kite has proceeded with its infringing activity, and with specific intent to cause (or willful blindness to causing) infringement of the '858 patent by developing, utilizing, selling, and offering to sell the Black Kite Platform.

150. Black Kite's infringement of the '858 patent has been and continues to be willful and deliberate, and this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

151. Unless Black Kite is enjoined from infringing the '858 patent, BitSight will suffer irreparable injury for which damages are an inadequate remedy.

COUNT 6: FALSE ADVERTISING, 15 U.S.C. § 1125(a)

152. BitSight incorporates the foregoing paragraphs of the Complaint by reference as if fully set forth herein.

153. BitSight and Black Kite are direct competitors in the cyber risk management solutions market.

154. Black Kite has made and continues to make false and misleading statements of fact, in commercial advertising and promotion, regarding the nature, quality, and performance of its products and those of its competitors, including BitSight, that have deceived or have the tendency to deceive a substantial segment of the buying audience. As articulated above, Black Kite's statements falsely or deceptively misleadingly claim, including without limitation, that:

a. Black Kite has 290 controls and that BitSight has 40 controls.

b. Black Kite has extensive integrations with RSA Archer, Splunk, OneTrust, and ServiceNow while BitSight only has "partial" integrations.

c. Black Kite offers extensive digital footprint discovery while BitSight only offers "partial" digital footprint recovery.

d. BitSight's grading methodology is "Proprietary and Non-Standard" while Black Kite's grading methodology is "Standards-based."

e. That it takes "days" to add a new vendor using BitSight but with Black Kite this can be done "instant[ly]."

f. That Black Kite has a ransomware likelihood indicator but BitSight does not.

g. That Black Kite has custom questionnaire mapping but BitSight does not.

h. That Black Kite's offerings can have questionnaires and other security attestations added but BitSight's cannot.

155. Black Kite's false and misleading statements constitute false advertising in violation of § 43(a) of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B), because as purportedly direct comparative superiority claims, they are literally false and/or misleading and/or, as establishment claims, they are literally false and misleading because there is no reliable basis to establish these propositions.

156. Black Kite causes, and has caused, its false and misleading advertising to enter interstate commerce, including by making false and/or misleading statements in national Internet advertising and point-of-purchase advertising.

157. Black Kite's false and misleading statements are material in that they are likely to influence consumers' purchasing decisions and because they are direct comparative superiority claims that relate to inherent qualities or characteristics of BitSight's and Black Kite's products.

158. Black Kite's false and misleading statements have actually deceived or have the tendency to deceive a substantial segment of its audience.

159. As a direct and proximate result of the wrongful acts of Black Kite alleged above, BitSight has suffered, and will continue to suffer, substantial damage to its business reputation, goodwill, and market share, as well as diversion of sales from itself to Black Kite and loss of profits in an amount not yet ascertained. Black Kite's false advertising will continue to harm

BitSight, causing irreparable injury for which there is no adequate remedy at law, unless permanently enjoined by this Court pursuant to 15 U.S.C. § 1116.

160. Based on the foregoing, BitSight is entitled to enhanced monetary damages of up to three times the amount of BitSight's actual damages and/or Black Kite's profits resulting from Black Kite's false advertising, in an amount to be proven at trial, and the costs of the action, pursuant to 15 U.S.C. § 1117. BitSight is also entitled to an accounting of Black Kite's profits resulting from its Lanham Act violations.

161. Upon information and belief, Black Kite's false advertising is willful, knowing, calculated to deceive, and was undertaken in bad faith. As a result, this Court should determine that this is an exceptional case and award BitSight its attorneys' fees and costs incurred in prosecuting this action pursuant to 15 U.S.C. § 1117.

162. The false and/or misleading statements above have injured and are likely to further injure BitSight because Black Kite has generated confusion about the scope and quality of BitSight's cyber risk management solutions, depressing customer demand for BitSight's offerings and leading to declining sales. The statements have also harmed and continue to harm BitSight's business relationships and goodwill with its existing customers.

COUNT 7: DECEPTIVE TRADE PRACTICES,
Mass. Gen. Laws ch. 93A, § 11

163. BitSight incorporates the foregoing paragraphs of the Complaint by reference as if fully set forth herein.

164. The Massachusetts Unfair Practices Act prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." Mass. Gen. Laws ch. 93A, § 2(a). In construing violations of this provision, the statute instructs courts to "be guided by interpretations given by the Federal Trade Commission and the Federal Courts to § 5(a)(1) of the Federal Trade

Commission Act (15 U.S.C. § 45(a)(1)), as from time to time amended." Mass. Gen. Laws ch. 93A, § 2(b).

165. Black Kite's false and misleading advertising constitutes unfair or deceptive acts or practices in the conduct of any trade or commerce in violation of Mass. Gen. Laws ch. 93A.

166. Black Kite's conduct in violation of Mass. Gen. Laws ch. 93A took place primarily and substantially in Massachusetts. Black Kite is headquartered in Massachusetts. BitSight is, and always has been headquartered in Massachusetts. Black Kite's unfair and deceptive acts occurred in Massachusetts. Moreover, the harm to BitSight arising out of Black Kite's tortious conduct has been and will continue to be felt principally in Massachusetts.

167. As stated above, Black Kite has disseminated advertisements regarding Black Kite's products and BitSight's products that contain false, deceptive, and misleading representations regarding the capabilities of Black Kite's products compared to those of BitSight. Black Kite knows or should know that those representations are false, deceptive and misleading. Black Kite's false and misleading statements are material in that they are likely to influence consumers' purchasing decisions and because they are direct comparative superiority claims that relate to inherent qualities or characteristics of BitSight's and Black Kite's products. Black Kite's false and misleading statements have actually deceived or have the tendency to deceive a substantial segment of its audience. Black Kite's false, deceptive, and misleading direct comparative advertising claims constitute deceptive acts and practices in violation of §§ 2 and 11 of the Massachusetts Unfair Practices Act, Mass. Gen. Laws ch. 93A, §§ 2(a), 11.

168. Black Kite's acts, conduct, and practices described above, and the effects of those acts, conduct and practices, have occurred and are occurring primarily and substantially within the Commonwealth of Massachusetts.

169. As a result of Black Kite's unlawful conduct, BitSight has suffered, and will continue to suffer, substantial damage to its business reputation and goodwill, as well as diversion of trade and loss of profits in an amount not yet ascertained. Black Kite's unlawful conduct will continue to harm BitSight, causing irreparable injury for which there is no adequate remedy at law, unless permanently enjoined by this Court under Mass. Gen. Laws ch. 93A, § 11.

170. Based on the foregoing, BitSight is entitled to recover its actual damages and its reasonable attorneys' fees and costs pursuant to Mass. Gen. Laws ch. 93A, § 11

171. Upon information and belief, Black Kite's unlawful acts are willful and knowing. As a result, this Court should award BitSight up to triple, but no less than double, its actual damages pursuant to Mass. Gen. Laws ch. 93A, § 11.

COUNT 8: FALSE ADVERTISING,
Mass. Gen. Laws ch. 266, § 91

172. BitSight incorporates the foregoing paragraphs of the Complaint by reference as if fully set forth herein.

173. Black Kite has disseminated advertisements regarding Black Kite's products and BitSight's products within the Commonwealth of Massachusetts that contain false, deceptive, and misleading representations regarding the capabilities of Black Kite's products compared to those of BitSight. Black Kite knows or should know that those representations are false, deceptive and misleading. Black Kite's false and misleading statements are material in that they are likely to influence consumers' purchasing decisions and because they are direct comparative superiority claims that relate to inherent qualities or characteristics of BitSight's and Black Kite's products. Black Kite's false and misleading statements have actually deceived or have the tendency to deceive a substantial segment of its audience. Upon information and belief, Black Kite has done so with knowledge that its advertisements contain untrue, deceptive, and/or misleading claims.

Black Kite's intentional dissemination of untrue, deceptive, and/or misleading representations within the Commonwealth of Massachusetts constitutes a violation of Mass. Gen. Laws ch. 266, § 91.

174. Black Kite's false and misleading advertising in violation of Mass. Gen. Laws ch. 266, § 91 took place primarily and substantially in Massachusetts. Black Kite is headquartered in Massachusetts. BitSight is, and always has been, headquartered in Massachusetts. Black Kite's unfair and deceptive acts occurred in Massachusetts. Moreover, the harm to BitSight arising out of Black Kite's tortious conduct has been and will continue to be felt principally in Massachusetts.

175. As a result of Black Kite's unlawful conduct, BitSight has suffered, and will continue to suffer, substantial damage to its business reputation and goodwill, as well as diversion of trade and loss of profits in an amount not yet ascertained. Black Kite's unlawful conduct will continue to harm BitSight, causing irreparable injury for which there is no adequate remedy at law, unless permanently enjoined by this Court pursuant to Mass. Gen. Laws ch. 266, § 91.

PRAYER FOR RELIEF

WHEREFORE, BitSight respectfully requests that the Court enter the following relief in its favor and against Black Kite:

1. Judgment that Black Kite has infringed and continues to directly infringe each of the Asserted Patents, either literally or under the doctrine of equivalents;

2. Judgment that Black Kite has willfully infringed one or more claims of the Asserted Patents;

3. Judgment finding Black Kite liable for false advertising in violation of § 43(a) of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B), with respect to its marketing and advertising of its offerings and its comparisons of its offerings to BitSight's;

4. Judgment that Black Kite has willfully, knowingly, and deliberately committed acts of false advertising and that this is an "exceptional case" under § 35 of the Lanham Act, 15 U.S.C. 1117(a);

5. Judgment finding that Black Kite has violated Massachusetts Unfair Practices Act, Mass. Gen. Laws ch. 93A, §§ 2, 11, and Mass. Gen. Laws ch. 266, § 91, which prohibit deceptive trade practices and false advertising;

6. Permanent injunctions enjoining the aforesaid acts of infringement, false advertising, and deceptive trade practices by Black Kite, its officers, agents, servants, employees, attorneys, parent and subsidiary entities, assigns and successors in interest, and those persons acting in concert with them, including related individuals and entities, customers, representatives, distributors, and dealers. In the event that the Court finds that an injunction with respect to the Asserted Patents is not warranted, BitSight requests, alternatively, an award of post-judgment royalty to compensate for future infringement of the Asserted Patents;

7. An award of all monetary relief adequate to compensate for damages resulting from Black Kite's infringement of the Asserted Patents, including lost profits, but in no event less than a reasonable royalty under 35 U.S.C. § 284 for Black Kite's infringement, including all pre-judgment and post-judgment interest at the maximum rate allowed by law;

8. Judgment awarding treble patent damages pursuant to 35 U.S.C. § 284 as a result of Black Kite's willful conduct in relation to the Asserted Patents;

9. Declaration that the case is an exceptional case and that Black Kite be required to pay BitSight's attorneys' fees pursuant to 35 U.S.C. § 285;

10. An award pursuant to § 35 of the Lanham Act, 15 U.S.C. § 1117, and/or Mass. Gen. Laws ch. 93A, § 11, of up to three times the amount of BitSight's actual monetary damages

according to proof, but in no case less than double its damages, exclusive of interest and costs plus prejudgment interest, resulting from Black Kite's false advertising;

11. An award pursuant to § 35 of the Lanham Act, 15 U.S.C. § 1117, of an accounting of Black Kite's profits resulting from its Lanham Act violations and a disgorgement of those profits in an amount to be proven at trial;

12. An award of BitSight's attorneys' fees, costs, and disbursements incurred in prosecuting this action, pursuant to § 35 of the Lanham Act, 15 U.S.C. 1117(a), and/or Mass. Gen. Laws ch. 93A, § 11; and

13. For such other and further relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff BitSight hereby demands a jury trial on all issues so triable.

Dated: September 5, 2023

Respectfully submitted,

/s/ Douglas J. Kline

Douglas J. Kline (BBO# 556680)
Robert D. Carroll (BBO# 662736)
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, MA 02210
Tel.: (617) 570-1000
Fax: (617) 523-1231
dkline@goodwinlaw.com
rcarroll@goodwinlaw.com

Naomi L. Birbach (*pro hac vice* forthcoming)
Timothy Keegan (*pro hac vice* forthcoming)
GOODWIN PROCTER LLP
620 Eighth Avenue
New York, New York 10018
Tel.: (212) 813-8800
Fax: (212) 355-3333
nbirbach@goodwinlaw.com
tkeegan@goodwinlaw.com

Attorneys for Plaintiff, Bitsight Technologies Inc.