

HARVEY ■ SISKIND LLP

November 9, 2015

Naomi Jane Gray  
ngray@harveysiskind.com  
<http://www.shadesofgraylaw.com/>

**VIA FEDEX EXPRESS**

Mr. Omer Trajman  
Chief Executive Officer  
Rocana, Inc.  
548 Market Street, #22538  
San Francisco, CA 94104-5401

Re: Splunk/Rocana

Dear Mr. Trajman:

This firm represents Splunk Inc. with respect to certain enforcement matters. As you know, Splunk provides the leading software platform for real-time operational intelligence. Splunk software and cloud services enable organizations to search, monitor, analyze and visualize machine-generated big data coming from websites, applications, servers, networks, sensors and mobile devices. We understand that Rocana, Inc. ("Rocana") produces a data analytics product that seeks to compete directly with Splunk's software products and services. Splunk believes in competing fairly and openly in the free marketplace, and is confident that Rocana shares that commitment.

Since at least 2004, Splunk has expended great effort and substantial sums developing and protecting its products, services, intellectual property, and goodwill. Splunk has sold its products and services throughout the world and is renowned for its innovative, high-performance disruptive technologies. Splunk has received numerous awards and accolades, both for its company performance and for its products and services. As a result, Splunk and its products and services have achieved broad recognition among industry participants.

In view of Splunk's success, and the high regard in which it is held within the industry, it was naturally concerned when it learned that a September 22, 2015 blog post on Rocana's website and a Rocana whitepaper titled "Improving Event Data Management and Legacy Systems" make false, misleading, disparaging and unsubstantiated statements about Splunk's products and services, and seek to divert customers from Splunk. *See* <http://blog.rocana.com/rocana-vs-splunk-it-operations-showdown>. The post makes the following statements:



Mr. Omer Trajman

November 9, 2015

Page 2

- “Total operational awareness of everything going on within your data center, your infrastructure, is what Splunk has historically tried to do,” said Don Brown (@tensigma), co-founder and COO, Rocana. “But because of scalability and pricing issues Splunk can’t do it anymore.” This falsely suggests that Splunk software cannot provide “total operational awareness” because of “scalability and pricing issues” – impliedly, because Splunk’s products are too expensive and its technology cannot scale to serve the data needs of larger businesses. This statement is demonstrably false, since Splunk’s 10,000+ customers include 80 of the top 100 revenue-generating companies in the United States (as measured by *Fortune* magazine), as well as users that index, analyze, and visualize massive data volumes. Plainly, Splunk’s product can be scaled to serve the needs of large businesses and organizations. The quote also falsely suggests that Rocana’s product can handle data volumes that Splunk cannot.

- “There are systems out there, such as Splunk, that claim to do Big Data but they don’t actually have reliability guarantees.” This implies that Splunk provides no reliability guarantee, while Rocana does. In fact, Rocana specifically states on its website that it does not guarantee data collection reliability. (See, e.g., <http://blog.rocana.com/reliable-collection-from-log-files> (“This all sounds good, are you saying you never lose data? No. With file-based logs, data loss scenario exists ...”). Splunk software, meanwhile, implements multiple protections against data loss and overall system reliability across its data processing steps, including collection, indexing, storage and processing. And since the greatest risk of loss occurs before data reaches the system, Splunk provides its universal forwarder free of charge for a reliable, secure method of data transport into Splunk.

- “Rocana seems to start around 3 TB/day, which not coincidentally is a range that would generally be thought of as (1) challenging for Splunk, and for the budgets of Splunk customers and (2) not a big problem for well-implemented Hadoop,” said Curt Monash (@curtmonash), president of Monash Research in a recent blog post on DBMS2.” This statement suggests that processing 3 terabytes of data per day would be “challenging for Splunk,” but not a problem for a system utilizing a “well-implemented Hadoop.” Splunk has very large numbers of customers who use Splunk to process and analyze more than 3 terabytes of data per day. It is very common for Splunk customers to ingest over 3 terabytes per day, even hundreds of times this volume, which Rocana alleges would be “challenging for Splunk.” The quoted language is also misleading in its suggestion that 3 terabytes per day would be “challenging ... for the budgets of Splunk customers.” This assertion rests on unsubstantiated assumptions about the data analytics needs and corresponding budgets of Splunk customers. Rocana does not have a statistically significant notion of Splunk price points at high data volumes and any assertion on Splunk prices would not be grounded in facts.



- “Hadoop has been designed for handling large volume and velocity of data,” added Monash in an interview. ‘Splunk was designed with similar objectives but it is an older system and it was designed for functionality first and scalability second.’” This false and misleading statement suggests that Splunk is not designed for scalability and that as “an older system” cannot actually handle large volume and velocity of data. However, Splunk has many customers with massive data volumes and/or global server clusters spanning data centers across multiple continents. Splunk can store data in, and analyze data across, Splunk, SQL, NoSQL, and Hadoop data repositories. Accordingly, the implication that Splunk cannot scale like Hadoop is misleading and inaccurate.

- “For network data analysis to effectively help the business, IT needs to be alerted about unexpected events as they happen. This requires a system that can collect and analyze data in real time.” Rocana’s suggestion that Splunk cannot collect, analyze and alert upon data in real time is demonstrably false. Splunk’s real-time alert tools perform exactly these functions.

- “Rocana is using machine learning to more quickly identify which machines or groups of machines are the likely source of the problem – which is the same process as identifying which readings are anomalous,” said Monash. ‘By way of contrast Splunk takes a similar approach to BI but does less of it and does not have the machine learning integration.’” As a statement of fact, Rocana must have actual substantiation to support the claim that its product can “more quickly identify [than Splunk] which machines or groups of machines are the likely source of the problem.” This statement also falsely asserts that Splunk does not have machine learning integration. Splunk’s Caspida™ and Metafor™ technologies provide Splunk’s customers with anomaly and breach detection capabilities, as well as behavioral analytics.

- “Jason Bloomberg, (@thebizwizard), president of Intellyx, adds, ‘Splunk focuses on data correlation while Rocana offers analysis deeper than correlation that can provide more intelligent anomaly detection.’” This claim implies that Splunk can only perform correlation, not intelligent anomaly detection. Splunk’s products do enable intelligent anomaly detection, and its Caspida™ technology also performs anomaly detection, advanced machine learning and analytics.

- “Splunk is a proprietary system that doesn’t publish their file formats, enable direct access to files, or offer open APIs.” The suggestion that Splunk does not enable open access to its files, or open API access to its functions, is demonstrably false. Splunk provides data export and forwarding in standard documented data formats, and a Hadoop record reader that enables Hadoop, Hive, Pig, and Spark access to raw data files stored in the Hadoop



Distributed File System. Moreover, Splunk publishes its API and fully documented software development kits for 6 programming languages.

- “The more data you put in there the more they can tax you in order to do anything,” warned Trajman of choosing Splunk. “Eventually the cost to exit becomes impossible.” This dire warning is designed to scare customers into thinking that Splunk will hold customer data hostage. But Splunk actually *lowers* its unit price as customer use gets bigger, and the features described in the preceding paragraph enable any customer to transfer its data out of Splunk easily and with no license or service cost. Moreover, Splunk offers customers a variety of pricing options that permit unlimited indexing of data without any limitation upon number of users, data ingested or stored, Splunk software usage or infrastructure footprint. And finally, Splunk’s products for Hadoop are priced based on the number of Hadoop nodes, not data ingested, processed or stored.

Some of the statements noted above consist of quotes from individuals who are identified as unrelated third parties, but who, upon closer inspection, are or may in fact be affiliated with Rocana, triggering disclosure requirements under applicable FTC guidelines. The blog post itself was authored by David Spark, whose byline asserts that he is a “Veteran Tech Journalist.” Mr. Spark’s LinkedIn profile, however, describes him as the owner of a “brand journalism firm that specializes in building influencer relations through content.” His claimed specialties include “custom publishing, branded journalism, content marketing, influencer relations, [and] ... content strategy ...” Accordingly, Mr. Spark appears to be a writer for hire by brands seeking to promote a commercial message, and it appears likely that he was paid by Rocana to author the false and defamatory blog post in question. Moreover, Mr. Spark quotes Jason Bloomberg, the president of Intellyx, a company that “works with enterprise digital professionals to ... connect the dots between the customer and the technology ...” See <http://intellyx.com/about/>. Mr. Bloomberg’s profile states that he “advises business executives on their digital transformation initiatives, ... and helps technology vendors and service providers communicate their agility stories.” *Id.* As quoted in the post, Mr. Bloomberg appears to be an unrelated third party. His professional profile, however, suggests that he is paid to work with clients just like Rocana to “communicate their agility stories.” Mr. Spark also quotes a post by Curt Monash, president of Monash Research, on the DBMS2 blog. Mr. Spark does not identify Mr. Monash as being affiliated with Rocana. In the quoted blog post, however, Mr. Monash refers to Rocana as his client. See <http://www.dbms2.com/2015/09/17/rocana-world/#more-9745>. Each of these individuals, while presented as independent third parties in the blog post, thus appears to have an affiliation with Rocana, and may have received financial or other comparable consideration to make false or misleading statements favorable to Rocana.



As you are no doubt aware, "Advertisers are subject to liability for false or unsubstantiated statements made through endorsements, or for failing to disclose material connections between themselves and their endorsers." 16 C.F.R. § 255.1(d). "Where there exists a connection between the endorser and the seller of the advertised product that might materially affect the weight or credibility of the endorsement ... such connection must be fully disclosed." *Id.* § 255.5. When an advertiser pays compensation to an endorser, or provides some other benefit to the endorser, in exchange for the endorsement, the advertiser must disclose that fact "clearly and conspicuously." *Id.* Accordingly, to the extent that Messrs. Spark, Bloomberg, Monash or any of the other purported third-party individuals received compensation or a benefit in exchange for their statements in the blog post, Rocana's failure to disclose that fact is in violation of the FTC guidelines.

In addition to the blog post, Rocana's whitepaper makes the following false and/or misleading statements:

- "Increasingly, businesses are looking for alternatives to increasing Splunk spend due to cost structure alone. A recent study by Blue Hill Research determined that the one-year TCO for a 1 TB/day implementation of Splunk Enterprise was nearly \$1,000,000, with the three-year TCO exceeding \$2M. Because of Splunk's cost structure, most businesses are very selective about which data is ingested in order to save money. This decision to sample data often causes problems down the line when data needed is not available." The prices cited in the study - including the license price itself, as well as maintenance, hardware and storage costs - are wildly inaccurate, and false. As factual statements, Rocana must have substantiation to support its claims that: (1) businesses are increasingly looking for alternatives to increasing Splunk spend due to cost structure alone, (2) most businesses are very selective about which data is ingested in order to save money, and (3) the decision to sample data often causes problems."

- "Another reason businesses are looking for alternatives to Splunk is the 'hostage' clause in the license agreement for Splunk Enterprise. The agreement sets limited conditions for daily ingest volumes. When these limits are exceeded, access to data is blocked until the license violation is rectified. Often this means purchasing an unanticipated, unbudgeted license upgrade. Worse yet, event data volumes typically surge right before or when problems are occurring, so this licensing policy often means that Splunk becomes unavailable just when it is needed most." The assertion that Splunk software holds customers hostage is false and misleading because Splunk software includes features that permit license limits to be exceeded specifically to assure that data is available at critical times and that customers are aware, in advance, of the need ultimately to increase their licenses. The suggestion that Splunk "often" becomes unavailable for this reason is similarly false and misleading.



Mr. Omer Trajman

November 9, 2015

Page 6

- “Managing and using Splunk is so complicated that the community of Splunk experts has become known as ‘ninjas’ for their advanced skillset. The complexity is twofold: (a) configuring the actual hardware infrastructure and capacity planning and (2) implementing the ‘brute-force’ user model to find problems and build solutions.” This statement is false and misleading as Splunk’s software allows for rapid deployment following download, often in minutes or hours. Splunk documentation and guides provide simple architectural and deployment guidance, and Splunk tutorials get users up to speed quickly. Splunk also actively educates its customers against “brute force” searching and recommends analytic functions to target actionable data and eliminate noise.

- “Like a roach motel, Splunk is a one-way street. Splunk is a completely proprietary product; there is no way to access data other than through Splunk-provided tools. The data and indexes are closed. The only APIs are those provided by Splunk.” Comparing Splunk to a roach motel is disparaging and intentionally defamatory. The statement is also misleading. Among other tools, Splunk provides a Hadoop record reader that enables all Hadoop and related tools (Spark HBASE, Hive, Pig) to read Splunk’s raw data files. Splunk data is thus fully compatible with open source projects.

- “All data access is query-based, either directly or through the API.” This statement is false. Splunk is a real-time streaming data analytics pipeline that operates by applying rules, models, analytics, and machine learning; optionally forwarding raw or analyzed data to third-party systems; persisting data to disk and indexing it; and replaying historic data streams through the pipeline for historic analysis.

- “Additionally, the proprietary nature of Splunk has limited the pool of so-called ‘ninjas.’ The scarcity of Splunk professionals results in an excessive cost to hire. Also, because these resources are in great demand, they are frequently targeted by recruiters resulting in a high risk of turnover.” This is false. Splunk has realized successful paid deployments of its Enterprise product at over 10,000 paid customers. Each deployment may be used by tens, hundreds, or thousands of users. Moreover, there are hundreds of thousands of users of its free version. Contrary to Rocana’s intentionally false statements, a key to Splunk’s explosive growth has been its ease of deployment and use.

- “Rocana provides a modern alternative that is better [than Splunk] in several regards: simpler and greater scalability, open data access and formats, out-of-the-box functionality for augmented IT ops, open integration and rich analytics, significantly lower TCO.” This statement is false or misleading in numerous respects. As an express superiority



Mr. Omer Trajman  
November 9, 2015  
Page 7

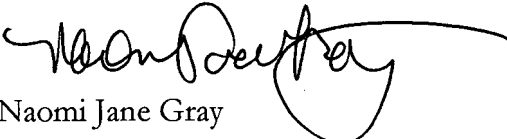
claim, Rocana must be able to substantiate each of these claims based upon factual evidence in existence prior to the making of the claims. Rocana cannot meet this standard.

Rocana's false, misleading and disparaging statements are plainly intended to confuse and deceive consumers, influence their purchasing decisions, and divert customers from Splunk. As such, Rocana is engaging in acts of false advertising, unfair competition, trade libel, and defamation. Accordingly, Splunk demands that Rocana immediately and permanently (1) cease making any of the false and misleading claims discussed above; (2) refrain from making any false, misleading or unsubstantiated statements about Splunk's products and services in the future; (3) remove the blog post from its website and withdraw it from any other location where it has been published; (4) withdraw the whitepaper and destroy all copies of it, whether electronic or hard copy; (5) assure Splunk that it has taken such action as Rocana deems appropriate and sufficient to prevent further violations of Splunk's rights by Rocana's employees; and (6) confirm in writing that each of the following actions has been taken, or will immediately be taken, by Rocana. Until such time as Rocana provides the written assurances above, Rocana should preserve all information regarding the creation of the Rocana blog post and any other marketing materials that make reference to Splunk, and all communications relating to the creation of the post and other materials.

Splunk welcomes the opportunity to discuss these issues with Rocana to assure itself that Rocana does not tolerate, and will not participate in, acts of false advertising, unfair competition, trade libel and defamation. If Rocana does not immediately cease and desist from these acts, then the continuation of this conduct must be considered either to be acts attributable to Rocana and the individuals making the false statements undertaken with conscious disregard of Splunk's rights, or that Rocana has authorized or ratified the wrongful conduct described in this letter. Please provide us with your written response by close of business on **November 23, 2015**.

This letter is written without prejudice to Splunk's rights, all of which are expressly reserved.

Very truly yours,

  
Naomi Jane Gray