

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
ALEXANDRIA DIVISION**

UBIQUITI INC.,

Plaintiff,

v.

BRIAN KREBS,

and

KREBS ON SECURITY, LLC,

Defendants.

Civil Action No.

**COMPLAINT AND  
DEMAND FOR TRIAL BY JURY**

**COMPLAINT AND DEMAND FOR TRIAL BY JURY**

1. Ubiquiti Inc. files this defamation action because blogger Brian Krebs<sup>1</sup> falsely accused the company of “covering up” a cyberattack by intentionally misleading customers about a so-called data “breach” and subsequent blackmail attempt in violation of federal law and SEC regulations.<sup>2</sup> The opposite is true: Ubiquiti promptly notified its customers about the attack and instructed them to take additional security precautions to protect their information. Ubiquiti then notified the public in the next filing it made with the SEC. But Krebs intentionally disregarded these facts to target Ubiquiti and increase ad revenue by driving traffic to his website, [www.KrebsOnSecurity.com](http://www.KrebsOnSecurity.com).

---

<sup>1</sup> This Complaint refers to Defendants Brian Krebs and Defendant Krebs on Security LLC collectively as “Krebs.” They acted jointly and in concert at all times relevant to this Complaint.

<sup>2</sup> Brian Krebs, *Whistleblower: Ubiquiti Breach “Catastrophic,”* KrebsOnSecurity (March 30, 2021), <https://krebsonsecurity.com/2021/03/whistleblower-ubiquiti-breach-catastrophic/>. This document is attached as **Exhibit A** and incorporated by reference. The March 30 article has been updated since it was published, as discussed *infra*. **Exhibit A** reflects Krebs’s March 30 article as it appeared on the date it was published.

2. There is no evidence to support Krebs's claims; indeed, only one source propped up his false story against Ubiquiti: Nickolas Sharp, *the Ubiquiti employee that was behind the cyberattack*.

3. On December 1, 2021, federal prosecutors with the U.S. Attorney's Office from the Southern District of New York issued a press release announcing that they had charged Sharp on four felony counts for "stealing confidential data and extorting" Ubiquiti "while posing as [an] anonymous attacker."<sup>3</sup>

4. Krebs reviewed the press release and he knew that his sole source had been indicted for his criminal involvement in the cyberattack. Despite these damning facts, Krebs published a story on his blog the next day doubling down on his false accusations against Ubiquiti and intentionally misleading his readers into believing that his earlier reporting *was not sourced by Sharp, the hacker behind the attack*.<sup>4</sup>

5. Instead of acknowledging that the source from his previous story was indicted by federal prosecutors for his crimes against Ubiquiti, Krebs calls Sharp "a Ubiquiti employee" when referencing Sharp's contributions to his reporting. But in the very next sentence, Krebs describes Sharp as "a *former Ubiquiti developer*" who "was arrested and charged with stealing data and trying to extort his employer while pretending to be a whistleblower."

---

<sup>3</sup> United States Attorney's Office, *Former Employee Of Technology Company Charged With Stealing Confidential Data And Extorting Company For Ransom While Posing As Anonymous Attacker*, Department of Justice, JUSTICE.GOV, <https://www.justice.gov/usao-sdny/pr/former-employee-technology-company-charged-stealing-confidential-data-and-extorting> (Dec. 2, 2021). This document is attached as **Exhibit B** and incorporated by reference.

<sup>4</sup> Brian Krebs, *Ubiquiti Developer Charged With Extortion, Causing 2020 "Breach,"* KrebsOnSecurity (Dec. 2, 2021), <https://krebsonsecurity.com/2021/12/ubiquiti-developer-charged-with-extortion-causing-2020-breach/>. This document is attached as **Exhibit C** and incorporated by reference.



6. Krebs alternated his descriptions of Sharp, first he describes Sharp as a current employee. He then describes Sharp as a “former Ubiquiti developer” to deceive readers into believing that the sourcing for his original story was a legitimate source—someone other than Sharp. Krebs, therefore, intentionally concealed the fact that the only support for his reporting came from the very person who had just been indicted for hacking and attempted blackmail.

7. The federal indictment against Sharp is central to Krebs’s follow-up story. Still, Krebs repeats the false assertion—that he fabricated against Ubiquiti several months earlier—that “[i]n March, a Ubiquiti employee warned that the company had drastically understated the scope of the incident, and that the third-party cloud provider claim was a fabrication.”

8. Krebs intentionally disregarded the truth by publishing false claims against Ubiquiti that were invented by the man responsible for the attack. The hacker’s account was

facially implausible, Krebs avoided obvious sources of public information that rebut his false and preconceived narrative against Ubiquiti, and Krebs doubled down on his attack against Ubiquiti despite possessing uncontroverted evidence that his source was incredible *and actually involved in the attack*.

9. Krebs's course of conduct makes clear that he was determined to publish stories that adhere to his preconceived narrative that Ubiquiti and other companies disregard their customers' online security. Krebs intentionally misrepresented the truth because he was financially incentivized to do so. His entire business model is premised on publishing stories that conform to this narrative.

10. Despite overwhelming facts showing that his reporting is pure fiction, Krebs has refused to retract or correct his disinformation campaign against Ubiquiti.

11. Even worse, Krebs *doubled down* on his false claims on December 5, 2021, by publishing an update to his March 30 article that not only repeated his earlier false claims about Ubiquiti from the original story but also failed to disclose that the original source for his article was the perpetrator of the attack.<sup>5</sup> Krebs instead intentionally misrepresented this fact in the same way that he had in the December 2 article—by alternatively referring to Sharp as a “former Ubiquiti developer” in the context of the criminal indictment and then separately as “a security professional at Ubiquiti” in the context of Sharp's false claims against Ubiquiti.

12. As a result of these knowing misrepresentations from Krebs, Ubiquiti has suffered substantial harm. Ubiquiti brings this lawsuit as a last resort to recover compensatory and

---

<sup>5</sup> Brian Krebs, *Whistleblower: Ubiquiti Breach “Catastrophic,”* KrebsOnSecurity (Dec. 5, 2021), <https://krebsonsecurity.com/2021/03/whistleblower-ubiquiti-breach-catastrophic/>. The December 5, 2021 update was published at the same URL, and with the same title, as the original March 30, 2021 article (**Exhibit A**). The updated version of the article is attached as **Exhibit D** and incorporated by reference.

punitive damages, to set the record straight, and to hold Krebs accountable for his intentional misrepresentations about Ubiquiti.

### **PARTIES**

13. Ubiquiti is a technology company that was founded in 2003. The company manufactures and sells wireless data communication and wired products. Ubiquiti develops technology platforms for high-capacity distributed internet access, unified information technology, and consumer electronics for professional, home, and personal use. Ubiquiti is incorporated in the state of Delaware and its headquarters are in the state of New York.

14. Defendant Brian Krebs is a resident of Virginia and is a freelance journalist who covers computer security. Krebs publishes a blog titled, “Krebs on Security.”

15. Defendant Krebs on Security LLC is a Virginia limited liability company. Defendant Brian Krebs is the registered agent, manager, and sole member of Krebs on Security LLC.

16. Under the principles of *respondeat superior* and similar doctrines, Defendant Krebs on Security LLC is responsible for the acts and omissions of Defendant Brian Krebs, the sole manager and member of Defendant Krebs on Security LLC, and vice versa.

17. Defendant Brian Krebs publishes his blog personally and by and through his LLC Krebs on Security. Krebs continues to conduct business in the Commonwealth of Virginia under that entity name, and he continues to publish content on the “Krebs on Security” blog.

### **JURISDICTION AND VENUE**

18. This Court has subject matter jurisdiction over this suit pursuant to 28 United States Code section 1332 because there is complete diversity of citizenship between Plaintiff and Defendants and the amount in controversy exceeds \$75,000.00, exclusive of interest and costs.

19. This Court has personal jurisdiction over Defendants pursuant to Virginia Code section 8.01-328 *et seq.*, because Defendants are Virginia residents, they transacted business in Virginia, and repeatedly and deliberately traveled and resided in Virginia during the drafting and publication of the subject defamatory statements against Ubiquiti.

20. Venue is proper in this District pursuant to 28 United States Code section 1391 because a substantial part of the events giving rise to Ubiquiti's claims occurred in the Alexandria Division of the Eastern District of Virginia, and because all Defendants are subject to personal jurisdiction in this District.

### **FACTS**

#### ***Ubiquiti Employee Nickolas Sharp Attempts to Blackmail Ubiquiti by Orchestrating an "Outside" Cyberattack.***

21. On December 28, 2020, Ubiquiti discovered suspicious activity on its cloud infrastructure and soon realized that certain company information had been accessed without authorization.

22. Ubiquiti assembled a team to investigate the security issue and discovered a "backdoor" access point in its system. One of the members of Ubiquiti's investigative team was an employee named Nickolas Sharp.

23. A short time after Ubiquiti discovered the attack, the unknown "hacker" sent an anonymous ransom note via the platform Keybase. The "hacker" claimed that he accessed Ubiquiti's systems as an outsider and taken information from Ubiquiti (including elements of its source code). The "hacker" also demanded 25 Bitcoin from Ubiquiti for the return of the data and the hacker's silence and an additional 25 Bitcoin for the hacker to reveal the location of a second "backdoor" access point in Ubiquiti's system. At the time, 50 Bitcoin was worth approximately \$2 million.

24. Ubiquiti's investigators identified the second "backdoor" so the company refused to pay any ransom to the "hacker." Ubiquiti then promptly alerted its users about the attack by emailing customers, describing the incident, and directing them to change their passwords and enable two-factor authentication.

25. Ubiquiti also alerted its investors (and the public) to the attack in its February 5, 2021 10-Q filed with the SEC.<sup>6</sup> The 10-Q explained that the company had "became aware that certain of our information technology systems hosted by a third-party cloud provider were improperly accessed and certain of our source code and the credentials used to access the information technology systems themselves had been compromised ... As a result, it is possible that the source code and other information could be publicly disclosed or made available to our competitors."

26. Ubiquiti also informed investors and the public of the ransom note that the company had received, stating that Ubiquiti had "received a threat to publicly release these materials unless [Ubiquiti] made a payment, which [Ubiquiti] ha[d] not done."

27. In addition, Ubiquiti alerted law enforcement that it was the victim of an extortion attempt.

28. As Ubiquiti continued to investigate the ransom note and the suspicious activity on its cloud infrastructure, several factors suggested that the attack was an inside job and that Sharp was behind the blackmail scheme.

29. Through its investigation, Ubiquiti learned that Sharp had used his administrative access codes (which Ubiquiti provided to him as part of his employment) to download gigabytes

---

<sup>6</sup> The SEC requires publicly-traded companies to file form 10-Qs each quarter with material disclosures related to financial performance.

of data. Sharp used a Virtual Private Network (“VPN”) to mask his online activity, and he also altered log retention policies and related files to conceal his wrongful actions.

30. Ubiquiti shared this information with federal authorities and the company assisted the FBI’s investigation into Sharp’s blackmail attempt. The federal investigation culminated with the Federal Bureau of Investigation executing a search warrant on Sharp’s home on March 24, 2021.

31. Once Sharp realized that he was being investigated by the FBI, he knew that he needed a new strategy. So he decided to partner with Brian Krebs—a journalist with a preconceived narrative against Ubiquiti—to falsely accuse Ubiquiti of intentionally misleading its investors, customers, and the public to downplay the ransom attack and to falsely inflate Ubiquiti’s stock price and market capitalization.

***After the FBI Searches His Home, Sharp Enlists Brian Krebs to Spread a False Narrative About Ubiquiti, to Devastating Effect.***

32. With the walls closing in on him following the FBI raid, Sharp concocted a new plan to impersonate a “whistleblower” to attack Ubiquiti and blame the company for committing securities fraud in responding to the blackmail scheme. Sharp manufactured this lie to try to conceal the fact that he, himself, was responsible for hacking and extorting Ubiquiti.

33. As part of this plan, Sharp sought to create a false narrative in the media by contacting journalists covering technology and cybersecurity and posing as a “whistleblower” informant who would provide journalists with scandalous inside information about Ubiquiti’s supposed improprieties.

34. Sharp found a blogger with a preconceived narrative against Ubiquiti that was more than willing to publish Sharp’s false claims. That reporter was Brian Krebs.



35. Sometime between the FBI executing its search warrant on March 24 and March 29, 2021, Sharp contacted Krebs and, on information and belief, pitched a false, fantastical story painting Ubiquiti as the villain after victimizing the company. Sharp falsely claimed that Ubiquiti intentionally downplayed the severity of an external hack, mischaracterized the true nature of an “outside” attack, and silenced attempts to honestly deal with the problem and protect the information of the company’s customers. According to Sharp, Ubiquiti took this action to mislead investors and the public and to protect Ubiquiti’s stock price.

36. Sharp’s story was, of course, nonsense. There was never an outside attack; *Sharp himself* orchestrated the blackmail attempt using administrative credentials he was provided over the normal course of his employment.

37. Krebs knew that Sharp’s story was not plausible and Krebs disregarded obvious sources of information in order to print his preconceived narrative against Ubiquiti. Krebs did not have any evidence indicating that Sharp’s story was true because no such evidence exists. But Krebs decided to publish Sharp’s false accusations to drive traffic—and ad revenue—to his blog.

38. Krebs chose to work with Sharp to harm Ubiquiti’s reputation by printing these uncorroborated and unverified false claims against the company. Krebs’s blog victimized Ubiquiti a second time for being the target of Sharp’s cyber-attack.

39. On March 30, 2021, Krebs published an article on his blog titled, “Whistleblower: Ubiquiti Breach ‘Catastrophic.’”<sup>7</sup> In the article, Krebs claims without any evidence that Ubiquiti had intentionally deceived customers by “massively downplay[ing]” the impact of a “catastrophic” data breach. Krebs falsely claimed that the attack was perpetrated by an external

---

<sup>7</sup> **Exhibit A.**

hacker. Krebs also alleged that Ubiquiti's description of the so-called "breach" was a "fabrication" designed to mislead the public.

40. Ubiquiti's SEC filings from the previous month demonstrate the company disclosed the improper access of information *and* the fact that Ubiquiti had received a ransom demand that threatened to publicize Ubiquiti's source code and other private information. But Krebs concealed these facts and deliberately omitted them from his story to avoid contradicting his false claims.<sup>8</sup>

41. Instead, Krebs's story gave the distinct impression to his readers that Ubiquiti—in response to a catastrophic "hack" caused by malicious outside forces—engaged in fraudulent conduct in violation of federal law and SEC regulations to protect its bottom line.

42. Krebs also admitted in the article that he relied on a single source to whom he gave the pseudonym "Adam," and described as a "security professional at Ubiquiti." While Krebs stated that he referred to Sharp by a pseudonym because Sharp "fear[ed] retribution by Ubiquiti," the intention was far more sinister: to conceal from readers the fact that Sharp was responsible for the criminal attack against Ubiquiti.

43. Krebs published "Adam's" account because it conformed to Krebs's preconceived narrative that Ubiquiti and other companies intentionally and recklessly disregard their customers' cybersecurity—which Krebs leverages to drive traffic to his blog as the only "reliable" source of information on data security.

44. Krebs falsely accused Ubiquiti of committing fraud, violating federal law, and violating SEC regulations, and he manufactured the claim that "access to customers' devices

---

<sup>8</sup> Krebs has read previous Ubiquiti SEC filings. In a 2015 story, Krebs specifically referenced Ubiquiti's relevant SEC filings.

deployed in corporations and homes around the world was at risk” and that Ubiquiti was determined to conceal the facts and had “overruled efforts to decisively protect customers.”

45. Krebs’s statements against Ubiquiti are demonstrably false. But he published the story anyway because his financial and personal interests are served by his preconceived narrative that technology companies fail to protect the data and privacy of their customers. By misleading customers in this way, Krebs has carved out a niche as a “trusted” source for best practices to protect their data and information. If Krebs had written the truth about Ubiquiti’s response to Sharp’s cyberattack, Krebs’s expertise would not be needed.

46. Krebs’s March 30, 2021 story was published to a global audience and his account was read by an untold number of people. The story was subsequently (and foreseeably) republished in numerous outlets around the world, including publications in Italy,<sup>9</sup> New Zealand,<sup>10</sup> and, of course, throughout the Commonwealth of Virginia and the United States.<sup>11</sup>

---

<sup>9</sup> See, Michele Nasi, *Incidente di sicurezza per Ubiquiti: definito catastrofico da un dipendente dell'azienda*, IISoftware.it (March 31, 2021), [https://www.ilsoftware.it/articoli.asp?tag=Incidente-di-sicurezza-per-Ubiquiti-definito-catastrofico-da-un-dipendente-dell-azienda\\_22772](https://www.ilsoftware.it/articoli.asp?tag=Incidente-di-sicurezza-per-Ubiquiti-definito-catastrofico-da-un-dipendente-dell-azienda_22772).

<sup>10</sup> Sasha Karen, *Ubiquiti breach claimed to be ‘catastrophically worse than reported,’* ARN (March 31, 2021), <https://www.arnnet.com.au/article/687330/ubiquiti-breach-claimed-catastrophically-worse-than-reported/>.

<sup>11</sup> Dan Goodin, *Ubiquiti breach puts countless cloud-based devices at risk of takeover*, Ars Technica (March 31, 2021), <https://arstechnica.com/gadgets/2021/03/ubiquiti-breach-puts-countless-cloud-based-devices-at-risk-of-takeover/>; Mitchell Clark, *Ubiquiti is accused of covering up a ‘catastrophic’ data breach — and it’s not denying it*, The Verge (March 31, 2021), <https://www.theverge.com/2021/3/31/22360409/ubiquiti-networking-data-breach-response-whistleblower-cybersecurity-incident>; Charlie Osborne, *Whistleblower claims Ubiquiti Networks data breach was ‘catastrophic,’* ZD Net (March 31, 2021), <https://www.zdnet.com/article/whistleblower-claims-ubiquiti-networks-data-breach-was-catastrophic/>.

***Even After Sharp is Arrested and Publicly Outed as the Blackmailer, Krebs Refuses to Acknowledge the Truth and Correct His Reporting.***

47. Sharp was arrested and indicted on various criminal charges in December 2021. The Department of Justice announced the indictment on its website via a press release—which identified Sharp by name but referred to Ubiquiti as “Company-1”—on December 1, 2021.<sup>12</sup>

48. The press release describing the indictment against Sharp discussed his unlawful scheme to “secretly steal[] gigabytes of confidential files from [Ubiquiti,] where he was employed, and then, while purportedly working to remediate the security breach, [Sharp] extort[ed] the company for nearly \$2 million for the return of the files and the identification of a remaining purported vulnerability.”

49. It also detailed that Sharp had sent Ubiquiti a “ransom note [which] sought 50 Bitcoin ... which was the equivalent of approximately \$1.9 million ... in exchange for the return of the stolen data and the identification of a purported ‘backdoor,’ or vulnerability, to Company-1’s computer systems.”

50. The press release also explained the nature of Sharp’s disinformation campaign in the media:

SHARP subsequently re-victimized his employer by causing the publication of misleading news articles about the company’s handling of the breach that he perpetrated ... SHARP caused false news stories to be published about the [blackmail attempt] ... In those stories, SHARP identified himself as an anonymous whistleblower within Company-1 who had worked on remediating the Incident. In particular, SHARP falsely claimed that Company-1 had been hacked by an unidentified perpetrator who maliciously acquired root administrator access to Company-1’s AWS accounts. In fact, as SHARP well knew, SHARP had taken Company-1’s data using credentials to which he had access in his role as Company-1’s AWS cloud administrator, and SHARP had used that data in a failed attempt to extort Company-1 for millions of dollars. Following the publication of these articles, between March 30, 2021, and March 31, 2021,

---

<sup>12</sup> **Exhibit B.**

Company-1's stock price fell approximately 20%, losing over \$4 billion in market capitalization.

**Department of Justice**

U.S. Attorney's Office

Southern District of New York

SHARE 

FOR IMMEDIATE RELEASE

Wednesday, December 1, 2021

**Former Employee Of Technology Company Charged With Stealing Confidential Data And Extorting Company For Ransom While Posing As Anonymous Attacker**

Damian Williams, the United States Attorney for the Southern District of New York, and Michael J. Driscoll, Assistant Director-in-Charge of the New York Office of the Federal Bureau of Investigation ("FBI"), announced the arrest today of NICKOLAS SHARP for secretly stealing gigabytes of confidential files from a New York-based technology company where he was employed ("Company-1"), and then, while purportedly working to remediate the security breach, extorting the company for nearly \$2 million for the return of the files and the identification of a remaining purported vulnerability. SHARP subsequently re-victimimized his employer by causing the publication of misleading news articles about the company's handling of the breach that he perpetrated, which were followed by a significant drop in the company's share price associated with the loss of billions of dollars in its market capitalization.

SHARP was arrested earlier today in the District of Oregon and will be presented this afternoon before U.S. Magistrate Judge John V. Acosta. The case was assigned to U.S. District Judge Katherine Polk Failla.

U.S. Attorney Damian Williams said: "As alleged, Nickolas Sharp exploited his access as a trusted insider to steal gigabytes of confidential data from his employer, then, posing as an anonymous hacker, sent the company a nearly \$2 million ransom demand. As further alleged, after the FBI searched his home in connection with the theft, Sharp, now posing as an anonymous company whistle-blower, planted damaging news stories falsely claiming the theft had been by a hacker enabled by a vulnerability in the company's computer systems. Now the alleged theft and lies have been exposed, and Sharp is facing serious federal charges."

FBI Assistant Director Michael J. Driscoll said: "We allege Mr. Sharp created a twisted plot to extort the company he worked for by using its technology and data against it. Not only did he allegedly break several federal laws, he orchestrated releasing information to media when his ransom demands weren't met. When confronted, he then lied to FBI agents. Mr. Sharp may have believed he was smart enough to pull off his plan, but a simple technical glitch ended his dreams of striking it rich."

51. Media outlets across the globe reported on Sharp as the “mastermind” behind the failed extortion attempt,<sup>13</sup> including Reuters.<sup>14</sup> That reporting made clear that “Company-1” was in fact Ubiquiti.

52. Yet amazingly, even though his source “Adam” (Sharp) had been arrested for orchestrating the very criminal plot that he claimed Ubiquiti had lied about, Krebs *still* refused to remove or clarify his March 30 article.

53. Instead, he chose to double down on his false accusations against Ubiquiti and refused to walk back from or retract his smear campaign. Krebs published an article the day after the indictment against Sharp was announced, December 2, 2021.<sup>15</sup> In it, Krebs repeats the false assertion that “[i]n March, a Ubiquiti employee warned that the company had drastically understated the scope of the incident, and that the third-party cloud provider claim was a fabrication,” *despite the fact that this claim had come from the very person who had just been indicted for attempting to blackmail Ubiquiti.*

54. In the very next sentence of the article, Krebs discloses that “a former Ubiquiti developer was arrested and charged with stealing data and trying to extort his employer while pretending to be a whistleblower.”

55. Of course, the “Ubiquiti employee” and the “former Ubiquiti developer” that Krebs referenced are the same person: Sharp. This odd phrasing—first referring to Sharp as an

---

<sup>13</sup> Mitchell Clark, *Ubiquiti hack may have been an inside job, federal charges suggest*, The Verge (Dec. 1, 2021), <https://www.theverge.com/2021/12/1/22812761/ubiquiti-data-breach-aws-doj-indictment-inside-job>.

<sup>14</sup> Brian Pierson, *Former Ubiquiti employee charged with hacking, extorting company*, Reuters (Dec. 1, 2021), <https://www.reuters.com/markets/currencies/former-ubiquiti-employee-charged-with-hacking-extorting-company-2021-12-01/>.

<sup>15</sup> Exhibit C.

“employee” and then as a “developer”—was a transparent attempt by Krebs to hide from his readers the fact that there were no legitimate sources for his stories.

56. While refusing to correct or retract his March 30 article, Krebs would use the same deceptive tactics to update and republish the March 30 article.

57. On December 5, 2021, Krebs published an “update” to the March 30 article that was buried underneath the article’s headline, lead paragraph, and an image of Ubiquiti’s logo.<sup>16</sup>

58. The “update” stated that, “[t]he Justice Department has indicted a former Ubiquiti developer for allegedly causing the 2020 ‘breach’ and trying to extort the company.”

HOME
ABOUT THE AUTHOR
ADVERTISING/SPEAKING

## Whistleblower: Ubiquiti Breach “Catastrophic”

March 30, 2021 149 Comments

On Jan. 11, **Ubiquiti Inc.** [NYSE:UI] — a major vendor of cloud-enabled Internet of Things (IoT) devices such as routers, network video recorders and security cameras — disclosed that a breach involving a third-party cloud provider had exposed customer account credentials. Now a source who participated in the response to that breach alleges Ubiquiti massively downplayed a “catastrophic” incident to minimize the hit to its stock price, and that the third-party cloud provider claim was a fabrication.



**Update, Dec. 5, 2021:** The Justice Department has indicted a former Ubiquiti developer for allegedly causing the 2020 “breach” and trying to extort the company.

*Original story:*

A security professional at Ubiquiti who helped the company respond to the two-month breach beginning in December 2020 contacted KrebsOnSecurity after raising his concerns with both Ubiquiti’s whistleblower hotline and with European data protection authorities. The source — we’ll call him **Adam** — spoke on condition of anonymity for fear of retribution by Ubiquiti.

<sup>16</sup> Exhibit D.

59. Krebs knew about the press release, he linked to it in his story. This confirms that Krebs had *actual knowledge* that Sharp was responsible for the cyberattack.

60. Krebs intentionally disregarded this fact, and he concealed from his readers that his only source was not a whistleblower at all but had actually been charged for carrying out the attack. Adding insult to injury, Krebs continued to repeat the attacker's self-serving account despite knowing that it bears no relationship with the truth.

61. Krebs's reckless disregard in republishing Sharp's lies is manifest—particularly given that the Department of Justice identified Sharp as the person behind the attack.

62. Some of Krebs's readers confronted Krebs on Twitter when they realized that his "source" "Adam" was the very person who had been indicted. Krebs responded online but, instead of admitting that the March 30 article relied entirely on someone who had been indicted for very crime at issue in the article, doubled down and make the bewildering claim that "the facts in the piece are correct."<sup>17</sup>

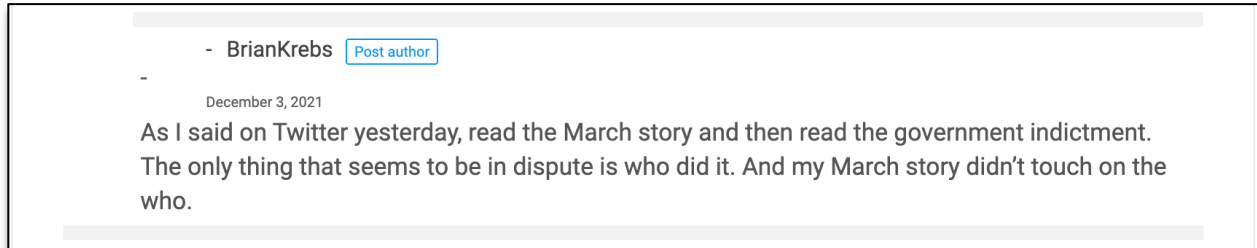



---

<sup>17</sup> Brian Krebs (@briancrebs), Twitter (Dec. 2, 2021), <https://twitter.com/briancrebs/status/1466556868466143232>. This document is attached as **Exhibit E** and incorporated by reference.



63. And in response reader comments to the December 2, 2021 article that discussed the indictment against Sharp, Krebs likewise replied that “[t]he only thing that seems to be in dispute is who did it. And my March story didn’t touch on the who.”<sup>18</sup>



64. Krebs’s defense is bogus. Because of Krebs’s continued refusal to retract or correct the March 30 article, to this day, anyone reading the March 30 article (including the December 5, 2021 update) naturally and foreseeably comes away with the understanding that the “whistleblower” “source” named “Adam” was *not* the person responsible for the blackmail attempt and that his accusations against Ubiquiti are *credible*. Of course, had Krebs disclosed that the anonymous source making allegations of illegality and misfeasance against Ubiquiti was *indicted* for perpetrating the incident at the center of Krebs’s reporting, it would be manifest that Krebs’s sole source (and his accusations) had no credibility whatsoever, and Krebs’s own credibility would have suffered.

65. To this day, the March 30, 2021 article and the December 5, 2021 update remain online where they can be accessed by anyone with an internet connection. The article *still* alleges that Ubiquiti “massively downplayed a ‘catastrophic’ incident to minimize the hit to its stock price,” that Ubiquiti’s “third-party cloud provider claim was a fabrication,” and repeats Mr. Sharp’s claim that Ubiquiti “silenced and overruled efforts to decisively protect customers.” Krebs drafted the article to create the false impression that a malicious external actor “breached”

---

<sup>18</sup> Exhibit C.

Ubiquiti's security systems, and Ubiquiti, to protect its stock price, broke federal laws and SEC regulations in an attempt to "cover[] up" the incident, lying to its shareholders and the public.

66. The damage caused by Krebs's false reporting has been substantial: in the 24-hour period after Krebs's first article was published, Ubiquiti's stock price fell approximately 20%, which translated to Ubiquiti losing \$4 billion in market capitalization.

67. And more, stockholders and opportunistic plaintiffs' lawyers took note and quickly threatened class action litigation based solely on the allegations in Krebs's false reporting because the story led them, predictably and foreseeably, to falsely believe that Ubiquiti had defrauded investors by lying about the supposed external "breach." And indeed, these threats would soon materialize into class action litigation against the company.

68. In addition to civil litigation, Krebs's article also led numerous government agencies to send document preservation notices and inquiries regarding Sharp's actions. Tellingly, these each referenced Krebs's article, either by parroting the falsehoods that Krebs had published or by citing directly to the article.

69. Ubiquiti, while suffering the havoc that Krebs's reporting was causing, and in an effort not to compromise the confidential nature of the criminal investigation into Sharp, had little choice but to sit and wait until federal authorities moved on Sharp.

70. Ubiquiti brings this litigation because of Krebs's refusal to do the right thing and retract the March 30 article or the December 2, 2021 update, which continue to malign Ubiquiti's reputation, damage its relationships with its stockholders, and disrupt its business operations.

#### **COUNT ONE - DEFAMATION PER SE**

71. Plaintiff repeats and re-alleges each of the foregoing paragraphs in this Complaint as if set forth fully herein.

72. Defendant Krebs published an “update” to his March 30, 2021 article titled, *Whistleblower: Ubiquiti Breach “Catastrophic,”* on December 5, 2021 to a new global online audience.

73. The article—which conceals the fact that the “former Ubiquiti developer” who was “indicted” was in fact the “security professional at Ubiquiti” who Krebs characterized as a “whistleblower” “source” and referred to as “Adam”—contains the following defamatory statements:

- (a) “Now a source who participated in the response to that breach *alleges Ubiquiti massively downplayed a ‘catastrophic’ incident to minimize the hit to its stock price ....*”
- (b) “According to Adam, the hackers obtained full read/write access to Ubiquiti databases at Amazon Web Services (AWS), which was the alleged ‘third party’ involved in the breach. *Ubiquiti’s breach disclosure, he wrote, was ‘downplayed and purposefully written to imply that a 3rd party cloud vendor was at risk and that Ubiquiti was merely a casualty of that, instead of the target of the attack.’*”
- (c) Finally, the article in its entirety implies that Ubiquiti suffered a severe data breach via a malicious external actor and Ubiquiti intentionally lied to its investors and the public about the nature and severity of the “breach” to protect its stock price and actively instructed its employees not to take reasonable precautions to protect customer data.

74. On information and belief, Krebs’s December 5, 2021 Update that republished the March 30, 2021 article was read and recirculated widely online, reaching an untold number of viewers.

75. Krebs’s statements in the December 5, 2021 Update were understood by those who read them to be statements of fact regarding Ubiquiti.

76. Krebs’s statements are false. Indeed, they are a fictional account created by Sharp in a failed effort to conceal his own criminal conduct, which is confirmed by the Department of Justice’s press release and the indictment against Sharp. There was no malicious external actor who “breached” Ubiquiti’s security systems; it was Sharp who misused the credentials Ubiquiti

had provided him to access information. In reality, Ubiquiti acted appropriately in investigating suspicious activity on its cloud infrastructure and identifying Sharp as the true culprit, which led to his arrest and indictment. In no way did Ubiquiti mischaracterize Sharp's actions, mislead its investors or the public, or instruct employees not to take steps that would have protected customer data.

77. Ubiquiti in no way approved the false and defamatory accusations published by Krebs.

78. Krebs acted with actual malice, intentionally disregarding the truth by intentionally disregarding key information about Sharp and intentionally obfuscating Sharp's role in his reporting by falsely creating the perception that Sharp and "Adam" were not the same person. Evidence of the Krebs's actual malice includes:

- (a) Krebs published the December 5, 2021 Update after the Department of Justice announced that Sharp, Krebs's sole source, had been indicted for orchestrating the blackmail plot against Ubiquiti, demonstrating that Sharp was not merely an inherently unreliable source, but also was the principal in the criminal plot against the company.
- (b) Krebs published the December 5, 2021 Update after the Department of Justice issued its press release explaining that Sharp had planted false media articles about Ubiquiti's handling of Sharp's blackmail attempt, which was an overt reference to Krebs's reporting: "SHARP subsequently re-victimized his employer by causing the publication of misleading news articles about the company's handling of the breach that he perpetrated."
- (c) Krebs published the December 5, 2021 Update without having any corroborating witnesses or other factual evidence (because none exists) to support Sharp's false accusations against Ubiquiti.
- (d) There were obvious sources of information that rebutted Krebs's false narrative—including press releases that Krebs *actually read* from the Department of Justice, statements Ubiquiti published to customers, and in publicly-available SEC filings.

- (e) In publishing the December 5, 2021 Update, Krebs intentionally concealed from his readers the fact that Sharp and his so-called “whistleblower” “source” “Adam” were the same person. He did so by publishing the additional text detailing the indictment in the Update underneath the article’s headline, lead paragraph, and an image of Ubiquiti’s logo and also by alternatively referring to Sharp as a “former Ubiquiti developer” when referencing the indictment, but then as a “security professional” when referring to “Adam” and his criticisms of the company. The December 5, 2021 Update intentionally conceals the fact that the criticisms and allegations against Ubiquiti are being made by the very person who was indicted for blackmailing the company.
- (f) Krebs also took steps outside of the December 5, 2021 Update to conceal the fact that Sharp was his “source” “Adam.” In a December 2, 2021 article published by Krebs, he likewise alternatively referred to Sharp as a “Ubiquiti employee” when discussing “Adam” and then referred to him as a “developer” when discussing the Sharp’s indictment.
- (g) Krebs’s preconceived narrative against Ubiquiti—that it was “covering up” a “breach”—is in service of his financial interests. Specifically, Krebs’s business model is to convince consumers that they need to read his blog to learn about clandestine and misleading actions from companies regarding their cyber security. This drives traffic and lucrative ad revenue to Krebs’s blog.
- (h) When confronted with overwhelming facts exposing that his claims against Ubiquiti were demonstrably false, Krebs refused to apologize or back down. Instead, he doubled down on his false accusations and continued to conceal from readers the fact that his story lacked any corroboration whatsoever ***and the fact that it was invented by the man behind the cyberattack.***
- (i) Krebs has confirmed his agenda and his actual malice against Ubiquiti by linking to the story and by falsely claiming that the Sharp incident is evidence of Krebs’s stature and ability as a cybersecurity expert with inside information on breaking stories.

79. Krebs’s actions were malicious, willful, and wanton, and evidence a conscious disregard for the rights of Ubiquiti. Accordingly, punitive damages are appropriate.

80. Krebs’s December 5, 2021 Update is defamatory *per se* because it is susceptible of but one meaning. That Ubiquiti lied to its investors and the public by mischaracterizing the severity and nature of a security breach from an external source and by directing its employees not to take reasonable steps to protect customer data. These accusations necessarily prejudice

Ubiquiti in its profession as a provider of technology platforms for high-capacity distributed Internet access, unified information technology, and consumer electronics.

81. Krebs's statements are also defamatory *per se* because they attribute criminal conduct to Ubiquiti by falsely alleging that Ubiquiti (a public company) lied to investors and the public about a security breach to fraudulently protect its stock price. In other words, Krebs's statements accuse Ubiquiti of committing securities fraud, a serious crime involving moral turpitude.

82. As a proximate result of Krebs's false and defamatory statements, Ubiquiti has suffered severe reputational harm, including, *inter alia*, injury to its reputation, a severe decrease in its stock price, a resulting drastic decrease in market capitalization, deteriorating relationships with stockholders, increased and unwarranted scrutiny from government agencies, and the reputational and financial costs stemming from the class action litigation premised on Krebs's false reporting.

#### COUNT TWO - DEFAMATION PER SE

83. Plaintiff repeats and re-alleges each of the paragraphs in this Complaint as if set forth fully herein.

84. Defendant Krebs published his false and defamatory article about Ubiquiti titled, *Whistleblower: Ubiquiti Breach "Catastrophic,"* on March 30, 2021 to a global online audience.

85. The article contains the following defamatory statements:

- (a) "Now a source who participated in the response to that breach *alleges Ubiquiti massively downplayed a 'catastrophic' incident to minimize the hit to its stock price ....* "
- (b) "According to Adam, the hackers obtained full read/write access to Ubiquiti databases at Amazon Web Services (AWS), which was the alleged 'third party' involved in the breach. *Ubiquiti's breach disclosure, he wrote, was 'downplayed and purposefully written to imply that a 3rd party cloud vendor was at risk and that Ubiquiti was merely a casualty of that, instead of the target of the attack.'*"

- (c) Finally, the article in its entirety implies that Ubiquiti suffered a severe data breach via a malicious external actor and Ubiquiti intentionally lied to its investors and the public about the nature and severity of the “breach” to protect its stock price and actively instructed its employees not to take reasonable precautions to protect customer data.

86. Krebs’s March 30, 2021 article was read and recirculated widely online, reaching an untold number of viewers.

87. Krebs’s statements in the March 30, 2021 article were understood by those who read them to be statements of fact regarding Ubiquiti.

88. Krebs’s statements are false. Indeed, they are a fictional account created by Sharp in a failed effort to conceal his own criminal conduct, which is confirmed by the Department of Justice’s press release and the indictment against Sharp. There was no malicious external actor who “breached” Ubiquiti’s security systems; it was Sharp who misused the credentials Ubiquiti had provided him to access information. In reality, Ubiquiti acted appropriately in investigating suspicious activity on its cloud infrastructure and identifying Sharp as the true culprit, which led to his arrest and indictment. In no way did Ubiquiti mischaracterize Sharp’s actions, mislead its investors or the public, or instruct employees not to take steps that would have protected customer data.

89. Ubiquiti in no way approved the false and defamatory accusations published by Krebs.

90. Krebs acted with actual malice, intentionally disregarding the truth by intentionally disregarding key information about Sharp and intentionally obfuscating Sharp’s role in his reporting by falsely creating the perception that Sharp and “Adam” were not the same person. Evidence of the Defendants’ actual malice includes:

- (a) Krebs published the March 30, 2021 article without having any corroborating witnesses or other factual evidence (because none exists) to support Sharp’s false accusations against Ubiquiti.

- (b) There were obvious sources of information that rebutted Krebs's false narrative—including statements Ubiquiti published to customers that Krebs *actually read* and publicly-available SEC filings.
- (c) Krebs's preconceived narrative against Ubiquiti—that it was “covering up” a “breach”—is in service of his financial interests. Specifically, Krebs's business model is to convince consumers that they need to read his blog to learn about clandestine and misleading actions from companies regarding their cyber security. This drives traffic and lucrative ad revenue to Krebs's blog.
- (d) When confronted with overwhelming facts exposing that his that his claims against Ubiquiti were demonstrably false, Krebs refused to apologize or back down. Instead, he doubled down on his false accusations and continued to conceal from readers the fact that his story lacked any corroboration whatsoever and the fact that it was invented by the man behind the cyberattack.
- (e) Krebs has confirmed his agenda and his actual malice against Ubiquiti by linking to the story and by falsely claiming that the Sharp incident is evidence of Krebs's stature and ability as a cybersecurity expert with inside information on breaking stories.

91. Krebs's actions were malicious, willful, and wanton, and evidence a conscious disregard for the rights of Ubiquiti. Accordingly, punitive damages are appropriate.

92. Krebs's March 30, 2021 article is defamatory *per se* because it is susceptible of but one meaning, that Ubiquiti lied to its investors and the public by mischaracterizing the severity and nature of a security breach from an external source and by directing its employees not to take reasonable steps to protect customer data. These accusations necessarily prejudice Ubiquiti in its profession as a provider of technology platforms for high-capacity distributed Internet access, unified information technology, and consumer electronics.

93. Krebs's statements are also defamatory *per se* because they attribute criminal conduct to Ubiquiti by falsely alleging that Ubiquiti (a public company) lied to investors and the public about a security breach to fraudulently protect their stock price. In other words, Krebs's statements accuse Ubiquiti of committing securities fraud, a serious crime involving moral turpitude.



94. As a direct and proximate result of Krebs's false and defamatory statements, Ubiquiti has suffered severe reputational harm, including, *inter alia*, injury to its reputation, a severe decrease in its stock price, a resulting drastic decrease in market capitalization, deteriorating relationships with stockholders, increased and unwarranted scrutiny from government agencies, and the reputational and financial costs stemming from the class action litigation premised on Krebs's false reporting.

**JURY DEMAND**

95. Plaintiff hereby demands a trial by jury on all issues and claims so triable.

**PRAYER FOR RELIEF**


WHEREFORE, Plaintiff Ubiquiti Inc. demands judgment against Defendant Brian Krebs as follows:

- (a) awarding compensatory damages in an amount to be determined at trial, but greater than \$75,000.00;
- (b) awarding Ubiquiti \$350,000 in punitive damages or in an amount to be determined at trial;
- (c) awarding Plaintiff all expenses and costs, including attorneys' fees; and
- (d) such other and further relief as the Court deems appropriate.

(SIGNATURE PAGE FOLLOWS)

Dated: March 29, 2022

Respectfully Submitted,

Handwritten signature of Daniel P. Watkins in blue ink.

---

Thomas A. Clare, P.C. (VSB #39299)

Daniel P. Watkins (VSB #84592)

CLARE LOCKE LLP

10 Prince Street

Alexandria, VA 22314

Telephone: (202) 628-7400

Email: [tom@clarelocke.com](mailto:tom@clarelocke.com)

Email: [daniel@clarelocke.com](mailto:daniel@clarelocke.com)

*Attorneys for Plaintiff*