IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
EASTERN DIVISION

Case No. 4:25-cv-00062

| | |
|---|---|
| MrBeastYouTube, LLC,<br><br>Plaintiff,<br><br>vs.<br><br>Leroy Nabors,<br><br>Defendant. | **COMPLAINT AND DEMAND FOR JURY TRIAL** |

Plaintiff MrBeastYouTube LLC ("Beast" or the "Company"), by and through its undersigned counsel, hereby submits this Complaint against Leroy Nabors ("Nabors" or "Defendant"):

## NATURE OF THE ACTION

1. Leroy Nabors worked for Beast for approximately two years. When he joined the company, he agreed by contract to return all Beast property in his possession at the Company's request. Nabors breached that contract.

2. In the days leading up to his termination of employment—which he admits he knew "was coming"—he exfiltrated thousands of confidential Beast documents, including but not limited to financial data, sensitive memoranda regarding business transactions, private employee compensation information, and capitalization tables containing highly sensitive information about Beast's investors. A list of the thousands of documents Nabors exfiltrated, identified by file name, is attached hereto as **Exhibit A**.[1]

3. Nabors has declined Beast's multiple requests to return these documents. He continues to have them in his possession unlawfully, months after he was terminated.

4. Beast initially engaged Nabors as a consultant in Beast's IT department from July 11, 2023 until December 2023.

[1] **Exhibit A** is the subject of Beast's forthcoming motion to seal.

5. Nabors' daughter, Kaylie Nabors, is the sole managing member of a company called Vine Networks LLC ("Vine"), which was contracted—by Nabors—to manage Beast's entire IT network. Together, Nabors and his daughter had direct access to that network. Vine continued to have access to Beast's network for months following Nabors' termination of employment.

6. As part of Nabors' engagement, he executed the Company's standard non-disclosure agreement, which provided in relevant part:

> Upon the request of Company at any time or upon the termination of Employee's employment with the Company for any reason, Employee shall promptly (but in no event more than ten (10) days after written request of Company) deliver to the Company property as well as all records, manuals, articles, devices, equipment, customer lists, financial information, and other items which disclose or contain Proprietary or Confidential Information in any form, including all copies thereof, whether prepared by Employee, the Company or others.

7. In December 2023, Beast shifted Nabors away from IT responsibilities and placed him on the Company's Development Team. From that point forward, Nabors no longer had primary responsibilities in IT.

8. Beast's Development Team is deliberately flexible and multi-purpose, tackling issues ranging from content production to fundraising to political advocacy.

9. Nabors' role on the Development Team was formalized when he joined Beast as a full-time employee on February 1, 2024, as Development Director.

10. Nabors was terminated on October 1, 2024. That termination was not a surprise to him (he admitted to a member of Beast's Human Resources department that he "had a hint it was coming" the month prior). And he took steps to prepare for it. In the days and weeks leading up to his expected termination, Nabors systematically exfiltrated thousands of Beast's confidential files, taking them outside the Company's corporate IT network and onto an unidentified device. Nabors then tried to cover these actions up by wiping his laptop, which had access to those files and records of his actions.

11. Nabors' attempts to cover his tracks, though, were unsuccessful. The "wipes" he did were incomplete, and Beast's forensic investigation, following Nabors' termination, was able to uncover both the dates of the attempted deletions, as well as some of the information he tried to conceal.

12. When Beast confronted Nabors about the information he had downloaded, he lied and claimed the files had been "wiped" on his last day of employment (which was demonstrably false—he had tried to "wipe" the files several days prior, *before* he was told he was being terminated, but *after* he admittedly "[saw] it coming.").

13. When pressed further, Nabors lied again. This time, he claimed that the mass download of Beast information was a routine "backup" he conducted in the "normal course of business." But Beast did not have a routine "backup" policy under which thousands of confidential documents would be mass downloaded to an unidentified external device. Nor did Nabors ever turn over (or identify the storage location of) this alleged "backup" to a Beast employee, belying any notion that his conduct was for Beast's benefit.

14. It was not even Nabors' responsibility to conduct such backups in the months leading up to his October 2024 termination, because Beast had removed him from his primary IT responsibilities as of December 2023.

15. Making matters worse, Beast subsequently learned that Nabors also had been "syncing" information to a personal DropBox account—one which he could access after leaving the Company, and to which Beast has no access. In other words, Nabors had set up a system for taking files outside of Beast's secure network and used it to upload thousands of Beast's most confidential files; as a result, he continues to have access to those files today.

16. The Company has repeatedly demanded that he return the information he stole. Nabors has refused and, in his most recent communication regarding the issue, claimed to be entirely unaware of *any* alleged "backups." To date, Nabors has not permitted an inspection of his DropBox account, and has not returned any of the information or documents he exfiltrated from

Beast. His conduct is a direct violation of his Agreement with Beast, which required that he return and not retain any Beast information after his employment ended.

17. This lawsuit follows.

## THE PARTIES

18. Beast is a limited liability corporation organized and existing under the laws of the State of North Carolina, having its principal place of business in Greenville, North Carolina.

19. Leroy Nabors is a natural person. Nabors' last known address is 4349 Glen Castle Way, Winterville, North Carolina, 28590. During his time at Beast, Nabors routinely interacted with Beast's operations throughout the state of North Carolina. Upon information and belief, Nabors also maintains a residence in Jonesboro, Texas.

## JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under the laws of the United States.

21. Venue is appropriate in this district pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to Beast's claims occurred in this district.

## FACTUAL ALLEGATIONS COMMON TO ALL CLAIMS

### A. Beast Is A Growing Media and Consumer Products Company That Creates Cutting-Edge Viral Social Media Content.

22. Beast was created in 2013 by Jimmy Donaldson when he was just 13 years old.

23. Donaldson grew up in Greenville, North Carolina. He attended high school in the area, where he was a baseball player prior to his graduation in 2016. He then briefly attended East Carolina University, before he elected to focus his time on growing Beast and its affiliated businesses.

24. In a little over a decade, Donaldson (better known by his internet moniker, MrBeast) has grown his internet enterprise to have the largest YouTube following in the world (with over 340 million subscribers), the third largest following on TikTok (with over 106.3 million

followers), over 63.6 million followers on Instagram, and over 31 million followers on X (formerly Twitter).

25. Beast's business strategy focuses on leveraging the algorithms underlying various social media channels (especially YouTube) to cause his content to go "viral." "Going viral" is an internet phenomenon in which a social media post quickly grows exponentially in popularity, being "liked," viewed, or otherwise shared by users such that it rapidly reaches other users in a very short period of time. As a particular piece of content goes viral, Beast's revenue (which is generated from sponsorships and ads shown along with Beast's content) grows. As one market observer noted, Beast's business model is "self-perpetuating. The more viral he becomes, the more brands want to work with him, and the bigger his own AdSense earnings get. He can then entice viewers with even bigger giveaway videos. It's a never-ending cycle."[2]

26. Beast has also diversified into other endeavors. For example, recently, Beast partnered with Amazon MGM Studios to create a reality TV show called Beast Games, in which contestants competed for significant cash prizes via competitions that paralleled those found in some of Beast's social media content.

27. Beast is also renowned for philanthropic endeavors, donating millions of dollars each year to various charities, including, by way of example, funding surgeries to restore sight for 1,000 blind individuals, funding massive food drives to provide millions of free meals, building wells in Africa to provide clean water to hundreds of thousands of people, and distributing millions of dollars' worth of free clothing to those in need around the world.

28. Across all endeavors, Beast employs roughly 350 people.

## B. Beast Takes Significant Efforts To Maintain The Confidentiality Of Its Competitively Sensitive Information.

29. Beast takes seriously the protection of its confidential and proprietary information. To that end, the Company requires that its workers and contractors agree to certain non-disclosure

[2] Alexander, Julia (December 28, 2018). "MrBeast, YouTube's viral philanthropist, explains where all that money comes from". *The Verge* (last visited March 27, 2025).

provisions when they are hired. In relevant part, those agreements require employees to keep confidential, not disclose, and, critically, return to the Company any and all confidential and proprietary information in their possession at the Company's request.

30. Beast also maintains stringent security measures to preserve the secrecy of its confidential information (including content, business plans, social media strategy, financials, and the like). This is particularly important in light of the considerable investment Beast has made in developing and curating its competitively valuable confidential and trade secret information, and the emphasis the market places on Beast's content being cutting edge and original.

31. Beast has, and at all times relevant to this matter had, written policies and procedures governing its information technology and the security of Company information. Beast's policies and procedures relate, *inter alia*, to computer controls, data access, IT disaster recovery, network security, user setup procedures, password administration and management, data backup, security audits, security breach investigations, email best practices, and mobile device security.

32. Beast limits access to confidential and trade secret information to certain employees, and stores its confidential and trade secret information electronically in a secure network system. Beast routinely audits user access to critical shared folders and each critical function stakeholder must approve the list of personnel with access. All Beast computers are protected from unauthorized access with individual user names and passwords, and passwords must be regularly changed. All Beast electronic applications require user authentication and have a session timeout mechanism in place.

33. Beast also restricts building access to areas containing sensitive information, and access to these areas requires proper door access that is only granted if an individual's job duties require access to these areas. Access to Beast's server rooms is limited to IT and facilities staff who have been granted access by the security team, and the list of people who have access is reviewed on a regular basis.

### C. Nabors Was Engaged As An IT Contractor For Several Months In 2023 and Thereafter Was Hired As An Employee To Perform Special Projects For The Development Team Until His Termination In October 2024.

34. Defendant Nabors was first engaged by Beast as a contractor in its IT department on July 11, 2023. Like all Beast personnel with access to confidential information, Nabors was required to execute a non-disclosure agreement. That agreement required, in relevant part, that "[u]pon the request of Company at any time or upon the termination of Employee's employment with the Company for any reason, Employee shall promptly (but in no event more than ten (10) days after written request of Company) deliver to the Company property as well as all records, manuals, articles, devices, equipment, customer lists, financial information, and other items which disclose or contain Proprietary or Confidential Information in any form, including all copies thereof, whether prepared by Employee, the Company or others." A true and correct copy of Nabors' executed non-disclosure agreement is attached here as **Exhibit B**.

35. In his role with Beast, Nabors initially was responsible for working on Beast's IT network, including working with the servers that housed post-production Beast content. Beginning in late 2023, Nabors' job responsibilities shifted away from IT. He was instead engaged as an employee, responsible for special projects for the Development Team in 2024, until his termination from employment.

36. Nabors' employment was terminated on October 1, 2024. During the termination meeting, Beast asked Nabors whether he had any Company information that he needed to return. Nabors represented that he had only "patch cords" and some "stuff" that he "found" to return. That day, Nabors returned his Company-issued laptop, which Beast later learned he had attempted to wipe and factory-reset four days prior.

37. At no point during the termination meeting did Nabors mention that he had downloaded thousands of documents onto another device in the weeks leading up to his termination. Likewise, he made no mention of uploading thousands of documents to a personal

DropBox account. Finally, at no point during this meeting was Nabors given permission to "wipe" his Company-issued devices. Instead, he was instructed to coordinate with Human Resources for their return, which he promised to do.

38. Following Nabors' termination and Beast's discovery of Nabors' illicit conduct, Beast took steps to sever ties with Vine.

**D. Beast's Post-Termination Review Of Nabors' Devices Showed That He Had Systematically Exfiltrated Thousands Of Beast's Confidential Files And Other Information In The Weeks Prior To His Termination And Then "Wiped" Those Devices.**

39. Following Nabors' termination, Beast conducted a review of his activity on the Company's systems to ensure that no Company confidential information was being improperly retained. The Company's initial review showed that, contrary to Nabors' representations during the termination meeting, he had downloaded more than one thousand Beast confidential files from the Company's Google Vault on September 23, 2024. The files downloaded included highly confidential information about business strategy, financial information, capitalization tables, financing documents, individual employee personal information, and other MrBeast intellectual property. *See also* **Exhibit A**. These documents are subject to the protective measures described *supra* for Beast's confidential information.

40. There was no legitimate business purpose for Nabors—initially an IT contractor responsible for post-production IT needs, and then an employee on the Development Team with no primary IT responsibilities—to even access (let alone download local copies of) this type of information, which had no relation to either of his roles. His access to, and download of, thousands of confidential Beast documents was well outside his scope of authority.

41. Beast was immediately concerned by these findings, showing exfiltration of the Company's confidential information, in violation of Nabors' non-disclosure agreement. Therefore, a member of Beast's Human Resources department confronted Nabors about the downloads on October 8, 2024. During that telephone call, Nabors claimed that the downloads were part of his

normal course of "backing up" the Company's information. This made no sense. Nabors was no longer responsible for Beast's general IT needs. Any "backups" he performed would have been well outside of his scope of authority and not in accordance with any Beast policy or practice. Nor did Nabors ever turn over (or identify the storage location of) any alleged "backup" to a Beast employee.

42. When pressed during the October 8, 2024 discussion to explain what he meant by these downloads being his "norm" of "backing up" information, Nabors changed his story, claiming he had downloaded the files for an "expansion" so he could "hand it over" to other Beast employees (no such "hand off" had ever been requested; nor did one ever occur). Critically, during the October 8, 2024 call, Nabors let slip what appears to have been his real motivation: he said he had a "hint" that his termination was coming and that was why he had taken certain actions on his computer.

43. The day of Nabors' termination, he returned a Company-issued laptop. The Company discovered that Nabors had tried to wipe the device by factory-resetting it, such that no information about his activity would remain on the device.

44. On October 8, 2024, the Company again demanded that Nabors return all Company information in his possession and confirm what he had improperly retained, this time through a formal demand from the Company's counsel at Paul Hastings LLP. The Company demanded he respond within 10 days, per the terms of the non-disclosure agreement that Nabors had executed. Nabors did not respond within the contractually mandated 10-day period.

45. On October 21, 2024, the Company again demanded return of all Company information via another letter from its counsel. Again, Nabors did not respond.

46. Meanwhile, Beast continued its investigation into his actions. As part of that process, Beast personnel found multiple hidden cameras located throughout Beast's offices.

47. No Beast employee recalls installing those cameras. Nabors, conversely, was well-known among colleagues to surreptitiously record meetings.

48. The cameras were subsequently taken down by Beast personnel. To date, Nabors has not provided Beast with access to the camera feeds, which—upon information and belief—are controlled by Nabors and/or Vine, the company owned by Nabors' daughter.

49. Beast personnel also found a mini-PC attached to Beast's Company server. This device had a single application installed on it: a program called "Synchro," an application that allows users to remotely access and control the network. A review of the mini-PC showed at least two separate logins by accounts affiliated with Nabors. At no point had Beast authorized or instructed Nabors to install this mini-PC or use it to access the Company's servers.

50. Nabors finally responded to Beast's requests that he comply with his contractual obligations through counsel on November 15, 2024. Nabors' counsel stated that "[a]ll MrBeast devices are in North Carolina" in Nabors' residence, and that Nabors "can facilitate someone being let into his home to return these devices." Importantly, Nabors also represented, through counsel, that "[h]e does not believe he has any MrBeast data, documents, or other information. As is standard practice, he wiped all of his laptops the same day he was terminated."[3]

51. Nabors' representations were false. First, Nabors wiped the laptop several days *prior* to his termination (just a few days after he had improperly downloaded Beast's confidential information), not on the day of his termination. Second, and more importantly: Beast discovered that Nabors' attempt to "wipe" the laptop was partially unsuccessful, such that Beast was able to see what Nabors had been using his laptop for in the days leading up to his termination. Beast found proof that Nabors had synced thousands of Beast confidential files to a personal cloud storage account with DropBox.

52. The files Nabors exfiltrated included (but were not limited to) financial data, sensitive memoranda regarding business transactions, and capitalization tables containing highly sensitive information about Beast's investors.

[3] In addition to wiping a laptop and desktop, Nabors factory-reset three Apple MacBooks, two Apple iPads, and one Apple Watch before returning them to the Company. Efforts to recover data from all six Apple devices were unsuccessful, and therefore, all Company data and confidential information stored on them has been lost forever.

53. Continued retention and potential disclosure by Nabors of these documents would inflict serious harm to Beast. For example, much of the financial data is in draft form. Misinterpretation of that data would cause significant confusion about Beast's business performance, undermining trust between Beast and its investors, customers, and the public. Disclosure of financial data in draft form could also hinder Beast's future fundraising efforts, because investors depend on accurate financial information to guide their decision-making.

54. Similarly, Beast's capitalization tables contain highly sensitive information about its investors and their equity stakes. Disclosure of this non-public data, without investors' consent, would infringe on those investors' privacy and destroy trust between Beast and its investors.

55. Disclosure of sensitive memoranda regarding Beast's business transactions, too, would jeopardize Beast's relationships with its vendors and other business partners, as well as disclose proprietary elements of Beast's business model. Disclosure of this information would, *inter alia*, reveal how Beast produces its uniquely successful videos, putting it at a dire competitive disadvantage.

56. Nabors had no legitimate business reason to access, use or retain such files, especially after December 2023, when he was stripped of his IT responsibilities and shifted to the Development Team. And, certainly, he had no reason for syncing those files to a personal DropBox account that existed outside of Beast's servers, and to which Beast does not have access, such that he could access them through DropBox even after trying to "wipe" his computer.

57. Beast, therefore, again confronted Nabors about his improper retention of Beast confidential information via his downloading of files and use of the personal DropBox account, which he at one point claimed were routine "backups."

58. To date, Nabors has not permitted an inspection of his DropBox account, which he admitted had synced thousands of Beast documents. He has refused to return Beast's confidential documents, and his counsel has ceased responding to counsel for Beast altogether.

59. On information and belief, Nabors continues to have access to the personal DropBox account to which he uploaded Beast files during his employment, in violation of his non-disclosure agreement.

**FIRST CAUSE OF ACTION**

**Misappropriation of Trade Secrets**

**Defend Trade Secrets Act, 18 U.S.C. § 1836 *et seq*.**

60. Beast incorporates the allegations contained in the above paragraphs of this Complaint as if fully set forth herein.

61. The documents and other data Nabors exfiltrated include trade secrets of Beast, including but not limited to business information that derives independent actual and potential commercial value from not being generally known or readily ascertainable by persons who can obtain economic value from its disclosure or use.

62. The documents and other data Nabors exfiltrated are the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

63. With neither express nor implied authority, Nabors misappropriated Beast's documents and other data by exfiltrating them to an unknown device and his personal Dropbox account.

64. Nabors knew, or should have known, that the thousands of Beast documents he exfiltrated, *en masse* and without authorization, included trade secrets of Beast.

65. Nabors' actions were intentional, willful, and malicious, and Beast is entitled to its actual damages and punitive and exemplary damages as a result.

**SECOND CAUSE OF ACTION**

**Misappropriation of Trade Secrets**

**N.C.G.S. § 66-152 *et seq*.**

66. Beast incorporates the allegations contained in the above paragraphs of this Complaint as if fully set forth herein.

67. The documents and other data Nabors exfiltrated include trade secrets of Beast, including but not limited to business information that derives independent actual and potential commercial value from not being generally known or readily ascertainable by persons who can obtain economic value from its disclosure or use.

68. The documents and other data Nabors exfiltrated are the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

69. With neither express nor implied authority, Nabors misappropriated Beast's documents and other data by exfiltrating them to an unknown device and his personal Dropbox account.

70. Nabors knew, or should have known, that the thousands of Beast documents he exfiltrated, *en masse* and without authorization, included trade secrets of Beast.

71. Nabors' actions were intentional, willful, and malicious, and Beast is entitled to punitive and exemplary damages and an award of its attorneys' fees as a result.

## THIRD CAUSE OF ACTION

### Breach of Contract

72. Beast incorporates the allegations contained in the above paragraphs of this Complaint as if fully set forth herein.

73. Nabors' non-disclosure agreement provided that he must not retain any Beast confidential information after his employment. It further provided that he was obligated to return any Beast information in his possession at the Company's demand.

74. The Company repeatedly demanded that Nabors return all Beast confidential information in his possession.

75. Nabors did not return the Beast confidential information in his possession, in breach of his contractual obligation to do so.

76. As a direct and proximate result of Nabors' breaches, Beast has sustained and will continue to sustain damages.

## FOURTH CAUSE OF ACTION

### Request for Permanent Injunction

77. Beast incorporates the allegations contained in the above paragraphs of this Complaint as if fully set forth herein.

78. Nabors improperly obtained and retained Beast confidential information, in violation of his non-disclosure agreement. He refuses to return that information.

79. The information in Nabors' possession includes (without limitation) confidential financial data, sensitive memoranda regarding business transactions, private employee compensation information, and capitalization tables containing highly sensitive information about Beast's investors.

80. If Nabors is not ordered to return the information he improperly has in his possession, Beast will be permanently and irreparably harmed.

81. For example, much of the financial data is in draft form. Misinterpretation of that data would cause significant confusion about Beast's business performance, undermining trust between Beast and its investors, customers, and the public. Disclosure of financial data in draft form could also hinder Beast's future fundraising efforts, because investors depend on accurate financial information to guide their decision-making.

82. Beast's capitalization tables contain highly sensitive information about its investors and their equity stakes. Disclosure of this data, without investors' consent, would infringe on those investors' privacy and destroy trust between Beast and its investors.

83. Disclosure of sensitive memoranda regarding Beast's business transactions, too, would jeopardize Beast's relationships with its vendors and other business partners, as well as disclose proprietary elements of Beast's business model. Disclosure of this information would, *inter alia*, reveal how Beast produces its uniquely successful videos, putting it at a dire competitive disadvantage.

## FIFTH CAUSE OF ACTION

### Conversion

84. Beast incorporates the allegations contained in the above paragraphs of this Complaint as if fully set forth herein.

85. Beast has an ownership interest in all the documents and other data Nabors exfiltrated.

86. Nabors wrongfully exfiltrated Beast's documents and other data and has refused to return them after multiple demands.

## SIXTH CAUSE OF ACTION

### Request for Declaratory Relief

87. Beast incorporates the allegations contained in the above paragraphs of this Complaint as if fully set forth herein.

88. Beast requests a declaration from this Court that it is entitled to the return, by Nabors, of all documents and other data he unlawfully exfiltrated from the Company.

## PRAYER FOR RELIEF

WHEREFORE, Beast prays for judgment against Nabors as follows:

A. Finding that Nabors is liable to Beast on all counts of this Complaint;

B. Damages from Nabors according to proof;

C. For permanent injunctive relief ordering the return of all Beast information improperly in his possession;

D. For punitive and exemplary damages as may be provided by law;

E. For Beast's attorneys' fees and costs as may be provided by law;

F. For prejudgment and post-judgment interest;

G. For such other relief as the Court may deem just and proper.

Dated: April 4, 2025

ROBINSON, BRADSHAW & HINSON, P.A.

/s/ Douglas M. Jarrell
Douglas M. Jarrell
N.C. State Bar No. 21138
djarrell@robinsonbradshaw.com
600 S. Tyron Street
Suite 2300
Charlotte, NC 28202
Telephone: (704) 377-8309
Facsimile: (704) 378-4000

PAUL HASTINGS LLP

JENNIFER S. BALDOCCHI*
jenniferbaldocchi@paulhastings.com
515 South Flower Street
Twenty-Fifth Floor
Los Angeles, CA 90071-2228
Telephone: (213) 683-6000
Facsimile: (213) 627-0705

EMILY R. PIDOT*
KAVEH DABASHI*
emilypidot@paulhastings.com
kavehdabashi@paulhastings.com
200 Park Avenue
New York, NY 10166
Telephone: (212) 318-6000
Facsimile: (212) 319-4090

BRIAN A. FEATHERSTUN*
brianfeatherstun@paulhastings.com
101 California Street
Forty-Eighth Floor
San Francisco, CA 94111
Telephone: (415) 856-7000
Facsimile: (415) 856-7100

*Attorneys for Plaintiff*
*MrBeastYouTube, LLC*

*Special appearance forthcoming