

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

BLINK HEALTH LTD.,

Plaintiff,

-against-

HIPPO TECHNOLOGIES LLC f/k/a
EVERYMED LLC,

Defendant.

Case No. 18 CV 2258

**COMPLAINT AND DEMAND
FOR JURY TRIAL**

Plaintiff Blink Health Ltd. (“Blink” or the “Company”), by its undersigned attorneys, hereby submits the following Complaint and Demand for Jury Trial against Defendant Hippo Technologies LLC, formerly known as Everymed LLC (“Defendant”), seeking relief for violations of the Defend Trade Secrets Act (18 U.S.C. § 1836 *et seq.*), misappropriation of trade secrets, unfair competition, tortious interference with contract, tortious interference with prospective business relations, unjust enrichment, and replevin as set forth below. Blink alleges on personal knowledge as to all facts known to it, and on information and belief as to all other facts, as follows:

SUMMARY OF THE ACTION

1. This is a case of corporate theft, greed, and corruption.
2. Plaintiff Blink is a pioneering healthcare technology company that has disrupted the complex industry of prescription-drug sales in order to provide medications to uninsured and underinsured Americans at affordable prices.
3. Defendant Hippo is a rogue and fraudulent enterprise that is trying to cheat its way into the market by outright thievery. Defendant is attempting to side-step the process of honest business development and competition on the merits, in favor of stealing and misusing

Blink's valuable trade secrets, and proactively seeking out and encouraging former Blink employees who had access to Blink's trade secrets and related confidential and/or proprietary information to violate their obligations to Blink and steal and continue to steal for the benefit of Defendant. Lacking any ingenuity of its own, Defendant's second-rate copycat competitor business appears to be premised entirely on a blatant and cynical misappropriation of all aspects of Blink's unique and proprietary business model, methods, processes, research, strategies, and technology, as described in detail below.

4. On information and belief, in furtherance of its unlawful copycat scheme, Defendant has committed numerous overt acts, including lying to potential investors who are being unwittingly swept up in Defendant's unlawful scheme; filing false intellectual-property applications; using a pirated marketing slogan; peddling a fake corporate narrative to consumers, the press, and others; and employing executives with a demonstrated history of fraud and dishonesty.

5. Defendant should be prevented from continuing to operate its illegal enterprise, and it should be required to pay damages both for the harm it has caused and to prevent future misconduct.

6. Plaintiff Blink is a trailblazing first-mover in the industry. It has devoted substantial resources to revolutionizing the U.S. prescription-drug market through its first-of-its-kind business model, which is founded on closely guarded confidential and/or proprietary information and trade secrets, including patent-pending methods and processes that streamline and automate highly complex billing and payment processes for prescription drugs. These trade secrets include Blink's confidential (i) innovative contracting structure, which establishes unique relationships with customers and a pharmacy benefit manager and allows for exceptional

leverage in negotiating prices up the supply chain on behalf of customers; (ii) patent-pending back-end process for approving the filling of pre-purchased prescription medications; (iii) back-end process for reconciling the payments the Company receives from customers with the prices of the medications customers actually pick up at pharmacies; (iv) source code, which facilitates the back-end prescription-filling and balance-billing processes, methods, and transactions required to create a seamless experience for the consumer; (v) print and digital marketing plans, strategies, and materials, including its detailed marketing playbook, contact lists, and underlying marketing and regulatory research contained in the data room to which select Hippo employees had access while at Blink; (vi) internal fraud-prevention strategies, rules, methods, and processes; (vii) business strategy documents, including product roadmaps, as embodied, for example, in investor and board of director presentations (collectively, the “Blink Trade Secrets” or “Trade Secrets”); and/or (viii) related confidential and/or proprietary information, including unpublished marketing slogans.

7. Copycat companies have long ripped off industry leaders to short-cut hard work. But it is not every case where the wrongdoers leave behind as many digital fingerprints and other evidence of their misconduct. Defendant here has left a long trail of incriminating evidence of its misdeeds.

8. As alleged below, for example, Defendant Hippo brazenly displayed on its website a unique identifying number belonging to Blink, and it is unabashedly using confidential marketing slogans crafted specifically for Blink in internal Blink documents.

9. On information and belief, Defendant knowingly obtained and illegally accessed Blink Trade Secrets and related confidential and/or proprietary information, and has used (and continues to use) that stolen property for its own benefit and in unfair competition with Blink at

thousands of “pharmacies nationwide.” On information and belief, Defendant improperly obtained these Blink Trade Secrets and related confidential and/or proprietary information by proactively seeking out and/or obtaining such information from at least five former executive and technical Blink employees, consultants, and an applicant with knowledge of and access to the Blink Trade Secrets, including Eugene Kakaulin, Charles Jacoby, Art Semyonov, Michael Tanenbaum, and Judith Trepanier (the “Five Insiders”), as well as Richard Muhlstock, an applicant for employment at Blink. On information and belief, in addition to inducing the Five Insiders to violate their contractual and other obligations to Blink not to misuse or disclose Blink Trade Secrets and related confidential and/or proprietary information, Defendant has, among other things, engaged in a corrupt, unlawful, pervasive, and ongoing scheme to induce current and former Blink employees to violate their own agreements and duties to Blink to extract additional Blink Trade Secrets and related confidential and/or proprietary information from them through deceitful means. Perhaps unsurprisingly, this is not the first time some of Hippo’s founders have robbed another company to try to get ahead.

10. Defendant was co-founded by two former Blink executives, Jacoby and Kakaulin, who had little relevant experience before Blink and who have a demonstrated track-record of fraudulent conduct that was concealed from Blink. Notably, Defendant continues to employ Jacoby despite his existing non-compete with Blink. Based on the knowledge Defendant’s employees and/or contractors gained while at Blink, Defendant, on information and belief, targeted its hiring efforts at others who had accessed, obtained, and/or created Blink Trade Secrets and related confidential and/or proprietary information, in order to obtain such information for Defendant’s own benefit. For example, on information and belief, Defendant engaged the services of a computer engineer named Art Semyonov, who, while serving as a

software-engineering consultant to Blink, had access to restricted databases with Blink's confidential and proprietary source code. Semyonov was granted such access under a strict non-disclosure agreement ("NDA") with the Company. Pursuant to his NDA, Semyonov obtained copies of Blink's confidential and proprietary source code, which automates Blink's core consumer experience and back-end prescription filling and payment reconciliation (balance-billing) processes. Despite his clear contractual obligation to do so, Semyonov never returned the code he obtained from his work at Blink, nor did he ever provide assurances to Blink that he permanently destroyed Blink's proprietary code. Instead, on information and belief, Defendant engaged Semyonov, and at least four other programmers connected to him through the professional social-media platform LinkedIn, in order to duplicate Blink's system. The lengths to which Defendant is willing to go to illegally use Blink Trade Secrets and related confidential and/or proprietary information and to unfairly compete against the Company know no bounds.

11. On December 7, 2017, Blink demanded in writing that Defendant immediately cease and desist from continuing its unlawful conduct. Ex. A. Ignoring Blink, Defendant instead publicly launched its business and website, which on information and belief are based on Blink Trade Secrets and derive from confidential and/or proprietary information Defendant knew were misappropriated by the Five Insiders. On information and belief, in the face of Blink's cease-and-desist demand, Defendant also doubled-down on its scheme to steal Blink Trade Secrets and related confidential and/or proprietary information and to target former Blink employees who had access to Blink's Trade Secrets to encourage them to violate their obligations to Blink and steal for the benefit of Defendant. Further, on information and belief, Defendant lied to prospective investors to raise capital by misrepresenting that it has created intellectual property which in fact has been ripped off from Blink.

12. The Company previously sought relief in New York state court against principally Jacoby and Kakaulin and also Defendant, but the individuals sought to delay and obstruct Blink's ability to have its day in court by seeking to arbitrate the individual claims against them. The Company voluntarily dismissed that action to ensure that each bad actor would be held responsible in the appropriate forum. Since the filing of the state court action, Defendant has officially launched its illegal product in the marketplace, using Blink Trade Secrets in interstate commerce, in violation of the Defend Trade Secrets Act ("DTSA").

13. Most recently, Defendant has continued its illegal scheme, including, on information and belief, by attempting to corrupt additional current and former Blink employees and a Blink job applicant by inducing them to steal or attempt to steal Blink Trade Secrets and related confidential and/or proprietary information. Defendant's continuing misconduct is causing ongoing and irreparable harm to Blink's business nationwide. Therefore, Blink seeks redress in this Court to hold Defendant publicly accountable under the DTSA for Defendant's blatant and intentional theft and misuse of stolen Blink Trade Secrets and for its unfair competition.

14. Blink brings this action to enjoin Defendant from (a) continuing its illegal use of stolen Blink Trade Secrets and related confidential and/or proprietary information, (b) unfairly competing against Blink, (c) tortiously interfering with Blink's contracts and business relationships, and (d) retaining copies of Blink Trade Secrets and related confidential and/or proprietary information. Blink also seeks to recover no less than \$50 million in damages already caused—and that continue to be caused—by Defendant's misconduct, punitive damages no less than \$200 million, attorney's fees for Defendant's willful and malicious misappropriation,

disgorgement of the ill-gotten gains Defendant has unjustly attained by its illegal acts, and/or reasonable royalties.

PARTIES

15. Blink is a Bermuda corporation with its principal place of business in New York, New York.

16. Defendant is limited liability company registered in Delaware on January 5, 2017.

JURISDICTION AND VENUE

17. This Court has subject-matter jurisdiction over Count 1 pursuant to 28 U.S.C. § 1331 and supplemental jurisdiction over Counts 2–7 pursuant to 28 U.S.C. § 1367.

18. This Court has personal jurisdiction over Defendant pursuant to Federal Rule of Civil Procedure 4(k)(1)(A) and N.Y. C.P.L.R. §§ 301, 302(a)(1)–(3).

19. Venue is proper in this Court by operation of 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to this action occurred in this District.

FACTUAL BACKGROUND

A. Blink’s Groundbreaking Business Model and Trade Secrets

20. Blink is a consumer-focused healthcare technology company that serves uninsured and underinsured patients in need of prescription medications. The Company is led by three pharmaceutical sales and technology entrepreneurs: Geoffrey Chaiken, the Chief Executive Officer; Matthew Chaiken, the Chief Operating Officer; and William Doyle, the Executive Chairman. The Company’s mission is to ensure that all Americans have access to affordable prescription medications at all pharmacies nationwide.

21. Blink obtains for its customers unparalleled access to negotiated prices on more than 15,000 medications and handles the entire payment process in advance of a customer’s trip to the pharmacy. Customers purchase prescription medications using Blink’s free website and

mobile applications and then can pick them up at most pharmacies throughout the United States by showing a dynamic-benefits “Blink Card.” Unlike existing insurance cards or manufacturer coupons, the Blink Card is enabled by Blink’s unique contracting structure and operates in conjunction with a patent-pending technology that ensures customers have a successful experience at the pharmacy.

22. Blink’s revolutionary product and technology, and their underlying processes and methods, which are the result of years of intense market research and trial and error, are aimed at solving the specific needs of several different populations in the U.S. prescription medication supply chain. First and foremost, Blink provides ease of access and true price transparency to consumers: customers pay lower prices for prescription medications negotiated at scale, they receive additional discounts made possible by Blink’s relationships with entities such as pharmaceutical manufacturers and nonprofit healthcare organizations, and they experience a virtually seamless process for purchasing their prescription medications. Additionally, Blink’s contracting structure is valuable, among other things, because it provides the pharmacy benefit manager with greater flexibility to contract with a partner whose unique structure facilitates better information flow to patients. Likewise, doctors benefit from Blink’s technology and product by being able to see Blink’s guaranteed prices before writing a prescription. Finally, branded-drug manufacturers gain access, through Blink, to customers and the ability to provide targeted benefits to them rather than through their insurance companies or employers, as is currently done.

23. The Blink Card system is built on proprietary confidential processes and technology that are embodied in confidential source code developed at significant expense and written by numerous Blink software engineers subject to strict NDAs with the Company.

24. Blink was the first to develop and operationalize this groundbreaking prescription-medication e-commerce system, and it has closely guarded its underlying Trade Secrets and related confidential and/or proprietary information, including by filing confidential patent applications and by taking consistent measures to protect the secrecy of such information, such as requiring its employees and third parties to sign strict NDAs. Since Blink announced its market entry in early 2016, nobody unaffiliated with Blink has been able to replicate or reverse-engineer Blink's patent-pending prescription savings platform. Leading industry experts (including some of the largest pharmacy benefit managers, which act as intermediaries between patients and pharmacies in the sale and distribution of drugs), when exposed to select aspects of Blink's inner workings on a need-to-know basis and under strict NDAs, have been surprised by the unique structure and processes innovated by Blink to execute its mission. And, as alleged below on information and belief, Defendant has only been able to replicate Blink's innovative business model by using Trade Secrets that it knew were misappropriated from the Company.

25. The Company's one-of-a-kind business model and technology to lower drug prices nationwide are based on at least seven categories of Trade Secrets and related confidential and/or proprietary information.

26. **Contracting Structure:** Blink's innovative contracting structure establishes unique relationships with a pharmacy benefit manager and customers throughout the United States, allows for exceptional leverage in negotiating prices up the supply chain on behalf of customers, facilitates information sharing and provides true price transparency for doctors and patients, often results in cheaper prescriptions for customers, and is core to Blink's business model. The Company has invested millions of dollars in researching, designing, and developing this structure. The details of Blink's contractual relationships are confidential to Blink and each

of the pharmacy industry participant third parties with whom it contracts—all of whom are subject to confidentiality provisions in those contracts. Designing and proving the efficacy of this exceptional contracting structure also was a critical step in attracting investors and business partners, and knowledge of its details would be invaluable to a competitor like Defendant.

27. **Authorization Process:** Blink’s patent-pending back-end process for funding and approving the filling of pre-purchased prescription medications (the “Authorization Process”) gives the Blink Card system an unparalleled competitive advantage over alternative options such as insurance co-pays or coupon cards. The Authorization Process is described at a high level in two confidential patent applications seeking nationwide protection, as well as in the source code described below.

28. **Balance-Billing Process:** Blink’s back-end process for reconciling the payments the Company receives from customers with the payments it makes to pharmacies (the “Balance-Billing Process”) ensures billing accuracy and corrects for user error. The Balance-Billing Process is described at a high level in an unpublished provisional patent application that Blink allowed to lapse in order to protect the secrecy of the technology from eventual publication. Jacoby was directly involved in Blink’s decision to refrain from filing the application in order to keep its contents confidential.

29. **Source Code:** Blink’s source code facilitates the back-end prescription-filling and balance-billing processes, methods, and transactions required to create a seamless experience for consumers nationwide. The source code performs novel instructions and carries out specified functions using a unique combination of data fields, data sets, and processes that collectively have never been used to manage pharmacy benefits and accomplish pharmaceutical transaction and payment processing and reconciliation in the manner executed by Blink. Furthermore,

individual elements of the processes created by Blink have not been used in the industry in the manner in which Blink uses them for these processes.

30. **Marketing Plans:** Blink's print and digital marketing plans, strategies, and materials enable Blink to efficiently inform patients about significant discounts on medications, and, in some cases, to offer free pharmaceuticals in a manner that has never been done before in the industry. This is facilitated in part by Blink's unique marketing strategies and materials including its step-by-step guide to direct mail operations and plans (including materials for distribution in doctors' offices), digital marketing strategies, email and mail lists, and extensive market research, as well as healthcare regulatory-compliance research—all of which was created at significant cost to Blink. Without the confidential inside knowledge that Blink learned through trial and error and its experience in the market, such material and insight could not be replicated.

31. **Fraud-Prevention Strategies:** Blink's internal fraud-prevention strategies, rules, methods, and processes, developed by the Company, with Kakaulin's involvement subject to an NDA and the Company's standard invention-assignment agreement, at significant expense through trial and error in the course of its operations screen for and prevent potential fraud on its system and serve to significantly mitigate the Company's exposure to financial risk.

32. **Business Strategy Documents, Including Product Roadmaps:** Blink's confidential business strategy, embodied in investor and board of director presentations, includes forward looking plans, contemplated product enhancements and new features (including product roadmaps), growth strategy discussions, and analyses of strategic opportunities, as well as descriptions of successes, challenges, key metrics, U.S. market analyses, user feedback, financial data and key performance indicators that inform the Company's strategies and plans and are

internal to the Company. Blink's confidential internal product roadmap is embodied in an evolving set of strategy documents created and added to over time based on trial and error in the marketplace. The roadmap documents outline and track the progress of the company's potential and future (both short- and long-term) product plans and technologies; programs for consumers, doctors, and administrators; deals throughout the United States; and features of Blink's backend systems. The product roadmap documents include shared confidential internal documents created to advance the envisioned projects and are valuable because they could permit a potential competitor to launch products, plans, and/or deals that Blink has in the pipeline in advance of Blink's anticipated schedule and beat Blink to market without requiring a competitor to invest the resources that Blink has expended to create these plans. The information contained in the investor and board of director presentations, including the confidential product strategies internal to Blink, would be invaluable to any third party seeking to compete with Blink, because it would provide any competitor years of market research, product experimentation, and trial and error, collection of user feedback, analysis, and strategic insights. This information cannot be reverse-engineered because it only can be learned through the planning, research, trial and error, and analysis that results from observing the internal operations and being privy to the internal data and metrics of Blink's business.

33. Since officially launching in February 2016, Blink has grown rapidly and now provides hundreds of thousands of customers nationwide with access to lifesaving and/or life-changing prescription medications, including many of those that customers previously could not afford. Many of Blink's customers lack prescription drug insurance coverage or cannot afford their medications with the coverage they do have. Publicly available data show that more than 40% of Americans previously reported skipping doses or entire prescriptions because of costs.

Prior to Blink's launch, consumers could not pre-purchase prescription medications at guaranteed prices online and pick them up at local pharmacies. Existing consumer options, such as coupons, only approximated the price customers would pay at the pharmacy counter. Not surprisingly, roughly 30% of prescriptions were abandoned at the POS because of the "sticker shock" experienced by customers when they first learned the price of their prescription. Now, instead of being forced to forgo critical medications because of their financial status or lack of insurance coverage, Blink's customers can secure pricing before going to the pharmacy and access their prescriptions at substantially lower prices. Customers have reported that Blink is essential to providing them access to necessary medications at a time when drug prices are rapidly increasing.

34. In the more than two years that Blink has been innovating in the prescription-medications market, no competitor has come close to replicating the groundbreaking Blink Card system, including its Authorization Process and Balance-Billing Process. On information and belief, Defendant only gained a toehold in the market by procuring and using Blink Trade Secrets and related proprietary and/or confidential proprietary information it knew were stolen from the Company.

B. Blink Has Taken Consistent and Unambiguous Efforts to Maintain the Secrecy and Value of Its Trade Secrets

35. Since its inception, Blink has undertaken significant efforts to maintain the confidentiality and value of its Trade Secrets and other proprietary information. For example, since 2016, the Company has implemented a policy for the classification and handling of information, including Trade Secrets. Pursuant to that policy, source code and documents classified as Sensitive Business Information—i.e., "Information about Blink Health's plans, finances or procedures, or any other proprietary information that would cause great damage to

the company were it to be disclosed to unauthorized parties”—should only be shared on a “need-to-know basis” and must be protected from disclosure to unauthorized third parties through the use, for example, of encrypted file transfers and third-party NDAs.

36. Blink’s employee handbook also plainly puts its employees on notice of what information the Company considers to be confidential and how that information should be protected. It provides a non-exhaustive illustrative list of “confidential information,” including “business plans, strategies, budgets, projections, forecasts, financial and operating information, business contracts, databases, financial and account numbers, HIPAA protected medical information, customer and vendor information, advertising and marketing plans, proposals, training materials and methods, and other information not available to the public.” The handbook further explains that (a) “it is each employee’s responsibility to keep Confidential Information in confidence”; (b) employees “must not use, reveal, or divulge any such information unless it is necessary . . . to do so in the performance of your duties”; (c) confidential information should be provided only on a “need-to-know basis and must be authorized by [a] manager”; and (d) employees must protect the secrecy of confidential information regardless of whether or not it is specifically marked as confidential.

37. Blink also consistently enters into NDAs with investors, employees, and consultants prohibiting counterparties from making any unauthorized disclosures of confidential information, defined as “valuable proprietary and confidential information concerning [the Company’s] business, business relationships and financial affairs,” and from using confidential information for their own or another’s benefit. These NDAs provide extensive, non-exhaustive illustrations of what may constitute confidential information, including “trade secrets, technical information, know-how, research and development activities of the Company, product, service

and marketing plans” and “customer and supplier information”—much of the information squarely at issue here. The NDAs explain that confidential information may be contained in various media, including “patent applications, computer programs in object and/or source code” and “supplier and customer lists”—again, some of the precise Blink Trade Secrets and related confidential and/or proprietary information at issue here. The NDAs require counterparties to “protect the integrity and confidentiality” of confidential information and to return any such information to the Company upon the termination of their engagement with the Company. They also include defined periods of non-competition and non-solicitation of customers or employees. The Company (or its predecessor-in-interest Vital Matters LLC) entered into substantially similar NDAs containing the above-referenced terms with, among others, Eugene Kakaulin, Charles Jacoby, Art Semyonov, Michael Tanenbaum, and Judith Trepanier, which NDAs govern the access, use, and disclosure of Blink Trade Secrets and confidential and/or proprietary information by these individuals. Further, access to Blink’s Trade Secrets was at all relevant times limited by password protection.

38. In addition to the standard-form NDAs entered into in connection with employment or consulting work, Blink also enters into project-specific NDAs with employees staffed on particular matters. Such NDAs remind employees that, in the course of such projects, participating employees may come into contact with confidential and proprietary information. These project-specific NDAs reiterate the terms of the general employment NDAs and further prohibit disclosure of project-specific confidential information “outside the designated project working group.”

39. In yet another effort to protect Blink Trade Secrets and related proprietary and/or confidential information, the Company conspicuously marks as confidential any investor-facing informational materials containing such information.

40. The Company further protects Trade Secrets by entering into NDAs with anyone seeking access to its proprietary information—regardless of whether it is confidential. NDA counterparties include applicants for employment, prospective investors, investors, and outside vendors—all of whom are required to execute such agreements before receiving access to proprietary information. The Company’s NDA with Richard Muhlstock, an applicant for employment as Chief Marketing Officer, refers to “Proprietary Information” in light of Muhlstock’s limited access to only such information necessary to conduct the interview.

C. Defendant Knowingly Obtained Stolen Trade Secrets from Former Blink Employees, Consultants, and Applicants

41. Defendant formally put its malicious and unlawful scheme to replicate and unfairly compete with Blink into action at some point during early 2017.

42. Armed with the knowledge that Blink’s wildly successful business was built upon years of research and development of confidential business processes, Defendant began proactively seeking to hire former Blink employees with intimate knowledge and possession of those Blink Trade Secrets and related confidential and/or proprietary information in order to help create a second-rate copycat of Blink. The role of each of the co-conspirators is detailed below:

Defendant’s Co-Founders, Former Blink General Counsel Charles Jacoby and Former Blink CFO Eugene Kakaulin, Stole Blink Trade Secrets and Attempted to Blackmail Blink

43. On information and belief, Defendant began employing Jacoby and Kakaulin for the specific purpose of obtaining Blink Trade Secrets and related confidential and/or proprietary information they had accessed and possessed in connection with their work for Blink.

44. Jacoby was Blink's General Counsel from July 2014 until August 2016.¹ In that role, he was responsible for managing all legal matters and legal analyses for the Company. He also was charged with controlling access to and ensuring the protection of all of Blink's confidential and proprietary information, including its Trade Secrets, and managing the Company's intellectual property portfolio, including confidential patent applications such as those for the Authorization Process. In addition to his contractual duties under his employment agreement and NDA, as the Company's attorney, Jacoby owed Blink various duties described by the New York Rules of Professional Conduct, including the general duty to refrain from "knowingly reveal[ing] confidential information . . . or us[ing] such information to the disadvantage of a client or for the advantage of the lawyer or a third person." N.Y. Rules of Prof'l Conduct r. 1.6. Even today, Jacoby remains duty-bound not to reveal confidential information of his former client Blink or use such information to Blink's disadvantage. *See id.* r. 1.9(c).

45. Jacoby also was involved in the management of the Company's legal disputes and its compliance program, which included implementing policies and procedures, responding to policy concerns raised by the workforce, and managing the process for Blink's financings. In the course of his responsibilities as General Counsel, Jacoby regularly accessed highly confidential and competitively sensitive information of the Company, including documents protected by the attorney-client privilege and work-product doctrine. Indeed, it is difficult to conceive of sensitive information within the Company to which Jacoby was *not* exposed, given the trust and confidence the Company (regrettably) placed in him.

¹ After August 2016 until his departure from the Company, Jacoby served as Deputy General Counsel.

46. Kakaulin was Blink's Vice President and Chief Financial Officer from September 2015 to July 2016. In that role, Kakaulin was responsible for overseeing all financial matters for the Company. He also was regularly involved in Blink's short- and long-term strategy discussions, was involved in creating Blink's fraud-prevention strategies, and had access to and received updates regarding the Company's confidential internal product roadmap. As an officer of Blink, Kakaulin was responsible for managing the company's data room, which included documentation of the Company's most valuable and secret information.

47. In recognition of the highly confidential nature of the information with which they would (and did) come into contact, Jacoby and Kakaulin each entered into an NDA with the Company. They each expressly promised, during the terms of their employment and thereafter, to use Blink's confidential information, including Trade Secrets, only in the performance of their duties for the Company and not for their own benefit or the benefit of any other person or business entity. They also expressly promised not to use or disclose to any third party any confidential information or trade secrets, including Blink Trade Secrets to which they had access. Jacoby and Kakaulin were well aware of their legal obligations regarding the sensitivity and proprietary nature of that information. Pursuant to their respective NDAs, their non-disclosure and non-use obligations continue in force and remain binding. Moreover, Kakaulin's non-compete agreement ran through July 2017, and Jacoby's remains enforceable through April 2018.

48. In their roles at the Company and subject to their NDAs, Jacoby and Kakaulin had access to various aspects of Blink's proprietary and highly confidential business model, including Blink Trade Secrets and related confidential and/or proprietary information. For example, Jacoby and Kakaulin had access to documents embodying and describing Blink's

confidential contractual relationships with other key players in the pharmaceutical industry and the Company's confidential efforts to secure financing and capital investments, as reflected in Blink presentations to investors and the board of directors.

49. Given their inexperience in the industry, Jacoby and Kakaulin required extensive support from other Company employees in order to understand the mechanics of such relationships. Such support included, for example, in the case of Kakaulin, providing him with a cheat-sheet-type summary of a relevant third-party contract and correcting his misinterpretations of Blink's e-commerce data.

50. On information and belief, Defendant Hippo Technologies LLC, which was co-founded by Jacoby and Kakaulin, is premised entirely on the illegal copying of Blink's innovative confidential and proprietary business model.

51. For example, forensic analyses have revealed that Jacoby improperly accessed and, on information and belief, transferred to his personal email account (a) confidential Blink files relating to a dispute with a third-party investor named Michael Karsch, who was represented by an attorney who has also represented both Jacoby and Kakaulin, and (b) personal digital communications belonging to Geoffrey Chaiken. Importantly, Jacoby was only granted access to these files in the first instance in his capacity as Blink's General Counsel.

Astonishingly, some of the confidential information and personal communications Jacoby accessed in the course of his work as Blink's General Counsel were incorporated into Karsch's later federal complaint against Blink. *See Karsch v. Blink Health Ltd.*, No. 17-cv-3880 (VM) (S.D.N.Y. filed May 23, 2017).

52. In a shocking attempt to cover his tracks, Jacoby erased or corrupted the hard drives of his Blink-issued laptops before returning them upon his separation from the Company.

Crucially, a forensic analysis of the laptops showed that Jacoby's laptop was wiped after Blink had served Jacoby with document-retention notices. Indeed, in a transparent effort to delay Blink from discovering that he had destroyed evidence of his crimes, Jacoby, through his lawyer, continually represented to Blink that he was preserving documents pursuant to his legal obligations. These deceitful acts are evidence of the extent to which a founding member of Defendant would go to harm Blink for the benefit of Defendant.

53. After threatening to use the personal communications he stole as blackmail to extort the Company out of a salary increase and additional equity, Jacoby was placed on administrative leave on or about October 7, 2016.

54. On February 5, 2017, Jacoby and Blink entered into an agreement to settle their dispute over Jacoby's termination and mutually release any claims arising before that date. The agreement does not purport to release claims arising after February 5, 2017.

55. Shockingly, just two months later, on April 19, 2017, Defendant filed two applications with the U.S. Patent and Trademark office to trademark the name "Hippo." Revealingly, "Hippo" was described as a web-based platform to provide information relating to "insurance coverage and pricing of prescription medications, enabling customers to manage prescriptions and choose pharmacies based on cost and other factors, and payment processing for retail and mail order prescriptions." On information and belief, this trademark application—undoubtedly filed at the direction of Jacoby—relates to Defendant's second-rate copycat venture based on Blink Trade Secrets and related confidential and/or proprietary information.

56. Kakaulin, for his part, has a history of stealing trade secrets to launch copycat competitors. In 2013, Kakaulin co-founded a company premised entirely on marketing and selling knockoffs of Nespresso-brand disposable coffee pods. Kakaulin and his company refused

to comply with Nespresso's cease-and-desist demands, so Nespresso filed an action against the company in this District, alleging unfair competition in addition to various trademark and copyright violations. *See generally Nespresso USA, Inc. v. HiLine Coffee Co.*, No. 14-cv-3292 (SHS) (S.D.N.Y. filed May 6, 2014). Kakaulin conspicuously failed to disclose this lawsuit to Blink when he was hired, and Blink's diligence did not uncover it, because only his company was a named defendant, not Kakaulin personally. Blink would never have hired Kakaulin as Chief Financial Officer if he had disclosed that he had recently been sued for blatantly misappropriating a competitor's intellectual property. In another shameless example of Kakaulin's duplicity, even after his departure from Blink, Kakaulin falsely held himself out as Blink's CFO in order to meet with a former employee of another company in the industry, who was seeking employment with Blink, in order to learn that company's confidential proprietary processes, which, on information and belief, Kakaulin subsequently gave to Defendant to brazenly incorporate into its own copycat product.

57. On January 31, 2017, Kakaulin and Blink entered into an agreement to settle their dispute over Kakaulin's July 2016 departure from the company and to mutually release any claims arising before the execution of that agreement. The agreement does not purport to release claims arising after January 31, 2017.

58. Blink may exercise its rights to pursue claims against Jacoby and Kakaulin in their individual capacities in due course. In this action, Blink is not asserting any claims covered by any arbitration agreements.

Defendant Engaged Former Blink Software-Engineering Contractor Art Semyonov to Repurpose Stolen Blink Source Code

59. In August 2015, the Company engaged Art Semyonov as a contractor to perform software-engineering services subject to a consulting agreement incorporating an NDA. As part

of his job functions, Semyonov had access to certain Blink Trade Secrets and related confidential and/or proprietary information, including source code to facilitate the Company's software processes, such as the Authorization Process and Balance-Billing Process.

60. On information and belief, Defendant hired Semyonov in order to replicate Blink's source code. Although Semyonov appears to have concealed public descriptions of his work for Defendant, at least four other software engineers who hold themselves out as employees of Defendant are all connected to Semyonov on the professional social-media platform LinkedIn. On information and belief, the networking arrangement between these five engineers would not have occurred without Semyonov's involvement in the Hippo venture.

61. It is implausible that a software engineer such as Semyonov could write source code for Defendant—which Jacoby has described to investors as a “clone” of Blink, with the same functionality—that is anything other than a blatant rip-off of Blink Trade Secrets and related confidential and/or proprietary information, including Blink's source code. On information and belief, by, among other things, engaging the same software engineer who worked on Blink's proprietary confidential source code to design the copycat Hippo system, Defendant has knowingly and willfully misappropriated Trade Secrets and induced Semyonov to breach his own contractual non-disclosure and confidentiality obligations to Blink.

Defendant Recruited Former Blink Deputy Chief of Staff Michael Tanenbaum to Disclose Stolen Blink Trade Secrets

62. Blink employed Michael Tanenbaum as Deputy Chief of Staff from September 2015 to in or around June 2016, subject to an employment agreement incorporating an NDA that includes the confidentiality and non-compete language described above. In connection with his job responsibilities, which included supporting the Company's strategic initiatives, Tanenbaum had access to certain Blink Trade Secrets and related confidential and/or proprietary information,

including but not limited to marketing materials, business plans, and product roadmap documents.

63. On information and belief, Defendant specifically hired Tanenbaum in an effort to obtain his knowledge of Blink Trade Secrets and related confidential and/or proprietary information, in furtherance of Defendant's malicious scheme to plunder Blink's business through improper means.

Defendant Enlisted Former Blink Chief of Staff Judith Trepanier to Steal Blink's Comprehensive Marketing Playbook

64. In September 2015, Blink engaged Judith Trepanier as a consultant to perform marketing, distribution, and business-development services and then employed her from January 2016 to August 2017. After Trepanier was unsuccessful in business development, the Company repositioned her to a role supporting the head of direct-mail marketing, who had more than 35 years of experience. Trepanier's consulting services for and employment by the Company were both subject to NDAs to protect the Company's Trade Secrets and related confidential and/or proprietary information to which Trepanier had access in order to perform her responsibilities.

65. Trepanier's responsibilities included supporting the Company's strategic initiatives, including coordinating print marketing activities pursuant to the Marketing Playbook, which describes, among other things, Blink Trade Secrets and related confidential and/or proprietary information, including the Company's processes and strategies for maximizing the effectiveness and minimizing the cost of print-marketing campaigns around the country.

66. On information and belief, Defendant enlisted Trepanier in its brazen and continuing effort to obtain Blink's Trade Secrets and related confidential and/or proprietary information through deceptive means. As described further below, on February 14, 2018, Trepanier attempted to trick a current Blink employee into giving her a copy of the Marketing

Playbook, and she even instructed him to provide it in hard-copy (*i.e.*, a non-forensically traceable) format. The Marketing Playbook would only be helpful—and indeed, extremely valuable—to a company operating in the U.S. retail prescription-drugs industry. Trepanier’s efforts to obtain the Marketing Playbook underscore its value and the fact that it cannot be reverse-engineered.

Defendant Mobilized Candidate for Blink Chief Marketing Officer Richard Muhlstock to Procure Blink Proprietary Information

67. On information and belief, Richard Muhlstock entered the Blink offices in or around April 2017 as an agent of Defendant under the guise of seeking a job with Blink. At that time, Muhlstock entered into an NDA with Blink in connection with his application and interview for the position of Chief Marketing Officer. In his NDA, executed on April 25, 2017, Muhlstock agreed to “hold in confidence and [not to] possess or use (except as required to evaluate the proposed business relationship within the U.S.) or disclose any Proprietary Information.” The NDA defines Proprietary Information as “business, technical or other information, materials and/or ideas.” This NDA governs Muhlstock’s access, use, and disclosure of Blink Proprietary Information

68. In the course of Muhlstock’s interview and subject to the terms of Muhlstock’s NDA, Muhlstock received access to select Proprietary Information, including general information about Blink’s primary sources of customer acquisition and high-level outreach efforts made by Blink to healthcare providers. On information and belief, Muhlstock deceived Blink into disclosing this information, which Blink otherwise only would have done for the specific purpose of probing a genuine candidate’s qualifications for the job and testing the candidates’ ability to “think on his/her feet.”

69. To protect its Trade Secrets and related confidential and/or proprietary information, Blink only disclosed to Muhlstock this limited Proprietary Information, which was necessary to conduct his interview for the role of Chief Marketing Officer.

70. Ultimately, Blink did not hire Muhlstock as Chief Marketing Officer.

71. On the professional social-media site LinkedIn, Muhlstock holds himself out as Defendant's Chief Marketing Officer, a position he claims to have held since October 2017.

72. On information and belief, Defendant knowingly obtained Blink's Proprietary Information from Muhlstock and induced him to breach his contractual obligations to Blink under his NDA to maintain such information in confidence.

73. On information and belief, Defendant targeted and hired some, if not most, of the Five Insiders for the very purpose of obtaining Blink Trade Secrets and/or related confidential and/or proprietary information to which these individuals had access and were contractually and/or otherwise bound to maintain as confidential. Further, on information and belief, Defendant instructed one or more of the Five Insiders to impersonate Blink employees for the purpose of meeting with third parties.

D. Defendant was Caught Red-Handed Knowingly Using—and Continues to Use—Stolen Blink Trade Secrets and Blink Proprietary Information

74. Defendant's entire venture is an illegal copycat business with no legitimate grounds for existence.

75. On information and belief, Defendant used and continues to use Blink Trade Secrets and related confidential and/or proprietary information in every aspect of its copycat enterprise. On information and belief, Defendant knows this information was improperly retained and/or provided to Defendant by former Blink employees and contractors who now work for or assist Defendant in its illicit scheme to plunder Blink.

76. **Confidential Marketing Information:** Despite whatever efforts it may have taken to cover its tracks, Defendant’s own slavish copying betrayed its illegal conduct. For example, Defendant brazenly stole Blink’s proprietary material—including text for online “Frequently Asked Questions” and Blink slogans that were created but never publicly used. Defendant’s primary company slogan is “Save Money. Fill Better.” But that slogan was drafted by a copywriter retained by Blink during early marketing strategy sessions. It appears as a proposed slogan in a number of internal Blink presentations and documents to which Jacoby was exposed. Blink did not ultimately choose that slogan to use in its own public marketing, but it remains Blink’s intellectual property. Defendant has stolen the slogan for use in a sham trademark application it filed and on its cheap imitation website.

77. **Business Model, Contracting Structure, and Authorization Process:** Defendant’s entire business model is a rip-off of Blink’s proprietary system, including its unique contracting structure and patent-pending Authorization Process: customers join for free, Defendant claims to negotiate low prices for prescription medications, customers purchase medication directly from Defendant over a website or mobile application, and customers then pick up that pre-paid authorized medication from a contracting pharmacy by showing a “Hippo card.”

78. **Blink’s BIN and Portions of Blink’s Confidential Patent Application Regarding the Authorization Process:** In its apparent haste to portray itself as a legitimate business to the outside world, Defendant carelessly pirated the unique National Council for Prescription Drug Programs Processor Identification Number (“BIN”) used by Blink with a pharmacy benefit manager and used it in a version of its copycat “Hippo card” that appeared in Defendant’s website. Specifically, as of December 29, 2017, the BIN shown on the sample

“Hippo card” displayed on the homepage of Defendant’s website was “018050,” **Blink’s own unique BIN** used with a pharmacy benefit manager. (This BIN has since been edited, as Defendant apparently learned to better cover its tracks.) This conclusively demonstrates that Defendant possessed and used Blink material in the course of establishing its directly competing enterprise. In fact, it appears that the screenshots on the Hippo website are shameless copies of portions of a confidential Blink patent filing, which describes the Authorization Process at a high level, that Jacoby managed and had access to.

79. **Balance-Billing:** One of the key aspects of Blink’s proprietary technology is the Balance-Billing Process, a system by which the initial, paid-in-advance purchase price of a prescription medication may be adjusted after the patient picks up the medication at the pharmacy based on a number of factors. The precise methodology for this system is a closely guarded proprietary Trade Secret to which both Jacoby and Kakaulin had access in the course of their employment at Blink.

80. Despite Blink’s consistently maintaining the secrecy of the back-end processes that enable Balance-Billing for years, Defendant appears to have adopted the Balance-Billing Process as its own. For example, on the “Charges and Payments” page of Defendant’s website, in response to the “Frequently Asked Question” “Why did you charge me less than I originally paid?” Defendant explains, “The information you entered was not an exact match with the prescription sent by your doctor. Because the cost of the medication prescribed by your doctor was less than the price of the medication you paid for in the Hippo app, we issued you a refund.” In response to the question “Why did you charge me more than I originally paid?” Defendant responds, in part, “You might have been charged an additional amount for your medication if the specific medication you purchased in the Hippo app was different from what your doctor

prescribed you. In order for your prescription to get filled, we might have charged you slightly more than your original price.” These explanations strongly suggest that Defendant has copied Blink’s Balance-Billing Process step by step.

81. As Jacoby is well aware, by virtue of his role as legal counsel for Blink, the Company filed confidential patent applications relating to some of the above-described proprietary and innovative intellectual property. Those patent applications were not filed publicly, a decision in which Jacoby himself was involved, and in the interim Blink continues to aggressively protect this information as Trade Secrets. Additionally, Blink continues to safeguard related information not described in the patent applications, such as specific processes used to enable the Balance-Billing Process and data choices made to inform those processes, as confidential. There is therefore no legitimate means by which Defendant could have gained access to this information other than by obtaining stolen Blink Trade Secrets.

82. Defendant’s unabashed copying of Blink’s patent-pending and other confidential technologies is particularly egregious considering the continuing professional duty Defendant’s co-founder Jacoby owes his former client Blink to keep the content of Blink’s nonpublic patent applications confidential and refrain from using confidential client information for his own or another’s benefit.

83. **Investor Presentations Reveal Hippo Is a “Clone”:** As if the flagrant copying of Blink’s business model, marketing information, BIN, patent applications, and confidential processes were not enough, Defendant’s employees also shamelessly have marketed Defendant by express reference to Blink. On information and belief, Jacoby has described Defendant in discussions with potential contracting partners as a “clone” of Blink.

84. On information and belief, Defendant has presented to venture capital firms considering investments in it, during which its employees, including Jacoby and Kakaulin, shared Blink's Trade Secrets and other confidential proprietary information under the guise of describing Defendant's business plan. On information and belief, some of the investors whom Defendant has tried to entice include those with whom Blink purposely did not meet in an effort to limit disclosure and protect the confidentiality of its Trade Secrets and related confidential and/or proprietary information.

85. Moreover, on information and belief, Defendant used and is using misappropriated Blink Trade Secrets in an attempt to raise funds from investors or potential investors for its own benefit, all with the intentional and malicious purpose of harming Blink. On information and belief, Defendant obtained, used, and continues to use Blink's business strategy and product roadmap documents, embodied, for example, in its investor and board of director presentations, which Defendant knew were misappropriated by one or more of the Five Insiders in order to attract investors. Indeed, Blink has received inquiries from potential investors expressing concern about information that has been shared with them.

86. Blink is the only possible source of Defendant's knowledge, through one or more of the Five Insiders, of the Trade Secrets. Neither of Defendant's co-founders, Jacoby or Kakaulin had any prior experience in the industry before beginning his employment at Blink. The vast majority, if not all of the information possessed by Defendant about creating and operating a company that provides low-cost prescription drugs to uninsured or underinsured patients was learned through one or more of the Five Insiders' access to Blink Trade Secrets and related confidential and/or proprietary information.

87. It is implausible that Defendant—founded by Jacoby and Kakaulin, who met at Blink and who had no substantive background in the industry and only two years or less of experience working at Blink—would be able to legitimately and successfully replicate Blink’s business model when no other competitor in the prescription drug space has been able to do so. Blink has been operating as a known and widely respected company in this space for several years under intense scrutiny by competitors in the marketplace, yet no experienced competitor has been able to figure out how Blink’s proprietary system works or replicate Blink’s business model. On information and belief, Defendant’s entire business is premised on Blink’s stolen and misappropriated Trade Secrets and related confidential and/or proprietary information. Defendant has full knowledge that some or all of the Five Insiders engaged in the specific acts of misappropriation and theft of Blink Trade Secrets and related confidential and/or proprietary information described above and below. It was Defendant’s willful and malicious intent that the Five Insiders do so.

88. **Source Code:** On information and belief, by engaging one or more of the same computer programmers, including Semyonov, who worked on Blink’s proprietary system to design the copycat Hippo system, Defendant has further misappropriated Blink Trade Secrets and related confidential and/or proprietary information and has induced Semyonov to breach his own contractual obligations to Blink.

89. **Defendant’s Lame Cover-Up Attempt:** On or about December 7, 2017, Blink delivered to Defendant a cease-and-desist letter informing Defendant that its illegitimate business activities were infringing upon Blink’s rights to its Trade Secrets and related confidential and/or proprietary information. *See Ex. A.* While Defendant continues to operate and, on information and belief, perpetuate a fraud on the marketplace by failing to disclose to

potential investors its use of misappropriated Blink Trade Secrets and related confidential and/or proprietary information, the cease-and-desist letter appears to have had some limited effect. At some point in December 2017—*after* the cease-and-desist letter was sent—Defendant changed its response to the “Frequently Asked Question” of “Is Hippo a legitimate company?” to state that “Hippo was born in 2017,” rather than in 2016, as the post had indicated as of at least December 19, 2017.

90. This was a clear admission of wrongdoing by Defendant—knowing full well that the copycat venture (still to be incorporated) was using misappropriated Blink Trade Secrets and/or related confidential and/or proprietary information at some point in late 2016. Changing Hippo’s published founding date from 2016 to 2017 was a feeble attempt to conceal Defendant’s misconduct in order to avoid liability or minimize damages, and yet another display of Defendant’s willingness to peddle in falsehoods.

91. **Defendant’s Coordinated LinkedIn Cover-Up:** On information and belief, Defendant engaged in a further scheme to cover its tracks and defraud investors, industry professionals, and the general public by directing its employees and contractors to sanitize their profiles on the professional social-media platform LinkedIn. For example, Jacoby’s LinkedIn profile falsely indicates that his tenure at Blink ended in August 2016, when in fact he did not formally separate from the Company until February 2017. Such misinformation could dupe otherwise-wary investors into believing that Jacoby was not breaching his professional duties of loyalty and confidentiality and other obligations to Blink, when in fact he was doing just that.

92. In another example of Defendant’s duplicity, on information and belief, Defendant caused four Russian computer programmers it had hired to duplicate Blink’s source code, who are all mutually connected to Semyonov, to conceal their true residences on LinkedIn.

Although their Facebook and/or Twitter profiles all clearly show they, like Semyonov, live in Russia, most of their LinkedIn profiles show their location as New York City, an apparent attempt to cover-up their mutual connection to Semyonov, and/or to suggest that the Defendant is conducting a legitimate business with a substantial group of employees that have a local community presence. For his part, Semyonov's LinkedIn profile makes no mention of working for Defendant, which strongly suggests Defendant wanted to keep Semyonov's and his associates' help secret.

E. Defendant Continues Its Brazen Scheme to Steal Blink Trade Secrets by Deceitfully Interfering with Blink's Contractual Relationships with Current Employees

93. On information and belief, in addition to Defendant's intentional inducement of Trepanier, Semyonov, Tanenbaum, and Muhlstock to violate the terms of their NDAs with Blink by improperly communicating Blink Trade Secrets and related confidential and/or proprietary information to Defendant, Defendant has also induced Trepanier to further its scheme to improperly obtain such information from current and former Blink employees through deceptive conduct.

94. On February 14, 2018, Trepanier requested to meet with a current Blink employee. During that meeting, Trepanier alerted the employee to Defendant's planned launch of a prescription-payment program identical to Blink's. After discussing details of Defendant's product launch that, on information and belief, only an insider would know, Trepanier asked the employee for a physical copy of the Company's Marketing Playbook. Trepanier expressly requested that the copy not be electronic, likely because she knew that an electronic copy would leave a digital trail of both Defendant's interference with the Company's contractual relationship with current Blink employees and Defendant's improper acquisition of Blink Trade Secrets and related confidential and/or proprietary information contained in the Marketing Playbook. The

employee advised Trepanier that the Marketing Playbook is confidential and proprietary and contains Blink Trade Secrets, so he could not provide it to Trepanier.

95. Trepanier claimed she was not planning to provide the information to Defendant but that it was for a different company for which she provided freelance consulting services. However, on information and belief, Trepanier's knowledge of Defendant's nonpublic business plans indicates that Trepanier was in fact affiliated with Defendant at the time she sought to surreptitiously obtain a hard copy of the Marketing Playbook.

F. Blink Is Irreparably Harmed by Defendant's Conduct and Will Continue to Be Irreparably Harmed in the Absence of Injunctive Relief

96. Blink has suffered irreparable harm as a result of Defendant's violations of law and tortious activity, and will continue to suffer irreparable harm if Defendant is not enjoined to cease its misconduct. Among other forms of harm to Blink, the intellectual property of the Company, including its Trade Secrets and related confidential and/or proprietary information, is at risk of being further disclosed and used against it; current and prospective investors have approached Blink concerned that a new competitor may have coopted its business model, which impacts Blink's ability to raise capital; current employees are concerned that the fruits of their hard work may be stolen, damaging the Company to which they have dedicated themselves; and Blink's internal communications of business strategies have been hampered, given concerns about Defendant's theft.

COUNT 1
(Defend Trade Secrets Act, 18 U.S.C. § 1836 *et seq.*)

97. Blink repeats each of the allegations above as if fully set forth herein.

98. The Trade Secrets at issue, which are solely owned by Blink, comprise Blink's confidential (i) innovative contracting structure, which establishes unique relationships with customers and a pharmacy benefit manager and allows for unparalleled leverage in negotiating

prices up the supply chain; (ii) patent-pending back-end process for funding and approving the filling of pre-purchased prescription medications; (iii) back-end process for reconciling the payments the Company receives from customers with the prices of the medications customers actually pick up at pharmacies; (iv) source code, which facilitates the back-end prescription-filling and balance-billing processes, methods, and transactions required to create a seamless experience for the consumer; (v) print and digital marketing plans, strategies, and materials, including its detailed marketing playbook, contact lists, and underlying marketing research; (vi) internal fraud-prevention strategies, rules, methods, and processes; and (vii) business strategy documents, including product roadmaps, as embodied, for example, in investor and board of director presentations. As described above, each of these Trade Secrets is used in interstate commerce to sell medications online to consumers.

99. The Company took reasonable steps to ensure the confidentiality of its Trade Secrets (as set forth non-exhaustively in Section B, above), including by disclosing such information only to necessary persons, only to the extent necessary in each instance, and only subject to NDAs and/or policies governing strict limits on disclosure and use. The Company also sought geographically limited patent protection so as to maintain the confidentiality of the business methods contained in its confidential patent applications.

100. As described non-exhaustively above in Sections A and B, Blink's Trade Secrets derive independent economic value by virtue of their confidentiality, and the significant time, effort, and expense that Blink expended to create them, which is only underscored by the efforts that Defendant undertook to pilfer them and copy Blink's business.

101. Upon information and belief, Defendant has knowingly obtained stolen Blink Trade Secrets and has used and continues to use them in interstate commerce to slap together and

promote its own copycat business, including through its prescription sales website, with knowledge that the Trade Secrets were misappropriated by one or more of the Five Insiders in connection with their work or interview with Blink.

102. Blink lacks an adequate remedy at law and is entitled to an injunction barring Defendant from misappropriating or continuing to misappropriate Blink Trade Secrets or related confidential and/or proprietary information, including by using or disclosing stolen Blink Trade Secrets or related confidential and/or proprietary information that it possesses.

103. Blink is entitled to recover money damages for the harm it has suffered as a result of Defendant's misappropriation, as well as disgorgement of Defendant's unjust enrichment, and/or an order compelling Defendant to pay reasonable royalties to the extent that Defendant is not enjoined from the above violations.

104. By virtue of Defendant's willful and malicious misappropriation of Blink Trade Secrets and related confidential and/or proprietary information, and/or Defendant's ordering, direction, and/or ratification of such conduct by its employee(s), Blink is also entitled to exemplary or punitive damages and attorney's fees in bringing this action.

COUNT 2

(Misappropriation of Trade Secrets under New York Common Law)

105. Blink repeats each of the allegations above as if fully set forth herein.

106. Defendant is familiar with and/or possesses Blink Trade Secrets and related confidential and/or proprietary information that it has a common law duty not to use or disclose other than in the furtherance of Blink's interests.

107. Blink Trade Secrets and related confidential and/or proprietary information are the product of considerable investment by Blink and are closely guarded by the Company.

108. Defendant is a competitor of Blink.

109. The Blink Trade Secrets and related confidential and/or proprietary information in Defendant's possession could not be acquired or duplicated by Defendant by legitimate and proper means.

110. Defendant knowingly obtained stolen Blink Trade Secrets and related confidential and/or proprietary information as described above and has used and/or disclosed, and inevitably will continue to use/or disclose, Blink Trade Secrets or related confidential and/or proprietary information for its own benefit.

111. Defendant's use and disclosure of misappropriated Blink Trade Secrets and related confidential and/or proprietary information has irreparably harmed Blink and will continue to irreparably harm Blink as described above.

112. Blink lacks an adequate remedy at law and is entitled to an injunction barring Defendant from misappropriating or continuing to misappropriate Blink Trade Secrets and related confidential and/or proprietary information, including by using or disclosing stolen Blink Trade Secrets and related confidential and/or proprietary information that it possesses.

113. Blink is also entitled to recover money damages for the harm it has suffered from Defendant's conduct, as well as disgorgement of Defendant's unjust enrichment, including to the extent that Defendant is not enjoined from the above violations.

114. By virtue of the gross wanton, malicious, and outrageous nature of Defendant's conduct in misappropriating Blink Trade Secrets or related confidential and/or proprietary information, and/or Defendant's ordering, direction, and/or ratification of such conduct by its employee(s), Blink is also entitled to exemplary or punitive damages.

COUNT 3
(Unfair Competition under New York Common Law)

115. Blink repeats each of the allegations above as if fully set forth herein.

116. Blink possesses certain Blink Trade Secrets and related confidential and/or proprietary information with which Defendant is familiar and which Defendant has a common-law duty not to use or disclose to anyone apart from Blink.

117. Blink Trade Secrets and related confidential and/or proprietary information are the product of considerable investment by Blink and are closely guarded within the Company.

118. Defendant is a competitor of Blink.

119. The Blink Trade Secrets and related confidential and/or proprietary information in Defendant's possession could not be acquired or duplicated by Defendant by legitimate and proper means.

120. Defendant acquired Blink's Trade Secrets and related confidential and/or proprietary information by improper means for use against Blink's interest and for the commercial benefit of Defendant.

121. As described above, Defendant misappropriated Blink Trade Secrets and related confidential and/or proprietary information as described above that belonged exclusively to Blink, and Defendant has used and/or disclosed, and inevitably will continue to use/or disclose, Blink Trade Secrets or related confidential and/or proprietary information for its own benefit and in bad faith.

122. Defendant's use and disclosure of misappropriated Blink Trade Secrets and related confidential and/or proprietary information has irreparably harmed Blink and will continue to irreparably harm Blink.

123. Blink lacks an adequate remedy at law and is entitled to an injunction barring Defendant from misappropriating or continuing to misappropriate Blink Trade Secrets and

related confidential and/or proprietary information, including by using or disclosing stolen Blink Trade Secrets and related confidential and/or proprietary information.

124. Blink is also entitled to compensatory damages for the harm it has suffered from Defendant's conduct, and to the extent that Defendant is not enjoined from the above violations.

125. By virtue of the gross wanton, malicious, and outrageous nature of Defendant's conduct in unfairly competing against Blink, and/or Defendant's ordering, direction, and/or ratification of such conduct by its employee(s), the Company is also entitled to punitive damages.

COUNT 4

(Tortious Interference with Contract under New York Common Law: Current and Former Blink Employees, Contractors, Applicants, and Other Third Parties)

126. Blink repeats each of the allegations above as if fully set forth herein.

127. Blink had and continues to have contractual relationships with certain of its current and former employees, contractors, applicants, and other third parties, including NDAs requiring those current and former Blink employees, contractors, applicants, and third parties not to use, disclose, or rely on the Blink Trade Secrets and related confidential and/or proprietary information to which they were exposed during their work or interviews with Blink.

128. On information and belief, Defendant, knowing that certain current and former Blink employees, contractors, applicants, or other third parties are contractually obligated not to use, disclose, or rely on Blink Trade Secrets or related confidential and/or proprietary information in their possession, intentionally, without justification, and through dishonest, unfair, and/or improper means induced and/or has attempted to induce, and will continue to induce and/or attempt to induce, those current and former Blink employees, contractors, and applicants to breach their contractual obligations as described herein, to the detriment of Blink and to the benefit of Defendant, a direct competitor with Blink.

129. On information and belief, Defendant acted solely out of a desire to harm Blink.

130. Blink has incurred damages and is entitled to compensatory damages as a result of Defendant's tortious interference with its contractual relations with certain Blink current and former employees, contractors, applicants, and other third parties and will be irreparably injured if Defendant is not enjoined from continuing its tortious interference.

131. By virtue of the gross wanton, malicious, and outrageous nature of Defendant's conduct and/or Defendant's ordering, direction, and/or ratification of such conduct by its employee(s) Blink is also entitled to punitive damages.

COUNT 5

**(Tortious Interference with Prospective Economic Advantage under
New York Common Law: Potential Applicants and Other Third Parties)**

132. Blink repeats each of the allegations above as if fully set forth herein.

133. Blink had continuing and customary business relationships with potential applicants and other third parties.

134. On information and belief, Defendant knew of Blink's continuing and customary relationships with potential applicants and other third parties and intentionally interfered with them by directing its employees to hold themselves out as a Blink employees for the purpose of deterring these potential applicants from being hired by Blink.

135. On information and belief, Defendant acted solely out of malice, and/or used dishonest, unfair, or improper means, including by, among other things, misappropriating Blink Trade Secrets and related confidential and/or proprietary information and engaging in unfair competition against Blink.

136. Blink has incurred damages and is entitled to compensatory damages as a result of Defendant's tortious interference with its business relationships with certain Blink potential

applicants and other third parties and will be irreparably injured if Defendant is not enjoined from continuing its tortious interference.

137. By virtue of the gross wanton, malicious, and outrageous nature of Defendant's conduct, and/or Defendant's ordering, direction, and/or ratification of such conduct by its employee(s), Blink is also entitled to punitive damages.

COUNT 6
(Unjust Enrichment under New York Common Law)

138. Blink repeats each of the allegations above as if fully set forth herein.

139. On information and belief, Defendant has unjustly benefitted from its knowing wrongful access to and use of some or all of Blink's stolen Trade Secrets and related confidential and/or proprietary information by virtue of establishing its entire business on such Trade Secrets and related confidential and/or proprietary information.

140. Blink has been and continues to be harmed by defendant's wrongful conduct.

141. Equity and good conscience require Defendant to return any and all Blink Trade Secrets and related confidential and/or proprietary information in its possession and to disgorge any and all benefits, including ill-gotten remunerations, Defendant has obtained by using such Trade Secrets and related confidential and/or proprietary information.

COUNT 7
(Replevin under New York Common Law)

142. Blink repeats each of the allegations above as if fully set forth herein.

143. Blink's possessory rights to its Trade Secrets and related confidential and/or proprietary information are superior to those of Defendant, which possesses no rights to the Trade Secrets or related confidential and/or proprietary information.

144. On December 7, 2017, Blink demanded that Defendant cease and desist its use of misappropriated Blink Trade Secrets and related confidential and/or proprietary information, but Defendant ignored Blink's demand and instead continued its unlawful conduct.

145. Defendant continues to unlawfully retain possession of and to use misappropriated Blink Trade Secrets and related confidential and/or proprietary information.

146. Blink has been and continues to be harmed by Defendant's wrongful conduct.

147. Equity and good conscience require Defendant to return any and all Blink Trade Secrets and related confidential and/or proprietary information in its possession.

JURY DEMAND

148. Blink hereby demands a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Blink respectfully requests that this Court enter judgment as follows:

A. For a preliminary and permanent injunction ordering Defendant and its agents to immediately:

1) refrain from misappropriating Blink Trade Secrets and related confidential and/or proprietary information, including by acquiring, using or disclosing misappropriated Blink Trade Secrets and related confidential and/or proprietary information;

2) refrain from unfairly competing with Blink; and

3) refrain from tortiously interfering with the contracts and business relations of Blink;

B. For an Order directing Defendant and its agents to return Blink's property—including, without limitation, Blink Trade Secrets and related confidential and/or proprietary information—as set forth in the Complaint;

C. For an Order directing Defendant to file with the Court and serve on Blink within thirty (30) days after the service on Defendant of such injunction a report in writing, under oath, setting forth the manner and form in which Defendant has (a) complied with the injunction and (b) returned Blink's property, including, without limitation, Blink Trade Secrets and related confidential and/or proprietary information;

D. For an Order restraining Defendant and its agents from destroying any and all files or documents wrongfully obtained from Blink that are currently in its possession;

E. For general and compensatory damages according to proof at trial, but in an amount no less than \$50 million;

- F. For punitive and/or exemplary damages in an amount no less than \$200 million;
- G. For disgorgement of all ill-gotten gains Defendant has unjustly attained by its illegal acts, and/or an order compelling Defendant to pay reasonable royalties to the extent that Defendant is not enjoined from the above violations and for the use of Blink Trade Secrets;
- H. For prejudgment interest;
- I. For an Order awarding Blink its attorney's fees and costs;
- J. For an Order awarding Blink such other and further relief as the Court deems just and proper.

Dated: New York, New York
March 14, 2018

GIBSON, DUNN & CRUTCHER LLP

By: /s/ Orin Snyder
Orin Snyder
Alexander H. Southwell
Angelique Kaounis (application for
admission *pro hac vice* forthcoming)
Babak Ghafarzade

200 Park Avenue
New York, New York 10166
Tel.: (212) 351-4000
Fax: (212) 351-4035
OSnyder@gibsondunn.com

Attorneys for Plaintiff Blink Health, Ltd.

EXHIBIT A

PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP

1285 AVENUE OF THE AMERICAS
NEW YORK, NEW YORK 10019-6064

TELEPHONE (212) 373-3000

LLOYD K. GARRISON (1946-1991)
RANDOLPH E. PAUL (1946-1956)
SIMON H. RIFKIND (1950-1995)
LOUIS S. WEISS (1927-1950)
JOHN F. WHARTON (1927-1977)

WRITER'S DIRECT DIAL NUMBER

(212) 373-3166

WRITER'S DIRECT FACSIMILE

(212) 492-0166

WRITER'S DIRECT E-MAIL ADDRESS

aehrlich@paulweiss.com

UNIT 3601, OFFICE TOWER A, BEIJING FORTUNE PLAZA
NO. 7 DONGSANHUAN ZHONGLU
CHAOYANG DISTRICT
BEIJING 100020
PEOPLE'S REPUBLIC OF CHINA
TELEPHONE (86-10) 5928-6300

12TH FLOOR, HONG KONG CLUB BUILDING
3A CHATER ROAD, CENTRAL
HONG KONG
TELEPHONE (852) 2646-0300

ALDER CASTLE
10 NOBLE STREET
LONDON EC2V 7JU, U.K.
TELEPHONE (+44 20) 7367 1600

FUKOKU SEIMEI BUILDING
2-2 UCHISAIWAICHO 2-CHOME
CHIYODA-KU, TOKYO 100-0011, JAPAN
TELEPHONE (81-3) 3597-8101

TORONTO-DOMINION CENTRE
77 KING STREET WEST, SUITE 3100
PO BOX 226
TORONTO, ONTARIO M5K 1J3
TELEPHONE (416) 504-0520

2001 K STREET, NW
WASHINGTON, DC 20006-1047
TELEPHONE (202) 223-7300

500 DELAWARE AVENUE, SUITE 200
POST OFFICE BOX 32
WILMINGTON, DE 19899-0032
TELEPHONE (302) 655-4410

MATTHEW W. ABBOTT
EDWARD T. ACKERMAN
JACOB A. ADLERSTEIN
ALLAN J. ARFFA
ROBERT A. ATKINS
DAVID J. BALL
SCOTT A. BARSHAY
PAUL M. BADJA
JOHN F. BAUGHMAN
J. STEVEN BAUGHMAN
LYNN B. BAYARD
CRIG A. BENSON
MITCHELL L. BERG
MARK S. BERGMAN
DAVID M. BERNICK
JOSEPH J. BIANCHI
BRUCE BIRENBOIM
H. CHRISTOPHER BOEHNING
ANGELO BONVINO
DAVID W. BROWN
SUSANNA M. BUERGER
PATRICK S. CAMPBELL*
JESSICA S. CAREY
JEANETTE R. CHAN
GEOFFREY R. CHEFIGA
ELLEN N. CHING
WILLIAM A. CLAREMAN
LEWIS R. CLAYTON
JAY COHEN
KELLEY A. CORNISH
CHRISTOPHER J. CUMMINGS
CHARLES E. DAVIDOW
THOMAS V. DE LA BASTIDE III
ARIEL J. DECKELBAUM
ALICE BELISLE EATON
ANDREW J. EHRICH
GREGORY A. EZRING
LESLIE GORDON FAGEN
ROSS A. FIELDSTON
BRAD J. FINKELSTEIN
BRIAN P. FINNEGAN
ROBERTO FINZI
PETER E. FISCH
ROBERT C. FLEDER
MARTIN FLUMENBAUM
ANDREW J. FOLEY
ANDREW J. FORMAN*
HARRIS B. FREIDUS
MANUEL S. FREY
ANDREW L. GAINES
KENNETH A. GALLO
MICHAEL E. GERTZMAN
ADAM M. GIVERTZ
SALVATORE GOGLIORMELLA
NEIL GOLDMAN
ROBERTO J. GONZALEZ*
CATHERINE L. GOODALL
ERIC GOODISON
CHARLES H. GOOGE, JR.
ANDREW G. GORDON
JUDI GROFMAN
NICHOLAS GROOMBRIDGE
BRUCE A. GUTENPLAN
ALAN S. HALPERIN
JUSTIN G. HAMILL
CLAUDIA HAMMERMAN
BRIAN S. HERMANN
MICHELE HIRSHMAN
MICHAEL S. HONG
DAVID S. HUNTINGTON
AMRAN HUSSEIN
LORETTA A. IPPOLITO
JAREN JANGHORBANI
BRIAN M. JANSON
JEH C. JOHNSON
MEREDITH J. KANE

JONATHAN S. KANTER
BRAD S. KARP
PATRICK N. KARSNITZ
JOHN C. KENNEDY
BRIAN KIM
DAVID M. KLEIN
ALAN W. KORNBERG
DANIEL J. KRAMER
DAVID K. LAKHDHIR
STEPHEN P. LAMB*
JOHN E. LANGE
GREGORY F. LAUFER
BRIAN C. LAVIN
XIAOYU GREG LIU
JEFFREY D. MARELL
MARCIO V. MASOTTI
EDWIN S. MAYNARD
DAVID W. MAYO
ELIZABETH R. MCCOLM
ALVARO MEMBRILLERA
MARK F. MENDELSON
CLAUDINE MEREDITH-GOUJON
WILLIAM B. MICHAEL
JUDIE NG SHORTELL*
CATHERINE NYARADY
JANE B. O'BRIEN
ALEX YOUNG K. OH
BRAD R. OKUN
KELLEY D. PARKER
VALERIE E. RADWANER
CARL L. REISNER
DORIN L. REISNER
WALTER R. REISNER
WALTER RIEMAN
RICHARD A. ROSEN
ANDREW N. ROSENBERG
JACQUELINE P. RUBIN
CHARLES F. "RICK" RULE*
RAPHAEL M. RUSSO
ELIZABETH M. SACKSTEDER
JEFFREY D. SAFERSTEIN
JEFFREY B. SAMUELS
DALE M. SARRO
TERRY E. SCHIMEK
KENNETH M. SCHNEIDER
ROBERT B. SCHUMER
JOHN M. SCOTT
STEPHEN J. SHIMSHAK
DAVID R. SICULAR
MOSES SILVERMAN
STEVEN SIMKIN
JOSEPH J. SIMONS
ERIC ALAN STONE
AIDAN SYNNOTT
SCOTT M. SONTAG
TARUN M. STEWART
ERIC ALAN STONE
AIDAN SYNNOTT
RICHARD C. TARLOWE
MONICA K. THURMOND
DANIEL J. TOAL
LIZA M. VELAZQUEZ
LAWRENCE G. WEE
THEODORE V. WELLS, JR.
STEVEN J. WILLIAMS
LAWRENCE I. WITDORCHIC
MARK B. WLAZLO
JULIA MASON WOOD
JENNIFER H. WU
BETTY YAN*
JORDAN E. YARETT
KAYE N. YOSHINO
TONG YU
TRACEYA ZACCONE
TAURIE M. ZEITZER
T. ROBERT ZECHOWSKI, JR.

*NOT ADMITTED TO THE NEW YORK BAR

December 7, 2017

By Federal Express

Everymed LLC d/b/a Hello Hippo
95 Fifth Avenue
New York, NY 10003

and

Everymed LLC d/b/a Hello Hippo
1732 First Avenue
Suite 20213
New York, NY 10128

To whom it may concern,

It has come to our attention from multiple sources that Everymed LLC d/b/a Hello Hippo ("Hello Hippo") has attempted, and/or is attempting, to misappropriate for its own use confidential, proprietary and commercially sensitive information that belongs exclusively to Blink and that constitute Blink trade secrets. We are also aware that Hello Hippo is competing with Blink's business in reliance on these trade secrets. Blink takes its trade secrets and other confidential information very seriously and will take all appropriate measures to ensure their full protection.

It has also come to our attention that Charles Jacoby is currently providing services to Hello Hippo and that Mr. Jacoby has been involved in Hello Hippo's efforts to misappropriate and disclose Blink trade secrets. It is our understanding that Mr. Jacoby

Everymed LLC d/b/a Hello Hippo

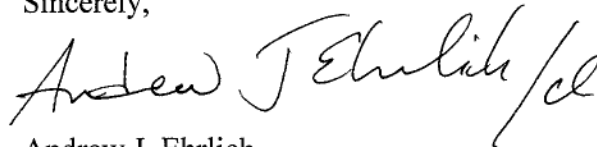
2

actually formed Hello Hippo and began to misappropriate Blink trade secrets *while he was serving as Blink's deputy general counsel*. To the extent you do not already know (which would be difficult to fathom given your relationship with Mr. Jacoby), you are now on notice that Mr. Jacoby is subject to both a non-competition agreement and a confidentiality agreement with Blink that preclude him from competing with Blink and from disclosing or using any confidential Blink information or trade secrets.

We demand that you (and anyone acting on your behalf and/or at your direction) immediately cease and desist these and any related activities, including without limitation (i) any effort to misappropriate Blink trade secrets including disclosing Blink confidential information to potential investors and (ii) any effort to tortuously interfere with Mr. Jacoby's contractual obligations to Blink and/or aid and abet any wrongful conduct by Mr. Jacoby that could harm Blink. If you do not immediately comply with these demands, legal action will be taken against you without further notice. We request a response to this letter by December 14, 2017.

This letter is sent without waiver of any of Blink's rights, remedies or defenses.

Sincerely,

A handwritten signature in black ink that reads "Andrew J. Ehrlich" followed by a stylized flourish or initials.

Andrew J. Ehrlich

cc: Charles Jacoby
Eugene Kakaulin