UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

TREVOR SLOAN, individually and on behalf of all others similarly situated, Plaintiff, v. ANKER TECHNOLOGY CORPORATION, a Delaware Corporation, and FANTASIA TRADING LLC, a Delaware Limited Liability Company, Defendants.	Case No.: _____ **Jury Trial Demanded**

CLASS ACTION COMPLAINT

Plaintiff Trevor Sloan brings this Class Action Complaint against Defendants Anker Technology Corporation and Fantasia Trading LLC, doing business as "eufy" and/or "Anker Innovations" (collectively "Anker" or "Defendants"), individually and on behalf of all others similarly situated, and complains and alleges upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys, as follows:

NATURE OF THE ACTION

1. Anker manufactures, distributes and sells its "eufy" branded security products. As part of its "eufy" security offering, Anker sells home security cameras, including its eufycam, Video Smart Lock, SoloCam, Floodlight Cam, Video Doorbell, and Solo Indoorcam lines of products (collectively, the "Camera Products"). The Camera Products are capable of recording

video, streaming video, and facial recognition.

2. Anker extensively markets that its Camera Products save all video recording and conducts all facial recognition locally (meaning on equipment located with and controlled by the consumer). As such, Anker represents in its marketing materials that only the end user should have access to the video information recorded by the Camera Products.

3. This differentiates Anker from its competitors, who often require that their similar cameras must access the internet to work. Indeed, Anker's most direct competitor, Nest (Google), requires that all cameras be connected to Nest servers, which record and process the data, before sending it back to the user.

4. Indeed, Anker's marketing focuses on these aspects of its Camera Products: promising that "your recorded footage will be kept private. Stored locally. With military-grade encryption. And transmitted to you, and only you." This is untrue.

5. In November 2022, security researcher Paul Moore noted that the Camera Products were uploading video thumbnails and facial recognition data to Anker's cloud server, despite his never opting into Anker's cloud services. Moore also found that a separate Camera Product linked to a different account was able to identify his face with the same unique ID — indicating that Anker is not only storing facial recognition data in the cloud, but also sharing that back-end information between accounts.

6. But these were not Moore's only findings. Moore also noted that he was able to view live footage from his camera over a web browser without any kind of authentication simply by navigating to the correct public-facing web address. Accordingly, the Camera Products were not made with end-to-end encryption. Anker's security marketing is undoubtedly false and misleading.

7. Consumers reasonably relied on Anker's marketing when purchasing the Camera

Products. Plaintiff and other members of the Class, however, did not receive the Products that they were promised, security cameras which did not share their data with any third parties, including Anker, and that were secured by strong encryption. Additionally, Plaintiff and other members of the Class have had their biometric information uploaded to Anker's servers without their authorization. Accordingly, Plaintiff brings this class action on behalf of all consumers who purchased the Camera Products from Anker, to recover restitution and damages, and for injunctive relief.

PARTIES

8. Plaintiff Trevor Sloan is a resident and citizen of Illinois who purchased and used eufy branded Video Doorbell and Floodlight Camera. Plaintiff purchased these Products in 2021, from Best Buy. Plaintiff purchased these Products, in part, because it purportedly stored all information locally and did not upload information to Anker's servers. Had Plaintiff known the Camera Products uploaded pictures and video online to Anker's servers, with minimal security, he would not have purchased the Camera Products or would have paid less.

9. Defendant Anker Technology Corporation is a Delaware corporation headquartered in Bellevue, Washington. Defendant manufactures various electronic devices and accessories under its own brand, Anker, as well as other brand names, including Eufy, Soundcore, Nebula, and Roav.

10. Defendant Fantasia Trading LLC is a Delaware limited liability company headquartered in Ontario, California. Defendant manufactures various electronic devices and accessories under its own brand, Anker, as well as other brand names including Eufy, Soundcore, Nebula, and Roav.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. §

1332 of the Class Action Fairness Act of 2005 because: (1) there are 100 or more putative Class Members, (ii) the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest and costs, and (iii) there is minimal diversity because Plaintiff and Anker are citizens of different states. This Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367.

12. This Court has personal jurisdiction over Anker because it has substantial aggregate contacts with this District, including engaging in conduct in this District that has a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout the United States, because Anker placed the Product into the stream of commerce directed at this District, and because Anker purposely availed itself of the laws of the United States and the State of Illinois.

13. In accordance with 28 U.S.C. § 1391, venue is proper in this District because the parties consented to jurisdiction of this Court, Anker transacts business in this District, and Anker has intentionally availed itself of the laws and markets within this District.

FACTUAL ALLEGATIONS

A. Background Information

14. Anker markets, distributes, and sells its "eufy" branded Camera Products throughout the United States. Consumers can purchase these Products online, either directly through Anker or another online retailer, or at brick-and-mortar store, such as Best Buy. These Camera Products are specifically marketed for home security, allowing consumers to view live and recorded video of the areas around their homes, to receive notifications regarding activity, and (with some cameras) to have two-way audio communication.

15. The Camera Products also have the BionicMind system, marketed as a "local artificial intelligence used for facial recognition." The BionicMind system allows users to have

their Camera Products differentiate between known individuals and strangers, using their faces. This system uses scans of face geometry to identify an individual.

16. Consumers who purchase the Camera Products must use the Eufy Security smartphone application. To set up the smartphone application, consumers provide their email address and other personally identifiable information. This application allows users to access their cameras, view live and historical video feeds, and adjust the cameras' settings. The Camera Products will communicate with this smartphone application to provide user notifications, such as notification of activity on the cameras.

17. The End User License Agreement ("EULA") for the application and the Camera Products provides that "you agree that this EULA, and any claim, dispute, action, cause of action, issue, or request for relief relating to this EULA, will be governed by the laws of Illinois, without giving effect to any conflicts of laws principles that require the application of the laws of a different jurisdiction. Any action or proceeding relating to this EULA must be brought in a federal or state court located in Cook County, Illinois and each party irrevocably submits to the jurisdiction and venue of any such court in any such claim or dispute."

B. Anker's Privacy Marketing

18. Anker recognizes that potential purchases of home security cameras are rightfully concerned regarding privacy. Anker engages in marketing efforts to persuade consumers on the benefits of the secure and private storage nature of "local" storage. Anker differentiates itself from competitors by advertising that the Camera Products store all recording locally, and that such information is encrypted. Accordingly, Anker touts that no one, other than the user, can access the data associated with the Camera Products. Anker, therefore, advertises and warrants that the Camera Products do not send Anker any data collected by the Products and that such data is always encrypted.

19. Each of the Camera Products, on the Product's label, advertise and warrant that:

> Your Privacy is something that we value as much as you do.
> To start, we're taking every step imaginable to ensure that your data remains private, with you.
> Whether it's your newborn crying for mom, or your victory dance after a game, your recorded footage will be kept private.
> Stored locally. With military-grade encryption.
> And transmitted to you, and only you.
> That's just the start of our commitment to protect you, your family, and your privacy.

Additionally, the Camera Products' label also advertises and warrants that "[a]ll your footage is securely stored locally[,] [e]nsuring the videos you record are for you and only you" and the Products have "Military-Grade AES-256 data encryption." Anker's privacy marketing does not end here.

20. Indeed, during the relevant time period, Anker's website included a "Privacy Commitment," which states that "eufy Security, privacy and protection are our top priorities. Both are integral to our daily operations, and to implementing measures that ensure your data is always safe." Anker noted that all information would be stored locally and be encrypted so only the user could see it. Similarly, Anker promised that its AI would not send pictures to the cloud.

Anker continued, noting that video would never be shared with Anker or any third parties unless expressly authorized:

- "To start, we're taking every step imaginable to ensure your data remains private, with you."
- "[Y]our recorded footage will be kept private. Stored locally. With military-grade encryption. And transmitted to you, and only you."
- "With secure local storage, your private data never leaves the safety of your home, and is accessible by you alone."
- "There is no online link available to any video."

However, such privacy representations would prove to be false.

21. Additionally, Anker's privacy policy, which is included on Anker's website, does not disclose that its camera would collect and store video and facial recognition information.

C. Security Professionals Find That Anker's Representations Are False

22. While consumers reasonably believed Anker's representations, it was not until November 2022 that consumers discovered the data associated with their Camera Products was being sent to Anker and was not protected using Military-Grade AES-256 data encryption.

23. On Thanksgiving day, security researcher Paul Moore posted a string of tweets and videos, demonstrating that the Camera Products were uploading name-tagged thumbnail images to Anker's cloud servers, without encryption. Put differently, Anker was accessing and storing the notification that the Camera Products send to customers' smart phones and other devices. Even worse, a very weak AES key was being used to encrypt video footage, which could be easily brute forced.[1] This was not "Military-Grade AES-256 data encryption."

24. On November 23, 2022, Moore uploaded a video that demonstrated his findings. With his Eufy Homebase unplugged, Moore walked in front of his camera. From an incognito web browser, Moore could pull up a thumbnail image of himself, an image of the feed shortly

[1] *See* https://twitter.com/Paul_Reviews/status/1594725532062580737;

before he was visible, and—perhaps more concerning—ID numbers indicating his recognized face and his status as the camera owner.[2] In other words, the Camera Products paired consumers' facial scans with other personally identifiable information from the consumer, which made Defendants capable of determining consumers' identities. This further suggests that all this information has been uploaded to a web server.

25. Moore's findings were confirmed by others. One day later, security firm SEC Consult summarized two years of analyzing a EufyCam, noting a similar transfer of thumbnails through a cloud service. The company also saw the weak keys, suggesting "hard-coded encryption/decryption keys which are identical for all sold Homebase devices," though it was unclear for what the keys were being used.[3] Additionally, media outlets seemed to be able to replicate the same results.[4]

26. Indeed, *the Verge* was able to stream video from Anker's Camera Products, because the stream was not encrypted. The reported noted that, "[t]his week, we repeatedly watched live footage from two of our own Eufy cameras using that very same VLC media player, from across the United States — proving that Anker has a way to bypass encryption and access these supposedly secure cameras through the cloud."[5]

27. That's a far cry from Anker's claim that footage is "sent straight to your phone—and only you have the key." Accordingly, Anker's advertisements and warranties that all camera data was stored locally, that Anker and others could not access the information, and that all information was encrypted is patently false, rendering Anker's Camera Products less valuable than a camera system that did have such security and privacy futures.

---

[2] *See* https://www.youtube.com/watch?v=qOjiCbxP5Lc.
[3] *See* https://sec-consult.com/blog/detail/the-eufycam-long-term-observation/.
[4] *See* https://www.theverge.com/2022/11/30/23486753/anker-eufy-security-camera-cloud-private-encryption-authentication-storage.
[5] *Id.*

D. Anker Unlawfully Collects Facial Recognition Information

28. Anker's actions do not only represent a serious breach of confidence, but also an illegal misappropriation of biometric data.

29. Biometric Data is particularly sensitive personal information. As the Illinois Legislature has found, "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

30. In recognition of these concerns over the security of individuals' Biometric Data, the Illinois Legislature enacted Biometric Information Privacy Act ("BIPA"), which provides, *inter alia*, that a private entity may not obtain and/or possess an individual's Biometric Data unless it: (1) informs that person (or their representative) in writing that a biometric identifier or biometric information is being collected or stored, *id.* 14/15(b)(1); (2) informs that person in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used, *id.* 14/15(b)(2); (3) receives a written release from the person (or their representative) for the collection of his or her biometric identifier or information, *id*. 14/15(b)(3); and (4) publishes publicly available written retention schedules and guidelines for permanently destroying Biometric Data, *id.* 740 ILCS 14/15(a).

31. Further, the entity must store, transmit, and protect from disclosure all Biometric Data using the same standard of care in the industry and in a manner at least as protective as the means used to protect other confidential and sensitive information. *Id.* 14/15(e).

32. In direct violation of each of the foregoing provisions of BIPA, Anker collected and captured facial recognition information from Plaintiff and Class members, as well as their

friends and family that appear on their cameras. This information was then uploaded to Anker's servers, and stored there, without notice, prior consent, or providing a publicly available policy establishing a retention schedule and guidelines for permanently destroying this Biometric Data. Additionally, Anker's methods for securing such information was woefully inadequate. Consequently, Anker violated BIPA.

TOLLING ALLEGATIONS

33. Any applicable statute of limitations should be tolled by the Discovery Rule. Here, Plaintiff and other Class members reasonably relied on Anker's representations regarding the fact that its Camera Products store all information locally, do not share such information with Anker, and was encrypted.

34. However, it was only on November 21, 2022, when security consultants voiced their concerns that the Camera Products were uploading data to Anker's servers and that the video feeds on these devices were not encrypted that Plaintiff and other Class members discovered that such representations were false.

35. Accordingly, the Statute of Limitations for all claims, for each Class member, should be tolled until November 21, 2022.

CLASS ACTION ALLEGATIONS

36. Plaintiff brings this action individually and as representative of all those similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the below-defined Class:

> **National Class:** All persons in the United States who purchased the Camera Products during the applicable statute of limitations.
>
> **Illinois Subclass:** All persons in the State of Illinois who purchased the Camera Products during the applicable statute of limitations.

The following are excluded from the Class: (1) any Judge presiding over this action and members

of his or her family; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which Defendants or its parent has a controlling interest (as well as current or former employees, officers, and directors); (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

37. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

38. The members of the Class are so numerous that individual joinder of all Class members is impracticable. On information and belief, Class members number in the thousands. The precise number or identification of members of the Class is presently unknown to Plaintiff, but may be ascertained from Defendants' books and records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

39. Common questions of law and fact exist as to all members of the Classes, which predominate over any questions affecting individual members of the Class. These common questions of law or fact include, but are not limited to, the following:

a) Whether the marketing, advertising, packaging, labeling, and other promotional materials for the Camera Products was deceptive;

b) Whether Anker's actions violate the consumer protection statutes invoked herein;

c) Whether Anker collected biometric information from consumers;

d) Whether Anker violated BIPA;

e) Whether Anker warranted that data collected by the Camera Products would be stored locally and would be encrypted;

f) Whether Defendants were unjustly enriched at the expense of Plaintiff and Class members;

g) Whether Plaintiff and Class members are entitled to damages, including compensatory, exemplary, and statutory damages, and the amount of such damages;

h) Whether Plaintiff and the other Class members have been injured and the proper measure of their losses as a result of those injuries; and

i) Whether Plaintiff and the Class members are entitled to injunctive, declaratory, or other equitable relief.

40. Anker engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

41. Plaintiff's claims are typical of the claims of the other Class members because, among other things, all such claims arise out of the same wrongful course of conduct engaged in by Anker in violation of law as complained of herein. Further, the damages of each Class member were caused directly by Anker's wrongful conduct in violation of the law as alleged herein.

42. Plaintiff is an adequate representative of the Class because he is a member of the Class and his interests do not conflict with the interests of the Class members that he seeks to represent. Plaintiff has also retained counsel competent and experienced in complex commercial and class action litigation. Plaintiff and his counsel intend to prosecute this action vigorously for the benefit of all Class members. Accordingly, the interests of the Class members will be fairly and adequately protected by Plaintiff and his counsel.

43. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff

and the Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Anker, so it would be impracticable for Class members to individually seek redress for Anker's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
Violation Of The Illinois Consumer Fraud and Deceptive Trade Practices Act ("ICFA")
815 ILCS 505/1, *et seq.*
(On Behalf of Plaintiff and National Class and,
alternatively, the Illinois Subclass)

44. Plaintiff re-alleges and incorporates the allegations above as if set forth herein.

45. Illinois law applies under the terms of the EULA.

46. Plaintiff and other Class members are persons within the context of the ICFA, 815 ILCS 505/1(c).

47. Anker is a person within the context of the ICFA, 815 ILCS 505/1(c).

48. At all times relevant hereto, Anker was engaged in trade or commerce as defined under the ICFA, 815 ILCS 505/1(f). 183.

49. Plaintiff and the proposed Class are "consumers" who purchased the Products for personal, family, or household use within the meaning of the ICFA, 815 ILCS 505/1(e).

50. The ICFA prohibits engaging in any "unfair or deceptive acts or practices … in the conduct of any trade or commerce…." ICFA, 815 ILCS 505/2.

51. The ICFA prohibits any deceptive, unlawful, unfair, or fraudulent business acts or practices including using deception, fraud, false pretenses, false promises, false advertising,

misrepresentation, or the concealment, suppression, or omission of any material fact, or the use or employment of any practice described in Section 2 of the Uniform Deceptive Trade Practices Act ("UDTPA"). 815 ILCS § 505/2. Plaintiff and the other Class members reasonably relied upon Anker's representation that the Camera Products stored all data locally and encrypted such data.

52. Anker's conduct, as described herein, constitutes unfair or deceptive acts or practices in the course of trade and commerce, in violation of 815 ICFA 505/1, *et seq*.

53. Anker violated the ICFA by representing that the Camera Products have characteristics or benefits that they do not have. 815 ILCS § 505/2; 815 ILCS § 510/2(7).

54. Anker advertised the Camera Products with intent not to sell them as advertised, in violation of 815 ILCS § 505/2 and 815 ILCS § 510/2(9).

55. Anker engaged in fraudulent and/or deceptive conduct, which creates a likelihood of confusion or of misunderstanding in violation of 815 ILCS § 505/2; 815 ILCS § 510/2(3).

56. Anker engaged in misleading and deceptive advertising that represented that the Camera Products stored all data locally and encrypted such data. Anker chose to advertise and label the Camera Products in this way to impact consumer choices and gain market dominance, as it is aware that all consumers who purchased the Camera Products were exposed to and would be impacted by its misrepresentation and would reasonably believe that the Camera Products stored all data locally and encrypted such data. However, the Camera Products do not store all data locally and encrypted such data, which has been demonstrated by security experts and the media.

57. Anker intended that Plaintiff and each of the other Class members would reasonably rely upon its misrepresentations, characterizations, warranties, and material misrepresentations concerning the true nature of the Camera Products.

58. Anker's misrepresentations, concealment, omissions and other deceptive conduct were likely to deceive and cause misunderstanding and/or in fact caused Plaintiff and each of the

other Class members to be deceived about the true nature of the Camera Products.

59. Plaintiff and Class members have been damaged as a proximate result of Anker's violations of the ICFA and have suffered damages as a direct and proximate result of purchasing the Camera Products.

60. As a direct and proximate result of Anker's violations of the ICFA, as set forth above, Plaintiff and the Class members have suffered ascertainable loss of money caused by Anker's misrepresentations.

61. Had they been aware of the true nature of the Products, Plaintiff and Class members either would have paid less for the Products or would not have purchased them at all.

62. Plaintiff and the Class members are therefore entitled to relief, including restitution, actual damages, treble damages, punitive damages, costs and attorney's fees, under sections 815 ILCS 505/10a of the ICFA. Plaintiff and Class members are also entitled to injunctive relief, seeking an order enjoining Anker's unfair and/or deceptive acts or practices.

COUNT II
Violation of the Federal Wiretap Act
8 U.S.C. §§ 2510, *et seq.*
(On Behalf of the National Class)

63. Plaintiff re-alleges and incorporates the allegations above as if set forth herein.

64. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of the contents of any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

65. The Wiretap Act protects both the sending and receipt of communications.

66. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

67. As set forth above, Anker represents, through its advertising, labeling, marketing, and packaging, that the Camera Products stored all data locally and encrypted such data. However,

when electronic notifications are sent between the Camera Products and the user's device (such as a notification that activity has been spotted on the camera), such communications are contemporaneously intercepted and sent to Anker's server.

68. The communications intercepted by Anker included "contents" of electronic communications made between the Camera Products and Plaintiff and other Class members, such as the image associated with the notification and any facial recognition information.

69. The transmission of data between the Class members' smart phones and their Camera Products were "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12). The Camera Products, Class members' smart phones, Anker's server, and the code used by Anker to direct communications to their servers are "devices" within the meaning of 18 U.S.C. § 2510(5).

70. Anker was not an authorized party to the communication because the Plaintiff and Class members were unaware of Anker's redirecting of the camera notification to its own server. Class members did not consent to Anker's interception of their camera notification.

71. After intercepting the communications, Anker then used the contents of the communications knowing or having reason to know that such information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(a).

72. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages to Plaintiff and the Class members, injunctive and declaratory relief, punitive damages, and reasonable attorneys' fee and other litigation costs.

COUNT III
Violation Of Biometric Information Privacy Act ("BIPA")
740 ILCS 14/1, *et seq.*
(On Behalf of Plaintiff and National Class and, alternatively, the Illinois Subclass)

73. Plaintiff re-alleges and incorporates the allegations above as if set forth herein.

74. Illinois law applies under the terms of the EULA.

75. BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . ." 740 ILCS 14/15(b).

76. Anker is a corporation and Fantasia is a limited liability company and thus both entities qualify as a "private entity" under BIPA. *See* 740 ILCS 14/10.

77. Plaintiff and the Class members are individuals who had their biometrics collected and stored by Anker. *See* 740 ILCS 14/10.

78. Anker systematically collected, used, and stored Plaintiffs and the Class members' Biometric Data derived from Plaintiff and the Class members' facial geometry without first obtaining the written release required by 740 ILCS 14/15(b)(3), and thereby uniformly invaded Plaintiff and each Class members' statutorily protected right to privacy in their biometrics.

79. Anker failed to properly inform Plaintiff or members of the Class in writing that their Biometric Data was being collected, stored, or otherwise obtained, and of the specific purpose and length of term for which those biometrics were being collected, stored, and used, as required

by 740 ILCS 14/15(b)(1)-(2).

80. In addition, Anker does not provide a written, publicly available retention schedule and guidelines for permanently destroying the Biometric Data of Plaintiff or the Class members, as required by BIPA. *See* 740 ILCS 14/15(a). Anker's failure to provide such a schedule and guidelines constitutes an independent violation of the statute.

81. Each instance in which Anker collected, stored, used, or otherwise obtained Plaintiff and/or Class members' Biometric Data, as described herein, constitutes a separate violation of the statutory right of Plaintiff and each Class member to keep private this Biometric Data, as set forth in BIPA, 740 ILCS 14/1, *et seq.*

82. On behalf of himself and members of the proposed Class, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Illinois Class by requiring Anker to comply with BIPA's requirements, including BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein, and for the provision of the requisite written disclosure to consumers; (2) statutory damages of $5,000.00 for each and every intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or, alternatively, statutory damages of $1,000.00 for each and every violation pursuant to 740 ILCS 14/20(1) if the violations are found to have been committed negligently; and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT IV
Unjust Enrichment
(In the Alternative and on Behalf of the National Class and, alternatively, the Illinois Subclass)

83. Plaintiff re-alleges and incorporates the allegations above as if set forth herein.

84. Plaintiff and the other members of the Class conferred benefits on Anker by purchasing the Camera Products.

85. Anker has been unjustly enriched in retaining the revenues derived from the purchase of the Products by Plaintiff and the other members of the Class.

86. Retention of those monies under these circumstances is unjust and inequitable because Anker's labeling of the Products was misleading to consumers, which caused injuries to Plaintiff and the other members of the Class because they would have not purchased the Camera Products if Anker had disclosed that the Camera Products were not secure.

87. Because Anker's retention of the non-gratuitous benefits conferred on them by Plaintiff and the other members of the Class is unjust and inequitable, Anker must pay restitution to Plaintiff and the other members of the Class for their unjust enrichment, as ordered by the Court.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class members, prays for judgment and relief against Anker as follows:

a) For an order declaring: (i) this is a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of the proposed Class described herein; and (ii) appointing Plaintiff to serve as representative for the Class and Plaintiff's counsel to serve as Class Counsel;

b) For an order enjoining Anker from continuing to engage in the unlawful conduct set forth herein;

c) For an order awarding restitution of the monies Anker wrongfully acquired by its illegal and deceptive conduct;

d) For an order requiring disgorgement of the monies Anker wrongfully acquired by its illegal and deceptive conduct;

e) For compensatory and punitive damages, including actual and statutory damages, arising from Anker's wrongful conduct and illegal conduct;

f) For an award of reasonable attorneys' fees and costs and expenses incurred in the course of prosecuting this action; and

g) For such other and further relief as the Court deems just and proper.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all

claims in this Complaint so triable.

Dated: December 20, 2022

Respectfully submitted,

/s/ Gary M. Klinger

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Telephone: 866.252.0878
gklinger@milberg.com

Trenton R. Kashima (*Pro Hace Vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
401 West C St., Suite 1760
San Diego, CA 92101
Tel: (308) 870-7804
tkashima@milberg.com

Nick Suciu III (admitted to the General Bar)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
6905 Telegraph Rd., Suite 115
Bloomfield Hills, MI 48301
Tel.:(313) 303-3472
Fax:(865) 522-0049
nsuciu@milberg.com

Attorneys for Plaintiff