ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of

Assurance No. 24-103

Investigation by LETITIA JAMES,
Attorney General of the State of New York, of

FANTASIA TRADING LLC,
POWER MOBILE LIFE LLC, AND
SMART INNOVATION, LLC,

Respondents.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York ("NYAG") commenced an investigation, pursuant to Executive Law § 63(12) and General Business Law § 349, into the data security and privacy practices concerning the eufy-branded line of smart home security products. This Assurance of Discontinuance ("Assurance") contains the findings of the NYAG's investigation and the relief agreed to by the NYAG and Fantasia Trading LLC, Power Mobile Life LLC, and Smart Innovation, LLC (collectively, "Respondents"), whether acting through their respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries (collectively, the "Parties").

FINDINGS OF NYAG

1. Respondent Fantasia Trading LLC is a Delaware company with a mailing address at 5350 Ontario Mills Pkwy, Suite 100, Ontario, CA 91764.

2. Respondent Power Mobile Life LLC is a Washington company with a mailing address of 10800 NE 8th St., Suite 900, Bellevue, WA 98004.

3. Respondent Smart Innovation, LLC is a Delaware company with a mailing address of 10800 NE 8th St., Suite 900, Bellevue, WA 98004.

4. Respondents distribute a line of eufy-branded smart home security products. Those products are designed, developed, and manufactured by their parent company, Anker Innovations Technology Co., Ltd. and/or certain of its subsidiaries and affiliates (collectively, "Anker").[1] These eufy-branded smart home security products includes both cameras and camera-integrated devices, such as video doorbells and video smart locks ("eufy home security products"). Between January 1, 2018 and January 23, 2023, Respondents marketed, sold, and distributed more than 100,000 eufy security cameras, video doorbells, and eufy video smart locks to New York consumers.

5. Consumers can view footage from their eufy home security products through an online web portal, available at https://mysecurity.eufylife.com, as well as a free mobile application that Anker operates. The eufy mobile application can also be configured to provide a notification when a eufy home security product is activated. The notification can include still frames from the relevant video footage, such as the image of a person walking to a consumer's door.

6. The eufy home security products were marketed to consumers with assurances that their data would be kept private and secure, including claims that Respondents had taken "every step imaginable to ensure your data remains private," and that "every facet of our technology and process that we adopt has been tested and proven to protect your data under EU and US law." Through these statements, Respondents represented, expressly and by

[1] Counsel for Respondents have represented that Anker does not itself sell or distribute products in the United States, and that Anker's eufy-branded products are only sold and distributed in the United States through Respondents Fantasia Trading and Power Mobile Life.

implication, that there were reasonable safeguards to protect the confidentiality of consumer data.

7. Respondents' marketing also included many claims about specific privacy and security features, including that data on eufy home security products "never leaves the safety of your home, and is accessible by you alone," that the products use "End-to-End encryption," that "[d]ata during transmission is encrypted," that "[a]ll recorded footage is encrypted on-device and sent straight to your phone—and only you have the key to decrypt and watch the footage," that "[i]f you subscribe to our cloud storage service, your videos are securely stored in the cloud," and that "[t]here is no online link available to any video."[2]

8. These assurances were false. Respondents and Anker, the developer of the eufy-security products, had not adopted reasonable safeguards to protect consumer data, creating risks to consumers' privacy and security.

9. First, prior to November 1, 2022, neither Respondents nor Anker implemented end-to-end encryption when transmitting livestream video from a eufy home security device to the eufy web portal. For at least a portion of the connection between the security device and web portal, the video was not protected by any encryption (neither end-to-end nor transport-layer encryption).

10. Second, neither Respondents nor Anker had appropriate, functioning safeguards in place to ensure that only authorized users could view video with the relevant URL through the web portal. Due to flaws in the design and implementation of Anker's security controls, a user's active video stream could be accessed by anyone with the relevant URL, without authentication.

---

[2] *See* https://web.archive.org/web/20220815163349/https://us.eufy.com/pages/privacy-commitment (eufy's privacy commitment as of August 15, 2022).

11. Moreover, it may have been possible to deduce video stream URLs without obtaining them from users, as URLs were created according to deterministic rules. A security measure designed to mitigate this risk by validating that a link had come from a trusted user had not been implemented properly, and so was ineffective.

12. Neither Respondents nor Anker identified the flaws in these security controls because they did not have necessary processes in place to test the controls they had implemented or to identify risks to the security and privacy of customers' video.

13. Third, neither Respondents nor Anker had informed consumers or requested consent for a Covered Product to upload and store thumbnail images derived from videos onto Anker AWS servers in the United States when a consumer enabled push notifications.

14. In November 2022, a security researcher publicly disclosed several of the security and privacy issues described above. Anker acted promptly to remediate these issues, implementing end-to-end encryption for web-based streams and enhancing access control measures. Respondents have also represented that Respondents and Anker have taken steps to improve their information security programs, including: (i) requiring R&D personnel to complete comprehensive training regarding secure development principles; (ii) continued engagement of external vendors to assess the security and privacy of eufy products; (iii) establishing more robust internal policies, standards, and guidelines concerning product security; (iv) deploying more robust vulnerability scanning tools; and (v) establishing a bug bounty program.

Violations of Law

15. Respondents' conduct violated Executive Law § 63(12), which authorizes the NYAG to pursue repeated fraudulent or illegal acts, and General Business Law §§ 349 and 350, which prohibit deceptive acts and practices and false advertising.

16. Respondents neither admit nor deny the NYAG's Findings, paragraphs 1-14 above.

17. The NYAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the NYAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12), and General Business Law §§ 349 and 350.

PROSPECTIVE RELIEF

18. For the purposes of this Assurance, the following definitions shall apply:

a. "Covered AV Information" is a subset of Covered Information, consisting of all video, audio, images, and live stream data captured by a Covered Product.

b. "Covered Information" shall mean information inputted into, stored on, captured with, accessed, or transmitted by a Covered Product.

c. "Covered Product" shall mean any internet-enabled device that a Respondent or Anker designs, markets, or offers to consumers in New York primarily for personal and residential use to record, transmit, or store images or video for home security or monitoring purposes, and any related software and service that a Respondent or Anker designs, markets, or offers to consumers in New York to view, collect, or store images or video. Covered Products include devices marked under the eufy Security and eufy Baby line of products and any successor product.

d. "Product Developer" shall mean a Respondent or affiliate of a Respondent that develops or produces a Covered Product.

e. "Product Operator" shall mean a Respondent or affiliate of a Respondent that operates a web-based application or system in support of a Covered Product.

19. Respondents shall comply with Executive Law § 63(12) and General Business Law §§ 349 and 350 in connection with the privacy and/or security of each Covered Product, and shall not misrepresent the existence or strength of any encryption or other security feature of a Covered Product, or whether any unauthorized third party is capable of viewing videos or images captured on a Covered Product.

20. Beginning ninety (90) days after the Effective Date, Respondents shall regularly substantiate that, for each Covered Product a Respondent markets, sells, or distributes, the Product Developer and Product Operators have established, implemented, and maintained the security requirements of this Assurance. Substantiation shall include, but not be limited to, obtaining and reviewing, not less than annually, the documentation and reports required by Paragraphs 22 through 27, and a written certification by the Product Developer and Product Operators of compliance with these provisions. Respondents shall document and maintain records reflecting that the documentation, reports, and certifications have been obtained and reviewed. All documentation, reports, and certification shall be maintained by Respondents for at least five (5) years.

21. Beginning ninety (90) days after the Effective Date, Respondents shall clearly and conspicuously disclose to consumers any settings or features of any Covered Product that cause Covered AV Information to be transmitted from the Covered Product, and the categories of Covered AV Information that is transmitted.

SOFTWARE SECURITY PROGRAM

22. Beginning ninety (90) days after the Effective Date, Respondents shall regularly substantiate that, for each Covered Product a Respondent markets, sells, or distributes, the Product Developer and Product Operator have implemented and maintained a

written and comprehensive software security program ("Software Security Program") that is designed to protect the privacy and security of Covered Information. The Software Security Program shall, at a minimum, include the following processes:

a. Assess and document, at least once every twelve (12) months, internal and external risks to the security of Covered Products that could result in the unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of Covered Information;

b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control for the internal and external risks the Product Developer and Product Operator identified that are appropriate to (i) the size and complexity of the operation of the Product Developer and Product Operator; (ii) the nature and scope of the activities of the Product Developer and Product Operator; and (iii) the volume and sensitivity of Covered Information;

c. Assess, at least once every twelve (12) months the sufficiency of any safeguards in place to address the internal and external risks the Product Developer and Product Operator identified, and modify the Software Security Program based on the results to ensure that the safeguards comply with (b) above;

d. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months, and modify the Software Security Program based on the results to ensure that the safeguards comply with (b) above;

e. Select and retain service providers capable of maintaining reasonable security practices, contractually require service providers to implement and maintain reasonable safeguards to protect Covered Information, and take reasonable steps to verify service

providers are complying with the contractual requirements; and

f. Evaluate and adjust the Software Security Program in light of any changes to the operations or business arrangements of the Product Developer or Product Operator, or any other circumstances that the Product Developer or Product Operator know or have reason to know may have a material impact on the effectiveness of the Software Security Program. At a minimum, the Product Developer and Product Operator must evaluate the Software Security Program at least once every twelve (12) months and modify the Software Security Program based on the results.

23. Beginning ninety (90) days after the Effective Date, Respondents shall regularly substantiate that, for each Covered Product a Respondent markets, sells, or distributes, the Product Developer has appointed a qualified employee to be responsible for implementing, maintaining, and monitoring the Software Security Program. The appointed individual shall have credentials, background, and expertise in information security appropriate to the level, size, and complexity of the individual's role in implementing, maintaining, and monitoring the Software Security Program. The appointed individual shall report at a minimum semi-annually to the Chief Executive Officer and senior management, and shall report at a minimum semi-annually to the Board of Directors or equivalent governing body, or an appropriate committee thereof, concerning the Product Developer's security posture, the security risks faced by the Product Developer, and the Software Security Program.

24. Beginning ninety (90) days after the Effective Date, Respondents shall regularly substantiate that, for each Covered Product a Respondent markets, sells, or distributes, the Product Developer has provided notice of the requirements of the AOD to its management-level employees responsible for implementing, maintaining, or monitoring the Software Security

Program and shall implement appropriate training of such employees. The notice and training required under this paragraph shall be provided to the appropriate employees within sixty (60) days of the effective date of the AOD, or within thirty (30) days of when an employee first assumes responsibility for implementing, maintaining, or monitoring the Software Security Program. Notice and training shall be documented in writing, which shall be maintained by the designated individual referenced in Paragraph 23 of this Assurance for at least five (5) years.

INFORMATION SAFEGUARDS AND CONTROLS

25. Beginning ninety (90) days after the Effective Date, Respondents shall regularly substantiate that, for each Covered Product a Respondent markets, sells, or distributes, the Product Developer and Product Operator have established and implemented, and documented in writing, a vulnerability management program to identify, assess, and remediate security vulnerabilities. The vulnerability management program shall include at least the following:

a. reasonable penetration testing assessments of all in-production web-based applications and systems, and mobile applications that are associated with the Covered Product, conducted not less than annually by an independent, qualified third party. The results of the penetration testing assessments shall be documented in a report that shall be maintained by the designated individual referenced in Paragraph 23 of this Assurance for at least five (5) years.

b. vulnerability testing of all web-based applications and systems that are associated with the Covered Product, conducted not less than twice annually.

26. Beginning ninety (90) days after the Effective Date, Respondents shall regularly substantiate that, for each Covered Product a Respondent markets, sells, or distributes, the Product Developer has established and implemented, and documented in writing, appropriate policies and procedures for secure software development, such as the

implementation of Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST), in connection with all web-based applications, mobile applications, and other software, whether public-facing or internal, that are associated with the Covered Product.

27. Beginning ninety (90) days after the Effective Date, Respondents shall regularly substantiate that, for each Covered Product a Respondent markets, sells, or distributes, the Product Developer and Product Operator have established and implemented, and documented in writing, appropriate policies and procedures for the encryption of Covered Information. Such policies and procedures shall require at least the following:

a. encryption of all Covered AV Information collected by the Covered Product while in storage and in transit;

b. end-to-end encryption where a Respondent or the Product Developer has represented to consumers that end-to-end encryption is used; and

c. use of appropriate encryption algorithms with necessary properties of confidentiality, integrity, authentication, and forward secrecy as defined by the National Institute of Standards and Technology (NIST).

MONETARY PAYMENT

28. Respondents shall pay to the State of New York $450,000 in penalties and costs. Payment shall be made payable to the State of New York in full within fourteen (14) days of the effective date of this Assurance. Payment shall be made by wire transfer in accordance with instructions provided by an NYAG representative and shall reference AOD No. 24-103.

MISCELLANEOUS

29. If the NYAG believes a Respondent has failed to comply with a provision of the Assurance, and if in the NYAG's sole discretion the failure to comply does not threaten the

health or safety of the citizens of New York or create an emergency requiring immediate action, prior to taking legal action for any alleged failure to comply with the Assurance, the NYAG shall provide notice to the Respondent. The Respondent shall have 14 days from receipt of such notice (the "Notice Period") to provide a written response, including either a statement that Respondent believes it is in full compliance with the relevant provision or a statement explaining why it did not comply with the relevant provision, and how it has come into compliance or when it will come into compliance. Respondents shall not seek a declaratory judgment concerning any alleged failure to comply with the Assurance during the Notice Period.

30. Respondents expressly agree and acknowledge that the NYAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 37, and agree and acknowledge that in such event:

a. any statute of limitations or other time-related defenses are tolled from the effective date of this Assurance;

b. the NYAG may use statements, documents, or other materials produced or provided by Respondents prior to or after the effective date of this Assurance;

c. any civil action or proceeding shall be adjudicated by the courts of the State of New York, and that Respondents irrevocably and unconditionally waive any objection based upon personal jurisdiction, inconvenient forum, or venue; and

d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

31. If a court of competent jurisdiction determines that a Respondent has violated the Assurance, Respondent shall pay to the NYAG the reasonable cost, if any, of obtaining such

determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

32. This Assurance is not intended for use by any third party in any other proceeding. This Assurance is not intended, and should not be construed, as an admission of liability by Respondents.

33. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of Respondents. The Respondents shall include in any such successor, assignment or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of the NYAG.

34. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

35. Any failure by the NYAG to insist upon the strict performance by a Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the NYAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by the Respondent.

36. All notices, reports, requests, and other communications pursuant to this Assurance shall reference Assurance No. 24-103, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to Respondent Fantasia Trading LLC, to:

Alex Ma, or in his absence, to the Anker Legal & Compliance Team
5350 Ontario Mills Pkwy, Suite 100, Ontario, CA 91764

If to Respondent Power Mobile Life LLC, to:

Alex Ma, or in his absence, to the Anker Legal & Compliance Team
10800 NE 8th St., Suite 900, Bellevue, WA 98004

If to Respondent Smart Innovation, LLC, to:

Alex Ma, or in his absence, to the Anker Legal & Compliance Team
10800 NE 8th St., Suite 900, Bellevue, WA 98004

If to the NYAG, to:

Nathaniel Kosslyn, Assistant Attorney General, or in his absence, to the person holding the title of Bureau Chief,
Bureau of Internet & Technology,
28 Liberty Street, New York, NY 10005

37. The NYAG has agreed to the terms of this Assurance based on, among other things, the representations made to the NYAG by Respondents and their counsel and the NYAG's own factual investigation as set forth in the Findings, paragraphs (1)-(14) above. The Respondents represent and warrant that neither they nor their counsel have made any material representations to the NYAG that are inaccurate or misleading. If any material representations by Respondents or their counsel are later found to be inaccurate or misleading, this Assurance is voidable by the NYAG in its sole discretion.

38. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by the Respondents in agreeing to this Assurance.

39. Respondents represent and warrant, through the signatures below, that the terms and conditions of this Assurance are duly approved.

40. The obligations of this Assurance set forth in Paragraphs 22 through 27 shall expire at the conclusion of the seven (7) year period after the Effective Date.

41. Unless a term limit for compliance is otherwise specified within this Assurance, the Respondents' obligations under this Assurance are enduring. Nothing in this Agreement shall relieve Respondents of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

42. Respondents agree not to take any action or to make or permit to be made any public statement denying, directly or indirectly, any finding in the Assurance or creating the impression that the Assurance is without legal or factual basis. Nothing in this paragraph affects Respondents' right to take legal or factual positions in defense of litigation or other legal proceedings to which the NYAG is not a party.

43. Nothing contained herein shall be construed to limit the remedies available to the NYAG in the event that the Respondents violate the Assurance after its effective date.

44. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

45. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the NYAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

46. Respondents acknowledge that they have entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

47. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

48. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

49. This Assurance may be executed in multiple counterparts by the Parties hereto. All counterparts so executed shall constitute one agreement binding upon all Parties, notwithstanding that all Parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the effective date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned, and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

50. The effective date of this Assurance shall be the date of the last signature entered below.

LETITIA JAMES **ATTORNEY GENERAL OF THE STATE OF NEW YORK** By: Nathaniel Kosslyn By: Nathaniel Kosslyn Bureau of Internet and Technology Office of the New York State Attorney General 28 Liberty St. New York, NY 10005 Phone: (212) 416-6578 Fax: (212) 416-8369 1.24.2025 Date	**FANTASIA TRADING LLC** By: Robinson Cheng By: Robinson Cheng, General Counsel 1.15.2025 Date **POWER MOBILE LIFE LLC** By: Robinson Cheng By: Robinson Cheng, General Counsel 1.15.2025 Date **SMART INNOVATION, LLC** By: Robinson Cheng By: Robinson Cheng, General Counsel 1.15.2025 Date