IN THE DISTRICT COURT
OF LANCASTER COUNTY, NEBRASKA

STATE OF NEBRASKA, ex rel. MICHAEL T. HILGERS, ATTORNEY GENERAL, Plaintiff, v. RESIDEO TECHNOLOGIES, INC., a Delaware Corporation, Resideo LLC a Delaware Limited Liability Company, Defendants.	Case No: CI25-_____ **COMPLAINT**

COMES NOW, the State of Nebraska, ex rel. Michael T. Hilgers, Nebraska Attorney General, by and through the undersigned attorneys ("Attorney General," "State," or "Plaintiff"), and hereby brings this action against the above-named Defendants Resideo Technologies, Inc. and Resideo LLC d/b/a Ademco Inc. (collectively, "ADI" or "Defendants"), to address a pattern of deceptive and unfair business practices related to the marketing and sale of ADI security and smart-home solutions. Defendants have promoted and continue to promote ADI as a trusted source for security and smart-home solutions, claiming to "help keep our communities safe, secure, comfortable and connected"[1] and provide "solutions for educational and healthcare facilities, entertainment venues, offices, homes and more."[2]

In truth, however, ADI has deceptively marketed security

[1] https://perma.cc/CS54-UZ9P.
[2] https://perma.cc/HB6E-4TMM.

products that themselves have major security vulnerabilities, including deceptive statements and material omissions when advertising and selling products manufactured by Hangzhou Hikvision Digital Technology Co., Ltd. (collectively with its relevant affiliates, "Hikvision") and Zhejiang Dahua Technology Co., Ltd. (collectively with its relevant affiliates, "Dahua"). Since at least 2019, Hikvision and Dahua have been subject to sanctions by the U.S. government for national-security risks and human-rights violations as researchers have repeatedly found that these companies' cameras are subject to serious security risks. Yet, on information and belief, ADI has previously been engaged in "white labeling" Hikvision and Dahua Cameras—including in 2021-2022 *after* Congress passed the National Defense Authorization Act ("NDAA")—using ADI's own "Capture" brand. ADI continues to make deceptive statements and omissions related to the Hikvision and Dahua cameras it sells.

The State seeks to obtain injunctive relief, restitution for consumers, civil penalties, and other equitable relief to address Defendants' violations of the Consumer Protection Act, Neb. Rev. Stat. § 59-1601 et seq. ("CPA"), and the Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301 et seq. ("UDTPA"), in connection with the advertisement, marketing, promotion, and sale by ADI of Hikvision and Dahua cameras to Nebraska consumers.

INTRODUCTION

1. ADI deceptively markets itself and video security equipment it sells that is manufactured by Hangzhou Hikvision Digital Technology Co., Ltd. (collectively with its relevant affiliates, "Hikvision") and Zhejiang Dahua Technology Co., Ltd. (collectively with its relevant affiliates, "Dahua").

2. Congress, under Section 889 of the FY 2019 National Defense Authorization Act ("NDAA")[3] and the 2021 Secure Equipment Act ("SEA"),[4] placed Hikvision and Dahua on lists of companies that pose security concerns and whose products are subject to restrictions.

3. In 2022, the Federal Communications Commission ("FCC") deemed that telecommunications and surveillance equipment from Hikvision and Dahua posed an "unacceptable risk" to national security, and placed them on the "covered list."[5] In October 2025, the FCC issued a National Security Advisory to "reiterate" that risk[6] and later that month unanimously voted to propose additional rules to implement the "covered list."[7]

4. However, ADI has a deep relationship with both Hikvision and Dahua and has engaged in a yearslong pattern and practice of deceptive and unfair conduct to profit off selling Hikvision and Dahua cameras to unwitting U.S. consumers.

5. First, *after* Congress acted to put Hikvision and Dahua on lists of companies that were threats to national security, ADI, on information and belief, "white labeled" Dahua cameras using ADI's "Capture" brand.[8] Therefore, for two years (2021-2022) ADI sold

---

[3] Section 889(f)(3)(B)-(C), *see* PDF p. 283 of https://www.congress.gov/bill/115th-congress/house-bill/5515/text.
[4] https://www.congress.gov/bill/117th-congress/house-bill/3919/text.
[5] https://docs.fcc.gov/public/attachments/DOC-389524A1.pdf.
[6] https://docs.fcc.gov/public/attachments/DA-25-927A1.pdf.
[7] https://docs.fcc.gov/public/attachments/FCC-25-71A1.pdf.
[8] https://perma.cc/YZ42-65EB.

"Capture" brand cameras that were, on information and belief, actually Dahua-manufactured cameras.

6. Second, even to this day, ADI makes deceptive statements and omissions regarding the Hikvision and Dahua cameras that it sells.

7. An article on ADI's website that is marketing the benefits of Hikvision's suite of video surveillance products assures customers that "[a]ll data remains within the client's local network."[9] ADI's product page for Hikvision similarly promotes "video surveillance solutions for residential, commercial and institutional applications," with no statement or disclaimer about whether the products are appropriate for only certain types of "institution[s]," including those with critical infrastructure.[10] There is also no statement or disclaimer on either page that discloses Hikvision's security issues and its presence on U.S. government lists.

8. On ADI's product page for Dahua, it touts its "high performance security."[11] There is no statement or disclaimer clarifying this statement by disclosing Dahua's security issues and presence on U.S. government lists.

9. ADI's failure to disclose the risks of Hikvision and Dahua products while marketing them to consumers is deceptive and unfair.

10. ADI knows that consumers value security because it prominently advertises "NDAA COMPLAINT" on some of the cameras it sells.[12]

[9] https://perma.cc/B9B6-S4TY.
[10] https://perma.cc/MJD2-F8T3.
[11] https://perma.cc/G7QX-LMB9.
[12] https://perma.cc/L6JK-5M2A; https://perma.cc/K9KP-FDSZ.

Capture BY ADI 5MP CCTV Camera IR Motorized Zoom Turret -Brand New - Free P&P (3

Brand New

$39.14

Buy It Now

+$29.69 shipping estimate

Located in United Kingdom

Customs services and international tracking provided

sunflow9996 99.9% positive (2.1K)

Sponsored

Capture BY ADI 5MP CCTV Camera HD IR Fixed Eyeball -Brand New - Free P&P (3)

Brand New

$36.53

or Best Offer

+$29.61 shipping estimate

Located in United Kingdom

Free returns

Customs services and international tracking provided

sunflow9996 99.9% positive (2.1K)

Sponsored

Capture BY ADI 5MP CCTV Camera HD IR Varifocal Turret -Brand New - Free P&P (3)

Brand New

$39.14

Buy It Now

+$29.69 shipping estimate

Located in United Kingdom

Customs services and international tracking provided

sunflow9996 99.9% positive (2.1K)

Sponsored

NEW LOW PRICE

ADI Capture CCTV Security System 4 Channel NVR With 4x 5mp Cameras.

Brand New

$195.75

or Best Offer

+$114.66 shipping estimate

Located in United Kingdom

Customs services and international tracking provided

nowandthen1976 100% positive (732)

11. Yet ADI provides no corresponding disclosure on its website to consumers that discloses the security risks of non-NDAA compliance for Hikvision and Dahua cameras.

12. On information and belief, ADI has even falsely labeled a Hikvision camera as NDAA complaint.[13]

13. ADI publishes an "NDAA Compliant Solutions" page that does not disclose to consumers the risks of these Hikvision and Dahua cameras.[14]

14. Hikvision and Dahua cameras also have experienced multiple security vulnerabilities and other risks that a reasonable consumer would find significant when evaluating ADI's express representations about security. These include backdoor and other vulnerabilities and documented human-rights violations.[15]

15. The bipartisan Congressional-Executive Commission on China (CECC)[16] stated in a letter to ADI: "The telecommunication and surveillance equipment manufactured by [Hikvision and Dahua] is a recognized threat to American users" because "they are vulnerable to spying from hackers and information requests from [People's Republic of China] PRC intelligence entities."[17]

16. As the CECC noted in a related letter issued the same day: "No data collected can be withheld from PRC authorities should they request it for intelligence purposes—a vulnerability that . . .

---

[13] https://ipvm.com/reports/cecc-adi.
[14] https://perma.cc/7S6A-5ASH.
[15] https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/Costco%20Letter%20Signed.pdf; https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/ADI%20Letter%20-%20Signed.pdf.
[16] *See* https://www.cecc.gov; *see also* https://www.cecc.gov/media-center/press-releases/letter-to-costco-and-adi-raises-concerns-about-sale-of-banned-hikvision.
[17] https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/ADI%20Letter%20-%20Signed.pdf.

customers should be notified of."[18]

17. Despite this, ADI's promotion and sale of Hikvision and Dahua video surveillance products does not disclose these risks and would lead a reasonable consumer to believe they are appropriate for home and business use.

18. By making deceptive assurance of security while not disclosing the serious risks of surveillance and exploitation from using Hikvision and Dahua products, ADI has engaged in unfair and deceptive trade practices in violation of the CPA and UDTPA.

19. ADI's conduct has placed Nebraska consumers at serious risk of harm by potentially making some of their intimate images and private locations vulnerable to exploitation and intrusion by foreign actors with a Congressionally found record of nefarious and untrustworthy conduct.

20. The Attorney General brings this action to enjoin Defendants, hold them accountable, and to protect Nebraskans from having their images and privacy further jeopardized by ADI's egregious and unconscionable acts.

AUTHORITY & PUBLIC INTEREST

21. The Nebraska Attorney General is responsible for enforcement of the CPA, UDTPA, and other state and federal laws that affect Nebraska consumers.

22. Under Neb. Rev. Stat. § 59-1608 the Attorney General may bring an action in the name of the State of Nebraska against any person to restrain and prevent the doing of any act prohibited by the CPA.

[18] https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/Costco%20Letter%20Signed.pdf.

23. Under Neb. Rev. Stat. § 87-303.05, the Attorney General may apply for and obtain, in an action in any district court of Nebraska, a temporary restraining order, or injunction, or both, prohibiting such person from engaging in any deceptive trade practices or engaging therein, or doing any act in furtherance thereof.

24. The Attorney General has reasonable cause to believe that Defendants have violated the CPA and UDTPA and brings this action in the public interest because Defendants have deceived, misled, and caused financial harm to consumers from Nebraska and other states.

25. The Attorney General believes this action to be in the public interest of the citizens of the State of Nebraska and brings this lawsuit pursuant to the CPA, the UDTPA, and his statutory and common law authority, powers, and duties.

PARTIES

26. The State of Nebraska, by and through its Attorney General and on behalf of all of Nebraska's citizens and consumers, is the Plaintiff in this action.

27. The Attorney General of Nebraska is Nebraska's Chief Law Enforcement Officer. The Attorney General is expressly authorized to enforce Nebraska's consumer protection laws, including both the Consumer Protection Act and the Uniform Deceptive Trade Practices Act. Neb. Rev. Stat. § 59-1608(1); 87-303.05(1).

28. In addition to that express statutory authority, the Attorney General has standing to bring a legal action, in the name of the State, when the object of that action is a suit to vindicate the public interest. *See*, *State ex rel. Meyer v. Peters*, 188 Neb. 817, 819-21, 199 N.W.2d 738, 739-41 (1972); *State v. Pacific Express Co.*, 80 Neb. 823, 115 N.W. 619, 620-23 (1908).

29. Defendant Resideo Technologies, Inc. is a Delaware corporation with its headquarters located at 16100 N. 71st Street, Suite 550, Scottsdale, Arizona.[19]

30. Defendant Resideo Technologies, Inc. "manage[s] [its] business operations through two business segments, Products and Solutions and ADI Global Distribution." *See* p. 3, Resideo 10-K.[20, 21]

31. ADI Global Distribution is the trade name under which Resideo Technologies Inc. conducts its distribution business.[22]

32. Defendant Resideo LLC f/k/a Ademco Inc. is a Delaware LLC and is part of Resideo Technologies, Inc. Resideo LLC is listed as a subsidiary on Resideo Technologies, Inc.'s 10-K.[23] Resideo LLC has an active registration with the Nebraska Secretary of State.[24] It lists its corporate address at 2 Corporate Center Drive, Melville, NY 11747.

33. The nature of Resideo LLC's business is manufacturing and/or distributing home comfort, connected home and security solutions.

34. Defendants transact business in Nebraska by marketing, offering, and selling Hikvision and Dahua-branded security cameras to Nebraska consumers, including through an ADI Global Distribution retail and/or warehouse branch at 9840 M Street, Omaha, Nebraska 68127.

35. Defendants act in concert to advertise, promote, and sell Hikvision and Dahua cameras in Nebraska. Defendants share

---

[19] https://www.sec.gov/Archives/edgar/data/1740332/000174033225000013/rezi-20250314.htm.
[20] https://d18rn0p25nwr6d.cloudfront.net/CIK-0001740332/3fe9de3a-59a5-47db-b954-b242781c2856.pdf.
[21] https://www.securitysystemsnews.com/article/honeywell-homes-and-adi-spin-be-renamed-resideo.
[22] https://perma.cc/A4X4-FTBW; *see also* https://www.sec.gov/Archives/edgar/data/1740332/000156459021008469/rezi-ex211_3594.htm
[23] *See* https://d18rn0p25nwr6d.cloudfront.net/CIK-0001740332/3fe9de3a-59a5-47db-b954-b242781c2856.pdf, at p. 126.
[24] https://www.nebraska.gov/sos/corp/corpsearch.cgi?acct-number=10262305.

common business purposes, operate as an integrated enterprise, and are collectively responsible for the deceptive and unfair practices alleged in this Complaint.

JURISDICTION AND VENUE

36. At all times relevant to this Complaint, Defendants were engaged in trade and commerce affecting consumers in Nebraska insofar as they marketed, offered, and sold home security cameras to Nebraska residents through ADI's website and its Nebraska retail and warehouse branch.

37. This Court has personal jurisdiction over Defendants because the conduct and injuries from which this Complaint arises took place in Nebraska, harmed Nebraskans, and specifically targeted Nebraskans.

38. This Court has jurisdiction over the subject matter of this action under Neb. Rev. Stat. §§ 59-1608, 59-1608.01, and 87-303.05, because Defendants have engaged in unfair, deceptive, and unconscionable acts or practices in Nebraska in violation of the CPA and UDTPA.

39. Venue is proper in this Court pursuant to Neb. Rev. Stat. §§ 25-403.01 and 25-403.02 because Defendants transact business in Nebraska, advertise and sell products to Nebraska residents, and the unlawful acts and practices alleged herein caused injury to consumers in this county and throughout the State.

FACTUAL ALLEGATIONS

I. Hikvision and Dahua Are Prohibited Companies with Repeated Security Issues

40. Hikvision and Dahua are companies that the U.S. Department of Defense ("DOD") designated as "Chinese military companies" under the FY21 National Defense Authorization Act ("NDAA"). This means, for example, that DOD has determined that Dahua is, or is owned or controlled by, a military-civil fusion contributor for the Chinese military.[25]

41. The U.S. Department of Commerce has listed Hikvision and Dahua on its Entity List for their role in mass surveillance of Uyghurs in Xinjiang, restricting U.S. exports of technology to the company.[26]

42. Additionally, Congress in Section 889 of the 2019 NDAA listed "video surveillance and telecommunications equipment" produced by Hikvision, Dahua, or any subsidiary or affiliate, as "Covered Telecommunications Equipment or Services," prohibiting Hikvision and Dahua equipment from being used in federal contracts and grant-funded projects due to cybersecurity and national security risks.[27]

---

[25] https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF, at p. 2, 5; https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744/appendix-Supplement%20No.%204%20to%20Part%20744; *see also* 86 Fed. Reg. 33,994 (June 28, 2021), https://www.federalregister.gov/documents/2021/06/28/2021-13753/notice-of-designation-of-chinese-military-companies-under-the-william-m-mac-thornberry-ndaa-for-fy21; FY 2021 NDAA § 1260H, *see* PDF p. 579, https://www.congress.gov/bill/116th-congress/house-bill/6395/text.

[26] https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list; https://www.sdmmag.com/articles/97227-hikvision-and-dahua-barred-from-selling-to-us-government-agencies; https://www.cnbc.com/2019/10/07/us-names-hikvision-chinese-security-bureaus-to-economic-blacklist.html?msockid=081d56a036cb68da37fd43db37aa69aa.

[27] https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf?download=1, at p. 283.

43. The FCC has also listed, as of March 12, 2021, "Video surveillance and telecommunications equipment produced by [Hikvision and] Dahua Technology Company, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment" as "Covered Equipment or Services."[28]

44. In 2021, Congress passed the Secure Equipment Act ("SEA"), which directed the FCC to no longer approve any equipment on the Covered List for marketing or sale within the United States related to critical infrastructure.[29]

45. The FCC therefore banned "the authorization of [Hikvision and Dahua's] products for marketing and sale in the United States, to the extent that the products are used 'for the purpose of ... physical security surveillance of critical infrastructure.'"[30] The D.C. Circuit affirmed in part and vacated in part for the FCC "to comport its definition [of 'critical infrastructure'] and justification for it with the statutory text of the NDAA."[31]

46. The FCC voted unanimously on October 28, 2025, to "[p]ropose a definition of 'critical infrastructure' as used on the Covered List and seek comment on the implementation of that definition" and to "[s]eek comment on whether any device modification made by an entity identified on the Covered List should require full certification."[32] These past and proposed actions by the FCC show the ongoing seriousness of the security risks involving

---

[28] https://www.fcc.gov/supplychain/coveredlist.
[29] *Hikvision USA, Inc. v. Fed. Commc'ns Comm'n*, 97 F.4th 938, 940 (D.C. Cir. 2024).
[30] *Hikvision USA, Inc. v. Fed. Commc'ns Comm'n*, 97 F.4th 938, 944 (D.C. Cir. 2024).
[31] *Hikvision USA, Inc. v. Fed. Commc'ns Comm'n*, 97 F.4th 938, 950 (D.C. Cir. 2024).
[32] https://docs.fcc.gov/public/attachments/DOC-415051A1.pdf, at p. 1. For a recording of the meeting, see https://www.fcc.gov/October2025.

Hikvision and Dahua.

47. Additionally, Australia removed Hikvision and Dahua cameras from government facilities, citing national security threats and human rights violations, as they have been "directly implicated in the alleged human rights abuses and mass surveillance of Uyghurs in Xinjiang."[33]

48. Bans of Dahua and Hikvision have been increasing around the world.[34]

49. In addition to their presence on government lists, Dahua and Hikvision have been subject to criticism for purposefully creating a "backdoor vulnerability" for wiretapping.[35]

50. Dating back to 2019, before Hikvision and Dahua were designated as Chinese Military Companies,[36] U.S. researchers at The Internet Protocol Video Market ("IPVM") discovered "that millions of [Dahua] cameras have been carrying the potential to be used as eavesdropping devices—even when the audio on the camera is disabled."[37]

51. IPVM is a respected authority on surveillance technology, recognized by Time magazine as a "leading source of information on the harms of facial-recognition technology."[38]

52. IPVM has released directory lists of numerous U.S. and

---

[33] https://www.bbc.com/news/world-australia-64577641.
[34] https://ipvm.com/reports/hikua-bans.
[35] https://ipvm.com/reports/security-exploits; https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/.
[36] https://www.war.gov/News/Releases/Release/Article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/.
[37] https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/.
[38] https://time.com/collection/time100-ai/6308784/john-honovich/.

Canadian companies that are engaging in original equipment manufacturing (OEM) or white-labeling of Hikvision, Dahua, and other Chinese-manufactured cameras.[39]

53. According to IPVM, it lists only those OEMs it has "verified by examining shipping records, product documentation, and/or testing products."[40]

54. Further, according to IPVM, "Dahua cybersecurity history has numerous vulnerabilities, many rated as critical, and it regularly fails to provide complete lists of affected models or firmware versions."[41]

55. Experts describe this "backdoor" vulnerability as "intentional," stating the backdoor has been "'placed into the product by the vendor' by using hard-coded credentials in firmware for cameras."[42]

56. Examples exposing Hikvision's pattern of security vulnerabilities include the following:

a. July 2023 — Child Sex Abuse Material on Sale. A 2023 IPVM report found that child sex abuse material was being sold online from hacked Hikvision cameras, with criminal sellers using Hikvision's Hik-Connect app to distribute the material.[43]

b. June 2023 — Embedded Backdoors Revealed. A 2023

[39] https://ipvm.com/reports/hikvision-oem-directory (Hikvision); https://ipvm.com/reports/dahua-oem (Dahua).
[40] https://ipvm.com/reports/dahua-oem (Dahua); *accord* https://ipvm.com/reports/hikvision-oem-directory (Hikvision).
[41] https://ipvm.com/reports/security-exploits.
[42] https://ipvm.com/reports/security-exploits.
[43] https://ipvm.com/reports/cp-sale-hack. The "Hik-Connect – for End user" app was developed by and is copyrighted by Hikvision, and is still available for download on the App Store; it was updated as recently as November 6, 2025, https://apps.apple.com/us/app/hik-connect-for-end-user/id1087803190.

BBC investigation determined that Hikvision engineers embedded backdoors which allowed unauthorized access to camera feeds. According to the BBC, volunteer "hackers" were able to use the backdoor mechanism to access cameras inside the BBC studio, zoom into the laptop of a user inside the studio and record his keystrokes, giving the hackers seemingly unfettered access to his computer.[44]

c. September 2021 — Command Injection Vulnerability. In 2021, the Cybersecurity & Infrastructure Security Agency (CISA) identifies a 2021 command injection vulnerability for Hikvision cameras in its known exploited vulnerabilities catalog.[45] This vulnerability was scored as a 9.8/10, indicating its critical nature.[46] A later investigation revealed that more than 10,600 U.S. cameras were affected.[47]

d. August 2018 — National Vulnerability Database Number, Common Vulnerabilities and Exposures ("CVE") Number CVE-2018-6414: "A buffer overflow vulnerability in the web server of some Hikvision IP Cameras allows an attacker to send a specially crafted message to affected devices. Due to the insufficient input validation, successful exploit can corrupt memory and lead to arbitrary code execution or crash the process."[48]

e. 2017 — IPVM Map of Known Breaches. In 2017, IPVM provided a map of known breaches of Hikvision

[44] https://www.bbc.com/news/technology-65975446.
[45] https://www.cisa.gov/news-events/alerts/2021/09/28/rce-vulnerability-hikvision-cameras-cve-2021-36260.
[46] https://perma.cc/KX92-Q3FS.
[47] https://therecord.media/experts-warn-of-widespread-exploitation-involving-hikvision-cameras.
[48] https://nvd.nist.gov/vuln/detail/CVE-2018-6414.

cameras worldwide, including hundreds across the United States.[49]

57. Examples exposing Dahua's pattern of security vulnerabilities include the following:

a. July 2025 — National Vulnerability Database Number, CVE Number CVE-2025-31700: "Attackers could exploit a buffer overflow vulnerability by sending specially crafted malicious packets, potentially causing service disruption (e.g., crashes) or remote code execution (RCE). Some devices may have deployed protection mechanisms such as Address Space Layout Randomization (ASLR), which reduces the likelihood of successful RCE exploitation. However, denial-of-service (DoS) attacks remain a concern."[50]

b. January 2023 — Dahua DSS Software[51] 12 Vulnerabilities Discovered and Analyzed. IPVM discovered and reported 12 CVEs impacting around 3,100 devices, with potential for chain attacks resulting in system takeover. A number of hidden features, some of which allow Server-Side Request Forgery (SSRF), Remote Code Execution (RCE), and unchecked ICMP requests, can be used for Distributed Denial of Service (DDoS) attacks.[52]

c. January 2022 — Dahua Broken Access Control Vulnerability. A critical-level vulnerability rated 9.8/10.0 by NIST that Dahua originally reported as

[49] https://ipvm-uploads.s3.amazonaws.com/report-assets/hik-hack-map/index.html.
[50] https://nvd.nist.gov/vuln/detail/CVE-2025-31700.
[51] DSS Software refers to Digital Surveillance System, which is "an all-in-one Central Management System (CMS) / Video Management System (VMS) that encompasses a wide range of features and functions within video surveillance." https://dahuawiki.com/DSS.
[52] https://ipvm.com/reports/security-exploits.

only 8.1. It allows attackers to reset device passwords. Dahua refused to publish an advisory on its U.S. site or disclose which North American models were affected, and an advisory published on its international site has since been removed.[53]

d. September 2021 — Dahua New Critical Vulnerabilities 2021.[54] Two new critical-level vulnerabilities rated 9.8/10.0 that allow authentication bypass without valid credentials. Dahua's response raised several distinct concerns that contradicted industry standards: 1) Dahua assigned lower severity ratings of 8.1 and 7.3 over the objections of the discovering researcher by manipulating CVSS criteria, later updated to 9.8 by NIST; 2) Dahua released a patch in July 2021 described as "Fix some tiny bugs" with no mention of the vulnerabilities; 3) Dahua subsequently waited two months before informing users of the vulnerabilities in September 2021.[55]

e. May 2020 — Dahua Critical Cloud Vulnerabilities. Dahua and 22 OEMs were discovered to have hard-coded cloud keys/passwords which could be used to gain full access to cloud connected equipment.[56]

f. March 2017 — Dahua cameras and DVRs/NVRs allowed unauthorized remote admin access to Dahua devices by downloading an unprotected configuration file containing usernames and passwords, an exploit the researcher who discovered it said worked 'like a damn Hollywood hack, click on one button and you

[53] https://ipvm.com/reports/security-exploits.
[54] https://ipvm.com/reports/dahua-21-critical.
[55] https://ipvm.com/reports/security-exploits.
[56] https://ipvm.com/reports/security-exploits.

> are in.' It worked by downloading an unprotected configuration file containing usernames and passwords, and its design indicated it was intentional. The vulnerability received DHS ICS-CERT's highest score of 10.0/10.0 and affected over 1 million Dahua devices globally.[57]

58. These security risks must be understood in the context of prior PRC state-sponsored hacking campaigns using "living off the land" (LOTL) tactics, which allow undetected monitoring of computer and camera activity. Because Hikvision and Dahua are Chinese military companies manufacturing these products, they may be facilitating LOTL techniques to capture information without users knowing.[58]

II. ADI Makes Misleading Representations and Omissions About the Security of the Hikvision and Dahua Products It Sells

59. ADI has engaged in a pattern or practice of, on information and belief, white labeling cameras manufactured by Dahua *after* the United States placed that company on a restricted list and continuing to sell Hikvision and Dahua cameras with deceptive representations and misleading omissions. When ADI does make disclosure regarding the NDAA, it does so in a deceptive manner, particularly given the fact that the vast majority (75%-90%) of certain products it lists are not able to be confirmed as NDAA-compliant.

---

[57] https://ipvm.com/reports/security-exploits; *see also* https://www.cisa.gov/news-events/ics-advisories/icsa-17-124-02.

[58] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a; https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a; https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3669159/combatting-cyber-threat-actors-perpetrating-living-off-the-land-intrusions/; https://www.cisa.gov/sites/default/files/2025-03/Joint-Guidance-Identifying-and-Mitigating-LOTL508.pdf.

a. ADI white labeled Dahua-manufactured cameras under ADI's "Capture" brand from 2021-2022

60. Congress, under Section 889 of the FY 2019 National Defense Authorization Act ("NDAA")[59] and the 2021 Secure Equipment Act ("SEA"),[60] placed Hikvision and Dahua on lists of companies that pose security concerns and whose products are subject to restrictions.

61. After this occurrence, on information and belief, ADI started white labeling Dahua cameras under ADI's "Capture" brand.[61] Consumers were therefore unwittingly purchasing cameras from a manufacturer that the federal government had just taken action on.

62. On information and belief (given the time period that consumers keep cameras), some Nebraska consumers still have these white labeled Dahua cameras in their homes and other locations.

63. On information and belief, ADI stopped using Dahua cameras in its "Capture" brand in 2022 but did not take steps to cure its prior deception. IPVM reported that ADI made the change without disclosure.[62]

b. ADI makes deceptive representations and omissions on its webpages related to Dahua and Hikvision

64. ADI has made multiple misleading representations and omissions related to itself and the Hikvision and Dahua products ADI

[59] Section 889(f)(3)(B)-(C), *see* PDF p. 283 of https://www.congress.gov/bill/115th-congress/house-bill/5515/text.
[60] https://www.congress.gov/bill/117th-congress/house-bill/3919/text.
[61] https://perma.cc/YZ42-65EB; https://ipvm.com/reports/adi-re-dahua (May 5, 2021 article reporting "ADI has started to secretly relabel Dahua with Huawei chips inside, IPVM has verified.").
[62] https://ipvm.com/reports/adi-stop-dahua-re

sells.

65. On its homepage, ADI states that it is a trusted source for security and smart-home solutions, claiming to "help keep our communities safe, secure, comfortable and connected."[63]

66. On its Solutions page, ADI assures consumers that it can provide "solutions for educational and healthcare facilities, entertainment venues, offices, homes and more."[64]

67. In an article devoted to extolling the benefits of Hikvision's suite of video surveillance products, ADI assures customers that "[a]ll data remains within the client's local network."[65]

68. On the product page for Hikvision, ADI promotes "video surveillance solutions for residential, commercial and institutional applications."[66]

69. On the product page for Dahua, ADI touts its "high performance security."[67]

70. ADI promotes Hikvision and Dahua products on its website without disclosing known risks and vulnerabilities in using the companies' products, including the prohibition on the use of the companies' products in critical infrastructure.

71. ADI provides or links to product user manuals that emphasize security protections and recommended configurations but omit disclosure of fundamental vulnerabilities and limitations.[68]

---

[63] https://perma.cc/CS54-UZ9P.
[64] https://perma.cc/HB6E-4TMM.
[65] https://perma.cc/B9B6-S4TY.
[66] https://perma.cc/MJD2-F8T3.
[67] https://perma.cc/G7QX-LMB9.
[68] *See, e.g.*, https://perma.cc/TP9S-C82N (linking to https://perma.cc/PGX5-V5MN at VII–IX (user manual listing specific actions under "Cybersecurity Recommendations" but failing to disclose known risks).

72. ADI publishes an "NDAA Compliant Solutions" page[69] but its description suggests that NDAA compliance is only relevant for certain projects, and fails to state or disclose to consumers that the issue of NDAA compliance relates to security generally. This is therefore a deceptive description.

73. These omissions were material because they involved product safety and performance and would be important to a reasonable consumer's purchasing decision.

74. ADI prominently markets NDAA compliance on various cameras, but at the same time makes deceptive statements and omissions related to Hikvision and Dahua cameras, which are not NDAA compliant.

75. Consumers also reasonably rely on product manuals as core, authoritative materials to assess product safety and make purchasing decisions.

76. ADI knew or should have known that consumers would rely on these materials in evaluating ADI's product offerings.

77. By highlighting security features and promoting Hikvision and Dahua products while omitting known or foreseeable vulnerabilities, ADI also created a misleading net impression that the products deliver robust security when used as intended.

78. By curating, disseminating, and directing consumers to these materials on its own website, ADI adopted and republished the content in furtherance of sales.

79. ADI's conduct occurred in the course of trade or commerce and affected the public interest.

80. As a direct and proximate result of these omissions,

[69] https://perma.cc/7S6A-5ASH.

consumers paid for products they otherwise would not have purchased or paid more than they would have paid had ADI not engaged in the deception.

c. ADI was questioned specifically in a letter by members of congress in 2023

81. In October 2023, Representative Christopher Smith and Senator Jeffrey Merkley, the co-chairs of the bipartisan Congressional-Executive Commission on China (CECC),[70] sent a letter to ADI's President.[71]

82. The letter stated in part: "The telecommunication and surveillance equipment manufactured by [Hikvision and Dahua] is a recognized threat to American users" because "they are vulnerable to spying from hackers and information requests from [People's Republic of China] intelligence entities."[72]

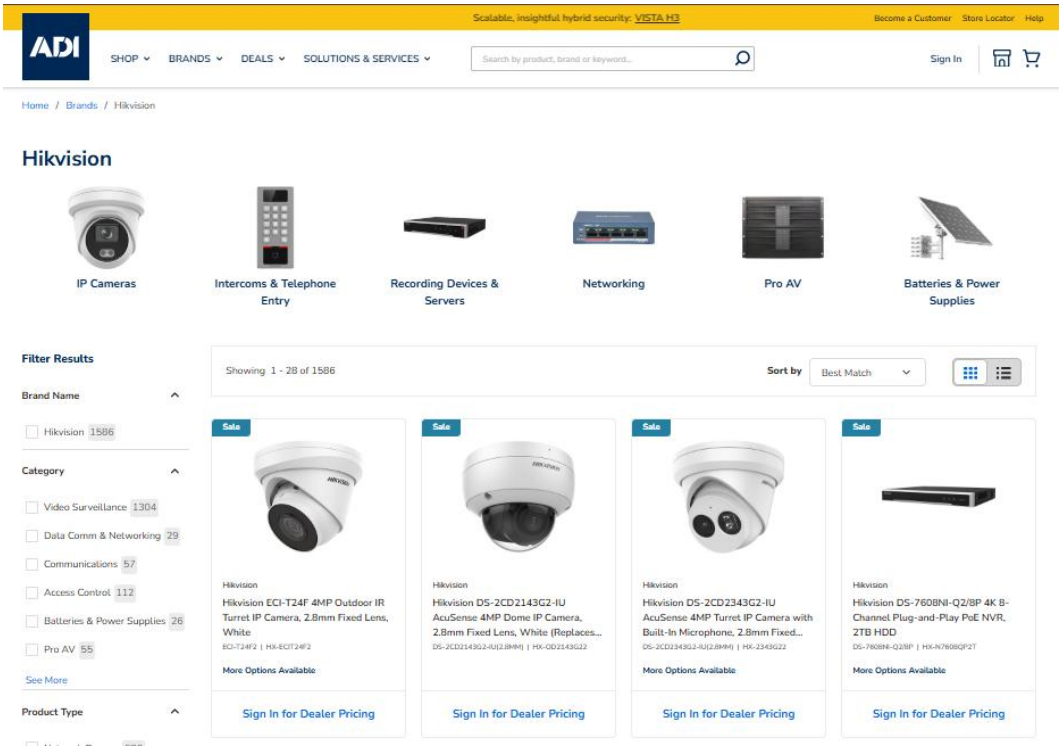
83. As the CECC noted in a related letter issued the same day: "No data collected can be withheld from PRC authorities should they request it for intelligence purposes—a vulnerability that . . . customers should be notified of."[73]

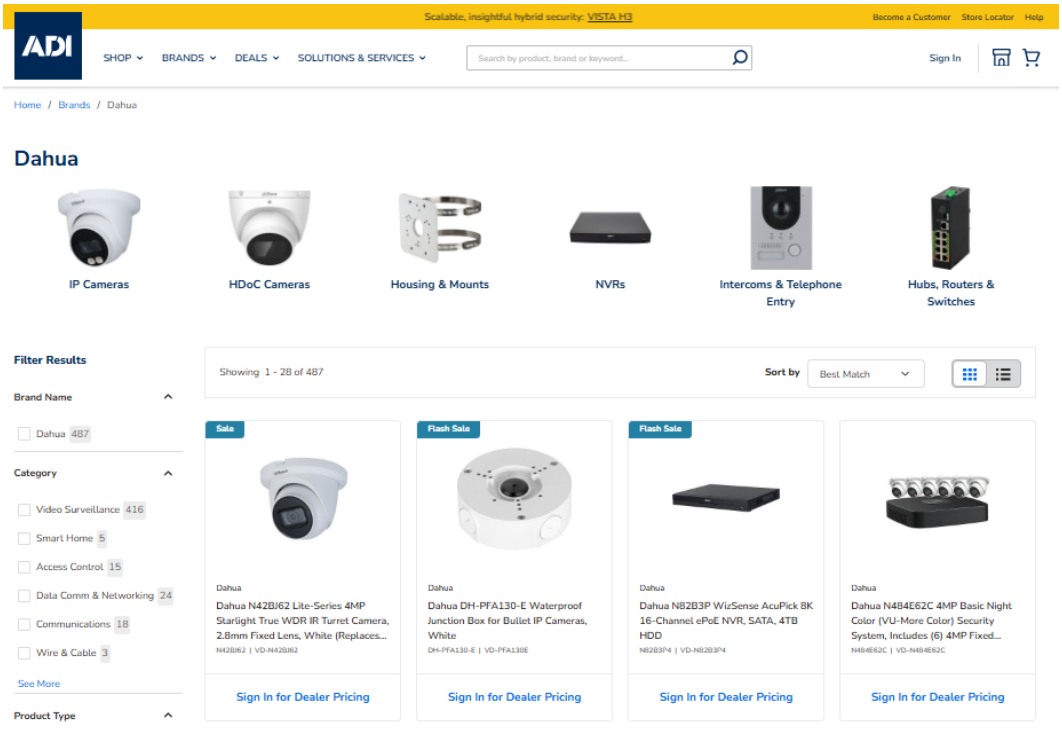
d. ADI's website still displays Hikvision and Dahua products

84. Nonetheless, the ADI website still prominently displays thousands of Hikvision and Dahua products.[74]

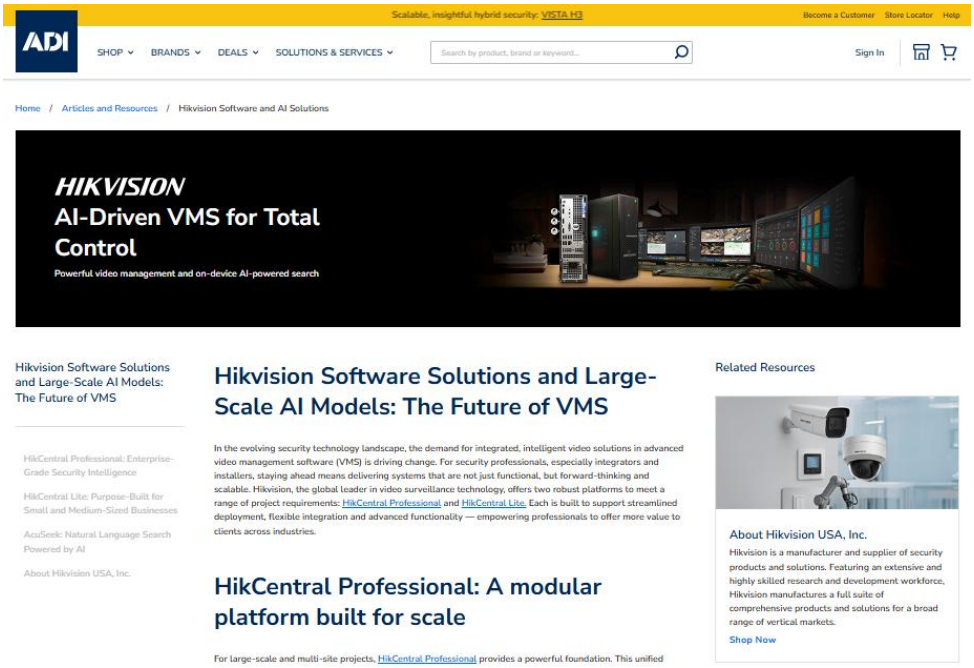
---

[70] *See* https://www.cecc.gov/.
[71] https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/ADI%20Letter%20-%20Signed.pdf; *see also* https://www.cecc.gov/media-center/press-releases/letter-to-costco-and-adi-raises-concerns-about-sale-of-banned-hikvision.
[72] https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/ADI%20Letter%20-%20Signed.pdf.
[73] https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/Costco%20Letter%20Signed.pdf.
[74] https://perma.cc/MJD2-F8T3 (Hikvision); https://perma.cc/F8Z9-28CL (Dahua).


Scalable, insightful hybrid security: VISTA H3
Become a Customer
Store Locator
Help
ADI
SHOP
BRANDS
DEALS
SOLUTIONS & SERVICES
Search by product, brand or keyword...
Sign In
Home / Brands / Hikvision
Hikvision
IP Cameras
Intercoms & Telephone Entry
Recording Devices & Servers
Networking
Pro AV
Batteries & Power Supplies
Filter Results
Brand Name
Hikvision 1586
Category
Video Surveillance 1304
Data Comm & Networking 29
Communications 57
Access Control 112
Batteries & Power Supplies 26
Pro AV 55
See More
Product Type
Showing 1 - 28 of 1586
Sort by
Best Match
Sale
Hikvision
Hikvision ECI-T24F 4MP Outdoor IR Turret IP Camera, 2.8mm Fixed Lens, White
More Options Available
Hikvision DS-2CD2143G2-IU AcuSense 4MP Dome IP Camera, 2.8mm Fixed Lens, White (Replaces...
Hikvision DS-2CD2343G2-IU AcuSense 4MP Turret IP Camera with Built-In Microphone, 2.8mm Fixed...
Hikvision DS-7608NI-Q2/8P 4K 8-Channel Plug-and-Play PoE NVR, 2TB HDD
Sign In for Dealer Pricing


Scalable, insightful hybrid security: VISTA H3
Become a Customer
Store Locator
Help
ADI
SHOP
BRANDS
DEALS
SOLUTIONS & SERVICES
Search by product, brand or keyword...
Sign In
Home / Brands / Dahua
Dahua
IP Cameras
HDoC Cameras
Housing & Mounts
NVRs
Intercoms & Telephone Entry
Hubs, Routers & Switches
Filter Results
Brand Name
Dahua 487
Category
Video Surveillance 416
Smart Home 5
Access Control 15
Data Comm & Networking 24
Communications 18
Wire & Cable 3
See More
Product Type
Showing 1 - 28 of 487
Sort by
Best Match
Sale
Flash Sale
Dahua
Dahua N42BJ62 Lite-Series 4MP Starlight True WDR IR Turret Camera, 2.8mm Fixed Lens, White (Replaces...
Dahua DH-PFA130-E Waterproof Junction Box for Bullet IP Cameras, White
Dahua N82B3P WizSense AcuPick 8K 16-Channel ePoE NVR, SATA, 4TB HDD
Dahua N4B4E62C 4MP Basic Night Color (VU-More Color) Security System, Includes (6) 4MP Fixed...
Sign In for Dealer Pricing

85. ADI even devoted an article to extolling the benefits of Hikvision's suite of video surveillance products, assuring customers that "[a]ll data remains within the client's local network."[75]



86. ADI does not disclose the known risks associated with Hikvision and Dahua products.

e. **ADI continues to deceive customers related to the risks of non-NDAA-listed products–and over 75%-90% of its listed products in certain categories are not certified as NDAA-compliant.**

87. ADI publishes an "NDAA Compliant Solutions" page[76] but its description suggests that NDAA compliance is only relevant for certain projects, and fails to state or disclose to consumers that the

[75] https://perma.cc/B9B6-S4TY.
[76] https://perma.cc/7S6A-5ASH.

issue of NDAA compliance relates to security generally.

88. These omissions were material because they involved product safety and performance and would be important to a reasonable consumer's purchasing decision.

89. According to IPVM, ADI Global also made false statements that a Hikvision camera was NDAA complaint when they were not.[77]

90. According to IPVM, ADI Global simply deleted this field when it was pointed out to them. *Id.*

91. ADI's deceptive statements and omissions regarding the security risks of non-NDAA compliant products are particularly concerning because the *vast majority* of products ADI offers for sale in certain categories are not NDAA-compliant. For these products, ADI cannot conclude that its manufacturer is not owned or controlled by a military-civil fusion contributor for the Chinese military.[78]

a. Only 201 out of the 804 IP bullet cameras that ADI offers for sale are listed as NDAA compliant.[79]

b. Only 311 out of the 1011 dome cameras that ADI offers for sale are listed as NDAA compliant.[80]

c. Only 197 out of the 2,152 network video recorders

[77] https://ipvm.com/reports/cecc-adi.
[78] https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF; https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744/appendix-Supplement%20No.%204%20to%20Part%20744; *see also* 86 Fed. Reg. 33,994 (June 28, 2021), https://www.federalregister.gov/documents/2021/06/28/2021-13753/notice-of-designation-of-chinese-military-companies-under-the-william-m-mac-thornberry-ndaa-for-fy21; FY 2021 NDAA § 1260H, see PDF p. 579, https://www.congress.gov/bill/116th-congress/house-bill/6395/text.
[79] https://perma.cc/CH77-EBTY (click box "Yes" for NDAA compliant and, number of products reduces from 804 to 201).
[80] https://perma.cc/3XWG-FMXM (click box "Yes" for NDAA compliant and, number of products reduces from 1011 to 311).

that ADI offers for sale are listed as NDAA compliant.[81]

III. ADI Makes Misleading Representations and Omissions About Human Trafficking and Anti-Slavery for the Products It Sells

92. ADI's website also makes it misleading for an additional reason, which is that ADI has made express representations about its disclosure of human trafficking and anti-slavery. This website states that ADI "does not tolerate human trafficking or slavery in its operations or its suppliers' operations."[82]

93. Given that ADI's website had an express page about the NDAA and it received a letter in October 2023 from the Congressional CECC, it is misleading for ADI not to disclose that Hikvision and Dahua are listed on the U.S. Department of Commerce's Entity List for their role in mass surveillance of Uyghurs in Xinjiang.[83]

CAUSES OF ACTION

94. ADI has routinely withheld material information and misled consumers in connection with the marketing, advertisement, and sale of its cameras and other surveillance equipment. The Attorney General brings this action to expose ADI's misleading and deceptive behavior, to prevent ADI from continuing to jeopardize Nebraskans' privacy and security, and to hold them accountable for their repeated violations of Nebraska's consumer protection laws.

---

[81] https://perma.cc/MX73-AVTX (click box "Yes" for NDAA compliant and, number of products reduces from 2,152 to 197).
[82] https://perma.cc/T4HA-FN39. Snap One Holdings Corp. became part of ADI in 2024 when it was acquired by ADI owner Resideo Technologies, Inc., https://perma.cc/NG4L-6DTM.
[83] https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain entities-to-the-entity-list; https://www.sdmmag.com/articles/97227-hikvision-and-dahua barred-from-selling-to-us-government-agencies; https://www.cnbc.com/2019/10/07/us-names-hikvision-chinese-security-bureaus-to-economic-blacklist.html.

COUNTS I–VI: VIOLATIONS OF THE CONSUMER PROTECTION ACT BY RESIDEO LLC AND RESIDEO TECHNOLOGIES, INC. – DECEPTIVE AND UNFAIR BUSINESS PRACTICES
(Neb. Rev. Stat. § 59-1602 et seq.)

95. The State of Nebraska re-alleges the facts above and incorporates them herein by reference.

96. Defendants Resideo LLC and Resideo Technologies, Inc. are "persons" within the meaning of the CPA, Neb. Rev. Stat. § 59-1601(1).

97. Defendants conducted "trade and commerce" within the meaning of the CPA, Neb. Rev. Stat. § 59-1601(2), by advertising, marketing, offering for sale, and selling Hikvision and Dahua cameras to Nebraska consumers.

98. The CPA, Neb. Rev. Stat. § 59-1602, prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce."

99. An act or practice is deceptive if it possesses the tendency or capacity to mislead or creates the likelihood of deception.

100. The CPA, Neb. Rev. Stat. § 59-1602, prohibits "unfair"

acts or practices in the conduct of any trade or commerce.

101. An act or practice is unfair if it is offensive to public policy, immoral, unethical, oppressive, unscrupulous, or falls within some common law, statutory, or other established concept of unfairness, or causes substantial injury to consumers.

102. Defendants engaged in deceptive and/or unfair acts or practices in violation of the CPA, Neb. Rev. Stat. § 59-1602, by, without limitation:

a. Representing, expressly or by implication, that ADI products "help keep our communities safe, secure, comfortable and connected," despite known security flaws and vulnerabilities from Hikvision and Dahua products;

b. Marketing ADI products as suitable for "educational and healthcare facilities, entertainment venues, offices, homes and more," without disclosing the associated surveillance risks from Hikvision and Dahua products;

c. Concealing material facts about Hikvision and Dahua, companies sanctioned by the U.S. government for national security and human rights violations;

d. Failing to disclose the material facts about security vulnerabilities from using Hikvision and Dahua products;

e. Curating, hosting, and promoting product user manuals that emphasize security features while omitting disclosure of fundamental vulnerabilities and limitations; and

f. Publishing NDAA information that misleadingly suggests that security risks are limited to federal government use;

103. Defendants' actions constitute deceptive and unfair acts or practices in the conduct of trade or commerce in violation of Neb. Rev. Stat. § 59-1602. Each and every sale, offer for sale, advertisement, misrepresentation, omission, and deceptive statement in connection with the sale of their cameras and other surveillance equipment constitutes a separate and independent violation of the CPA.

COUNTS VII–XI: VIOLATIONS OF THE UNIFORM DECEPTIVE TRADE PRACTICES ACT BY RESIDEO LLC AND RESIDEO TECHNOLOGIES, INC. – UNCONSCIONABLE BUSINESS PRACTICES (Neb. Rev. Stat. § 87-303.01)

104. The State of Nebraska re-alleges the facts above and incorporates them herein by reference.

105. Defendants Resideo LLC and Resideo Technologies, Inc. are "persons" within the meaning of the UDTPA, Neb. Rev. Stat. § 87-301(19).

106. An unconscionable act or practice by a supplier in connection with a consumer transaction constitutes a violation of the UDTPA. Neb. Rev. Stat. § 87-303.01(1).

107. The unconscionability of an act or practice is a question of law for the court. Neb. Rev. Stat. § 87-303.01(2).

108. Defendants engaged in unconscionable acts and practices in violation of Neb. Rev. Stat. § 87-303.01 by, without limitation:

a. Continuing to market and sell Hikvision and Dahua products in Nebraska despite knowledge that Hikvision and Dahua have been sanctioned by the U.S. government for national security and human rights concerns;

b. Exploiting consumer trust by advertising ADI products for use in homes and other sensitive locations while aware of ongoing surveillance vulnerabilities from Hikvision and Dahua products;

c. Failing to disclose that Hikvision and Dahua products are subject to backdoors and critical flaws and are

prohibited from use in critical infrastructure;

d. Marketing and selling Hikvision and Dahua products while aware of Hikvision and Dahua's placement on the U.S. Entity List for human rights violations, and failing to disclose that fact to consumers; and

e. Creating the false impression that Hikvision and Dahua products are safe for household use.

109. Defendants' marketing, advertisement, offer for sale, and sale of cameras and other surveillance equipment despite known security flaws and vulnerabilities constitute unconscionable acts and practices in violation of Neb. Rev. Stat. § 87-303.01. Each and every sale, offer for sale, advertisement, omission of material fact, and deceptive representation constitutes a separate and independent violation of the UDTPA. Neb. Rev. Stat. § 87-303.01(1).

COUNTS XII–XVI: VIOLATIONS OF THE UNIFORM DECEPTIVE TRADE PRACTICES ACT BY RESIDEO LLC AND RESIDEO TECHNOLOGIES, INC. – UNFAIR AND DECEPTIVE BUSINESS PRACTICES
(Neb. Rev. Stat. § 87-301 *et seq*.)

110. The State of Nebraska re-alleges the facts above and incorporates them herein by reference.

111. Section 87-302(a) of the UDTPA specifies multiple practices, which when conducted in the course of business, constitute a deceptive trade practice.

112. Defendants are "persons" within the meaning of the

UDTPA, Neb. Rev. Stat. § 87-301(19).

113. Defendants engaged in deceptive and/or unfair trade practices in violation of the UDTPA, Neb. Rev. Stat. § 87-302 by,

without limitation:

a. Representing, expressly or by implication, that ADI products have characteristics, benefits, or qualities they do not all have, including that they "help keep our communities safe, secure, comfortable and connected";

b. Misrepresenting that all ADI products are of a particular standard, quality, or grade, with respect to the degree of safety and security that consumers can expect;

c. Causing a likelihood of deception or of misunderstanding as to the security risks from using products that are not NDAA-compliant;

d. Causing a likelihood of deception or of misunderstanding as to which companies are and are not NDAA-compliant; and

e. Advertising cameras and other surveillance equipment for sale with assurances of safety and security despite known security flaws and vulnerabilities with Hikvision and Dahua products.

114. Each and every advertisement, offer for sale, sale, misrepresentation, omission, or failure to disclose a material fact in connection with the promotion and sale of their cameras and other surveillance equipment constitutes a separate and independent violation of the UDTPA. Neb. Rev. Stat. §§ 87-302, 87-303.01(1).

PRAYER FOR RELIEF

WHEREFORE**,** the State of Nebraska requests that this Court:

1. Permanently enjoin and restrain Defendants, their agents, employees, and all other persons and entities, corporate or otherwise, in active concert or participation with any of them, from engaging in conduct described in the Complaint that violates the Consumer Protection Act, pursuant to Neb. Rev. Stat. § 59-1608(1).

2. Permanently enjoin and restrain Defendants, their agents, employees, and all other persons and entities, corporate or otherwise, in active concert or participation with any of them, from engaging in unfair or deceptive acts or practices, in violation of the Consumer Protection Act, pursuant to Neb. Rev. Stat. § 59-1608(1).

3. Permanently enjoin and restrain Defendants, their agents, employees, and all other persons and entities, corporate or otherwise, in active concert or participation with any of them, from engaging in conduct described in the Complaint that violates the Uniform Deceptive Trade Practices Act, pursuant to Neb. Rev. Stat. § 87-303.05.

4. Permanently enjoin and restrain Defendants, their agents, employees, and all other persons and entities, corporate or otherwise, in active concert or participation with any of them, from engaging in deceptive or unconscionable acts or practices, in violation of the Uniform Deceptive Trade Practices Act, pursuant to Neb. Rev. Stat. § 87-303.05.

5. Order Defendants to pay civil penalties for each violation of the Consumer Protection Act and the Uniform Deceptive Trade Practices Act, pursuant to Neb. Rev. Stat. §§ 59-1614 and 87-303.11.

6. Order Defendants to restore to every person any money acquired by Defendants as a result of their violations of the Consumer

Protection Act and the Uniform Deceptive Trade Practices Act, pursuant to Neb. Rev. Stat. §§ 59-1608(2) and 87-303.05(1), including restitution and disgorgement of ill-gotten gains.

7. Order Defendants to pay the State's costs and attorney's fees in this matter, pursuant to Neb. Rev. Stat. §§ 59-1608(1) and 87-303.05(1).

8. Order such other and further relief as the Court deems just and equitable.

DATED December 22, 2025.

STATE OF NEBRASKA, Plaintiff

BY: MICHAEL T. HILGERS, #24483
Nebraska Attorney General

BY: *Tyrone E. Fahie*
Tyrone E. Fahie, #28125
Beatrice O. Strnad, #28045
Derek T. Bral, #26767

Assistant Attorneys Generals
1445 K Street, Room 2115
Lincoln, NE 68508
Telephone: (402) 471-2682
Fax: (402) 471-4725
tyrone.fahie@nebraska.gov
bebe.strnad@nebraska.gov
derek.bral@nebraska.gov

Attorneys for the Plaintiff