IN THE IOWA DISTRICT COURT FOR POLK COUNTY

STATE OF IOWA, *ex rel.* ATTORNEY GENERAL BRENNA BIRD, Plaintiff, v. **ADI GLOBAL DISTRIBUTION INC.**, Defendant.	Equity No. _____ **PETITION**

I. INTRODUCTION

1. Home security products such as security cameras are meant to promote the security of the purchaser by monitoring others who may pose a threat. However, Defendant ADI Global Distribution Inc.'s predecessor sold Chinese-made security products to Iowans that do the opposite—they risk third parties monitoring and spying on the purchaser and their loved ones. Adding salt in the wound is that the information (which may include sensitive audio or video) is susceptible to being accessed by the Chinese Communist Party under a Chinese intelligence law.

2. The State of Iowa, *ex rel.* Attorney General Brenna Bird (the "State," "Attorney General," or "Plaintiff") brings this action under the Iowa Consumer Fraud Act, Iowa Code § 714.16 (the "CFA" or "Act") to obtain relief for Iowa Consumers and ensure that misrepresentations about security cameras and other security products—which Iowa consumers often place in sensitive locations—are permanently stopped.

3. At issue in this lawsuit are the unlawful practices under the CFA attributable to security products sold through or by (i) Resideo Technologies, Inc.'s ADI Global Distribution business and (ii) ADI Global Distribution Inc. ADI Global Distribution Inc. now "hold[s], directly

or indirectly, the assets and liabilities associated with Resideo's ADI Global Distribution business"[1] as the result of a corporate spin-off. Given ADI Global Distribution Inc.'s assumption of liabilities with respect to Resideo's security products at issue, this Petition refers to Defendant ADI Global Distribution Inc. and the former Resideo Technologies Inc.' ADI Global Distribution business collectively as "ADI" or "Defendant."

4. ADI promotes itself as a trusted source for security and smart-home solutions, claiming to "help keep our communities safe, secure, comfortable and connected"[2] and provide "solutions for educational and healthcare facilities, entertainment venues, offices, homes and more."[3]

5. But that is a lie. ADI deceptively marketed security products with serious security risks, including by making deceptive statements and omissions related to material facts when advertising and selling products manufactured by Hangzhou Hikvision Digital Technology Co., Ltd. (collectively with its affiliates, "Hikvision") and Zhejiang Dahua Technology Co., Ltd. (collectively with its affiliates, "Dahua").

6. Congress, under Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 ("NDAA")[4] and the Secure Equipment Act of 2021 ("SEA"),[5] placed Hikvision and Dahua on lists of companies that pose security concerns and whose products are subject to restrictions.

---

[1] ADI Glob. Distrib. Inc., Information Statement (July 20, 2026), https://www.sec.gov/Archives/edgar/data/2105139/000121390026074253/ea029639601ex99-1.htm.
[2] https://www.adiglobal.com/ (last visited Sept. 29, 2026), archived at https://perma.cc/F5MC-9GPP.
[3] https://www.adiglobaldistribution.us/solutions (last visited Sept. 29, 2026), archived at https://perma.cc/RT82-9CAZ.
[4] Pub. L. No. 115-232, § 889(f)(3)(B)–(C), 132 Stat. 1636, 1918 (2018), https://www.congress.gov/bill/115th-congress/house-bill/5515/text.
[5] Pub. L. No. 117-55, 135 Stat. 423 (2021), https://www.congress.gov/bill/117th-congress/house-bill/3919/text.

7. 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 FCC's "Covered List."[6] In October 2025, the FCC issued a National Security Advisory to "reiterate" that risk[7] and later that month unanimously voted to propose additional rules to implement the Covered List.[8] On June 26, 2026, the FCC released a public notice, effective July 16, 2026, to "prohibit the continued importation and marketing of certain previously authorized covered equipment added to the Covered List in 2024 or earlier."[9]

8. To continue selling cameras and turning a profit, ADI engaged in a yearslong pattern and practice of deceptive and unfair conduct to sell Hikvision and Dahua cameras to unwitting U.S. consumers, including Iowa consumers. ADI's representations to Iowans were false, deceptive, and unfair. This Petition challenges ADI's unlawful acts and practices under the CFA.

9. *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 own "Capture" brand.[10] Therefore, for two years (2021–2022), ADI sold "Capture" brand cameras that were, on information and belief, actually Dahua-manufactured cameras—without telling Iowa consumers.

10. *Second*, ADI made deceptive statements and omissions about material facts regarding the Hikvision and Dahua cameras that it sold. An article on ADI's website marketing the benefits of Hikvision's suite of video surveillance products assured customers that "[a]ll data

[6] https://docs.fcc.gov/public/attachments/DOC-389524A1.pdf.
[7] https://docs.fcc.gov/public/attachments/DA-25-927A1.pdf.
[8] https://docs.fcc.gov/public/attachments/FCC-25-71A1.pdf.
[9] https://docs.fcc.gov/public/attachments/DA-26-635A1.pdf.
[10] https://perma.cc/YZ42-65EB.

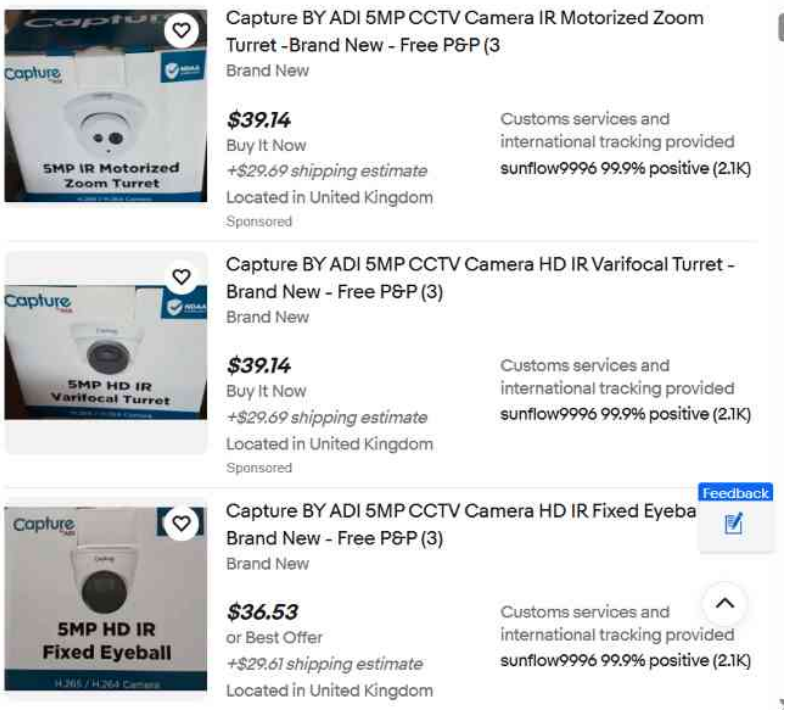
remains within the client's local network."[11] ADI's product page for Hikvision promoted "video surveillance solutions for residential, commercial and institutional applications," with no statement or disclaimer about whether the products are appropriate for only certain types of "institution[s]," including those with critical infrastructure.[12] There was also no statement or disclaimer on either page that discloses Hikvision's security issues and its presence on U.S. government lists.

11. ADI's product page for Dahua touted Dahua's "high performance security."[13] None of these pages disclosed Dahua's security issues and presence on U.S. government lists.

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

13. ADI knows that consumers value security because it prominently advertises "NDAA Compliant" on some of the cameras it sells.[14]

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



14. Yet ADI provided no corresponding disclosure to consumers of the security risks of non-NDAA-compliant Hikvision and Dahua cameras.

15. On information and belief, ADI even falsely labeled a Hikvision camera as NDAA compliant.[15]

16. ADI publishes an "NDAA Compliant Solutions" page that did not disclose to consumers the risks of these Hikvision and Dahua cameras when ADI was selling them.[16]

17. Hikvision and Dahua cameras also have experienced multiple security vulnerabilities and other risks that a consumer would find significant when evaluating ADI's express representations about security. These include vulnerabilities and documented human-rights violations.[17]

[15] https://ipvm.com/reports/cecc-adi, archived at https://perma.cc/V9PE-USKL.
[16] https://perma.cc/7S6A-5ASH; *see also* https://www.adiglobaldistribution.us/solutions/ndaa-compliant-solutions (live page).
[17] https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/ADI%20Letter%20-%20Signed.pdf

18. The bipartisan Congressional-Executive Commission on China ("CECC") warned ADI directly in a letter: "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."[18]

19. 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."[19]

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

21. By making deceptive assurances of security while not disclosing the serious risks of surveillance and exploitation from using Hikvision and Dahua products, ADI engaged in unfair and deceptive trade practices in violation of the CFA.

22. ADI's conduct has placed Iowa consumers at serious risk of harm by potentially making their intimate images and private locations vulnerable to exploitation and intrusion by foreign actors with a congressionally recognized record of nefarious and untrustworthy conduct. That risk is ongoing: on information and belief, many consumers keep their cameras for years, and some Iowa consumers may still have white-labeled Dahua cameras in their homes and businesses unaware of the security risks and violation of privacy.

23. Accordingly, the Attorney General brings this action under the CFA to enjoin ADI's unlawful practices; obtain appropriate relief for Iowa consumers; and protect Iowans from

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

having their privacy and security further jeopardized by ADI's deceptive and unfair acts and practices. The State also seeks reimbursement, civil penalties, and any other relief to which the State is entitled, including, but not limited to, disgorgement of all moneys or property acquired by ADI from its unlawful behavior.

II. JURISDICTION AND VENUE

24. The Attorney General, as Iowa's Chief Law Enforcement Officer, is expressly authorized to enforce the CFA, and this Court has subject-matter jurisdiction over this matter under Iowa Code § 714.16(7).

25. This Court has personal jurisdiction over Defendant because of its predecessor-in-interests' contacts with Iowa. Defendant is the current entity that contains Resideo Technologies, Inc.'s ADI Global Distribution business. Now a standalone company, Defendant "hold[s], directly or indirectly, the assets and liabilities associated with Resideo's ADI Global Distribution business."[20] The contacts of Resideo Technologies, Inc.'s ADI Global Distribution business with Iowa are therefore properly imputed to Defendant. *See Ostrem v. Prideco Secure Loan Fund, LP*, 841 N.W.2d 882, 896 (Iowa 2014) ("[C]ourts commonly impute a corporate predecessor's contacts to its successor in order to exercise personal jurisdiction over the successor."); *see also Lelchook v. Societe Generale de Banque au Liban S.A.L.*, 147 F.4th 226, 244 (2d Cir. 2025) ("When a successor company adopts liabilities that are "no secret" and for which the predecessor has already been subject to public legal battles, the successor has ample notice that it might become liable "in any venue" where liability accrued.").

26. ADI purposefully availed itself of the privilege of conducting business in Iowa by advertising, offering, and selling, on information and belief, security cameras and other video

[20] ADI Glob. Distrib. Inc., Information Statement (July 20, 2026), https://www.sec.gov/Archives/edgar/data/2105139/000121390026074253/ea029639601ex99-1.htm.

surveillance equipment—including Hikvision and Dahua cameras and ADI's "Capture" brand cameras—to consumers in Iowa. The conduct and injuries from which this Petition arises took place in Iowa, harmed Iowans, and targeted Iowans.

27. As recently as 2025, ADI directly marketed, offered, and sold security cameras and other video surveillance equipment to Iowa consumers through ADI's website, which on information and belief displayed thousands of Hikvision and Dahua products.[21] Additionally, at all relevant times, ADI's predecessor in interest sold security cameras and other video surveillance equipment to Iowa consumers.

28. As discussed below, ADI's statements and omissions regarding these products—which ADI directly marketed and sold to Iowa consumers—are unfair and deceptive and unlawful under the CFA.

29. The conduct described in this Petition arises from ADI's purposeful directed activities to Iowa and consumers in Iowa.

30. Venue is proper in Polk County because on information and belief it is a "county where the transaction or any substantial part of the transaction occurred" and because it is "where one or more of the victims reside." Iowa Code § 714.16(10).

III. PARTIES

31. Plaintiff is the State of Iowa, *ex rel.* Brenna Bird, Attorney General of Iowa. Under Iowa Code § 714.16(7), the Attorney General may seek civil enforcement of the CFA. The Attorney General brings this action on behalf of the people of the State of Iowa to protect the state and its residents from Defendant's unlawful business practices.

[21] https://perma.cc/MJD2-F8T3 (Hikvision); https://perma.cc/F8Z9-28CL (Dahua).

32. Defendant is ADI Global Distribution Inc., a Delaware corporation with principal executive offices at 275 Broadhollow Rd., Suite 400, Melville, New York 11747, and a registered agent at Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808.

33. One of Defendant's subsidiaries, ADI Global Distribution LLC,[22] is registered with the Iowa Secretary of State's Office and has a registered agent of Corporation Service, 505 5th Ave., Suite 729, Des Moines IA, 50309.

34. At all relevant times, Defendant (or its predecessor in interest) acted directly and through its affiliates, agents, and related entities to advertise, promote, and sell Hikvision and Dahua cameras and other video surveillance equipment in Iowa.

GENERAL ALLEGATIONS

IV. Hikvision and Dahua Are Designated Chinese Military Companies with Repeated Security Issues

35. Hikvision and Dahua are companies that the U.S. Department of Defense ("DOD") has designated as "Chinese military companies" under Section 1260H of the National Defense Authorization Act for Fiscal Year 2021.[23] This means, for example, that DOD has determined that Dahua is, or is owned or controlled by, a military-civil fusion contributor to the Chinese military.[24]

[22] See, e.g., Corporate Disclosure Statement (Dkt. 3) in ADI Global Distribution LLC v. U.S. Customs and Border Protection, No. 26-04035 (Court of International Trade, filed Sept. 18, 2026).
[23] *See* https://www.war.gov/News/Releases/Release/Article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/.
[24] U.S. Dep't of Def., Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (Jan. 7, 2025), https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF, at 2, 5; 15 C.F.R. pt. 744, Supp. No. 4; *see also* 86 Fed. Reg. 33,994 (June 28, 2021); William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1260H, 134 Stat. 3388 (2021).

36. The U.S. Department of Commerce has listed Hikvision and Dahua on its Entity List for their role in the mass surveillance of Uyghurs in Xinjiang, restricting U.S. exports of technology to the companies.[25]

37. 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.[26]

38. As of March 12, 2021, the FCC has also listed "[v]ideo 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.[27]

39. In 2021, Congress passed the SEA, which directed the FCC to no longer approve any equipment on the Covered List for marketing or sale within the United States.[28]

40. 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

[25] Addition of Certain Entities to the Entity List, 84 Fed. Reg. 54,002 (Oct. 9, 2019), 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.
[26] Pub. L. No. 115-232, § 889(f)(3)(B), 132 Stat. 1636, 1918 (2018), https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf, at 283.
[27] FCC, List of Equipment and Services Covered by Section 2 of the Secure Networks Act, https://www.fcc.gov/supplychain/coveredlist.
[28] *Hikvision USA, Inc. v. FCC*, 97 F.4th 938, 940 (D.C. Cir. 2024).

of . . . physical security surveillance of critical infrastructure.'"[29] 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."[30]

41. 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."[31] On June 26, 2026, the FCC released a public notice, effective July 16, 2026, to "prohibit the continued importation and marketing of certain previously authorized covered equipment added to the Covered List in 2024 or earlier."[32] These and similar actions by the FCC show the seriousness of the security risks involving Hikvision and Dahua.

42. Foreign governments have also taken action. Australia removed Hikvision and Dahua cameras from government facilities, citing national-security threats and human-rights violations, as the companies have been "directly implicated in the alleged human rights abuses and mass surveillance of Uyghurs in Xinjiang."[33] Bans of Hikvision and Dahua have been increasing around the world.[34]

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

[29] *Id.* at 944.
[30] *Id.* at 950.
[31] https://docs.fcc.gov/public/attachments/DOC-415051A1.pdf, at 1. For a recording of the meeting, see https://www.fcc.gov/October2025.
[32] https://docs.fcc.gov/public/attachments/DA-26-635A1.pdf.
[33] https://www.bbc.com/news/world-australia-64577641.
[34] https://ipvm.com/reports/hikua-bans, archived at https://perma.cc/MV2S-KLQQ.
[35] https://archive.is/THwyD (archive of 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/.

described one 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 and NVRs."[36]

44. 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]

45. 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] IPVM has released directory lists of numerous U.S. and Canadian companies that engage in original equipment manufacturing ("OEM") or white-labeling of Hikvision, Dahua, and other Chinese-manufactured cameras.[39] According to IPVM, it lists only those OEMs it has "verified by examining shipping records, product documentation, and/or testing products."[40]

46. 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]

47. 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.[42]

[36] https://archive.is/THwyD (archive of https://ipvm.com/reports/security-exploits).
[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/.
[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://archive.is/THwyD (archive of https://ipvm.com/reports/security-exploits).
[42] 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 September 2026. https://apps.apple.com/us/app/hik-connect-for-end-user/id1087803190.

b. *June 2023 – Embedded Backdoors Revealed.* A 2023 BBC investigation determined that Hikvision engineers embedded backdoors that 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.[43]

c. *September 2021 – Command Injection Vulnerability.* The Cybersecurity and Infrastructure Security Agency ("CISA") identified a 2021 command-injection vulnerability for Hikvision cameras in its Known Exploited Vulnerabilities Catalog.[44] This vulnerability was scored 9.8 out of 10, indicating its critical nature.[45] A later investigation revealed that over 10,600 U.S. cameras were affected.[46]

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

a. *July 2025 – CVE-2025-31700.* According to the National Vulnerability Database, "[a]ttackers 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."[47]

b. *January 2023 – 12 Dahua DSS Software Vulnerabilities.* IPVM discovered and reported 12 vulnerabilities in Dahua's Digital Surveillance System ("DSS") software[48] 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, remote code execution, and unchecked ICMP requests—can be used for distributed denial-of-service attacks.[49]

c. *January 2022 – Broken Access Control Vulnerability.* A critical-level vulnerability rated 9.8 out of 10 by the National Institute of Standards and Technology ("NIST"), which Dahua originally reported as only 8.1, allows attackers to reset device

[43] https://www.bbc.com/news/technology-65975446.
[44] https://www.cisa.gov/news-events/alerts/2021/09/28/rce-vulnerability-hikvision-cameras-cve-2021-36260.
[45] https://perma.cc/KX92-Q3FS.
[46] https://therecord.media/experts-warn-of-widespread-exploitation-involving-hikvision-cameras.
[47] https://nvd.nist.gov/vuln/detail/CVE-2025-31700.
[48] DSS 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.
[49] https://archive.is/THwyD (archive of https://ipvm.com/reports/security-exploits).

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.[50]

d. *September 2021 –Critical Vulnerabilities.* Two critical-level vulnerabilities rated 9.8 out of 10 allow authentication bypass without valid credentials.[51] Dahua's response contradicted industry standards: (1) Dahua assigned lower severity ratings of 8.1 and 7.3 over the objections of the discovering researcher by manipulating scoring 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; and (3) Dahua waited two months before informing users of the vulnerabilities in September 2021.[52]

49. These security risks must be understood in the context of prior People's Republic of China ("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.[53]

50. These risks matter to Iowa consumers. A company that sells cameras manufactured by designated Chinese military companies with a documented history of intentional backdoors and critical, actively exploited vulnerabilities cannot truthfully assure consumers that "[a]ll data remains within the client's local network" or that those cameras offer "high performance security"—at least not without disclosing those risks.

[50] https://archive.is/THwyD (archive of https://ipvm.com/reports/security-exploits).
[51] https://archive.is/25tES (archive of https://ipvm.com/reports/dahua-21-critical).
[52] https://archive.is/THwyD (archive of https://ipvm.com/reports/security-exploits).
[53] 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.

V. ADI Made Misleading Representations and Omissions About the Security of the Hikvision and Dahua Products It Sold

51. 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 did make disclosures regarding the NDAA, it did so in a deceptive manner, particularly given that the vast majority (75%–90%) of certain categories of products it listed at a relevant time period could not be confirmed as NDAA compliant.

A. ADI White-Labeled Dahua-Manufactured Cameras Under ADI's "Capture" Brand from 2021 to 2022

52. After Congress placed Hikvision and Dahua on lists of companies that pose security concerns and whose products are subject to restrictions, ADI, on information and belief, started white-labeling Dahua cameras under ADI's "Capture" brand.[54] Consumers were therefore unwittingly purchasing cameras from a manufacturer against which the federal government had just taken action.

53. On information and belief, given the length of time that consumers keep security cameras, some Iowa consumers may still have these white-labeled Dahua cameras in their homes and other locations.

54. 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.[55]

[54] https://perma.cc/YZ42-65EB; https://perma.cc/HXJ9-QM8E (archive of 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.").
[55] https://archive.is/Vsl2z (archive of https://ipvm.com/reports/adi-stop-dahua-re).

55. The true manufacturer of a product, especially one who has been recognized by the federal government as posing security risks, is a material fact that affects a consumer's purchasing decision. When the manufacturer is purposefully hidden, it is a deception and omission that is unlawful under the CFA.

B. ADI Made Deceptive Representations and Omissions on Its Webpages Related to Dahua and Hikvision

56. ADI made multiple misleading representations and omissions related to itself and the Hikvision and Dahua products ADI sold.

57. On its homepage, ADI states (and stated) that it is a trusted source for security and smart-home solutions, claiming to "help keep our communities safe, secure, comfortable and connected."[56]

58. On its Solutions page, ADI assures (and assured) consumers that it can provide "solutions for educational and healthcare facilities, entertainment venues, offices, homes and more."[57]

59. In an article devoted to extolling the benefits of Hikvision's suite of video surveillance products, ADI assured customers that "[a]ll data remains within the client's local network."[58]

60. On the product page for Hikvision, ADI promoted "video surveillance solutions for residential, commercial and institutional applications."[59]

61. On the product page for Dahua, ADI touted Dahua's "high performance security."[60]

[56] https://www.adiglobal.com/ (last visited Sept. 29, 2026), archived at https://perma.cc/F5MC-9GPP.
[57] https://www.adiglobaldistribution.us/solutions (last visited Sept. 29, 2026), archived at https://perma.cc/RT82-9CAZ.
[58] https://perma.cc/B9B6-S4TY.
[59] https://perma.cc/MJD2-F8T3.
[60] https://perma.cc/G7QX-LMB9.

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

63. ADI also provided or linked to product user manuals that emphasize security protections and recommended configurations but omitted disclosure of fundamental vulnerabilities and limitations.[61] Consumers reasonably rely on product manuals as core, authoritative materials to assess product safety and make purchasing decisions, and ADI knew or should have known that consumers would rely on these materials in evaluating ADI's product offerings.

64. By curating, disseminating, and directing consumers to these materials on its own website, ADI adopted and republished the content in furtherance of sales. And by highlighting security features and promoting Hikvision and Dahua products while omitting known or foreseeable vulnerabilities, ADI created a misleading net impression that the products deliver robust security when used as intended.

65. These omissions were material because they involved product safety and performance and would be important to a consumer's purchasing decision. As a direct and proximate result of these omissions, 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.

[61] *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)).

C. ADI Was Warned Directly by Members of Congress in 2023

66. In October 2023, Representative Christopher Smith and Senator Jeffrey Merkley, the co-chairs of the bipartisan Congressional-Executive Commission on China ("CECC"),[62] sent a letter to ADI's President.[63]

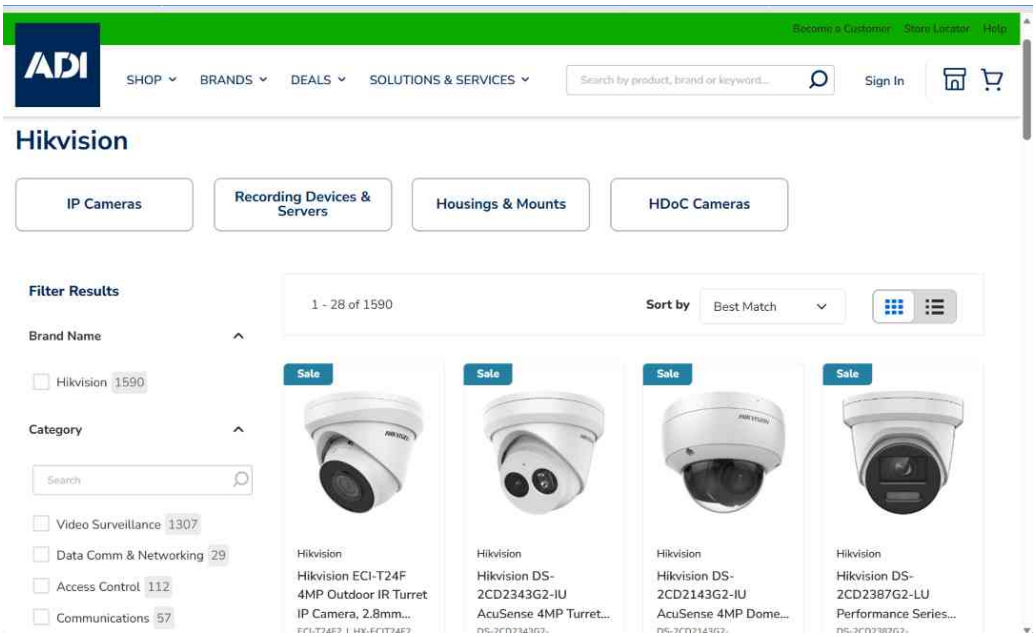
67. The letter stated in part: "The telecommunication and surveillance equipment manufactured by [Hikvision and Dahua] is a recognized threat to American users" because "they are vulnerable to spying from hackers and information requests from [People's Republic of China] intelligence entities."[64]

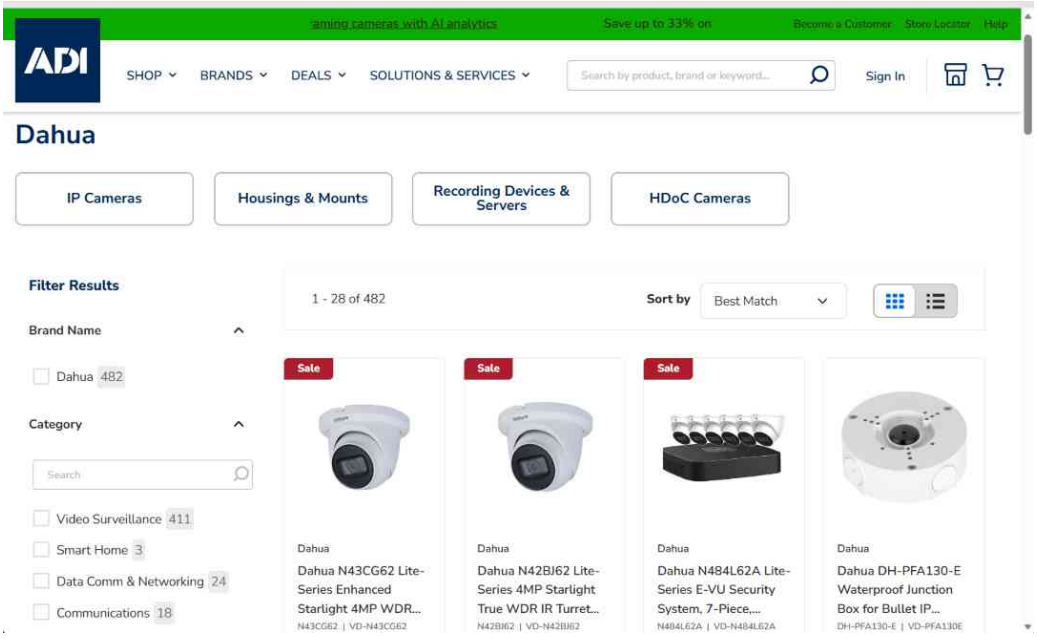
68. As the CECC noted in a related letter issued the same day: "No data collected can be withheld from PRC authorities should they request it for intelligence purposes—a vulnerability that . . . customers should be notified of."[65]

D. ADI's Website Advertised Hikvision and Dahua Products As Recently as 2025

69. Nonetheless, ADI's website continued to prominently display thousands of Hikvision and Dahua products as recently as 2025.[66]

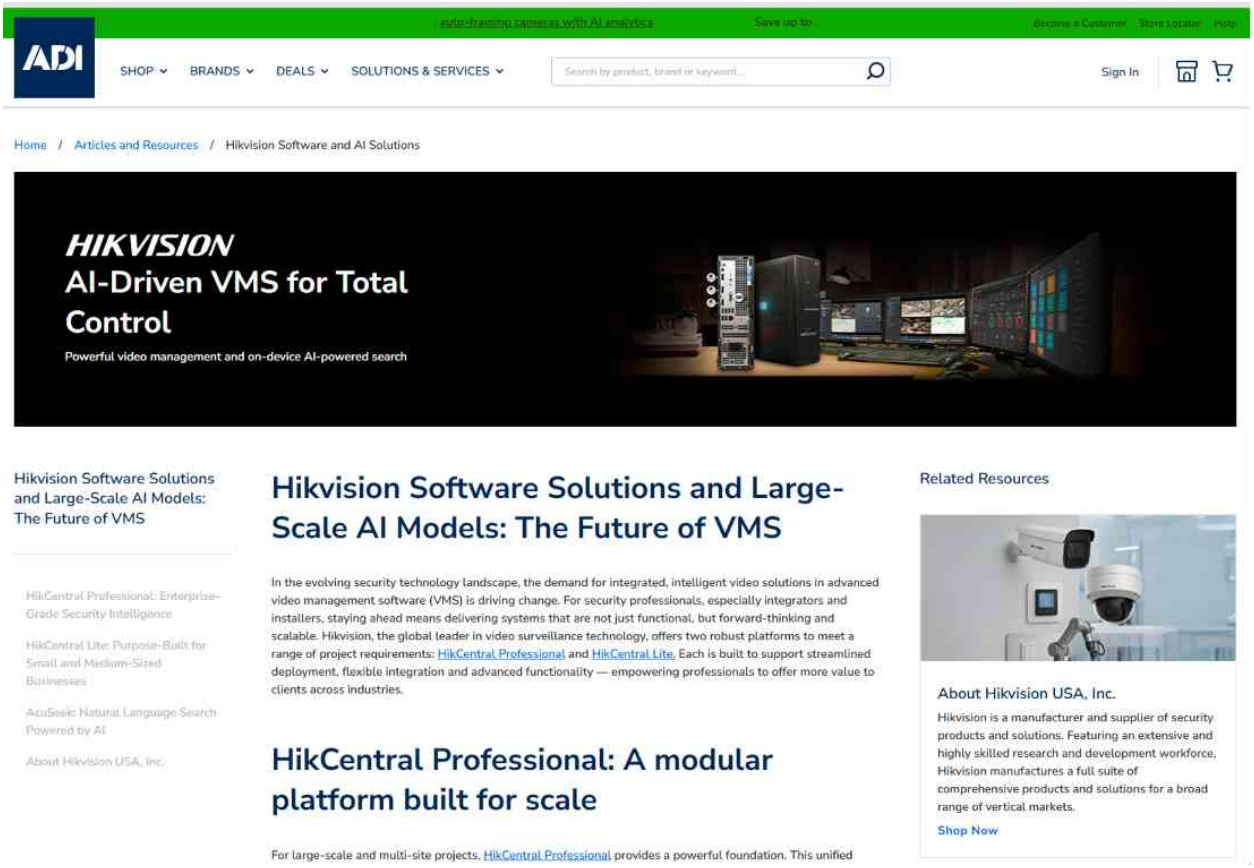
[62] *See* https://www.cecc.gov/ (last visited Sept. 30, 2026(.
[63] https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/ADI%20Letter%20-%20Signed.pdf; *see also* https://www.cecc.gov/media-center/press-releases/letter-to-costco-and-adi-raises-concerns-about-sale-of-banned-hikvision.
[64] https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/ADI%20Letter%20-%20Signed.pdf.
[65] https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/Costco%20Letter%20Signed.pdf.
[66] https://perma.cc/MJD2-F8T3 (Hikvision); https://perma.cc/F8Z9-28CL (Dahua).





70. While advertising these products, ADI even continued to host its article extolling the benefits of Hikvision's suite of video surveillance products and assuring customers that "[a]ll data remains within the client's local network."[67]

[67] https://perma.cc/B9B6-S4TY.



71. When selling Hikvision and Dahua cameras, ADI did not disclose the known risks associated with those products to consumers.

E. ADI's Deceptive Statements and Omissions About the Risks of Non-NDAA-Compliant Products

72. ADI prominently markets (and marketed) NDAA compliance on various cameras, but made deceptive statements and omissions related to Hikvision and Dahua cameras, which are not NDAA compliant.

73. ADI publishes an "NDAA Compliant Solutions" page,[68] but its description suggests that NDAA compliance is relevant only for certain projects, and it fails to state or disclose to consumers that the issue of NDAA compliance relates to security generally. The page is

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

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

74. According to IPVM, ADI also falsely represented that a Hikvision camera was NDAA compliant when it was not. When this was pointed out to ADI, ADI simply deleted the field.[69]

75. ADI's prior deceptive statements and omissions regarding the security risks of non-NDAA-compliant products are particularly concerning because, as recently as 2025, the vast majority of products ADI offered for sale in certain categories were not listed as NDAA compliant. For these products, ADI cannot conclude that the manufacturer is not owned or controlled by a military-civil fusion contributor to the Chinese military.[70] For example, in November 2025:

a. Only 201 of the 804 IP bullet cameras that ADI offers for sale were listed as NDAA compliant;[71]

b. Only 311 of the 1,011 dome cameras that ADI offers for sale were listed as NDAA compliant;[72] and

c. Only 197 of the 2,152 network video recorders that ADI offers for sale were listed as NDAA compliant.[73]

[69] https://ipvm.com/reports/cecc-adi, archived at https://perma.cc/V9PE-USKL.
[70] U.S. Dep't of Def., Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (Jan. 7, 2025), https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF, at 2, 5; 15 C.F.R. pt. 744, Supp. No. 4; *see also* 86 Fed. Reg. 33,994 (June 28, 2021); William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1260H, 134 Stat. 3388 (2021).
[71] https://perma.cc/CH77-EBTY (selecting "Yes" for NDAA compliant reduces the number of products from 804 to 201).
[72] https://perma.cc/3XWG-FMXM (selecting "Yes" for NDAA compliant reduces the number of products from 1,011 to 311).
[73] https://perma.cc/MX73-AVTX (selecting "Yes" for NDAA compliant reduces the number of products from 2,152 to 197).

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

76. ADI's website is misleading for an additional reason: ADI makes express representations about human trafficking and slavery in its supply chain. ADI's website states that its subsidiary Snap One "does not tolerate human trafficking or slavery in its operations or its suppliers' operations."[74]

77. Given that ADI's website has an express page about the NDAA, and that ADI received a letter in October 2023 from the 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 the mass surveillance of Uyghurs in Xinjiang.[75]

VII. CAUSES OF ACTION

A. Claims Under the Consumer Fraud Act and Civil Penalties

78. Under the Iowa Consumer Fraud Act:

> The act, use or employment by a person of an unfair practice, deception, fraud, false pretense, false promise, or misrepresentation, or the concealment, suppression, or omission of a material fact with intent that others rely upon the concealment, suppression, or omission, in connection with the lease, sale, or advertisement of any merchandise or the solicitation of contributions for charitable purposes, whether or not a person has in fact been misled, deceived, or damaged, is an unlawful practice.

Iowa Code § 714.16(2)(a).

[74] 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. Snap One, LLC is now a wholly owned subsidiary of ADI Global Distribution LLC which is in turn a wholly owned subsidiary of the public company ADI Global Distribution Inc. See, e.g., Corporate Disclosure Statement (Dkt. 3) in ADI Global Distribution LLC v. U.S. Customs and Border Protection, No. 26-04035 (Court of International Trade, filed Sept. 18, 2026).

[75] Addition of Certain Entities to the Entity List, 84 Fed. Reg. 54,002 (Oct. 9, 2019), 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.

79. "Deception" means "an act or practice which has the tendency or capacity to mislead a substantial number of consumers as to a material fact or facts." Iowa Code § 714.16(1)(*c*). An "unfair practice" is "an act or practice which causes substantial, unavoidable injury to consumers that is not outweighed by any consumer or competitive benefits." *Id.* § 714.16(1)(*i*). The State need not show that any consumer was misled, deceived, or damaged. *Id.* § 714.16(2)(*a*).

80. Defendant has engaged and continues to engage in the sale and advertisement of merchandise as defined in the Act, to consumers throughout Iowa. Merchandise "includes any objects, wares, goods, commodities, intangibles, securities, bonds, debentures, stocks, real estate or services." *Id.* § 714.16(1)(e).

81. Defendant sold and sells actual objects, wares, and goods, including security cameras and other video surveillance and smart-home equipment.

1. False and Deceptive Security Representations

82. The conduct described in the preceding paragraphs of this Petition constitutes "unfair practice, deception," "misrepresentation," and "concealment, suppression, or omission of . . . material fact with intent that others rely," unlawful practices under the Act. *Id.* § 714.16(2)(a). Defendant has violated the CFA by, without limitation:

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

b. Marketing ADI products as suitable for "educational and healthcare facilities, entertainment venues, offices, homes and more," and promoting Hikvision "video surveillance solutions for residential, commercial and institutional applications," without disclosing the associated surveillance risks from Hikvision and Dahua products or the prohibition on their use in critical infrastructure;

c. Representing that, with Hikvision's suite of video surveillance products, "[a]ll data remains within the client's local network," and touting Dahua's "high performance

security," when those manufacturers' products have been subject to intentional backdoors and critical, actively exploited vulnerabilities;

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

e. Selling Hikvision and Dahua products to Iowa consumers while failing to disclose material facts about their security vulnerabilities and about the PRC intelligence-access risks of which the CECC told ADI "customers should be notified."

83. The unfair, false, misleading, and/or deceptive acts committed by Defendant to misrepresent and conceal the security of the products it sells constitute unlawful conduct under the CFA and have caused or are likely to cause substantial injury to Iowa consumers.

84. Without an injunction from this Court, Defendant is likely to continue these practices, which would further harm Iowa consumers and the public.

85. Each instance of Defendant's unfair and deceptive practices constitutes a separate violation of the Act. The State is entitled to civil penalties of up to $40,000 per violation of the Act under Iowa Code § 714.16(7).

2. Concealment of Dahua-Manufactured "Capture" Brand Cameras

86. Defendant has also engaged in unfair practice, deception, and misrepresentation, and the concealment, suppression, or omission of material facts, in violation of the CFA, Iowa Code § 714.16(2)(a), by, without limitation:

a. On information and belief, white-labeling Dahua-manufactured cameras under ADI's "Capture" brand from 2021 to 2022, after Congress had placed Dahua on lists of companies that pose security concerns, and selling those cameras to Iowa consumers without disclosing that they were manufactured by Dahua with the intent that consumers rely on the omission; and

b. On information and belief, ceasing to use Dahua cameras in the "Capture" brand in 2022 without disclosure and without taking any steps to inform Iowa consumers who had purchased, and continue to use, white-labeled Dahua cameras.

87. The actual manufacturer, especially one who has been recognized by the federal government as posing security risks, of a security product is a material fact that could affect an Iowa consumer's decision to purchase a product.

88. The unfair, false, misleading, and/or deceptive acts committed by Defendant regarding the true manufacturer of its "Capture" brand cameras constitute unlawful conduct under the CFA and have caused or are likely to cause substantial injury to Iowa consumers.

89. Without an injunction from this Court, Defendant is likely to continue these practices, which would further harm Iowa consumers and the public.

90. Each instance of Defendant's unfair and deceptive practices constitutes a separate violation of the Act. The State is entitled to civil penalties of up to $40,000 per violation of the Act under Iowa Code § 714.16(7).

3. NDAA-Compliance Misrepresentations and Omissions

91. Defendant has also engaged in unfair practice, deception, and misrepresentation in violation of the CFA, Iowa Code § 714.16(2)(a), by, without limitation:

a. Publishing NDAA information, including its "NDAA Compliant Solutions" page, that misleadingly suggests NDAA compliance is relevant only for certain projects and that security risks are limited to federal government use;

b. Prominently advertising some cameras as "NDAA Compliant" while omitting any disclosure of the security risks of the non-NDAA-compliant Hikvision and Dahua products ADI sells, thereby causing a likelihood of deception or misunderstanding as to the security risks of using non-NDAA-compliant products;

c. On information and belief, falsely labeling a Hikvision camera as NDAA compliant; and

d. Offering for sale products the vast majority of which, in certain categories, are not listed as NDAA compliant, without disclosing to consumers that ADI cannot conclude that the manufacturers of those products are not owned or controlled by a military-civil fusion contributor to the Chinese military.

92. The unfair, false, misleading, and/or deceptive acts committed by Defendant regarding NDAA compliance constitute unlawful conduct under the CFA and have caused or are likely to cause substantial injury to Iowa consumers.

93. Without an injunction from this Court, Defendant is likely to continue these practices, which would further harm Iowa consumers and the public.

94. Each instance of Defendant's unfair and deceptive practices constitutes a separate violation of the Act. The State is entitled to civil penalties of up to $40,000 per violation of the Act under Iowa Code § 714.16(7).

4. Human-Trafficking and Anti-Slavery Misrepresentations and Omissions

95. Defendant has also engaged in unfair practice, deception, and misrepresentation in violation of the CFA, Iowa Code § 714.16(2)(a), by, without limitation:

a. Representing that ADI, through its subsidiary, "does not tolerate human trafficking or slavery in its operations or its suppliers' operations," while marketing and selling products manufactured by Hikvision and Dahua; and

b. Omitting the material fact that Hikvision and Dahua are listed on the U.S. Department of Commerce's Entity List for their role in the mass surveillance of Uyghurs in Xinjiang with the intent that others rely on the omission.

96. Defendant's omissions were material to Iowa consumers and rendered its affirmative representations misleading. These acts constitute unlawful conduct under the CFA and have caused or are likely to cause substantial injury to Iowa consumers.

97. Without an injunction from this Court, Defendant is likely to continue these practices, which would further harm Iowa consumers and the public.

98. Each instance of Defendant's unfair and deceptive practices constitutes a separate violation of the Act. The State is entitled to civil penalties of up to $40,000 per violation of the Act under Iowa Code § 714.16(7).

5. Unfair Trade Practices

99. Defendant has also engaged in unfair practice in violation of the CFA, Iowa Code § 714.16(2)(a), by, without limitation:

a. Marketing and selling Hikvision and Dahua products in Iowa despite knowledge that Hikvision and Dahua have been sanctioned by the U.S. government for national-security and human-rights concerns, and after being warned directly by the CECC in October 2023;

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

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

100. These practices cause and are likely to cause substantial injury to Iowa consumers—including the risk of exposure of their intimate images, private locations, and personal data to hackers and potential access by PRC intelligence entities—that consumers cannot reasonably avoid, because firmware backdoors, security vulnerabilities, the true manufacturer of white-labeled products, and foreign legal obligations are not discoverable by ordinary consumers, and that is not outweighed by any countervailing benefit to consumers or competition.

101. Without an injunction from this Court, Defendant is likely to continue these practices, which would further harm Iowa consumers and the public.

102. Each instance of Defendant's unfair practice constitutes a separate violation of the Act. The State is entitled to civil penalties of up to $40,000 per violation of the Act under Iowa Code § 714.16(7).

6. Reimbursement and Disgorgement

103. Through Defendant's deceptions, misrepresentations, false promises, omissions, and other unfair practices, Defendant has acquired moneys or property by a means unlawful under the CFA.

104. The CFA authorizes the court to "restore to any person in interest any moneys or property, real or personal, which have been acquired by means of a practice declared to be unlawful by this section[.]" Iowa Code § 714.16(7).

105. Further, where "the cost of administering reimbursement outweighs the benefit to consumers or consumers entitled to the reimbursement cannot be located through reasonable efforts, the court may order disgorgement of moneys or property acquired by the person," with the moneys or property awarded to the state to be used by the Attorney General for the administration and implementation of the CFA. *Id.*

106. For merchandise purchased by Iowa consumers related to Defendant's unlawful conduct where the cost of reimbursement does not outweigh the benefit to consumers and the consumers can be located through reasonable efforts, the Court should order full reimbursement to Iowa consumers.

107. For all revenues gained by Defendant as a result of Defendant's unlawful conduct where the cost of reimbursement outweighs the benefit to consumers or consumers cannot be located through reasonable efforts,, including circumstances where disaggregation of revenues to individual consumers will be difficult (e.g., revenue tied to privacy and security violations that are hard to attribute to individual consumers), the Court should order disgorgement of all of those revenues under Iowa Code § 714.16(7).

VIII. PRAYER FOR RELIEF

WHEREFORE, the State of Iowa, ex rel. Attorney General Brenna Bird, respectfully requests that the Court render judgment in the State's favor and:

a. Declare that Defendant has engaged in unfair practices, deceptions, misrepresentations, false promises, and the concealment, suppression, or omission of material facts against Iowa consumers in violation of the Iowa Consumer Fraud Act, Iowa Code § 714.16;

b. Preliminarily and permanently enjoin Defendant, its officers, directors, agents, servants, employees, successors, assigns, and all other persons and entities, corporate or otherwise, in active concert or participation with any of them, from engaging in the deceptive and unfair acts and practices described in this Petition;

c. Award the State civil penalties of up to $40,000 per violation under Iowa Code § 714.16(7);

d. Order reimbursement to Iowa consumers in accordance with Iowa Code § 714.16(7);

e. Order disgorgement of all funds and property acquired by Defendant from Iowa consumers through their misrepresentations, deceptions, false promises, omissions, and unfair practices, and award the funds and property to the State to be used by the Attorney General under Iowa Code § 714.16(7);

f. Award the State its costs and fees under Iowa Code § 714.16(11), including expert-witness expenses, costs incurred in pursuing this action and any investigation, reasonable attorneys' fees, and prejudgment and post-judgment interest at the highest lawful rates;

g. Declare that Defendant is liable for all penalties, reimbursement, and disgorgement awarded; and

h. Grant all other relief to which the State may be entitled.

DATED this 7th day of October, 2026.

Respectfully submitted,

BRENNA BIRD
ATTORNEY GENERAL OF IOWA

/s/ Laura L. Mommsen
Laura L. Mommsen, AT0011415
Assistant Attorney General
Daniel L. Barnes, AT0015826
Deputy Attorney General for Consumer Protection
1305 E. Walnut St.
Des Moines, Iowa 50319
(515) 281-8757
laura.mommsen@ag.iowa.gov
daniel.barnes@ag.iowa.gov

Brunn (Beau) Roysden*, AZ Bar No. 028698
Culper Law PLLC
111 W. Marshall Ave.
Phoenix, AZ 85013
Telephone: 602-315-7545
beau@culper.law
**Pro Hac Vice forthcoming*

Counsel for Plaintiff State of Iowa