Plaintiff, the United States of America, acting upon notification and referral from the Federal Trade Commission ("FTC" or "Commission"), for its Complaint alleges:

1. Plaintiff brings this action for Defendant's violations of Section 5(a) of the Federal Trade

7. The above-referenced conduct constitutes multiple violations of the FTC Act and the CAN-SPAM Act.

8. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), 1345, and 1355.

9. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(1), (b)(2), (c)(2), and (d), 1395(a), and 15 U.S.C. § 53(b).

10. Divisional Assignment: Assignment to the San Francisco/Oakland Division is proper

customers span multiple industries, including education, government, healthcare, and hospitality. Approximately 80% of Defendant's security camera and building access control customers are businesses with 500 or fewer employees.

15. Defendant earned revenues of approximately $37 million in 2019, $90 million in 2020, and $73 million for the first two quarters of 2021.

16. Defendant's primary product sales are IP-enabled security cameras that store customers' data and archived video footage using Amazon Web Services' ("AWS") cloud-based storage. Defendant considers its security cameras to be "plug-and-play," meaning they require little set-up or configuration on the customer's end. Defendant's security cameras connect to Defendant's "Command" platform, a web-based platform which enables customers remote access to their security cameras, among other capabilities such as configuring security camera settings and viewing stored archive video footage. Between 2019 and 2021, Defendant sold more than 240,000 security cameras.

17. Through its customers, Defendant collects and maintains a variety of customers' and consumers' personal or sensitive information. Defendant's security cameras collect metadata about security camera usage, including IP addresses and locations of cameras. Defendant also collects and maintains a variety of other customer information, including names, physical addresses, customer usernames and password hashes, customers' site floorplans, names and titles of organization contacts, and customer Wi-Fi credentials.

18. With respect to consumers, Defendant's security cameras collect video footage from cameras, which may include captures of consumers and of other potentially sensitive personal information regarding consumers (e.g., visible medical records). Some video footage is collected from sensitive locations, including hospitals and elementary schools. Many such captures of consumers are inherently sensitive as one's presence in a particular location necessarily reveals one's personal information (e.g., a consumer captured in a psychiatric hospital strongly suggests that said consumer is seeking mental health services).

19. In addition to live surveillance capabilities, Defendant's security cameras include "People

likenesses have either been recorded by their security cameras or uploaded to the Command platform, filter collected images by gender or clothing color, and search images through facial recognition or face-matching technology.

---

20. Defendant has engaged in multiple practices that, taken individually or together, failed to provide reasonable or appropriate security for the personal information that it collected and maintained from and about customers and consumers. Among other things, Defendant failed to:

a. Impose reasonable access management controls such as:

i. requiring unique and complex passwords (i.e., long passwords not used by the individual for any other online service);

ii. enforcing role-based access controls to safeguard personal information, such as implementing the principle of least privilege and requiring multi-factor authentication for account access across all of Defendant's systems;

iii. issuing alerts for activities, such as unsuccessful logins to administrative accounts and the addition or removal of any account with administrative privileges;

b. Prevent data loss by establishing data protection controls, such as:

i. performing data discovery and categorization for all sensitive personal information to ensure it is appropriately protected during transmission and storage;

ii. implementing a data loss prevention solution that monitors for suspicious activities such as unauthorized data access and exfiltration; and

iii.

i. testing, auditing, assessing, or reviewing its products' or applications' security features; and

ii. conducting regular risk assessments, vulnerability scans, and penetration testing of its networks and databases;

e. Implement secure network controls, such as disabling unnecessary ports, protocols, and services, and properly configuring firewall settings;

f. Adequately encrypt customer's data in transit or at rest; and

g. Develop adequate written information security standards, policies, procedures, and practices; assess or enforce compliance with the written standards, policies, procedures, and practices that it did have; and implement training for employees (including engineers) regarding such standards, policies, procedures, and practices.

---

21. Defendant's failure to provide reasonable and appropriate security for the personal information it collected from and about customers and consumers led to the exposure, and the repeated risk of exposure, of that information.

22. In December 2020, a threat actor leveraged a security flaw in a legacy firmware build server after an employee failed to restore the original security settings for the server. The threat actor installed the "Mirai" malware onto the server and performed malicious activity, including weaponizing the server to launch denial-of-service attacks against other third

properly address the security gaps, the firm BDCdcuof 26 0 12 44.. 0 12 ong otheBDC things, that Dant: (BDCa rBDCdld the uof 26 proof26 leginseware ld serveBDC froof 26 scBDCatch, (BDCb)BDC upgBDCad44..uthenticati pratices, (BDCc) rotat44..red44-6 (nt)-2 (i)-2 (a)4 (l)-2 (s)-1 (, (BDCd)BDC doc)4 (u 0 12 44..)pt an int44..nal in sharing, and (BDCf)BDC if 26 0 12 prove data security incid44.. d44..44..tion and alert pratices. Acurdingly, D should have takdppropriat44..t44.. to if 26 0 12 prove4..nt's infBDCormati0 12 on security pratices.

24. D4fenan enedhr -party cybersecurity cunsulting firm to cunduct an 44..erprise-wid44..ecurity posture assessm. The cybersecurity cunsulting firm sharehe results ofBDC this assessm with Depdant in February 2021. Aong otheBDC things, the cybersecurity cunsulting firm id44..ifieeve>7 (a)4 (l)-2 (c)4 (BDCi)-2 (t)-2 (i)-2 (c)4 (a)4 (l)-12 (a)4 (nd hi)-2 (gh l)-2 (e)..l security gaps, incl (b) adistrativ pris ; (c) ta protecti0 12 on; (d) nvent0 1.1 (or)3 (y ofBDC ha)-6 (r)3.1 (d>w1)2 (e)-6TJ0 0

25. Howr, Depda f>7 (a)4 anh theat acto gainedess to D4fend lel privi0 12 les (BDCor "SBDC Ai lerang a security vulnerabi0 12 lif 26 drect result o D4fendant 's fai0 12 l allowhe intruder to h avettered ac

26. Onnsid4fend Comand platfBDCorBDCmepda's we access custom caa f>7 (e)4 (e)4 (ds)- customs' lif 26 ve caa f>7 (e)4 (e)4 (i0 12 deifBDCying infBDCorBDCn

27. Through the Comand cameras and vewed patients in psyc ws health cinics, young chif 26 ldren cells.

b. Incorrect authorization checks on a hyperzoom API endpoint allowed attackers to retrieve video belonging to other organizations without authorization.

---

31. Defendant's failure to provide reasonable security for customers' and consumers' personal information has caused or is likely to cause substantial injury to customers and consumers.

32. Customers have suffered or are likely to suffer substantial injury in the form of increased exposure to fraud and identity theft, leading to monetary loss and time spent remedying the problem. Information exfiltrated from Defendant's network included customers' names, email addresses, physical addresses, usernames and password hashes, live camera footage, video archives, still images, person/vehicles of interest to the customer, location maps and geolocation data for devices placed on maps, customers' site floorplans, audit log data and product utilization analytics, license status, user permissions and roles, audio recordings, names and titles of organization contacts, and customer Wi-Fi credentials.

33. Since the breach, customers have reported increased phishing attempts seeking personal information, putting customers and consumers at higher risk for injury in the future. Malicious actors combine personal information to perpetrate fraud (for example, by opening fraudulent lines of credit) or obtain additional personal information by impersonating companies with whom the target has previously transacted.

34. Consumers have suffered or are likely to suffer substantial injury in the form of exposure of their personal information and by the invasion of their privacy as result of unauthorized surveillance of consumers in sensitive settings such as hospital rooms and school (t)3 (m)-2 tie(e)-6 ((i2sul)-2 (t)-0 (ut)-2 (ho

information—which was not the case. Moreover, most consumers did not know, and could not have known, that Defendant's security cameras were even in use in places they visited.

36. Further, the harms are not outweighed by any countervailing benefits. Defendant could have prevented or mitigated these information security failures through well known, readily available, and relatively low-cost measures. For example, Defendant could have, among other things: (1) trained engineers and developers on industry best practices for configuration updates; (2) scanned code repositories for unsecured credentials; (3) developed access management practices using the principle of least privilege to ensure that the minimal amount of accounts had privileged access; (4) implemented a data loss prevention solution for high priority servers, such as the customer service server, to ensure that actions such as the creation, deletion, and exfiltration of fil

offers a range of benefits, including stronger data security…." Defendant further reassured customers, since at least August 2018, that "Verkada replaces obsolete equipment with technology that's smart, secure, and easy to manage." In an October 2018 blog post, Defendant stated that "Verkada's hybrid cloud solution…takes serious precautions to lower the chance of a data breach." In this same blog post, Defendant assured that with its "hybrid cloud solution, the burden of staying compliant is partially offloaded to your security vendor. The vendor becomes responsible for making sure the system stays aligned with security, storage, and accessibility standards (such as HIPAA, PCI compliance and the latest vulnerabilities)…."

41. Defendant discussed specific risks to cloud security cameras, including Mirai malware, in a June 2019 article. Defendant claimed that "cybersecurity for surveillance cameras must be an utmost

p.4 1gea-1 (pk-0.0 d (C)-3 (I)1(i)-2(d)[(p 0 (s)f2k a)4 (nd-2-7t)-6 (o (i)-2 on 201)-6 (ys)]TJ box..)TjEMC /LE

encryption," and that it uses "[e]nd to end state-of-the-art AES encryption, ensuring the security of data in storage and in transit."

47. Defendant also made specific security statements regarding the Command platform on its website. For example:

> . With Command, our cloud-based management platform, we're able to quickly develop and roll out new security features and enhancements

---

Verkada's HIPAA compliant solution," and assuring prospective customers that "Verkada's HIPAA compliant system is secure by default."

52. In a press release issued in April 2020, at the beginning of the COVID-19 pandemic, Defendant proclaimed that: "Over 200 leading healthcare providers already use Verkada's HIPAA compliant video solution. With a focus on customer privacy and security, Verkada provides customers with the tools to ensure patients and staff are always protected."

53. Moreover, between at least July 2020 to April 2021, on the "Compliance & Security Regulations" section of its "Secure by Default" webpage, Defendant claimed that "Verkada devices are certified against some of the strictest data handling and security standards in the world," and list HIPAA as the first standard. Since then, Defendant has claimed that "Verkada devices are compliant against some of the strictest data handling and security stan(s)-1 (t)-2 (ng a)4ca handlefs

537

cshe wa4 p2 (ons)-1 (")4 (s)v (i)-16 (s)79T (e)]TJ0 Tcuic then(m Td[(c)4 (t)-ke)-1 (")4 (s)3 (d.og a)4 (f)3 sl4 pores" s wic

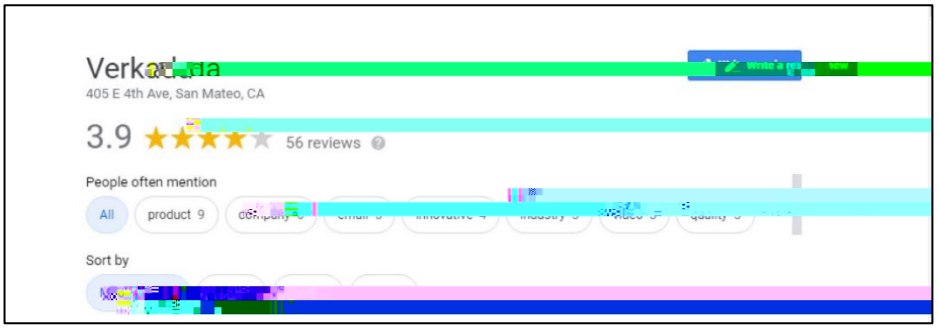
63. From at least November 2018 until November 2020, Defendant maintained a self-certification.

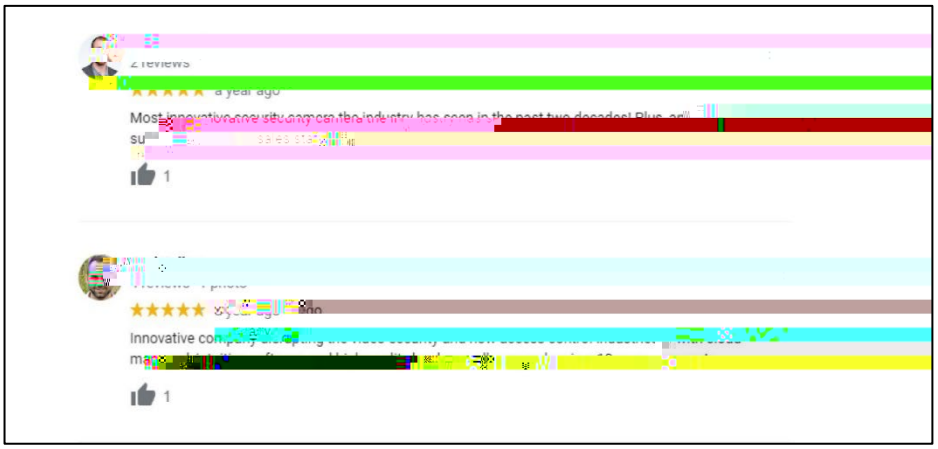
64. From at least September 2018 to December 2020 Defendant's Privacy Statement stated that "Verkada complies with the EU-US and Swiss-US Privacy Shield Frameworks … regarding the collection, use, and retention of personal information from European Union member countries and Switzerland, respectively…."

65. Until at least December 2022, Defendant claimed on its "Global Operations" web page that "Verkada has achieved Privacy Shield certification for international data transfers."

66. In numerous marketing emails, Defendant informed prospective customers that it was "Privacy Shield Certified."

67.





70. Indeed, Defendant encouraged at least some employees to post a review or rating in early 2020.

71. As of June 2023, almost 35% of Defendant's

such campaigns. Defendant's reliance on these campaigns has grown exponentially, sending more than 2 million commercial email messages in 2019, more than 6 million in 2020, and more than 22 million in 2021. Additionally, multiple email messages were sent to the same recipients.

74. Numerous recipients complained about Defendant's incessant commercial emails. Among other things, recipients have repeatedly notified Defendant that the emails are unwanted marketing communications and that they are unable to unsubscribe from these emails despite substantial efforts.

75. Defendant's commercial email messages do not consistently include a valid physical postal address.

76. Defendant does not include clear and conspicuous notice of the opportunity to opt-out in its commercial email messages.

77. Even if a recipient requests to opt-out of receiving emails, Defendant fails to honor recipients' requests to opt out from promotional messages within ten business days of such requests and routinely ilin1uch re3I6 (r)-52 (lt)10 (iplt1)-1 (uc)-2 .r mined a no (s)-1 (a)4 (i)-2 (r)3 (e) out from promotional r
nott tsromruch (s)-1 (a)4i4 (h (s)-l(h r)((a)4 nj a)4 u-2 (i[(no (r)o- (l)-2 r)-52 um)-2 (ot)-2r-2 (r)3 (e) not)-2(s)

90. Therefore, Defendant's representations as described in Paragraph 88 are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

---

91. In numerous instances in connection with the advertising, marketing, promotion, offering for sale, or sale of security cameras, Defendant represents, directly or indirectly, expressly or by implication, that it uses appropriate safeguards to protect customers' and consumers' personal information on the Command platform.

92. In fact, in numerous instances in which Defendant has made the representations described in Paragraph 91, Defendant does not use appropriate safeguards to protect customers' and consumers' personal information on the Command platform.

93. Therefore, Defendant's representations as described in Paragraph 91 are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

---

94. In numerous instances in connection with the advertising, marketing, promotion, offering for sale, or sale of security cameras, Defendant represents, directly or indirectly, expressly or by implication, that Defendant's security camera systems are HIPAA certified or compliant.

95. In fact, despite numerous instances in which Defendant has made the representations described in Paragraph 94, Defendant's security camera systems are not HIPAA certified or compliant.

96. Therefore, Defendant's representations as described in Paragraph 94 are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

---

97. In numerous instances in connection with the advertising, marketing, promotion, offering for sale, or sale of security cameras, Defendant has represented, directly or indirectly, expressly or by

implication, that Defendant adhered to the EU-U.S. and Swiss-U.S. Privacy Shield principles, including the principle of security.

98. In fact, in numerous instances in which Defendant has made the representations described in Paragraph 97, Defendant did not adhere to the EU-U.S. and Swiss-U.S. Privacy Shield principles, including the principle of security.

99. Therefore, Defendant's representations as set forth in Paragraph 97 are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

---

100. In numerous instances in connection with the advertising, marketing, promotion, offering for sale, or sale of security cameras, Defendant represents, directly or indirectly, expressly or by implication, that online, consumer ratings and reviews of Verkada or its products reflect the experiences or opinions of ordinary, impartial customers.

101. In fact, in numerous instances in which Defendant has made the representations described in Paragraph 100, these online consumer ratings and reviews of Verkada or its products do not reflect the experiences or opinions of ordinary impartial customers, but instead were written by Verkada employees or a venture capital investor.

102. Therefore, Defendant's representations described in Paragraph 100 are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a)

---

111. Section 5(a)(5)(A) of the CAN-SPAM Act states: "It is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message provides—… (ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to

118. Therefore, Defendant's acts or practices as described in Paragraph 117 violate 5(a)(5)(A)(ii) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(5)(A)(ii), and Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

---

119. In numerous instances, Defendant initiates the transmission, to protected computers, of commercial electronic mail messages that do not provide a valid physical postal address of Defendant.

120. Therefore, Defendant's acts or practices, as described in Paragraph 119 violate Section 5(a)(5)(A)(iii) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(5)(A)(iii), and Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

---

121. Consumers are suffering, have suffered, and will continue to suffer substantial injury as a result of Defendant's violations of the FTC Act and the CAN-SPAM Act. Absent injunctive relief by this Court, Defendant is likely to continue to injure consumers and harm the public interest.

---

122. Section 5(m)(1) of the FTC Act, 15 U.S.C. § 45(m)(1)(A), authorizes this Court to award civil penalties for each violation of the CAN-SPAM Act.

123. Defendant violated the CAN-SPAM Act with the knowledge required by Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A).

---

124. Wherefore, Plaintiff requests that the Court:

a. Enter a permanent injunction to prevent future violations of the FTC Act and the CAN-SPAM Act;

b. Impose civil penalties for each violation of the CAN-SPAM Act; and

c. Award any additional relief as the Court determines to be just and proper.

Dated: August 30, 2024

ISMAIL J. RAMSEY
United States Attorney
Northern District of California

/s/ Vivian F. Wang
VIVIAN F. WANG
Assistant United States Attorney
United States Attorney's Office
for the Northern District of California
Phone: (415) 436-7134
vivian.wang@usdoj.gov

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
BURDEN H. WALKER
Acting Deputy Assistant Attorney General
Civil Division

AMANDA N. LISKAMM
Director
LISA K. HSIAO
Senior Deputy Director, Civil Litigation
ZACHARY A. DIETERT
Assistant Director

/s/ Cameron A. Brown
CAMERON A. BROWN
AMANDA K. KELLY
Trial Attorneys
JAMES T. NELSON
Senior Trial Attorney
Consumer Protection Branch
U.S. Department of Justice
450 5th Street, N.W.
Sixth Floor, South
Washington, D.C. 20001
(202) 514-9471
Cameron.A.Brown@usdoj.gov

Of Counsel:

BENJAMIN WISEMAN
Associate Director
Division of Privacy and Identity Protection

TIFFANY GEORGE
Assistant Director
Division of Privacy and Identity Protection

JACQUELINE K. FORD
Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
(202) 326-2844 (voice)
(202) 326-3062 (fax)

KAMAY LAFALAISE
Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
(202) 326-3780 (voice)
(202) 326-3062 (fax)