UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

D-LINK SYSTEMS, INC.,

Defendant.

Case No. 3:17-cv-00039-JD

ORDER RE MOTION TO DISMISS

Re: Dkt. No. 25

In this enforcement action under Section 5(a) and Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(a) and 53(b), the Federal Trade Commission ("FTC") alleges that defendant D-Link Systems ("DLS") engaged in unfair and deceptive practices in the marketing and sales of routers and Internet-protocol ("IP") cameras. Dkt. No. 1. The FTC also sued D-Link Corporation, DLS's Taiwanese parent, but the parties agreed to dismiss it without prejudice. Dkt. No. 75. DLS moves to dismiss the complaint on a variety of grounds. Dkt. No. 25. The motion is granted in part and denied in part.

BACKGROUND

As alleged in the complaint, DLS sells router and IP camera products to consumers in the United States. Dkt. No. 1 ¶ 7. DLS marketed these products as providing good data security because they featured "the latest wireless security features to help prevent unauthorized access" and "the best possible encryption" protections, among other safeguards. *See id.* ¶¶ 21-24. The FTC alleges that, in fact, DLS failed to protect its products from "widely known and reasonably foreseeable risks of unauthorized access" by not providing "easily preventable" measures against "'hard-coded' user credentials and other backdoors," not maintaining the confidentiality of the private key DLS used with consumers to validate software updates, and not deploying "free software, available since at least 2008, to secure users' mobile app login credentials." *Id.* ¶ 15. As

a consequence, "consumers' sensitive personal information and local networks" are at significant risk of being accessed by unauthorized agents. *Id.* ¶¶ 16-18. DLS's practices constitute, in the FTC's view, unfair and deceptive conduct under the FTC Act.

DISCUSSION

I. PLEADING STANDARDS

DLS challenges the sufficiency of the complaint under Federal Rules of Civil Procedure 12(b)(6), 8(a), and 9(b). The standards governing the application of Rule 12(b)(6) are straightforward. To meet the pleading requirements of Rule 8(a) and to survive a Rule 12(b)(6) motion to dismiss, a claim must provide "a short and plain statement . . . showing that the pleader is entitled to relief," Fed. R. Civ. P. 8(a)(2), including "enough facts to state a claim . . . that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is plausible on its face if, accepting all factual allegations as true and construing them in the light most favorable to the plaintiff, the Court can reasonably infer that the defendant is liable for the misconduct alleged. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The plausibility analysis is "context-specific" and not only invites but "requires the reviewing court to draw on its judicial experience and common sense." *Id.* at 679.

Whether the FTC's complaint should also meet the specificity requirements of Rule 9(b) is a more nuanced question. There is no doubt that the gravamen of the deception claims is that DLS misled consumers about the data safety and security features of its products. That core allegation sounds in fraud and would appear to fit squarely within the rule in our circuit that such claims must meet the heightened pleading standards of Rule 9(b). *See Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1103-04 (9th Cir. 2003). The wrinkle is that the circuit has not yet had occasion to determine whether *Vess* and similar decisions apply to FTC deception claims, and the FTC says that Rule 9(b) should not apply because "[u]nlike the elements of common law fraud, the FTC need not prove scienter, reliance, or injury to establish a § 5 violation." Dkt. No. 28 at 12 (quoting *FTC v. Freedom Comm'cns, Inc.*, 401 F.3d 1192, 1203 n.7) (10th Cir. 2005)).

This argument is not persuasive. In essence, the FTC contends Rule 9(b) is inapplicable because fraud is not an essential element of its deception claims. But that is precisely the

truncated view of Rule 9(b) that our circuit has rejected. *Vess* requires a claim to satisfy Rule 9(b)'s specificity demands when the defendant is alleged to have engaged in fraudulent conduct, even though fraud is not a necessary element of the claim. *Vess*, 317 F.3d at 1103-04. Tellingly, *Vess* articulated this standard in the context of California's Unfair Competition Law ("UCL"), which like Section 5 outlaws deceptive practices without requiring fraud as an essential element. *Id.* Our circuit has consistently held that UCL and similar consumer claims rooted in allegations of false or misleading statements about a product sound in fraud and must meet Rule 9(b)'s requirements. *See, e.g.*, *Rubenstein v. Neiman Marcus Group LLC*, 687 Fed. Appx. 564, 567 (9th Cir. 2017); *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009). The FTC's deception claims are premised on exactly these types of misleading statements to consumers, and so Rule 9(b) must apply to them. Other district courts have reached the same conclusion. *See, e.g.*, *FTC v. Lights of Am., Inc.*, 760 F. Supp. 2d 848, 852-855 (C.D. Cal. Dec. 17, 2010) (applying rule to deception claims); *FTC v. ELH Consulting, LLC*, No. CV 12-02246-PHX-FJM, 2013 WL 4759267, at *1 (D. Ariz. Sept. 4, 2013) (same); *see also FTC v. Swish Marketing*, No. C-09-03814-RS, 2010 WL 653486, at *2-4 (N.D. Cal. Feb. 22, 2010) (finding "a real prospect" that Rule 9(b) applies but not deciding the issue).

Whether the FTC must also plead its unfairness claim under Rule 9(b) is more debatable. The parties have assumed that only Rule 8 applies. That was not necessarily unreasonable. Under Section 5(n), an act may be unfair if it: (1) causes or is likely to cause substantial injury to consumers; (2) is not reasonably avoidable by consumers; and (3) is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n). There is little flavor of fraud in these elements, and the FTC has expressly stated that the unfairness claim against DLS is not tied to an alleged misrepresentation. *See* Section III, below. At the same time, however, the FTC has said that for all of its claims "the core facts overlap, absolutely," Dkt. No. 42 at 13, and there is no doubt that the overall theme of the complaint is that DLS misled consumers about the data security its products provide. The FTC also acknowledges that DLS's misrepresentations are relevant to the unfairness claim because consumers could not have reasonably avoided injury in light of them. Dkt. No. 28 at 7.

Consequently, there is a distinct possibility that Rule 9(b) might apply to the unfairness claim. But the question presently is not ripe for resolution. As discussed below, the unfairness claim is dismissed under Rule 8. Whether it will need to satisfy Rule 9(b) will depend on how the unfairness claim is stated, if the FTC chooses to amend.

II. THE DECEPTION CLAIMS

Counts II through VI are grounded on allegedly deceptive practices by DLS. All are reviewed for sufficiency under Rule 9(b), with different outcomes depending on the specific allegations.

Count II states a plausible claim. This claim alleges that DLS has misrepresented the data security and protections its devices provide. Among other examples, the FTC alleges that DLS has made misleading statements to consumers about its data security policies and practices. *See* Dkt. No. 1 ¶ 20. The allegations in support of the claim identify specific statements DLS made at specific times between December 2013 and September 2015. *Id.*, PX 1. The allegations also specify why the statements are deceptive. Paragraphs 15-18 allege that DLS's routers and IP cameras do not protect against "critical and widespread web application vulnerabilities" identified since 2007, including "'hard-coded' user credentials," "command injection flaws" and "other backdoors." *Id.* ¶ 15. These allegations, along with others in the complaint, amply provide "the who, what, when, where and how of the misconduct charged." *Ebeid ex rel. United States v. Lungwitz*, 616 F.3d 993, 998 (9th Cir. 2010).

DLS says that Rule 9(b) requires an exacting identification of the IP camera models or router models with the alleged security flaws described in Paragraph 15. *See generally* Dkt. No. 25 at 13. This goes too far. While mere labels, conclusions and "[b]road allegations that include no particularized supporting detail do not suffice" for Rule 9(b) purposes, "this standard does not require absolute particularity or a recital of the evidence. . . . [A] complaint need not allege 'a precise time frame,' 'describe in detail a single specific transaction' or identify the 'precise method' used to carry out the fraud." *United States v. United Healthcare Ins. Co.*, 848 F.3d 1161, 1180 (9th Cir. 2016) (citing *Cooper v. Pickett*, 137 F.3d 616, 627 (9th Cir. 1997)) (other citations omitted). Count II identifies the time period during which DLS made the statements and provides

specific reasons why the statements were false -- for example, that the routers and IP cameras could be hacked through hard-coded user credentials or command injection flaws. Dkt. No. 1 ¶ 15(a). That is all Rule 9(b) demands.

DLS's suggestion that the complaint should allege specific consumer reliance on the statements, Dkt. No. 25 at 13, is also not well-taken. In this vein, DLS highlights that the security policy ends with a disclaimer: "It is up to the reader to determine the suitability of any directions or information in this document." *Id.* It is certainly true that the ultimate determination of whether a statement was deceptive depends on whether it was likely to have misled consumers acting reasonably under the circumstances. *See FTC v. Pantron I Corp.*, 33 F.3d 1088, 1095 (9th Cir.1994). But at this stage, the FTC simply needs to allege particularized facts leading to a plausible inference of liability, which it has done. Disclaimers, moreover, do not as a matter of law immunize statements that are otherwise deceptive. *See FTC v. Brown & Williamson Tobacco Corp.*, 778 F.2d 35, 42-44 (D.C. Cir. 1985). That point is particularly apt here, where the DLS disclaimer attempts a sweeping abandonment of responsibility that purports to dump on the consumer all of the risk that DLS may be wrong, reckless or outright lying about its data security features.

Counts III and VI also state plausible claims. The exhibits attached to the complaint identify the contents of the allegedly deceptive statements as well as the years those statements were made. Dkt. No. 1, PX 2-5 & 11. Paragraphs 15-18 offer specific facts to explain why and how the types of statements contained in these materials are false or misleading.

Counts IV and V fare less well under Rule 9(b). These counts center on alleged misrepresentations in promotional materials for IP cameras and graphic user interfaces (GUI's) for routers. *Id.*, PX 6-9. Exhibit 6, a promotional brochure for an IP camera, is the only dated exhibit supporting these counts, and even there the FTC has not alleged facts showing that such brochures are likely to mislead consumers. The brochure simply advertises a "surveillance camera" for the "home or small office" and contains no representations at all about digital security. *Id.*, PX 6. It is not plausible that a reasonable consumer would believe the camera is secure from digital attacks just because the word "SECURITY" is printed on the bottom corner of the brochure. After all, the

device is being marketed as a home security camera. The remaining exhibits contain more plausibly deceptive statements but fail to identify when those statements were made. These claims lack enough specificity to give DLS fair notice of its allegedly deceptive conduct, and are dismissed with leave to amend. *Semegen v. Weidner*, 780 F.2d 727, 731 (9th Cir. 1985).

III. THE UNFAIRNESS CLAIM

The parties hotly contest the viability of Count I, which alleges unfair practices under the FTC Act. DLS raises several broad objections, starting with the contention that the unfairness claim as a whole is an ultra vires reach by the FTC to assert authority over general data security practices. "Section 5 says nothing about data security . . . . If Congress wanted the FTC to regulate data security for the entire economy, it would have clearly said so." Dkt. No. 25 at 12. This contention echoes similar arguments in other cases attacking the FTC's authority to regulate data security practices, particularly in the absence of rulemaking. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

This type of challenge to the FTC's authority has been consistently rejected by other courts, with good reason. Congress intentionally made Section 5 open-ended, and "explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' by tying the concept of unfairness to a common-law or statutory standard or by enumerating the particular practices to which it was intended to apply." *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239-40 (citing and discussing Senate Report No. 597, 63d Cong., 2d Sess., 13 (1914)). The FTC is "charged with giving meaning to 'the elusive, but congressionally mandated standard of fairness,' *Sperry & Hutchinson Co.*, 405 U.S. at 244, which by its very nature, is 'a flexible concept with evolving content.' *FTC v. Bunte Bros., Inc.*, 312 U.S. 349, 353 (1941)." *FTC v. IFC Credit Corp.*, 543 F. Supp. 2d 925, 940 (N.D. Ill. 2008); *see also* 15 U.S.C. § 45(a)(2) ("The Commission is hereby empowered and directed" to prevent unfair practices). Consequently, the fact that data security is not expressly enumerated as within the FTC's enforcement powers is of no moment to the exercise of its statutory authority. *See also FTC v. Wyndham Worldwide Corp*, 799 F.3d 236, 259 (3d Cir. 2015) (finding that legislative acts affecting cybersecurity have not "reshaped the provision's [15 U.S.C. § 45(a)] meaning to exclude

cybersecurity").

DLS's next broad objection goes to fair notice. DLS says that the FTC has not "promulgate[d] clear, unambiguous standards" for fair practices in data security, Dkt. No. 25 at 10, and that fair notice requires that the FTC adopt standards before pursuing enforcement actions in federal court or at the Commission.

This misconstrues federal administrative law. Agencies are not required to anticipate problems and promulgate general rules before performing their statutory duties. *Sec. & Exch. Comm'n v. Chenery Corp.*, 332 U.S. 194, 201-02 (1947); *see also NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 292 (1974) (same). While "quasi-legislative" rulemaking may be an optimal way for agencies to proceed, requiring it as a precedent to all enforcement actions would "stultify the administrative process" and render it "inflexible and incapable" of meeting its statutory commands. *Chenery*, 332 U.S. at 202-03. Consequently, the choice "between proceeding by general rule or by individual, ad hoc litigation is one that lies primarily in the informed discretion of the administrative agency." *Id*. at 203; *see also Bell Aerospace*, 416 U.S. at 294 ("choice between rulemaking and adjudication lies in the first instance in the" agency's discretion). There can be no serious question that data security is a new and rapidly developing facet of our daily lives, and to require the FTC in all cases to adopt rules or standards before responding to data security issues faced by consumers is impractical and inconsistent with governing law.

DLS does not cite any authority to the contrary. It refers to *United States v. Trident Seafoods Corp.*, 60 F.3d 556, 559 (9th Cir. 1995), but *Trident* holds only that a corporation cannot be subject to a penalty "not clearly applicable either by statute *or* by regulation." *Id.* (emphasis added). DLS also cites *Montgomery Ward & Co. v. FTC*, 691 F.2d 1322, 1328-32 (9th Cir. 1982), but that case embraces *Chenery*, as it must, and holds only that the FTC cannot impose stricter standards in an adjudication than those plainly specified in a promulgated regulation.

DLS's final broad attack is on the time frame of the unfairness claim. DLS says that Section 5 applies to only current unfair practices, and because Paragraphs 15-18 in the complaint "are pleaded *in the past tense*," the FTC has not successfully pleaded an unfairness claim. Dkt. No. 25 at 4 (emphasis in original).

The better view is that the challenged paragraphs use the present perfect tense: "have failed", "repeatedly have failed", "has failed to take reasonable steps", "have failed to use free software", "instead have stored." Dkt. No. 1 ¶ 15. The present perfect is typically used to describe an action that started in the past and continues in the present. For example, the phrase "I have served as a federal judge since 2014" means that I started as a judge in 2014 and continue to be one today. It does not mean, as DLS would have it, that I was once a judge but stopped being one at some undefined time in the past. This is the most grammatically sensible reading of the complaint, and any lingering doubts have been dispelled by the FTC's position at the motion hearing that it is suing DLS for current and ongoing practices. Dkt. No. 42 at 8.

While DLS's general objections to the unfairness claim are unavailing, a specific issue of adequacy under Rule 8 has merit. As noted, Section 5(n) makes unfair an act or practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). This statutory definition has been used by the courts and the Commission as setting out the three elements of an unfairness claim under Section 45(n). *See, e.g., Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 972 (D.C. Cir. 1985); *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1155 (9th Cir. 2010).

The pleading problem the FTC faces concerns the first element of injury. The FTC does not allege any actual consumer injury in the form of a monetary loss or an actual incident where sensitive personal data was accessed or exposed. Instead, the FTC relies solely on the likelihood that DLS put consumers at "risk" because "remote attackers could take simple steps, using widely available tools, to locate and exploit Defendants' devices, which were widely known to be vulnerable." Dkt. No. 1 ¶ 17; *see also id.* ¶ 18 (attacker "could compromise" a router and thereby "could obtain" tax returns or other sensitive files).

That is effectively the sum total of the harm allegations, and they make out a mere possibility of injury at best. The FTC does not identify a single incident where a consumer's financial, medical or other sensitive personal information has been accessed, exposed or misused in any way, or whose IP camera has been compromised by unauthorized parties, or who has

suffered any harm or even simple annoyance and inconvenience from the alleged security flaws in the DLS devices. The absence of any concrete facts makes it just as possible that DLS's devices are not likely to substantially harm consumers, and the FTC cannot rely on wholly conclusory allegations about potential injury to tilt the balance in its favor. *Twombly*, 550 U.S. at 557. The lack of facts indicating a likelihood of harm is all the more striking in that the FTC says that it undertook a thorough investigation before filing the complaint, Dkt. No. 42 at 8, and that the DLS devices have had the challenged security flaws since 2011, *id.* at 18. This complaint stands in sharp contrast to complaints that have survived motions to dismiss in other cases involving data security issues. *See, e.g.*, *FTC v. Wyndham Worldwide*, 799 F.3d 236, 242 (3d. Cir. 2015) (sustaining complaint that alleged data theft of personal information of hundreds of thousands of consumers with over $10.6 million in fraudulent charges).

The FTC nevertheless contends that dismissal is unwarranted because "[t]he degree of likely substantial injury is a question of fact inappropriate for this stage of the case," Dkt. No. 28 at 6, and cites this Court's holding in *Brickman v. Fitbit, Inc.*, No. 15-CV-02077-JD, 2016 WL 3844327, at *3 (N.D. Cal. July 15, 2016), to that end. This misunderstands *Brickman*. That decision, in a case which did not involve Section 5(n) or the FTC, held only that consumer reliance on the defendant's allegedly deceptive marketing statements entailed disputes of fact not suited for resolution on a Rule 12(b)(6) motion. *Id.*; *see also Williams v. Gerber Products, Co.*, 552 F.3d 934, 938-39 (9th Cir. 2009). That is not the question here, particularly since the FTC has expressly divorced the unfairness claim from any of DLS's representations to consumers. Dkt. No. 42 at 12-13. *Brickman* is not at all germane.

If the FTC had tied the unfairness claim to the representations underlying the deception claims, it might have had a more colorable injury element. A consumer's purchase of a device that fails to be reasonably secure -- let alone as secure as advertised -- would likely be in the ballpark of a "substantial injury," particularly when aggregated across a large group of consumers. *See Neovi*, 604 F.3d at 1157 ("An act or practice can cause substantial injury by doing a small harm to a large number of people") (citation and quotes omitted). But the FTC pursued a different and ultimately untenable track.

CONCLUSION

Counts I, IV, and V of the complaint are dismissed with leave to amend. The motion to dismiss is denied in all other respects. If the FTC would like to amend, it should file a revised complaint that is consistent with this order by **October 20, 2017**.

IT IS SO ORDERED.

Dated: September 19, 2017

JAMES DONATO
United States District Judge

United States District Court
Northern District of California