IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

In re: Capital One Financial Corporation, Affiliate Marketing Litigation	)	Civil Action No. 1:25-cv-023 (AJT/WBP)

PRETRIAL ORDER #6
MEMORANDUM OPINION & ORDER ON DEFENDANTS' MOTION TO DISMISS

Lead Plaintiffs, on behalf of themselves and all others similarly situated, allege that Capital One Financial Corporation, Wikibuy, LLC, and Wikibuy Holdings, LLC (collectively the "Defendants" or "Capital One") are unlawfully misappropriating influencers' commissions through the Capital One Shopping browser extension (the "Extension" or "Capital One Shopping"). Before the Court is Defendants' Motion to Dismiss Pursuant to Rules 12(b)(1) and 12(b)(6), [Doc. No. 142] (the "Motion"), which the Court took under advisement following a hearing on May 14, 2025. Upon consideration of the Motion, the memoranda submitted in support thereof and in opposition thereto, the argument of counsel at the hearing, and for the reasons stated below, the Motion, [Doc. No. 142], is **GRANTED** as to Counts IV (conversion), VI (New York General Business Law), VII (California Unfair Competition Law), VIII (California Comprehensive Computer Data Access and Fraud Act), and IX (Pennsylvania Computer Offenses Law);[1] and is otherwise **DENIED**.

I. BACKGROUND

Lead Plaintiffs Ahntourage Media LLC; Just Josh, Inc.; Storm Productions LLC; TechSource Official; and ToastyBros, LLC (collectively the "Plaintiffs"), on behalf of themselves

[1] At the hearing, Plaintiffs' counsel consented to Count IX's dismissal.

and all others similarly situated,[2] allege the following in their Amended Consolidated Class Action Complaint (the "Complaint"):

In 2018, Capital One purchased a browser extension, now coined "Capital One Shopping" from Wikibuy. [Doc. No. 121] ¶ 17. Today, Capital One Shopping is a free web browser extension that permits consumers to search for online coupon codes for items already in their online shopping cart, compare prices, and earn rewards that are redeemable for gift cards when shopping with over 100,000 online merchants.[3] *Id.* ¶¶ 1, 18, 20-21, 24. A consumer who wants to use the Extension must go to the Capital One Shopping website or their web browser's extension store and affirmatively download the Extension. *Id.* ¶ 19. Once downloaded, the Extension will track when a consumer visits an online merchant that is partnered with Capital One Shopping, and if the consumer reaches the checkout screen, the Extension triggers a pop-up window that gives the user certain options, including: (i) permit the Extension to search for coupon codes, (ii) decline to search for coupon codes but activate rewards that can be redeemed towards gift cards, or (iii) click the "X" to close the pop-up window and not run the Extension at all. *Id.* ¶¶ 77, 101. In any case, the Extension is continuously running in the background of the consumer's browser and gathering data on every webpage the consumer visits, even where a consumer does not engage with the

[2] Plaintiffs proffer four proposed classes, defined as follows:

> **Nationwide Class:** All persons in the United States who participated in an affiliate commission program with a United States online merchant and had commissions diverted to Capital One as a result of the Capital One Shopping browser extension.
>
> **California Subclass:** All members of the Class who reside in California.
>
> **Pennsylvania Subclass:** All members of the Class who reside in Pennsylvania.
>
> **New York Subclass:** All members of the Class who reside in New York.

[Doc. No. 121] at 59-60.

[3] The Extension's disclosures notify users that it "earn[s] a commission when you make eligible purchases from certain Merchants using the Shopping Browser Companion or Mobile App." [Doc. No. 143-2] at 5. Further, the Capital One Shopping Global Privacy Policy discloses that a user permits the Extension to collect "[c]ookies and similar technologies data," but does not expressly notify users that the Extension may alter cookies already on the user's web browser. *See id.* at 25. In light of the Plaintiffs incorporating these documents into the Complaint—*see* [Doc. No. 121] ¶¶ 202, 242, 255—the Court has reviewed, considered, and incorporated these documents into this Memorandum Opinion and Order. *See Tellabs, Inc. v. Makor Issues & Rts., Ltd.*, 551 U.S. 308, 322 (2007).

Extension. *Id.* ¶ 23. Capital One's 2023 annual report shows that Capital One Shopping earned $7.5 billion in non-interest income. *Id.* ¶ 26.

Central to this case is affiliate marketing and tracking practices. Affiliate marketing is a multi-billion dollar industry[4] that is surging with the growth of social media, and merchants are increasingly turning to content creators, also referred to as influencers, to promote products and services.[5] *Id.* ¶ 27. In exchange for promoting products and services on the merchant's behalf, the influencer will generally receive a commission from each resulting sale,[6] *id.* ¶ 28, which is tracked through affiliate marketing tracking technology (*e.g.*, cookies, tracking codes, or other server-side functions that are unique to each influencer) that the merchant provides to the creator. *Id.* ¶¶ 2, 32, 39. If a consumer clicks an influencer's affiliate link, the link will direct the consumer to a specific product on merchant's website; a unique tracking code or cookie is stored on the consumer's web browser; and that tracking code logs the consumer's activity[7] so that any purchase resulting from the affiliate link can be attributed to the appropriate referring influencer. *Id.* ¶ 40; *see also id.* ¶¶ 30, 31, 42-43.

Most affiliate marketing agreements operate under a "last-click attribution model," whereby commissions are awarded to the last affiliate link that "leads the consumer to a merchant's specific website or landing page from which the consumer can complete the purchase." *Id.* ¶¶ 45-

[4] As of 2023, the affiliate marketing industry generated $15.7 billion in revenue, and this is projected to increase to $36.9 billion by 2030. [Doc. No. 121] ¶ 34. Affiliate marketing is approximately 16% of all e-commerce sales in the United States. *Id.* ¶ 38.

[5] According to one survey, 74% of consumers have purchased a product because of an influencer's recommendation. *Id.* ¶ 36.

[6] In 2022-2023, affiliate marketing commissions were generally between ten and forty percent of the item's total purchase price. *See id.* at 9. Approximately 80% of influencers make less than $80,000 per year, while 15% make between $80,000 to $1 million, and the top-1% make over $1 million per year. *Id.* ¶ 33.

[7] A cookie can be stored on the user's browser for between 24 hours to 90 days, depending on the time set by the merchant when creating the affiliate link. *Id.* ¶ 44. As a result, if a user does not originally purchase a product through the affiliate link, but returns to the website within the prescribed period, the influencer is still entitled to receive the commission, as long as the cookie is not overridden through another source (*e.g.*, the Extension or another influencer's advertisement for the same merchant). *See id.*

48. Under this model, an influencer who has directed a consumer to a merchant's website is awarded a commission after that consumer finalizes the purchase, unless the consumer subsequently clicks on another influencer's affiliate link before completing the purchase. In short, where multiple influencers advertise the same product and a consumer clicks on each influencer's affiliate link for that product, only the last-selected affiliate link that leads the consumer to the merchant's website before purchase is credited for the sale. *Id.* ¶ 45. Critically, as alleged by Plaintiffs, a qualifying "last click" is one that occurs "before reaching the online merchant's website" and does not include any clicks that occur when a user is already on the merchant's webpage (*i.e.*, clicks on the Extension). *Id.* ¶¶ 47-48.

Pursuant to the last-click attribution model, Plaintiffs have contractual agreements with merchants under which they earn commissions for promoting products and services that result in a sale.[8] *Id.* ¶¶ 2, 50; *see also id.* ¶¶ 51-57. For example, ToastyBros' agreement with AliExpress awards ToastyBros a commission for "every Qualifying Purchase by a Buyer on the AliExpress Platform which can be validly attributed to or traced to have originated from an advertisement published, displayed, disseminated and/or distributed by [ToastyBros] and/or [ToastyBros'] Advertising Channel." *Id.* ¶ 52. Notably, any commission paid to ToastyBros subject to this agreement is calculated by excluding any discounts or coupons applied to the purchase. *Id.* Similarly, ToastyBros' agreement with Walmart permits ToastyBros to earn commissions "on products that are actually purchased by a customer within the relevant cookie window after the

[8] By way of example, Ahntourage Media earned approximately $400,000 through affiliate marketing in 2024 and partners with Herman Miller as one source of its commissions. *Id.* ¶¶ 113, 144. In 2024 alone, Ahntourage Media generated at least 291 individual sales with Herman Miller that it was eligible to receive a commission for. *Id.* ¶ 115. The other Lead Plaintiffs also report generating a significant number of consumer purchases for merchants that they partner with. *See id.* ¶ 130 ("In the past year, Madison Avenue Spy has earned over $200,000 in affiliate link revenue."); *id.* ¶ 137 ("In 2024, TechSource earned approximately $105,000 in affiliate marketing revenue."); *id.* ¶ 146 ("ToastyBros earns approximately $280,000 in affiliate link marketing revenue per year."). Each Plaintiff has generated at least 500 consumer purchases per year, *id.* ¶¶ 115, 124, 131, 138, 147, and expects to continue affiliate link marketing in the coming years. *Id.* ¶¶ 116-120, 125, 132-33, 139, 148-149.

customer has initially entered [the Walmart] Site as long as the customer re-enters [the] Site directly during that time and not through another affiliate link." *Id.* ¶ 54. Plaintiffs allege that these agreements show the express intent by the merchants to award the influencer commission anytime "the creator's affiliate link was a consumer's final click external to the merchant's webpage" that yields a purchase, and any subsequent click, while already on the webpage, does not overcome an influencer's commission entitlement. *Id.* ¶ 58.

Plaintiffs allege that if a consumer navigates to a merchant's webpage through a Plaintiff's affiliate link and the consumer then uses the Extension, the Extension, in derogation of Plaintiffs' contractual rights, "artificially simulat[es] a referral click by the consumer" that makes it appear as if Capital One was the last-clicked affiliate link that navigated the consumer to the merchant's webpage, thereby eliminating the Plaintiffs' affiliate tracking codes from the user's browser and depriving the Plaintiffs of any commission for the sale.[9] *Id.* ¶¶ 3, 64-67, 76-78, 82, 97. In practice, the Extension creates the artificial referral click for Capital One's affiliate link by (i) surreptitiously forcing a refresh of the checkout page, (ii) injecting a hidden tab to overwrite the previous affiliate tracking code, and (iii) updating the browser's stored cookies to indicate that Capital One is the last-clicked affiliate link. *Id.* at 30-32; *id.* ¶ 102. Plaintiffs allege that the Extension was purposely designed in this manner. *Id.* ¶ 76.

As shown through various test purchases completed by Plaintiffs' expert (the "Expert Test Purchases"), where a consumer directly purchases a product through an influencer's affiliate link, the influencer receives a commission; however, if the Extension was engaged, the system credited the referral to Capital One's affiliate link and eliminated the influencer's affiliate link. *See id.* ¶¶ 86-91. Plaintiffs allege that this conduct is akin to "cookie stuffing" which arises where "the Web

[9] This technological process is described through a series of images throughout the Complaint. *See id.* at 23-33.

cookies used to determine the likely source of user traffic are overwritten without the user's knowledge."[10] *Id.* ¶¶ 95, 103, 106. Once installed, the Extension is continuously creating logs of a consumer's browsing and purchasing activity, meaning that Capital One allegedly has information about all affiliate tracking codes that were overridden by the Extension. *Id.* ¶¶ 71-72.

Plaintiffs' expert also completed a statistical analysis to determine the likelihood that the Plaintiffs were personally harmed by the Extension using the Monte Carlo simulation,[11] which allegedly demonstrates that for influencers who facilitate fifty affiliate link purchases "there is a 95.3% likelihood that at least one (and as many as 7) of their commissions have been stolen by Capital One." *Id.* ¶ 110; *see also id.* ¶ 107. For affiliates with 100 purchases, this likelihood grew to a 99.8% certainty. *Id.* Plaintiffs also performed a sensitivity analysis that showed even if Capital One only replaces an affiliate link 50% of the time, a creator with 100 purchases has a 97% likelihood of having at least one commission taken by Capital One. *Id.* ¶ 111; *see also id.* at 51 (demonstrating the results of the sensitivity analysis). Notably, given the Plaintiffs' allegations that they are responsible for generating over 500 consumer sales per year, *id.* ¶¶ 115, 124, 131, 138, 147, this sensitivity analysis shows that if the Extension only swaps the affiliate link 10% of the time, there is a 96% chance that Capital One took at least one commission from the Lead Plaintiffs; whereas, this probability increases to 100% if the Extension swaps the affiliate links 20% of the time or more. *See id.* at 51.

[10] According to one academic research paper, "cookie-stuffing fraud is typically completely opaque to an end user and goes against the advertising guidelines issued by the Federal Trade Commission for marketers," *id.* ¶ 104, and cybersecurity companies often classify extensions that use cookie stuffing as "malicious code" because the extension tries to alter "cookies that they are not authorized to alter." *Id.* ¶ 105.

[11] "The Monte Carlo simulation functions like series of weighted coin flips, and allows for the use of limited (here, publicly available) data to determine the probability of that an event occurred in the absence of discovery." *Id.* ¶ 108.

II. STANDARD OF REVIEW

A. Rule 12(b)(1)

Federal Rule of Civil Procedure 12(b)(1) provides that a party may move to dismiss a claim if the presiding court lacks subject-matter jurisdiction. FED. R. CIV. P. 12(b)(1). A plaintiff bears the burden of establishing jurisdiction, *Lovern v. Edwards*, 190 F.3d 648, 654 (4th Cir. 1999), and the defendant may either lodge a facial or factual attack on subject matter jurisdiction. *Hutton v. Nat'l Bd. of Exam'rs in Optometry., Inc.*, 892 F.3d 613, 620–21 (4th Cir. 2018). Where the defendant lodges a facial attack, the court must accept the factual allegations set forth in the complaint as true, *Beck v. McDonald*, 848 F.3d 262, 270 (4th Cir. 2017); *Kerns v. United States*, 585 F.3d 187, 193 (4th Cir. 2009), and construe the complaint in favor of the non-moving party. *S. Walk at Broadlands Homeowner's Ass'n, Inc. v. OpenBand at Broadlands, LLC*, 713 F.3d 175, 181-82 (4th Cir. 2013)

If a plaintiff lacks standing, a court necessarily lacks subject matter jurisdiction, *Pitt Cnty. v. Hotels.com, L.P.*, 553 F.3d 308, 312 (4th Cir. 2009), as "'Article III gives federal courts jurisdiction only over cases and controversies,' and standing 'is an integral component of the case or controversy requirement.'" *CGM, LLC v. BellSouth Telecommunications, Inc.*, 664 F.3d 46, 52 (4th Cir. 2011) (quoting *Miller v. Brown*, 462 F.3d 312, 316 (4th Cir. 2006)). The standing inquiry asks whether a party has a "sufficient stake in an otherwise justiciable controversy to obtain judicial resolution of that controversy." *Sierra Club v. Morton*, 405 U.S. 727, 731-32 (1972). To establish standing, a plaintiff must show they "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). At the motion to dismiss stage, a plaintiff must only plausibly allege these prongs. *Wikimedia Foundation v. Nat'l*

Sec. Agency, 857 F.3d 193, 212 (4th Cir. 2017) ("[W]hat may perhaps be speculative at summary judgment can be plausible on a motion to dismiss.").

B. Rule 12(b)(6)

Federal Rule of Civil Procedure 12(b)(6) provides for dismissal if the plaintiff does not "state a claim upon which relief can be granted." FED. R. CIV. P. 12(b)(6). To surpass a 12(b)(6) motion a plaintiff must only provide "a short and plain statement of the claim showing that the pleader is entitled to relief," FED. R. CIV. P. 8(a)(2), and the complaint "must contain sufficient factual matter, accepted as true, to 'state a claim that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). The "plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility" that a defendant is liable. *Id*. at 678 (quoting *Twombly*, 550 U.S. at 556). Moreover, neither "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements," nor "unadorned, the-defendant-unlawfully-harmed-me accusation[s]" suffice to meet the plausibility requirement. *Id.* When evaluating a motion to dismiss under Rule 12(b)(6), a court must accept all well-plead facts as true and draw all inferences in favor of the non-moving party. *E.I. du Pont de Nemours & Co. v. Kolon Indus., Inc.*, 637 F.3d 435, 440 (4th Cir. 2011)). Where a plaintiff incorporates a document into a complaint by reference, a court may review the full document in deciding the motion to dismiss without converting it to a motion for summary judgment. *See Tellabs*, 551 U.S. at 322.

III. ANALYSIS

A. Plaintiffs have plausibly alleged standing

Capital One argues that Plaintiffs have not alleged a cognizable injury that is fairly traceable to Capital One but does not challenge that Plaintiffs have properly alleged redressability. *See* [Doc. No. 143] at 4.

1. Injury-in-Fact

Plaintiffs allege they suffered economic injury by not receiving commissions that they were entitled to under their contracts with merchants. [Doc. No. 121] ¶ 152. To properly establish injury-in-fact, a plaintiff must show "an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). A "concrete" injury is one that "actually exist[s]," is "real, and not abstract," and an injury is "particularized" if it "affect[s] the plaintiff in a personal and individual way." *Spokeo*, 578 U.S. at 339-40. Each Lead Plaintiff must satisfy the standing inquiry to serve as a Lead Plaintiff in this action. *See Doe v. Obama*, 631 F.3d 157, 160 (4th Cir. 2011).

Plaintiffs argue that for the purposes of establishing Article III standing, they have sufficiently alleged financial harm through the Expert Test Purchases (*i.e.*, actual purchases on merchants' websites, with varying use of the Extension, where Lead Plaintiffs have a last-click attribution agreement with that merchant for commissions), which demonstrate the actual diversion of the affiliate link commissions that they were entitled to receive due to Capital One's extension, bolstered by statistical evidence of a near certain likelihood of harm for each Plaintiff because of Capital One's extension. [Doc. No. 180] at 16-17. Capital One challenges the sufficiency of Plaintiffs' allegations with respect to standing, arguing that (i) Plaintiffs' Expert Test Purchases cannot demonstrate that Plaintiffs ever had any "actual" commissions taken by Capital One, [Doc. No. 143] at 11; and (ii) Plaintiffs' statistical evidence is mere speculation and does not show that the Extension actually diverted any commission from Plaintiffs. *Id.* at 12-13.[12]

[12] Capital One also relies on *DiCocco* and *Hall* to argue that a party cannot independently create their own injury in order to establish standing. In *DiCocco*, the Fourth Circuit recognized that it was the *defendant's* allegedly discriminatory policy that compelled the plaintiff to resign, and any "injury" resulting from the resignation, was fairly traceable to the *defendant's* allegedly unlawful conduct. *See* 52 F.4th 588, 591, 592 (4th Cir. 2022). Similarly here, it is allegedly *Capital One's* purportedly unlawful conduct that is the but-for cause of any injury to Plaintiffs. In *Hall*, on the other hand, the plaintiff consented to receive text messages and then later tried to sue the defendant for sending messages that she consented to. *See Hall v. Xanadu Mktg.*, 682 F. Supp. 3d 1278, 1284 (N.D. Ga. July 6, 2023). Here,

As alleged in the Complaint based on the Expert Test Purchases, when the Extension was used as to Just Josh and Storm Productions, no commission was derived from the qualifying purchase; whereas, when the Extension was not used, Just Josh and Storm Productions received commissions from the Expert Test Purchases. *See* [Doc. No. 121] at 34-41. These Expert Test Purchases demonstrate, at this point, economic losses that plausibly allege a concrete injury that is directly traceable to the Extension.[13] *See Peters v. Aetna, Inc.*, 2 F.4th 199, 218 (4th Cir. 2021) (recognizing that financial loss is a concrete injury). Plaintiffs' statistical evidence also provides, at this point, a basis to find that Article III standing is plausibly alleged. Because each Lead Plaintiffs have over 500 purchases each year through their affiliate links, [Doc. No. 121] ¶¶ 115, 124, 131, 138, 147, there is a 96% probability that the Extension diverted at least one commission that they were entitled to, if the Extension diverts only 10% of purchases. *Id.* at 51. However, this increases to 100% if the Extension diverts 20% or more of purchases. *See id.* Although the Court recognizes that the probative value of the alleged statistical evidence and Expert Test Purchases may be viewed differently at the summary judgment stage or at trial,[14] they sufficiently establish

unlike in *Hall*, there are no allegations that would allow the reasonable inference that Plaintiffs consented to the Extension's alleged diversion of their commissions.

[13] In support of its position, Plaintiffs rely on Supreme Court and other lower court cases that have routinely found that "tester standing" is sufficient to satisfy a plaintiff's Article III injury. *See, e.g.*, *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 373-74 (1982). Capital One challenges the applicability of such cases, given they are normally only applied in the civil rights context, and this Court recognizes that this case does not raise precisely the same factual circumstances as a usual tester case. *See Mortland v. Omni Pittsburgh Corp.*, No. 18-cv-1067, 2021 WL 101560, at *3 (W.D. Pa. Jan. 12, 2021) (""A 'tester' is an individual who, without actual intent to avail themselves of the goods or services of a public accommodation, nonetheless poses as a purchaser to collect evidence of unlawful practices."); but neither the Supreme Court nor the Fourth Circuit has limited tester standing principles to the civil rights context exclusively, and the Supreme Court has expressly declined "to recognize an exception to traceability for injuries that a party purposely incurs" as it "ha[s] never recognized a rule of this kind under Article III." *See Fed. Election Comm'n v. Cruz*, 596 U.S. 289, 297 (2022).

[14] In that regard, the vast majority of cases that Capital One relies on in the Motion were decided within the context of proceedings other than a Rule 12 motion to dismiss. *See Clapper v. Amnesty Intern. USA*, 568 U.S. 398, 411-12 (2013) (summary judgment); *Summers v. Earth Island Inst.*, 555 U.S. 488, 497 (2009) (preliminary injunction)*; Lujan*, 504 U.S. at 561 (summary judgment); *Valley Forge Christian Coll. V. Ams. United for Separation of Church & State, Inc.*, 454 U.S. 464, 469 (1982) (summary judgment). In the one cited case, *Faculty v. New York University*, where the alleged statistical probabilities were found to be insufficient to establish standing at the motion to dismiss stage, the alleged statistical evidence was unquantified and far more facially speculative, making it distinguishable from the alleged quantified, almost near-certain probabilities set forth by Plaintiffs here. *See* 11 F.4th 68, 76 (2d Cir. 2021).

a plausible injury-in-fact for each Lead Plaintiff at the motion to dismiss stage. *See Wikimedia Foundation*, 857 F.3d at 212 ("[W]hat may perhaps be speculative at summary judgment can be plausible on a motion to dismiss.").

2. Traceability

Capital One next argues that Plaintiffs have not alleged that the harm that they suffered is fairly traceable to the Extension, by arguing that, at most, Plaintiffs merely experienced declining commissions, [Doc. No. 143] at 14-15, and there are independent third parties (*i.e.*, consumers, merchants, affiliate networks, etc.) that disrupt the causal chain between the consumer clicking an affiliate link and the creator receiving a commission, which cannot be traced to Capital One. *Id.* at 16. Plaintiffs argue that they have established a causal link between their injuries and the Extension based on their existing contracts with merchants, which show that they are entitled to the commissions at issue. *See* [Doc. No. 180] at 20-21.

To establish traceability, a plaintiff must show "a causal connection between the injury and the conduct complained of." *Lujan*, 504 U.S. at 560. The merchants' agreements cited in the Complaint demonstrate that Plaintiffs are entitled to the commission once a consumer (i) navigates to the merchant's website through the Plaintiffs' affiliated link, (ii) does not subsequently navigate to the website through another affiliate link, and (iii) makes a purchase. [Doc. No. 21] ¶¶ 45-58. As discussed *supra*, the Expert Test Purchases show a clear causal connection between engaging the Extension during a purchase and the Plaintiffs not receiving commissions that they are entitled to under their contracts with merchants. Once again, these alleged Expert Test Purchases, combined with the statistical evidence set forth by Plaintiffs, plausibly establish that Capital One's conduct is fairly traceable to each of the Plaintiffs' injuries.[15]

[15] Much of Capital One's arguments against finding traceability is based contentions not reasonably drawn from the allegations of the Complaint. For example, Capital One argues that the merchant or the affiliate networks themselves are in the best position to know who should be paid for a commission, and that Capital One is simply taking the

B. Plaintiffs have plausibly alleged Counts I, II, III, & V but have not plausibly alleged the remaining counts

As a threshold matter, the Plaintiffs' nine counts are premised on the following factual scenario: (i) a plaintiff executes an agreement with a merchant partner or affiliate network to earn commissions under the last-click attribution model; (ii) the plaintiff then directs a consumer to its merchant partner's website; (iii) once on the merchant's website, but prior to finalizing the purchase, the consumer clicks on the Extension; (iv) unknown to the consumer and merchant, Capital One knowingly overrides or otherwise modifies the cookies associated with the purchase to omit the Plaintiff's involvement in the transaction, with only Capital One's tracking code remaining tied to the transaction; (v) the consumer finalizes the purchase; and (vi) the merchant awards Capital One, but not the Plaintiff, a commission for the purchase.

In sum, Plaintiffs' well-pleaded allegations are that they are entitled to a commission for an online sale if they had a last-click attribution contract with that merchant; they navigated the consumer to the merchant's website; the consumer finalized the purchase; and the consumer did not make a recognized, nullifying click before finalizing the purchase, as contemplated in the merchant partner contract (*i.e.*, click on another affiliate link that was *external* to the merchant's website, clear their browser cookies, or permit the cookies to expire).[16] Once those conditions are met, Plaintiffs allege that their contracts entitle them to a commission irrespective of whether a

---

commission it negotiated with the merchants. *See* [Doc. No. 143] at 15-16. But that contention ignores that Plaintiffs allege that *the Extension* is responsible for overriding their affiliate link, such that neither the merchant nor the affiliate network knows that Plaintiffs have had any involvement in the transaction. Likewise, other lawsuits that Capital One has identified that these Plaintiffs have filed against similar browser extensions do not, based on the allegations of this Complaint, insulate Capital One from Plaintiffs' plausible factual allegations that *Capital One* harmed them, even if other browser extensions may have engaged in similar conduct.

[16] According to Capital One, "[t]he premise of Plaintiffs' case" is that "[Plaintiffs] are 'entitled' to commissions if they had any touchpoint in a consumer's purchasing journey," [Doc. No. 143] at 3, but Plaintiffs concede there are certain scenarios where they direct a consumer to a merchant partner's website but nevertheless are not entitled to a commission. *See* [Doc. No. 121] ¶ 54 ("Just Josh's, ToastyBros', and Class members' agreements with Capital One merchant partner Walmart provide that they will earn commissions 'on products that are actually purchased by a customer within the relevant cookie window after the customer has initially entered [the Walmart] Site as long as the customer re-enters [the] Site directly during that time and not through another affiliate link.'").

consumer later clicks on a link *internal* to the merchant's website, like the Extension.[17] However, Plaintiffs are not receiving commissions in such instances because the Extension allegedly overrides Plaintiffs' cookies to obfuscate Plaintiffs' role in the transactions, thereby interfering with the merchant's intent to award commissions to Plaintiffs, and Capital One's knowing interference causes the commission-earning process to not operate as the industry participants intended and contracted for.

Based on their allegations, Plaintiffs bring four common law claims[18] for unjust enrichment (Count I), interference with prospective economic advantage (Count II), intentional interference with contractual relations (Count III), and conversion (Count IV); three statutory claims for computer abuse under the federal Computer Fraud and Abuse Act (Count V), California Data Access and Fraud Act (VIII), and Pennsylvania Computer Offenses Law (Count IX); as well as two statutory consumer protection claims under the New York General Business Law (Count VI) and California Unfair Competition Law (Count VII). Each is discussed in turn, with the exception of the Pennsylvania Computer Offense Law claim, which Plaintiffs abandoned since the statute lacks a private right of action. *See Elansari v. Ramirez*, 816 F. App'x 630, 632 (3d Cir. 2020) ("§ 7611 [] do[es] not provide an express private right of action," and "there is no basis to imply one.").

[17] Capital One describes the crux of this lawsuit as Plaintiffs' frustrations with how the affiliate marketing attribution models operate when multiple creators are involved in a single purchase. In that respect, Capital One argues that Plaintiffs should be suing the merchants who adopted the attribution models Plaintiffs disfavor, rather than Capital One, because merchants can choose to award "other creators involved in a particular purchase" with a commission. [Doc. No. 143] at 18–19. However, the relied-upon shared attribution models for this argument (*i.e.*, time decay, rules-based, algorithmic models) appear nowhere in the Complaint, are raised for the first time in Capital One's Motion and therefore are beyond the scope of what the Court may consider in ruling on the Motion.

[18] With respect to Plaintiffs' common law claims, "Plaintiffs, like Capital One, assume that Virginia law applies here." [Doc. No. 180] at 22 n.12. Likewise, at this stage, the Court assumes Virginia substantive law applies and will revisit the choice of law analysis, as necessary, with the benefit of discovery. *See Ctr. for Excellence in Higher Educ., Inc. v. Accreditation All. of Career Sch.*, No. 1:22-cv-1223, 2023 WL 6282840, at *7 (E.D. Va. Sept. 26, 2023) ("[C]ourts are generally in a better position to decide a choice of law issue after discovery when the factual record is more developed." (collecting cases)).

1. Unjust Enrichment (Count I)

To state a claim for unjust enrichment under Virginia law, a plaintiff must allege that "(1) [plaintiff] conferred a benefit on the defendant; (2) defendant knew of the benefit and should reasonably have expected to repay plaintiff; and (3) defendant accepted or retained the benefit without paying for its value." *Podgoretsky v. Ocwen Loan Servicing LLC*, No. 1:14-cv-239, 2014 WL 12524654, at *2 (E.D. Va. Aug. 19, 2014) (citing *Schmidt v. Household Fin. Corp., II*, 276 Va. 108, 116 (2008)). The "benefits" at issue are the commissions Capital One receives when the Extension allegedly overwrites a Plaintiff's tracking code, depriving that Plaintiff of a commission. [Doc. No. 121] ¶ 163.[19] Capital One does not dispute that it retained such benefits and never paid Plaintiffs for their value; however, Capital One's position is Plaintiffs have failed to allege the first and second element of unjust enrichment. [Doc. No. 143] at 18–19.

Specifically, with respect to the first element, Capital One argues that it was the merchants, not Plaintiffs, conferring a benefit on Capital One pursuant to Capital One's separate contracts with its merchant partners and the prevailing last-click attribution model, as defined by Capital One. *Id.* Based on those same grounds, Capital One argues that it would be unreasonable to expect Capital One to repay Plaintiffs for commissions that Capital One was entitled to. *Id.* But none of the facts Capital One relies upon are part of Plaintiffs' allegations, and, therefore, are beyond what the Court may consider at this point. What is before the Court are Plaintiffs' allegations that Plaintiffs caused a consumer's placement on an affiliated merchant's website, at which point Capital One took advantage of that placement and knowingly diverted the benefits of that placement, not otherwise available to Capital One, from the Plaintiffs to itself. Although a close

[19] The Complaint contains two sets of paragraphs numbered 153 to 165, found between pages 59 to 66. In this unjust enrichment section, the citations to paragraphs 161 to 165 are found on pages 65 to 66.

issue, after viewing the allegations most favorably to the Plaintiffs, the Court concludes, at this point, that Plaintiffs have plausibly alleged that they have conferred a benefit on Capital One.

As to the second element, whether Capital One reasonably should have expected to pay Plaintiffs for that diverted commission, Plaintiffs' well-pleaded allegations, including excerpts of the Plaintiffs' contracts with merchants, appear to entitle Plaintiffs to the commissions at issue. *See* [Doc. No. 121] ¶¶ 50–58 (describing merchants' obligation to pay Plaintiffs a commission when they were the last-clicked external affiliate link and consumers finalized a purchase). Supplementing those excerpts are screenshots with image descriptions that demonstrate how the Extension injects a hidden tab to override a Plaintiff's tracking code, thereby, depriving that Plaintiff of a commission that is instead being conferred on Capital One. *Id.* ¶¶ 84–91, 165. Further, Plaintiffs have alleged that Capital One knew, or should have known, it was diverting Plaintiffs' "rightfully earned" commissions because Capital One knew that tracking codes are used by merchants to determine who may be entitled to a commission, *id.* ¶¶ 31, 67, 163, 165–66; Capital One would be entitled to a commission only if it had the last-clicked external affiliate tracking code, *id.* ¶ 64–70, 167; and Capital One swapped Plaintiffs' tracking codes for its own tracking code using the Extension, *id.* ¶¶ 67, 157, 165–67. At this stage, such allegations are sufficient to plausibly state a claim for unjust enrichment (Count I).[20]

2. Tortious Interference with Prospective Economic Advantage (Count II) and Tortious Interference with Contractual Relations (Count III)

To state a claim for tortious interference with prospective economic advantage and contractual relations under Virginia law, Plaintiffs must allege six elements:

[20] Because this finding is based solely on the allegations of the Amended Complaint, it is without consideration of what appear from the briefings to be multiple other factors not reflected in Plaintiffs' allegations, including various contracts and the role played by other participants operating in the online marketing industry.

> (1) existence of a business relationship or expectancy with a probability of future economic benefit;
> (2) defendant's knowledge of the relationship or expectancy;
> (3) reasonable certainty that, absent defendant's intentional misconduct, plaintiff would have continued the relationship and/or realized the expectancy;
> (4) defendant's intentional interference including the loss of the relationship or expectancy;
> (5) defendant's interference was done by improper methods; and
> (6) resulting damages.

Symbionics, Inc. v. Ortlieb, No. 1:08-cv-44, 2009 WL 10676530, at *9 (E.D. Va. Aug. 7, 2009). Capital One disputes the existence of all six elements.

With respect to the first element, Plaintiffs allege that the business relationships at issue are those between Plaintiffs and merchants, "including but not limited to Best Buy, Lenovo, Samsung, Walmart, Bloomingdale's, Gap, Neiman Marcus, Nordstrom, the Outnet, Saks Fifth Avenue, and Target." [Doc. No. 121] ¶ 174. Flowing from those relationships, Plaintiffs allege that they have a business expectancy to receive "referral links and commissions" for referring consumers to merchants' websites. *Id.* At least some of those business relationships are memorialized in "ongoing, valid, and enforceable contractual agreements with online merchants to promote products and services in exchange for commissions." *Id.* ¶¶ 44–45, 54, 182.

Against that backdrop, Capital One argues that "Plaintiffs do not identify any specific contract or expectancy that was interfered with." [Doc. No. 143] at 19. Beginning with the contractual interference claim, Capital One's position is the Complaint does not "address[] the substantive terms underlying Plaintiffs' claims" like "the relevant attribution model and the rules applicable when multiple creators are involved in the same transaction." *Id.* at 20–21. However, the plain meaning of the quoted contract provisions entitle Plaintiffs to a commission under the last-click attribution model, with some examples being:

- **AliExpress Platform:** Plaintiffs "will earn a commission for 'every Qualifying Purchase by a Buyer on the AliExpress Platform which can be validly attributed to or traced to have originated from an advertisement published, displayed, disseminated and/or distributed by Participant and/or Participant's Advertising Channel.'" [Doc. No. 121] ¶ 52.

- **Walmart:** Plaintiffs "will earn commissions 'on products that are actually purchased by a customer within the relevant cookie window after the customer has initially entered [the Walmart] Site as long as the customer re-enters [the] Site directly during that time and not through another affiliate link.'" *Id.*

In both examples, the contract does not use the phrase "last-click attribution model," but the conditions therein plainly align with how Plaintiffs define the last-click attribution model. As for Capital One's second contention that the Complaint does not address how multiple creators involved in a transaction may be credited, the contracts do, in fact, contemplate such scenarios and those contracts expressly strip Plaintiffs of their commissions where the customer "re-enters" the merchant's website "through another affiliate link" (*i.e.*, an external affiliate link). *See id.* ¶ 52. Those contracts further bar a creator from using tools to falsely make it appear as if the consumer re-entered the merchant website through their affiliate link, which is precisely what Plaintiffs allege the Extension does. *Id.* ¶ 56 (describing a prohibition on tools that "attempt[] to intercept, divert or redirect Internet traffic to or from any other website, or that potentially enables the diversion of Affiliate commissions from another website"). Taken together, such allegations readily distinguish this case from the ones cited by Capital One, where the conclusory allegations did not identify either the merchants or the pertinent contracts' terms.[21] *See e.g.*, *Marcantonio v. Dudzinski*, 155 F. Supp. 3d 619, 631 (W.D. Va. 2015) (dismissing tortious interference claim, in part, because the plaintiff did not describe the contract's "substantive content or terms"). For these

[21] Capital One contends that Plaintiffs must allege what attribution model was adopted by each merchant in separate contracts, but at this stage the Court will not require that level of detail in assessing whether Plaintiffs have stated a plausible claim for tortious interference.

reasons, Plaintiffs have plausibly alleged the existence of ongoing, valid, and enforceable contractual agreements that relate to the allegedly tortious conduct.

With respect to Plaintiffs' business expectancy claim, Capital One contends that any alleged expectancy is too speculative and based on mere subjective hope. [Doc. No. 143] at 19–21. To plead the existence of a valid business expectancy, there must be objective indicators the economic benefit would materialize, including a long-standing business relationship, prior statements of satisfaction with the plaintiff's performance, or evidence that plaintiff was the preferred choice for the transaction at issue. *See L-3 Commc'ns Corp. v. Serco, Inc.*, 926 F.3d 85, 94 (4th Cir. 2019). Here, Plaintiffs' business expectancy is alleged to be "based on the length and extent of the parties' relationships," including their volume of prior sales. Specifically, Plaintiffs allege that they worked with certain merchants for several years, [Doc. No. 121] ¶¶ 116–19, 125, 132–33, 139, 148–49, including Toasty Bros' long-standing nine-year relationship with AliExpress, *id.* ¶ 148, and Madison Avenue Spy's at least ten-year relationships with Bloomingdales, Gap, Neiman Marcus, Nordstrom, The Outnet, and Saks Fifth Avenue, *id.* ¶ 132. Plaintiffs also allege that their efforts have driven thousands of customers to make purchases from their merchant partners, as evidenced by their hundreds of thousands of dollars in revenue from commissions, *id.* ¶¶ 115, 124–26, 128–30, 137–38, 145–47. Drawing all reasonable inferences in favor of Plaintiffs, Plaintiffs plausibly allege that merchants will continue to partner with them based on past dealings where Plaintiffs were high-volume performers, *see id.* ¶¶ 116–20, 125, 132–33, 139, 149, and have therefore plausibly alleged a business expectancy that supports their tortious interference claim.

The second element, whether Capital One knew of the contracts between merchants, which Plaintiffs rest on allegations that Capital One *should have known* about such contracts since "Capital One's extension continuously uploaded to Capital One's server detailed logs of the affiliate links its extension replaced." [Doc. No. 180] at 26. Under Virginia law, actual knowledge of the contracts at issue is not required if the defendant had "knowledge of facts that, upon reasonable inquiry, should lead to disclosure of the existence of the contract or potential business relationship." *Simbeck, Inc. v. Dodd-Sisk Whitlock Corp.*, 44 Va. Cir. 54 (1997), *aff'd,* 257 Va. 53 (1999). Here, Plaintiffs have alleged that tracking codes are only created when a creator and merchant enter into commission-sharing agreements, [Doc. No. 121] ¶¶ 37, 67, 166, and Capital One maintained "detailed logs" that demonstrated it was overriding other creator's tracking codes, *id.* ¶¶ 72-75, 157, 175. Based on those allegations, Plaintiffs contend that they have plausibly alleged that Capital One knew they were diverting commissions away from some creators in connection with specific purchases, [Doc. No. 180] at 25–26; *see also* [Doc. No. 121] ¶¶ 67, 157, 165, 175, 184, and upon reasonable inquiry, Capital One could tie some of the tracking codes being overwritten to the specific creator.[22] These allegations are sufficient to plead the second element of Plaintiffs' tortious interference claims.

As for the third and fourth elements, Plaintiffs must allege that there is "reasonable certainty" that absent Capital One's conduct Plaintiffs would have earned commissions, and it was Capital One's interference that caused merchants to breach their agreements with Plaintiffs. [Doc. No. 143] at 22–23. As previously discussed, the alleged Expert Test Purchases show that Plaintiffs earned commissions where the Extension was not employed, and, in any case, Plaintiffs' well-pleaded allegations are that the Extension obfuscates Plaintiffs' involvement in consumers' transactions by omitting their tracking codes, thereby depriving merchants of the information they typically rely on to pay commissions to intended partners. *See* [Doc. No. 121] ¶¶ 67, 157, 165,

[22] Based on Plaintiffs' allegations, Capital One's logs would record the full affiliate link being replaced and often contain the identity of the creator, as reflected in the following example: https://www.newegg.com/abssa1 4400f4060tistratosaq
ua/p/N82E16883360464?utm_campaign=afchowl**toastybros**qp1sfsvpxsqhf&nrtv_cid=qp1sfsvpxsqhf&utm_mediu m=**affiliate**&utm_ source=howl-**toastybros**. [Doc. No. 121] ¶¶ 73–74 (emphasis added).

175, 184. Based on these allegations, Plaintiffs have plausibly alleged the third and fourth elements of this claim.

With respect to the fifth element, whether the defendant's interference was done by improper means, Capital One argues that Plaintiffs do not sufficiently allege any conduct that is "illegal or independently tortious," "violate[s] an established standard of a trade or profession," is "unethical," or constitutes "unfair competition." [Doc. No. 143] at 19 (citing *Tech. & Supply Mgmt., LLC v. Johnson Controls Bldg. Automation Sys., LLC*, No. 1:16-cv-303, 2017 WL 57134, at *6 (E.D. Va. Jan. 4, 2017)). Plaintiffs respond that improper means can be established by "violations of statutes . . . or recognized common-law rules." [Doc. No. 180] at 26 (citing *Duggin v. Adams*, 360 S.E.2d 832, 836–37 (Va. 1987)). Here, Plaintiffs have plausibly stated a claim for unjust enrichment, as stated *supra* Section III.B.1., and, a violation of the Computer Fraud Abuse Act ("CFAA"), as stated *infra* Section III.B.4. Plaintiffs have therefore plausibly alleged the fifth element of their tortious interference claims.

Finally, the sixth element is whether Plaintiffs were harmed and, as previously discussed in the standing section herein, Plaintiffs have plausibly alleged that they suffered economic injury. *See* [Doc. No. 121] ¶¶ 50–58.

For the above reasons, the Plaintiffs have plausibly alleged their tortious interference claims (Counts II and III).

3. Conversion (Count IV)

To state a claim for conversion under Virginia law, Plaintiffs must allege: (1) "the ownership or right to possession of the property at the time of the conversion;" (2) "the wrongful exercise of dominion or control by defendant over the plaintiff's property, thus depriving plaintiff of possession;" and (3) the property at issue can be the subject of a conversion claim. *Cumulus Inv., LLC v. Bernardi*, No. 1:20-cv-298, 2022 WL 20043085, at *3 (E.D. Va. July 21, 2022) (internal citation omitted). "Although a cause of action for conversion typically applies only to tangible property," the Virginia Supreme Court has recognized the conversion of intangible property in limited circumstances where the plaintiff is "entitled to immediate possession of" the property and her ownership interests arise from or merge with a document symbolizing ownership. *Mackey v. McDannald*, 298 Va. 645, 659 (2020) (cleaned up). Examples of documents that symbolize ownership include "a valid stock certificate, promissory note, or bond." *Id.* at 659–60.

Here, the property allegedly being converted is the tracking code (also referred to as a cookie, tracking tag, affiliate code, and server-side function) that merchants or affiliate networks provide to Plaintiffs, [Doc. No. 121] ¶ 32, that is stored on a consumer's browser, *id.* ¶ 43, which permits the merchant to credit the appropriate creator or creators after the purchase is finalized, *id.* ¶¶ 31, 188. Plaintiffs allege that "[a]t the time consumers made purchases on merchants' websites, Plaintiffs and Class members had a right to possess [their] tracking code," and "Capital One wrongfully exercised control over the Plaintiffs' and Class members' affiliate codes by intentionally causing the tracking codes to be overwritten with Capital One's tracking codes." *Id.* ¶¶ 188–89.

Based on those allegations, Capital One argues that tracking codes are intangible and undocumented, and therefore, cannot be considered "property" for a conversion claim under Virginia law. [Doc. No. 143] at 24. In response, Plaintiffs make four arguments: (i) tracking codes arise from contractual agreements with merchants, making them documented intangible property; (ii) "Virginia courts specifically recognize that electronic data can properly constitute the subject of a conversion claim;" (iii) "Virginia courts have also shown 'a distinct willingness to expand the scope of the doctrine of conversion in light of advancing technology;'" and (iv) where the Virginia caselaw is not a model of clarity, the viability of this claim should be resolved after discovery. [Doc. No. 180] at 27–28 (citing *E.I. DuPont de Nemours & Co. v. Kolon Indus., Inc.*, 688 F. Supp.

2d 443, 455 (E.D. Va. 2009)); *see also TK Elevator Corp. v. Shropshire*, No. 7:21-cv-00579, 2022 WL 564648, at *3 (W.D. Va. Feb. 23, 2022).

Plaintiffs have failed to plausibly allege that tracking codes are "property" that can be converted under Virginia law. Setting aside conclusory statements, Plaintiffs have not alleged that tracking codes arise from or merge with a document symbolizing ownership, such as a valid stock certificate, promissory note, bond, or shareholder interest agreement. *See Peele v. Twisted Crab - Chesapeake Square, L.L.C.*, 113 Va. Cir. 304 (2024). For instance, there are no excerpts from the merchant contracts that indicate who "owns" the tracking codes, *see* [Doc. No. 121] ¶¶ 50–58, 182, much less allegations that Plaintiffs have "a clear, definite, undisputed, and obvious property right" in the tracking codes that entitled them to "immediate possession" of those codes, *Mackey*, 298 Va. at 659–60, and when assessing what party has the most rights with respect to the tracking codes, it bears notice that it is consumers who store them on their browsers, delete tracking codes by clearing their cookies, and replace tracking codes by clicking on another external affiliate link. At most, Plaintiffs allege that each tracking code is unique to them, which suggests they may have some sort of interest in those tracking codes, but not plausibly an ownership or possessory interest.

Based on the non-conclusory statements in the Complaint, tracking codes are undocumented intangible property that cannot be the subject of a conversion claim under Virginia law; and Plaintiffs have therefore failed to plausibly allege a claim for conversion.[23] The conversion claim (Count IV) is hereby dismissed.

[23] Plaintiffs cite several Virginia cases recognizing a conversion claim for undocumented intangible property, but none of those cases support finding that tracking codes are property that can be converted under Virginia law, particularly in light of more recent cases from this District and the Supreme Court of Virginia. *See Mackey v. McDannald*, 298 Va. 645, 659–60 (2020); *Am. Conservative Union v. Inst. for Legislative Analysis*, No. 1:24-cv-500, 2025 WL 510236, at *10 (E.D. Va. Feb. 13, 2025).

4. Computer Fraud and Abuse Act (Count V)

To bring a civil claim under 18 U.S.C. § 1030(a)(4) of the CFAA, Plaintiffs must allege (1) a qualifying "loss" of at least $5,000 and (2) knowing and intentional unauthorized access. *See* 18 U.S.C. § 1030(a)(4), (g). Both elements are in dispute.

First, with respect to whether Plaintiffs allege that they suffered a qualifying "loss," the CFAA defines "loss" as limited to the costs "of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred or other consequential damages incurred *because of interruption of service*." *Id.* § 1030 (e)(11) (emphasis added). Capital One contends that "Plaintiffs still have not alleged facts showing that they lost revenue "*because* of [an] interruption of service" nor that it was an interruption "of the kind contemplated by the CFAA," like hacking, "that renders a website or computer inaccessible." [Doc. No. 143] at 25-26 (emphasis in original) (citing *Glob. Pol'y Partners, LLC v. Yessin*, 686 F. Supp. 2d 642, 653 (E.D. Va. 2010)). Specifically, Capital One notes there are no allegations that the "service" (*i.e.*, directing consumers to merchant's website) was interrupted such that consumers who clicked Plaintiffs' links were redirected elsewhere, received error messages, or that the merchant's website was otherwise inaccessible. [Doc. No. 143] at 25. In response, Plaintiffs argue that "Capital One misreads the Complaint" because the service at issue is "the commission attribution process, including communications between the merchant website and the merchant servers that attributed the sale to a Class member instead of Capital One," which is interrupted by commissions being redirected when Capital One swaps the tracking codes. [Doc. No. 121] ¶ 204 ("Capital One's cookie stuffing disrupted the commission attribution process, including communications between the merchant website and the merchant servers that attributed the sale to a Class member instead of Capital One.").

In support of their claim that they have plausibly alleged a qualifying "interruption of service" under the CFAA, Plaintiffs point to cases finding such an interruption where the plaintiff is the intended recipient of computer traffic (*e.g.*, emails, website visits), but the defendant swaps the electronic identifier field to redirect that traffic from the plaintiff to the defendant, and the plaintiff seeks to recover "loss" in the form of diverted customer orders and sales revenue. *See, e.g.*, *Integrity Applied Sci., Inc. v. Clearpoint Chems. LLC*, No. 1:18-cv-02235, 2020 WL 12584444, at *2 (D. Colo. Apr. 20, 2020) (redirecting email traffic); *RitLabs, S.R.L. v. RitLabs, Inc.*, No. 1:12-cv-215, 2012 WL 3263893 (E.D. Va. Aug. 9, 2012) (redirecting website traffic by swapping domain registrant field). Based on those cases, Plaintiffs contend that a comparable "interruption of service" occurred here: Capital One swaps Plaintiffs' tracking codes for Capital One's code (*i.e.*, swapping the identifier field), causing merchants to credit the purchases solely to Capital One, thereby causing a loss in the form of diverted commissions that Plaintiffs now seek to recover. Notwithstanding Capital One's contention that this conduct is not "hacking" and they never had "control"[24] over Plaintiffs' tracking codes, the common denominator in these cases is that the defendants are alleged to have used their programming prowess to alter the recipient field in order to redirect the information being communicated through computer traffic for their own financial benefit, amounting to an "interruption of a service." Plaintiffs have therefore sufficiently alleged the first prong of a CFAA claim.

Second, Capital One argues that Plaintiffs failed to allege any knowing and intentional unauthorized access because consumers affirmatively decided to download, install, and use the

[24] Defendants rely heavily on policy arguments about what the CFAA was intended to remedy, without addressing and distinguishing those cases that have found the CFAA's language applicable to conduct that goes beyond the traditional hacking scenario where one nefarious actor accesses a computer system for the sole purpose of causing "widespread disruption." *See, e.g.*, *eBay Inc. v. Digital Point Sols., Inc.*, 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009) (finding cookie-stuffing violates the CFAA); *Griffith v. TikTok, Inc.*, 697 F. Supp. 3d 963, 974 (C.D. Cal. 2023) (finding the defendant manipulated its cookies to bypass browsers' security settings to collect consumer information, in violation of the CFAA).

Capital One Shopping extension to authorize Defendants' involvement in their transaction. [Doc. No. 143] at 27. To use the Extension, consumers assent to the Capital One Shopping Online & Mobile Privacy Policy that permits Capital One to "collect" consumer's "[b]rowsing, product, and ecommerce data, which includes transaction data . . . pages viewed . . . advertising identifiers . . . and [c]ookies and similar technologies data," followed by a non-exhaustive list of examples of why and how that information will be used by Capital One. *Id.* at 27 (citing [Doc. No. 143-2] at 25–28). Capital One's position is that a consumer's choice to use the extension, coupled with the Capital One privacy policy, evidences the consumer's authorization to alter tracking codes associated with their purchases and "is fatal to Plaintiffs' CFAA claim." *Id.*

Plaintiffs counter that the Capital One Shopping Online & Mobile Privacy Policy at issue provides Capital One with some degree of authorization to access consumers' cookies, but Capital One exceeded that authorized access by "overwrit[ing] Plaintiffs' affiliate tracking codes." [Doc. No. 180] at 31–32. Under the CFAA, a person "exceeds authorized access" when they have approval to access a computer but use it "to obtain or alter information that falls outside the bounds of [their] approved access." *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012).

Here, the "unauthorized access" issue reduces to whether consumers who had reached a merchant's website through the Plaintiffs' affiliate links had a right to modify Plaintiffs' tracking codes, and, if so, whether consumers authorized Capital One to exercise those rights in a co-extensive manner under the Capital One Shopping Online & Mobile Privacy Policy.

First, Plaintiffs' allegations make clear that a consumer can modify tracking codes, absent Capital One's influence, by clicking another creator's affiliate link for the same product, clearing the cookies from their browser, or using specialized developer tools. [Doc. No. 121] ¶¶ 44, 54, 200. The next question is whether consumers authorized Capital One to step in their shoes to modify the tracking codes. In that respect, the parties point to the text of the Capital One Shopping Online & Mobile Privacy Policy, with Defendants arguing that they can modify Plaintiffs' tracking codes because consumers permit Capital One to use cookies to "measure" and "record" the interactions that consumers take while using the Extension. [Doc. No. 143-2] at 32. But modifying something is quite different from measuring or recording it, and Capital One's policy goes on to explain that Capital One will "use" cookies "to collect your information," "remember[] your choices," "test new features," "display advertising," and notify consumers of "price drop alerts, coupons, and rewards offers." *Id.* at 31–32. Nowhere does the policy expressly alert consumers that they are authorizing Capital One to do more than collect, measure, and record cookies. Even assuming consumers are authorizing some degree of modification via the "use" of their cookies (*e.g.*, authorizing Capital One to *add* a tracking code so that it can be credited as a creator who had a touchpoint with the purchase), consumers are not expressly authorizing Capital One to *override* Plaintiffs' tracking codes. Indeed, the latter purpose is not captured by the policy's enumerated reasons for why Capital One will "use" consumers' cookies. *Id.* at 31–32. For these reasons, the Plaintiffs have sufficiently alleged that Defendants are exceeding their authorized level of access.[25]

5. California Computer Data Access and Fraud Act (Count VIII)

Lead Plaintiff TechSource, on behalf of a California subclass, brings a claim under the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502, specifically under sections (c)(1), (c)(4), and (c)(8) related to interference with data, a computer, computer system, or computer network. To state a civil claim under the CDAFA, a

[25] At least one court has reached a similar conclusion, albeit on very different facts. In *WhatsApp Inc. v. NSO Group Technologies Limited*, 472 F. Supp. 3d 649 (N.D. Cal. 2020), the plaintiffs alleged that the defendants created WhatsApp accounts to send malware to other users using WhatsApp's system. *Id.* at 658. The defendants argued that they did not exceed authorized access because the terms of service granted them permission to access WhatsApp's computers and servers. *Id.* at 680. The court rejected this argument, noting that "no WhatsApp user had permission to access the technical call settings or evade WhatsApp's security." *Id.* at 658, 681.

plaintiff must allege (i) the defendant acted "without permission" and (ii) suffered "damage or loss by reason of a violation" of the statute. *Esparza v. Kohl's, Inc.*, 723 F. Supp. 3d 934, 944 (S.D. Cal. 2024). These two CDAFA elements are similar to the CFAA's unauthorized access and qualifying loss elements. *See Meta Platforms, Inc. v. BrandTotal Ltd.*, 605 F. Supp. 3d 1218, 1260 (N.D. Cal. 2022) ("Courts have held that CDAFA claims generally rise or fall with CFAA claims because the necessary elements of Section 502 do not differ materially from the necessary elements of the CFAA, except in terms of damages." (cleaned up)).

Capital One argues that a CDAFA claim survives a Rule 12(b)(6) motion only where a plaintiff alleges two additional elements, specifically, that (i) the defendant "circumvent[ed] technical or code-based barriers in place to restrict or bar [] access," *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 950 (N.D. Cal. 2014); and (ii) the plaintiff is the "owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or less by reason of a violation [of the CDAFA]." Cal. Penal Code § 502(e)(1) (emphasis added); *see also Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022, 1028 (N.D. Cal. 2011) (discussing ownership requirement). Plaintiffs argue that "it is not necessary to plead circumvention of technical barriers to show that Capital One acted 'without permission,'" and they sufficiently pleaded an ownership interest in the tracking codes at issue. [Doc. No. 180] at 32 n.17 (citing *Greenley v. Kochava*, Inc., 684 F. Supp. 3d 1024, 1049 (S.D. Cal. 2023)).

Even though California courts "often suggest that a defendant acts without permission when it circumvents 'technical or code-based barriers,'" *Rodriguez v. Google LLC*, No. 20-cv-04688, 2024 WL 1486139, at *4 (N.D. Cal. Apr. 5, 2024), a CDAFA claim does not require, as Capital One contends, some technical or code-based barriers to be allegedly circumvented, particularly where subsection (c)(8) does not require that the defendant act without permission. *Id.*; *see also Zarif v. Hwareh.com, Inc.*, No. 23-cv-0565, 2025 WL 486317, at *12 (S.D. Cal. Feb.

13, 2025) (finding that 'without permission' "is not limited to conduct that circumvents a device barrier or 'hacks' a computer system") (collecting cases). For these reasons and those discussed in the CFAA section herein, Plaintiffs have sufficiently alleged that Capital One acted without permission when swapping tracking codes.

With respect to who owned or leased the computer system or data at issue (*i.e.*, the tracking codes), Capital One argues that "TechSource has not (and cannot) allege that it owns or leases the data in question" because that data is "located in a cookie that is created by merchants and stored on a user's computer." [Doc. No. 191] at 18. Plaintiffs respond that they do have an ownership interest in tracking codes, in part, because those codes are generated by their unique affiliate links. [Doc. No. 180] at 32. This dispute turns on the definition of ownership, a term not defined by the CDAFA.

With respect to the ownership requirement, one California court interpreting the CDAFA noted that "[a]n owner may have complete property in the thing or may have parted with some interests in it," and where who "owns" something is not straightforward, "[o]wnership is a question of fact to be determined by a jury under appropriate instructions of law." *Garrabrants v. Erhart*, 98 Cal. App. 5th 486, 508 (2023) (citing BLACK'S LAW DICTIONARY (11th ed. 2019)). But as other California courts have observed in connection with a CDAFA claim, ownership is often linked to the entity who created the property at issue. For instance, where a plaintiff drafts emails or technical documents that are stored in a third-party's servers and then accessed by a defendant without authorization, a CDAFA claim is cognizable because the plaintiff author retains some ownership interest in the data at issue. *See Lindsay-Stern v. Garamszegi*, No. 14-01970, 2016 WL 11745948, at *5 (C.D. Cal. Oct. 13, 2016); *Oracle USA, Inc. v. Rimini St., Inc.*, 191 F. Supp. 3d 1134, 1142 (D. Nev. 2016), *aff'd in part, rev'd in part on other ground,* 879 F.3d 948 (9th Cir. 2018); *see also Christian v. Betak*, No. 24-cv-01867, 2025 WL 786056, at *6 (N.D. Cal. Mar. 11, 2025). But where a plaintiff's personal data (*e.g.*, financial information, health data) is collected or generated by a third-party, and stored by a third-party, the plaintiff may retain "some form of interest – for example, a privacy interest," but cannot necessarily claim an ownership interest in that data under the CDAFA. *Garrabrants*, 98 Cal. App. 5th at 509; *see Stuart v. County of Riverside*, No. 5:22-cv-00701, 2024 WL 3455263, at *19 (C.D. Cal. Apr. 22, 2024); *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1090 (N.D. Cal. 2018).

Here, Techsource, the Plaintiff who has asserted an CDAFA claim, has not adequately alleged that it creates or generates the tracking codes at issue and appears to indicate that merchants and affiliate networks are responsible for creating those codes that are then stored on consumers' browsers. The Complaint alleges that "an online merchant will provide an 'affiliate link' to the creator," [Doc. No. 121] ¶ 32, and "[a]n affiliate link is a custom URL assigned to a creator by an online merchant," *id.* ¶ 39. Merchants are therefore alleged to "provide" and "assign" affiliate links with embedded tracking codes. There is no allegation that Techsource or other Plaintiffs play a role in creating tracking codes, like the plaintiffs in *Lindsay-Stern* and *Oracle* who retained an ownership interest in the data at issue because they drafted portions of the files and emails (*i.e.*, the data at issue). For these reasons, the Complaint fails to plausibly allege the ownership requirement and the CDAFA claim (Count VIII) is dismissed.

6. New York General Business Law (Count VI)

Lead Plaintiff Storm Productions LLC, on behalf of a New York subclass, also brings a claim under Section 349 of the New York General Business Law ("GBL") for Capital One's alleged "unlawful deceptive acts or practices." *See* [Doc. No. 121] ¶¶ 206-17. In the Motion, Capital One argues that Plaintiffs have neither shown that its conduct was "consumer-oriented," instead of a private commercial dispute between competitors, [Doc. No. 143] at 29-30, nor misleading to consumers, as the allegedly misleading practice was fully disclosed through Capital One's disclosures to consumers. *Id.* at 30-31.

Section 349 of the GBL prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service" in New York. N.Y. GEN. BUS. L. § 349(a). To plausibly state a claim under Section 349, a plaintiff must allege three elements: "(1) the defendant's deceptive acts were directed at consumers, (2) the acts are misleading in a material way, and (3) the plaintiff has been injured as a result." *Duran v. Henkel of Am., Inc.*, 450 F. Supp. 3d 337, 346 (S.D.N.Y. 2020) (quoting *Maurizio v. Goldsmith*, 230 F.3d 518, 521 (2d Cir. 2000) (per curiam)). In pleading these requirements, a plaintiff must "only meet the bare-bones notice-pleading requirements of Rule 8(a)." *Pelman ex rel. Pelman v. McDonald's Corp*., 396 F.3d 508, 511 (2d Cir. 2005).

First, under the GBL, a practice is consumer-oriented where "the defendant's allegedly deceptive act or practice is directed to the consuming public and the marketplace," and the act is "focused on the seller's deception and its subsequent impact on consumer decision-making." *Himmellstein, McConnell, Gribben, Donoghue & Joseph, LLP v. Matthew Bender & Co., Inc.*, 37 N.Y.3d 169, 177 (2021) (citation omitted). "Although the statute is, at its core, a consumer protection device, corporate competitors [may] bring a claim under [Section 349] . . . so long as some harm to the public at large is at issue." *Securitron Magnalcok Corp. v. Schnabolk*, 65 F.3d 256, 264 (2d Cir. 1995) (citations and quotations omitted). At bottom, "the gravamen of the [GBL claim] must be consumer injury or harm to the public interest." *Azby Brokerage, Inc. v. Allstate Ins. Co.*, 681 F. Supp. 1084, 1089 n.6 (S.D.N.Y. 1988). If a plaintiff seeks to allege harm to the public interest, a plaintiff must allege "significant ramifications for the public at large," *Shred–It USA, Inc. v. Mobile Data Shred, Inc.*, 228 F.Supp.2d 455, 465 (S.D.N.Y. 2002), and where the core of the claim is merely harm to a competitor or other business—rather than consumers—courts generally find that the plaintiff has not sufficiently alleged public harm under Section 349. *See Gucci Am., Inc. v. Duty Free Apparel, Ltd.*, 277 F. Supp. 2d 269, 273 (S.D.N.Y. 2003) (collecting cases).

Storm Production alleges that the Extension misleads consumers about who is entitled to receive a commission resulting from their purchase by simulating the artificial referral click for Capital One, injecting a hidden tab to overwrite the previous affiliate tracking code, and updating the browser's cookies to indicate that Capital One is the last-clicked affiliate link. [Doc. No. 121] ¶¶ 102, 213. From this, Storm Productions alleges that the Extension engages in consumer-oriented conduct because the Extension does not disclose that it allegedly misappropriates the influencer's commission, and the public interest is harmed because influencers are deprived of their commissions. However, "the alleged harm to [the influencers] far outweighs any incidental harm to the public at large," and this is too insubstantial of a harm to plausibly establish a claim under Section 349. *See Fashion Boutique of Short Hills, Inc. v. Fendi USA, Inc.*, No. 91 CIV. 4544, 1992 WL 170559, at *4 (S.D.N.Y. July 2, 1982); *Gucci*, 277 F. Supp. 2d at 273 (S.D.N.Y. 2003).

Storm Productions also claims that Capital One was engaging in consumer-oriented conduct by pushing affiliates out of the market, thereby reducing consumer choice. [Doc. No. 121] ¶¶ 211-12. However, absent from the Complaint is any allegation that any affiliate *has* been pushed out of the market or *is actively* being pushed out of the market because of the Extension. Instead, the GBL claim rests entirely on a speculative belief that this may happen in the future with no plausible factual allegations to support this claim.[26]Accordingly, Storm Productions has not

[26] Notably, Storm Productions has made other allegations that demonstrate it is unlikely that the Plaintiffs will be entirely pushed out of the market. *See* [Doc. No. 121] ¶ 34 (alleging that the affiliate marketing industry revenues are expected to nearly double by 2030); *id.* ¶¶ 116-17 (demonstrating Storm Productions planned to continue partnering with merchants in the future).

plausibly alleged consumer-oriented conduct to support its GBL Claim, and the Motion is granted as to Count VI.

7. California Unfair Competition Law (Count VII)

Lead Plaintiff TechSource, on behalf of a California subclass, alleges that Capital One is also violating the California Unfair Competition Law ("UCL") by stealing credit for sales referrals that belonged to TechSource and the California class members. [Doc. No. 121] ¶ 223. In the Motion, Capital One argues that the claim should be dismissed because (i) the UCL only provides for equitable relief, and Plaintiff has not demonstrated a lack of adequate legal remedies; [Doc. No. 143] at 31; and (ii) Plaintiffs have not alleged "unfair" or "unlawful" conduct under the UCL, *id.* at 32-33.

The UCL only provides equitable relief, *Hodge v. Superior Ct.*, 145 Cal. App. 4th 278 (2006), and "[p]laintiffs [are] obligated to allege that they had no adequate legal remedy in order to state a claim for equitable relief." *See In re Apple Processor Litig.*, No. 22-16164, 2023 WL 5950622, at *2 (9th Cir. Sept. 13, 2023); *see also Guzman v. Polaris Indus. Inc.*, 49 F.4th 1308, 1312-13 (9th Cir. 2022); *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020). TechSource argues that it is entitled to restitution to restore it to the position it would have been had the Extension not diverted its commissions, primarily relying on *Cortez v. Purolator Air Filtration Products Company*, 23 Cal. 4th 163 (2000). *See* [Doc. No. 180] at 37.

However, where plaintiffs, like TechSource, "fail[] to explain how the money they seek through restitution is any different than the money they seek as damages," the UCL claim must be dismissed. *See In re Apple Processor Litig.*, 2023 WL 5950622, at *2 (cleaned up). Furthermore, *Cortez* was decided before *Apple Processor*, *Guzman*, and *Sonner*, which establish that where a federal court lacks equitable jurisdiction over a claim, it must be dismissed. *See Guzman*, 49 F.4th at 1314 ("Equitable jurisdiction is distinct from subject matter jurisdiction, although both are required for a federal court to hear the merits of an equitable claim.”). Here, TechSource has not plausibly alleged that it has no adequate legal remedy, the Court therefore does not have any equitable jurrisdiction and the Motion is therefore granted as to Count VII.

IV. CONCLUSION

For the reasons stated above, it is hereby

ORDERED that the Motion, [Doc. No. 142], be, and the same hereby is, **GRANTED** as to Counts IV (conversion), VI (New York General Business Law), VII (California Unfair Competition Law), VIII (California Comprehensive Computer Data Access and Fraud Act), and IX (Pennsylvania Computer Offenses Law); and is otherwise **DENIED**.

The Clerk is directed to forward a copy of this Memorandum Opinion and Order to all counsel of record.

/s/
Anthony J. Trenga
Senior United States District Judge

Alexandria, Virginia
June 2, 2025