No. 26-1660

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

CHRISTOPHER CALISE AND ANASTASIA GROSCHEN,
Plaintiff-Appellees,

v.

META PLATFORMS, INC. (F/K/A FACEBOOK, INC.),
Defendant-Appellant.

On Appeal from the United States District Court
for the Northern District of California, Oakland
No. 4:21-cv-06186
Hon. Jeffrey S. White

BRIEF OF AMICI CURIAE TECH JUSTICE LAW, CHECK MY ADS INSTITUTE, CONSUMER FEDERATION OF AMERICA, CONSUMER REPORTS, NATIONAL ASSOCIATION OF CONSUMER ADVOCATES, AND NATIONAL CONSUMER LAW CENTER IN SUPPORT OF PLAINTIFF-APPELLEES

Meetali Jain
Sarah Kay Wiley
Tech Justice Law
10 G Street, NE, Suite 600
Washington, DC 20002
(510) 570-4116

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

AMICI INTERESTS[1]

Check My Ads

Check My Ads (CMA) is an independent nonprofit global digital advertising watchdog. CMA serves the stakeholders that are most impacted by the digital advertising ecosystem (publishers, advertisers, policymakers, small businesses, and the public) by helping them understand not only how advertising budgets flow, but how they shape the information ecosystem. CMA's mission is to bring transparency and accountability to the notoriously opaque and purposefully complex digital advertising ecosystem and to work globally with policymakers to advance many common-sense safeguards to protect the public.

Consumer Federation of America

The Consumer Federation of America (CFA) is an association of nonprofit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education. Today, nearly 200 of these groups participate in the federation and govern it through their representatives on the organization's Board of Directors. CFA's robust history of consumer advocacy demonstrates a nexus with the interests of the consumers represented in this case. CFA has historically and continually advocated for the protection of consumers against scams and fraud in all forms. For many years, CFA has partnered with a number of groups and authorities to increase awareness about scams and offer recommendations to the public to protect themselves.

Consumer Reports

Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's

[1] No counsel for any party authored this brief in whole or in part, and no person other than amici curiae, their members, and their counsel made a monetary contribution to the preparation or submission of this brief. *See* Fed. R. App. P. 29(a)(4)(E). All parties consented to the filing of this brief.

consumers, and provides ad-free content and tools to 6 million members across the U.S.

National Association of Consumer Advocates

National Association of Consumer Advocates (NACA) is a nonprofit association of more than 1,600 attorneys and consumer advocates committed to representing consumers' interests. NACA's members are private and public sector attorneys, legal services attorneys, law professors, and law students whose primary focus is the protection and representation of consumers. They have represented hundreds of thousands of consumers in small-damages actions and consumer class actions. As a national organization fully committed to promoting justice for consumers, with an emphasis on those of modest means or those who are otherwise especially vulnerable, NACA's members have also long advocated to ensure that consumers have remedy and means of redress of injuries caused by unfair practices.

National Consumer Law Center

Since its founding as a nonprofit in 1969, the National Consumer Law Center ("NCLC") has used its expertise in consumer law to work for consumer justice and economic security for low-income and other disadvantaged people in the United States. NCLC's expertise includes policy analysis and advocacy, consumer law, litigation, expert witness services, and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitative practices, help financially stressed families build and retain wealth, and advance economic fairness.

Tech Justice Law

Tech Justice Law (TJL) is a nonprofit impact litigation and advocacy organization dedicated to reclaiming individual and collective humanity in the digital age. Through litigation and public education, TJL confronts technology business models that depend on surveillance and manipulation and works to hold technology companies accountable when they profit from deceptive practices that put consumers at risk. TJL accordingly has a direct interest in ensuring that platforms are held to the plain-language safety promises they make to the public, and that the consequences of breaking those promises are not diluted by rules that would let technology companies disclaim, after the fact, commitments they used to attract and retain user trust.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Civil Procedure 26.1(a), the undersigned counsel states that the nonprofit, non-governmental organizational amici listed above have no parent corporations and that no publicly held corporation owns 10% or more of their stock.

Date: August 5, 2026

/s/ Meetali Jain

Meetali Jain
Tech Justice Law Project
10 G Street, NE, Suite 600
Washington, DC 20002
(510) 570-4116
Counsel for Amici Curiae

INTRODUCTION

Meta Platforms, Inc. built one of the most profitable businesses in history by learning everything it can about its users and selling that knowledge to advertisers. Meta harvests data from every corner of a user's digital life; it not only collects what users type into Facebook, but what they do on millions of other websites tracked through the Meta Pixel, where they go, and what they click.[2] Meta then runs that data through an auction algorithm that matches advertisers with the users most likely to engage with their ads, determining "the size, placement, and positioning" of every ad a user sees.[3] The result is extraordinarily lucrative: Meta earned $59.36 billion in advertising revenue during the second quarter of 2026 alone.[4] Nearly all of that revenue—Meta's entire business—rests on users trusting that its platforms are a safe place to spend their time and their attention.

---

[2] *See, e.g.,* Surya Mattu et al., *How We Built a Meta Pixel Inspector*, The Markup (Apr. 28, 2022, at 08:00 UTC), https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector [https://perma.cc/KC7R-YCRV]; *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, Fed. Trade Comm'n (Mar. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking [https://perma.cc/6BN3-26FC].

[3] *Self-Serve Ad Terms*, Facebook (Aug. 22, 2025), https://www.facebook.com/legal/self_service_ads_terms [https://perma.cc/7QJH-RQXL].

[4] *Meta Reports Second Quarter 2026 Results*, Meta (July 29, 2026), https://s21.q4cdn.com/399680738/files/doc_news/Meta-Reports-Second-Quarter-2026-Results-2026.pdf [https://perma.cc/2BQC-KYMT].

To foster that trust, Meta made explicit affirmative promises to the users of its Facebook platform. In Facebook's 2021 Terms of Service, under a heading alleging to "[c]ombat harmful conduct and protect and support our community," Meta told Facebook users that "[i]f we learn of content or conduct [that is harmful to the community], we will take appropriate action."[5] In its Community Standards, Meta promised that "we remove content that purposefully deceives, willfully misrepresents or otherwise defrauds or exploits others for money or property."[6]

Under any plain-language reading, a reasonable consumer encountering these provisions would understand exactly what they say: that Meta has bound itself to act when it learns that scammers are exploiting its platform, and to remove advertisements focused on defrauding its users. That is precisely how the district court read them, holding that the Appropriate Action Provision and Removal Provision highlighted above contain "unambiguous and well-defined promises from Meta to users."[7]

Now, Meta requests that this Court find that the language it wrote itself and displayed to users is nothing more than an unenforceable "general monitoring

---

[5] Amended Class Action Complaint & Jury Trial Demanded at 9–10, Calise v. Meta Platforms, Inc., No. 4:21-cv-06186-JSW (N.D. Cal. Dec. 20, 2024), Dkt. No. 56.
[6] *Id.* at 11.
[7] Order Granting In Part and Denying In Part Defendant Meta Platforms, Inc's Mot. to Dismiss at 6, Calise v. Meta Platforms, Inc., No. 4:21-cv-06186-JSW (N.D. Cal. Sep. 22, 2025), Dkt. No. 57.

policy."[8] Such a finding would be detrimental for users and convenient for Meta, which has continued to knowingly, and for profit, put its users at risk by its inaction and facilitation of scams on its platform.

The stakes of this appeal extend well beyond the parties before the Court. Between 2021 and 2023, consumers were defrauded out of at least $2.7 billion from schemes originating on social media platforms.[9] To credit Meta's argument would be to hold that a platform can advertise safety to its users in the very documents that govern their relationship, while simultaneously designing its advertising engine to profit from the fraud those same documents promise to combat. Consumers are entitled to rely on what a company tells them it will do—especially when that company profits, to the tune of billions of dollars annually.

---

[8] Opening Brief of Meta Platforms, Inc. at 28, Calise v. Meta Platforms, Inc., No. 4:21-cv-06186-JSW (N.D. Cal. May 28, 2026), Dkt. No. 11.1 (quoting Barnes v. Yahoo! Inc., 570 F.3d 1096, 1108 (9th Cir. 2009)).

[9] *See FTC Data Shows Consumers Report Losing $2.7 Billion to Social Media Scams Since 2021*, Fed. Trade Comm'n (Oct. 6, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-data-shows-consumers-report-losing-27-billion-social-media-scams-2021 [https://perma.cc/8TEQ-E3QZ]; *see also* Class Action Complaint & Jury Trial Demand, Consumer Fed'n of Am. v. Meta Platforms, Inc., No. 2026-CAB-002643 (D.C. Super. Ct. Apr. 21, 2026); *Slam the Door on Phishing Scams*, Consumer Fed'n of Am., https://consumerfed.org/media/legacy/post_14128/Phishing-Tips.pdf [https://perma.cc/PZ9D-CTC7] (last visited Apr. 20, 2026); Susan Grant, *Take Control of the Call to Avoid Scams and Abuse*, Consumer Fed'n of Am (July 27, 2020), https://consumerfed.org/take-control-of-the-call-to-avoid-scams-and-abuse/ [https://perma.cc/VBN9-ZRCJ]; Janice Fahey & Liudmila Mignosa, *Phone Sense*, Consumer Fed'n of Am (Sep. 10, 2018), https://consumerfed.org/phone-sense/ [https://perma.cc/SMU4-6QXC].

Affirming the district court's decision does not require this Court to remake platform-liability law;[10] it requires only that Meta be held to the ordinary contract-law consequences of the promises it chose to make.

---

[10] Meta's Opening Brief repeatedly recasts its own Appropriate Action and Removal Provisions as "third-party conduct or content" as an attempt to bring them within the Limits on Liability Clause's disclaimer. *See* Opening Brief of Meta Platforms, Inc,. *supra* note 7, at 20–21 (arguing the Clause "directly answers" whether Meta must "identify and remove all prohibited third-party content"); *id.* at 32 (framing the question presented as "whether the ToS and Community Standards impose an affirmative obligation on Meta to monitor and remove third-party content"); *id.* at 40 (asserting the Clause disclaims "any responsibility for third-party conduct or content on Facebook"). But by its plain terms, the Limits on Liability Clause disclaims responsibility only for the conduct and content that third-party *users* themselves post, not for Meta's own, separately undertaken promise to act once it learns of that content. This is, moreover, the same maneuver this Court already rejected once in this very case. Meta previously argued that Section 230 barred liability because Plaintiffs' claims arose from Meta's handling of third-party advertisements; this Court held otherwise, explaining that "[t]o the extent that Meta manifested its intent to be legally obligated to 'take appropriate action' to combat scam advertisements, it became bound by a contractual duty separate from its status as a publisher," such that "Meta's duty arising from its promise to moderate third-party advertisements is unrelated to Meta's publisher status." *Calise v. Meta Platforms, Inc.*, 103 F.4th 732, 743 (9th Cir. 2024). Meta's Limits-on-Liability argument repackages that same rejected premise, that a promise to police third-party content is itself third-party conduct.

ARGUMENT

I. THE COURT SHOULD AFFIRM PLAINTIFFS' BREACH OF CONTRACT CLAIM AGAINST META

A. Facebook's Terms of Service and Community Standards Manifest Meta's Intent to be Contractually Bound

California's rules of contract interpretation alone govern this dispute, and they compel the conclusion that the "Appropriate Action and Removal Provisions" bind Meta to the promises it made to users. "[T]he intention of the parties is to be ascertained from the writing alone," and the words of a contract are to be understood in their "ordinary and popular sense" so long as the language "is clear and explicit and does not involve an absurdity." Cal. Civ. Code §§ 1638–39, 44. California law does not permit a drafter to disclaim, after the fact, the plain meaning of language it chose in the first instance. The writing itself is the measure of the parties' intent.

That principle finds application in *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009), which holds that a platform's language creates an enforceable promise where it "manifest[s] intention to be legally obligated to do something," (*id.* at 1107), measured by the "objective manifestations of intent" a reasonable person would draw from the words used, (*id.* at 1108). Meta's Terms of Service do exactly what *Barnes* requires. Under the Terms of Service sub-heading pledging to "[c]ombat harmful conduct and protect and support our Community," Meta advises that it “employs dedicated teams around the world and develop[s] advanced technical systems to detect misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community.” Meta then promises that “[i]f we learn of content or conduct like this [e.g., harmful conduct to others] we will take appropriate action—for example, offering help, removing content, removing or restricting access to certain features, disabling an account, or contacting law enforcement.”[11] That commitment is framed in the mandatory “will” and it is paired with concrete examples of what “appropriate” action includes. Read in their ordinary and popular sense, the only conclusion a reasonable consumer could draw from Meta’s language is that Meta has committed itself to act—and a reasonable consumer, having read that commitment, would order her conduct accordingly: trusting that reported scams would be addressed, and that Meta’s promised “dedicated teams” and “advanced technical systems” stood behind the platform she used every day.

Reading the Terms of Service and Community Standards as an integrated whole, as California law requires, only reinforces that conclusion. California Civil Code section 1641 provides that “the whole of a contract is to be taken together, so as to give effect to every part, if reasonably practicable, each clause helping to interpret the other.” Cal. Civ. Code § 1641. Viewed together with the Appropriate

[11] *Self-Serve Ad Terms*, *supra* note 3.

Action Provision, Meta's Community Standards speak with the same directness. In the Removal Provision, Meta represents that "we remove content that purposefully deceives, willfully misrepresents or otherwise defrauds or exploits others for money or property." That is a first-person, present-tense commitment, not a description of Meta's aspirations. A consumer reading this framework would not understand Meta to have reserved unfettered discretion to do nothing; she would understand it as a commitment that, once Meta has knowledge of harmful conduct like rampant scam advertising, it will respond. That is not the kind of "general monitoring policy" *Barnes*[12] held unenforceable—it is a specific, actionable promise that Meta's own users were entitled to rely upon, and, as shown below, one Meta has continued to break specifically and repeatedly.

B. Meta's Inaction and Facilitation of Scam Advertisements Breached Its Contractual Promises To Users

Meta has continued to knowingly harm its users. Facebook is, in Meta's own words, "a pillar of the global fraud economy."[13] An internal document uncovered by Reuters shows Meta estimates that approximately 15 billion "higher risk" scam

---

[12] 570 F.3d at 1107–08.

[13] Jeff Horwitz, *Meta Is Earning a Fortune on a Deluge of Fraudulent Ads, Documents Show*, Reuters (Dec. 28, 2025), https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/ [https://perma.cc/HND8-LRJM].

advertisements reach its users every single day.[14] A May 2025 presentation by Meta's own safety staff estimated that Meta's platforms "were involved in a third of all successful scams" committed in the United States.[15] This is not a new discovery Meta stumbled into after the fact—Meta has been on notice of pervasive scam advertising on Facebook since at least 2014, when an independent cybersecurity firm published a white paper documenting the problem.[16] Meta's promises to root out scams were made, and repeated, against this backdrop of full internal knowledge that its platform was inundated with fraud.

But Meta does not merely tolerate the scam advertising it has promised to eliminate, rather it has continued to build a lucrative revenue stream on top of it. Meta's own internal projections make the point starkly: in 2024, Meta anticipated that *more than 10% of its total earnings* would come from scam advertisements, illegal gambling, and the sale of prohibited goods on its platforms—approximately

---

[14] Horwitz, *supra* note 12. Meta has tried to downplay the risks their users face by noting, in a December 3, 2025 press release that they "removed more than 134 million scam ads." Although these numbers sound impressive, it accounts for removing less than 1% of the ads over the course of a year. *See, e.g., Scams Are Bad for Business: Our Ongoing Efforts to Fight Fraud*, Meta (Dec. 3, 2025), https://about.fb.com/news/2025/12/scams-are-bad-for-business-metas-efforts-to-fight-fraud/ [https://perma.cc/KQD9-TJN2].

[15] Horwitz, *supra* note 12.

[16] Andrei Cristian Serbanoiu, *Digging into Facebook Ads: Finding Clues that Indicate a Scam Pattern*, Bitdefender (Mar. 4, 2014), https://www.bitdefender.com/media/materials/white-papers/en/Bitdefender_WhitePaper_Facebook_ads.pdf [https://perma.cc/B4NG-2XDL].

$16 billion.[17] The "high risk" category of advertisements alone earns Meta roughly $7 billion in annualized revenue.[18] These are not marginal or incidental sums; they are figures Meta itself generated, tracked, and relied upon in its own internal business planning. A company that has calculated, to the billion, how much revenue fraud generates for its bottom line cannot credibly claim ignorance of the fraud, nor can it credibly claim that its public promises to eliminate that fraud were made in good faith.

Rather than working to eliminate this revenue, Meta has engineered its advertising systems to protect it. When Meta's own detection systems determine that an advertiser has as high as a 95% likelihood of running a scam, Meta's response is not to remove the advertiser from its platform—it is to charge that advertiser more.[19] Meta imposes what internal documents describe as a "penalty bid" fee that allows suspected fraudsters to keep buying access to Meta's users provided they pay more, meaning that the riskier the advertiser, the more money they must pay for advertising, and the more money Meta makes from letting them stay on the platform.[20] This is the inverse of any genuine anti-fraud program: Meta has converted its own fraud-detection capability, which could be used to protect users,

---

[17] Horwitz, *supra* note 12.
[18] *Id.*
[19] *Id.*
[20] *Id.*

into a pricing mechanism that instead protects Meta's revenue. Tellingly, a 2025 internal Meta review concluded that "[i]t is easier to advertise scams on Meta platforms than Google,"[21] not because Meta lacks the technical capacity to do better, but because Google's account-centric enforcement removes bad actors, while Meta's model is built to keep them paying.[22]

Meta's conduct with respect to Chinese advertising agencies confirms that this is a deliberate business choice, not an unfortunate byproduct of scale. Meta itself estimates that China accounts for roughly a quarter of all scam advertisements on its platforms. Rather than tightening scrutiny of this known high-risk channel, Meta pays eleven large Chinese ad agencies—"resellers"—a rough 10% commission to enlist advertisers and run ads through "agency accounts," and grants those agencies special protections unavailable to ordinary advertisers.[23] Under a system Meta internally calls "whitelisting" or "mistake prevention," Meta does not immediately remove ads purchased through top-tier agencies even after Meta's own automated

---

[21] Horwitz, *supra* note 12.

[22] *The $16 Billion Problem: How Meta's Scam Ad Revenue Impacts PPC Advertisers*, ClickGuard (Nov. 13, 2025), https://www.clickguard.com/blog/meta-scam-ad-revenue-impacts-ppc-advertisers/ [https://perma.cc/K8SX-PFZQ].

[23] Jeff Horwitz & Engen Tham, *Meta Tolerates Rampant Ad Fraud from China to Safeguard Billions in Revenue*, Reuters (Jan. 1, 2026), https://www.reuters.com/investigations/meta-tolerates-rampant-ad-fraud-china-safeguard-billions-revenue-2025-12-15/ [https://perma.cc/8EU8-ZMEM].

systems flag them for violating Meta's advertising rules.[24] Suspected scam ads from these whitelisted accounts continue running on users' feeds while they await—or undergo—human review, increasing the very risk to users that Meta had promised to guard against.[25] Meta, in other words, built a preferential lane for a category of advertiser it knows is disproportionately responsible for fraud, and then insulated that lane from the enforcement mechanisms it tells users are protecting them.

Meta has also effectively hamstrung the employees whose job was to make good on its promises. In 2023, Meta fired much of the staff responsible for reducing fraud on its platform, including the entire team that handled advertiser brand-impersonation concerns; internal documents concede a "lack of investment" in automated scam detection and classify scam ads internally as a "low severity" problem.[26] Then, in February 2025, Meta leadership went further, imposing an internal rule that barred its own ad-vetting teams from taking any action against a suspect advertiser that could cost Meta more than 0.15% of total company revenue—

[24] Jeff Horwitz, *Facebook Says Its Rules Apply to All. Company Documents Reveal a Secret Elite That's Exempt*, The Wall Street Journal (Sep. 13, 2021, at 10:21 ET), https://www.wsj.com/tech/facebook-files-xcheck-zuckerberg-elite-rules-11631541353?mod=djemalertNEWS [https://perma.cc/V68R-WWU6].
[25] *See* Horwitz & Tham, *supra* note 22.
[26] *See* Complaint ¶ 6, Comm'r of Dep't of Licensing & Consumer Aff. v. Meta Platforms, Inc., No. SX-25-CV (V.I. Super. Ct. Dec. 23, 2025) (citing Reuters reporting).

about $135 million against the roughly $90 billion Meta generated in just the first half of 2025.[27]

Finally, Meta has continued to ignore the very users it asked to help it police the platform. Meta's Community Standards promise that Meta will act on reports of scam and deceptive conduct, and Meta's own internal figures show that Facebook and Instagram users file approximately 100,000 valid reports of fraudsters messaging them every single week. As highlighted by internal documents, "Meta ignored or incorrectly rejected 96% of them."[28] Nor is that failure evenly applied: small advertisers can be shut down after as few as eight confirmed strikes for promoting financial fraud, while Meta's largest advertisers—its self-described "High Value Accounts"—can accumulate more than 500 strikes without consequence.[29] A user who takes the time to report a scammer, as Meta's own policies invite them to do, has a nineteen-in-twenty chance that Meta will do nothing at all. That is not inaction born of scale; it is the predictable result of a company that has built enforcement thresholds around protecting its highest-paying, highest-risk advertisers rather than the users it promised to protect.

No reasonable consumer, reading a promise to "combat harmful conduct" and to "remove content that purposefully deceives" or "defrauds or exploits others for

---

[27] Horwitz, *supra* note 12.
[28] *Id.*
[29] *Id.*

money or property," would understand those words to permit Meta to knowingly monetize the very fraud it promised to fight. To adopt Meta's contrary reading—that these provisions describe only a discretionary, non-binding "general monitoring policy"—would render the promise illusory, permitting Meta to continue to put users at risk and collect billions of dollars for the privilege.

II. THE COURT SHOULD AFFIRM PLAINTIFFS' BREACH OF THE IMPLIED COVENANT CLAIM.

A. Affirming Plaintiffs' Implied Covenant Claim Serves the Public Interest.

Under California law, "[t]he covenant of good faith and fair dealing, implied by law in every contract, exists merely to prevent one contracting party from unfairly frustrating the other party's right to receive the benefits of the agreement actually made." *Guz v. Bechtel Nat'l, Inc.*, 8 P.3d 1089, 1110 (Cal. 2000). The covenant is not a mere technicality; it is the mechanism by which courts ensure that parties who possess discretionary power over the rights of another exercise that power honestly. *Acree v. Gen. Motors Acceptance Corp.*, 112 Cal. Rptr. 2d 99, 106 (Cal. App. 4th 2001) (implied covenant "particularly applies where . . . the contract gives one party a discretionary power affecting the rights of the other"). Few relationships fit that description more squarely than the one between a dominant social media platform and the hundreds of millions of users who depend on it and who have no meaningful power to negotiate the terms under which their safety is protected.

A party "can breach the covenant without 'breach of a specific provision of the contract.'" *3500 Sepulveda, LLC v. Macy's W. Stores, Inc.*, 980 F.3d 1317, 1324 (9th Cir. 2020). That principle has particular force here, because a plaintiff need only show that Meta's conduct "demonstrates a failure or refusal to discharge contractual responsibilities, prompted not by an honest mistake, bad judgment or negligence, but rather by a conscious and deliberate act." *Careau & Co. v. Security Pacific Business Credit, Inc*., 272 Cal. Rptr. 387, 400 (Cal. App. 1990). Courts applying this standard have consistently allowed implied covenant claims against Meta to proceed where, as here, Meta's own conduct frustrated the safety purpose animating its Terms of Service. *See, In re Facebook, Inc*., 402 F. Supp. 3d 767, 802 (N.D. Cal. 2019) (even absent breach of the contract's literal terms, deliberate frustration of the contract's purpose states a covenant claim); *Chauhan v. Google LLC*, No. 23-cv-00702-KAW, 2023 WL 5004078, at *3 (N.D. Cal. Aug. 4, 2023) (covenant claim not duplicative of contract claim); *Doe v. Meta Platforms, Inc*., 690 F. Supp. 3d 1064, 1086 n.10 (N.D. Cal. 2023) (same).

Meta's bad faith has continued to extend beyond passive inaction to affirmative concealment. Meta maintains an "Ad Library" — a publicly searchable repository that Meta represents as a transparent record of ads it is running, or has recently run, on its platforms. However, when Japanese regulators began using the Ad Library to search for scam advertisements, Meta altered the underlying database to strip out "some fraudulent advertising of the sort that regulators would want to weed out," making the results regulators were reviewing "appear cleaner than they otherwise would have."[30] Tellingly, the tactic was not an isolated lapse: it succeeded so well that Meta incorporated it into a "general global playbook" for managing regulatory scrutiny in other markets, including the United States, enabling Meta "to stall regulators and put off advertiser verification unless new laws leave [it] no choice."[31] Manipulating a public-facing transparency tool specifically to deceive regulators investigating the very fraud at issue in this litigation highlights the "conscious and deliberate act" required to sustain an implied covenant claim. *Cousens v. Transamerica Life Ins. Co.*, 2025 WL 763476, at *1 (9th Cir. Mar. 11, 2025) (quoting *Chateau Chamberay Homeowners Ass'n v. Associated Int'l Ins. Co.*, 108 Cal. Rptr. 2d 776, 783 (Cal. App. 2001)).

Moreover, a recent industry audit confirms that Meta's lax verification practices are deliberate. The audit found that although there is no standard across advertising platforms for advertiser verification, unlike other platforms that require proof of identity from prospective advertisers before they can run ads, Meta does not

---

[30] Jeff Horwitz, *Meta Created 'Playbook' to Fend Off Pressure to Crack Down on Scammers, Documents Show*, Reuters (Jan. 5, 2026), https://www.reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31/ [https://perma.cc/7DX9-9GMX].

[31] *Id.*

require verification of a business's website, email address, industry, proof of identity, legal representative, or a company privacy policy before allowing that business to begin running ads on its platform.[32] These lax standards are a deliberate business decision by a company that, as detailed above, profits directly from lowering the barriers to entry for advertisers it knows are likely to be running scams.

Upholding Plaintiffs' implied covenant claim would vindicate more than the individual interests of Mr. Calise and Ms. Bohl. It would preserve the only meaningful check that ordinary users have against a platform that has arrogated to itself total, unreviewable discretion over whether, and against whom, to enforce the very safety promises it advertises to the public. If Meta is permitted to accept the benefit of representing to hundreds of millions of consumers that it "will take appropriate action" against harmful conduct, while ignoring with impunity that promise, concealing its wrongdoing, and promoting lax standards that frustrate any obligations it made to users, the covenant of good faith and fair dealing rings hollow for an entire industry. The public interest favors a rule that holds platforms to the promises they use to attract and retain the trust of their users. This Court should affirm the district court's order sustaining Plaintiffs' claim.

[32] *Advertiser Verification Report*, Check My Ads (June 15, 2026), https://checkmyads.org/report/advertiser-verification-report/ [https://perma.cc/ZFR2-C46X].

CONCLUSION

For the foregoing reasons, *amici curiae* respectfully request that this Court affirm the district court's order denying Meta's motion to dismiss the Amended Complaint and remand for further proceedings.

Date: August 5, 2026

/s/ Meetali Jain

Meetali Jain
Sarah Kay Wiley
Tech Justice Law
10 G Street, NE, Suite 600
Washington, DC 20002
(510) 570-4116

Counsel for Amici Curiae