TONY LOPRESTI (SBN 289269)
KAVITA NARAYAN (SBN 264191)
MEREDITH A. JOHNSON (SBN 291018)
LAURA S. TRICE (SBN 284837)
HANNAH M. GODBEY (SBN 334475)
BILL NGUYEN (SBN 333671)
OFFICE OF THE COUNTY COUNSEL
COUNTY OF SANTA CLARA
70 West Hedding Street, East Wing, Ninth Floor
San José, California 95110-1770
Telephone: (408) 299-5900
Facsimile: (408) 292-7240
Email: kavita.narayan@cco.sccgov.org
meredith.johnson@cco.sccgov.org

Counsel for Plaintiff the People of the State of California

[additional counsel listed on signature page]

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SANTA CLARA

PEOPLE OF THE STATE OF CALIFORNIA, ACTING BY AND THROUGH COUNTY OF SANTA CLARA COUNTY COUNSEL TONY LOPRESTI,

Plaintiff,

v.

META PLATFORMS, INC. and INSTAGRAM, LLC,

Defendants.

COMPLAINT FOR VIOLATIONS OF:

A. False Advertising Law [Bus. & Prof. Code, §§ 17500 *et seq.*];

AND

B. Unfair Competition Law [Bus. & Prof. Code, §§ 17200 *et seq.*]

EXEMPT FROM FILING FEES UNDER GOVERNMENT CODE § 6103

TABLE OF CONTENTS

I. INTRODUCTION

1. It is no accident that Meta platforms, including Facebook and Instagram, are involved in one third of Internet scams in the U.S. Every day, consumers across the world are exposed to 15 billion scam ads on Meta platforms. These ads deceive consumers, posing serious financial risks; increase costs for legitimate advertisers; and cause a wide range of harms to people and businesses worldwide. Meta assures the public, and promises its users and advertisers, that it is making every effort to protect them from scams. But behind the scenes Meta is actively participating in the creation and targeting of scam ads, snuffing out attempts to combat scam ads, and in fact *profiting* from the scam ads it claims to be trying to prevent.

2. Scam ads bring in about $7 billion of revenue for Meta each year. In fact, since 2024, Meta has charged advertisers it identifies as likely engaged in fraud ("scam advertisers") at *higher rates* than other advertisers, imposing a so-called "penalty bid" for such advertisers to participate in the process by which ads are placed. The resulting flood of competitors, many of which are scam advertisers, drives up prices for legitimate advertisers. And, because the winning bidder for a particular ad placement necessarily displaces the losers, scam ads routinely displace legitimate ads. No wonder, then, that billions of scam ads inundate Meta platforms each day.

3. Meta also supplies tools that help scammers create and develop their ads. Scam advertisers have access to Advantage+ creative: a suite of Meta-designed tools that create ads with minimal user input. Advantage+ creative uses artificial intelligence to rapidly generate alternate text and images—"like, 4,000 different versions" of an ad, as Meta CEO Mark Zuckerberg put it—with just a few clicks. Meta promotes these tools to improve ads and enhance user engagement, but they can and do also produce misleading ad content: A *Reuters* reporter trying out these tools declined to post the variants of his ad that they produced, determining that the AI-generated ads were materially more misleading than original drafts and therefore violated *Reuters*' policy against making false statements.

4. Meta further facilitates scams by promoting supposedly vetted Business Partners that Meta characterizes as "trusted experts." As of at least December 2025, to post their ads, scam advertisers could enlist the help of over 2,000 Business Partners. Some Business Partners have

helped scammers perpetuate their scams by, for example, helping them rent out "clean" Meta accounts that the scam advertisers can burn through: Once they have used a clean account to the point of being flagged or even banned, they can simply rent another account. Although Meta claims to have "vetted" its Business Partners for "technical and service excellence" in various specialties, revenue appears to be Meta's most valued metric of excellence. For example, to qualify for the membership tier of "Badged Partner" in the "Adtech" specialty, a Business Partner needs to show at least $2 million of spending in the last 180 days across its ad accounts.

5. Meta has a serious problem with scam ads. Yet, despite their ubiquity and their risks to both consumers and legitimate advertisers, Meta has deemed scam ads a "low severity" problem that just impacts "user experience." The company's internal documents from 2022 acknowledge a "lack of investment" in automated scam detection.

6. In fact, Meta has *divested* from anti-scam efforts that have been proven to be successful. In 2023, Meta laid off the *entire team* investigating scam ads that were hurting legitimate brands. In 2024, Meta disbanded a China-focused anti-scam team after the team's successful efforts cut too deeply into Meta's profits, leading to a resurgence in scam ads from China.

7. While Meta has reduced the number of its employees working on anti-scam measures, its platforms have retained even the most egregious scammers. According to a 2025 *Reuters* investigation, more than six months after a Meta employee's profile of the "Scammiest Scammers"—that week's most-complained-about advertisers—two such scammers remained on Meta platforms.

8. In parallel with abandoning the anti-scam efforts above, Meta has declined to implement universal advertiser verification—a proven, cost-effective identity-check process that Google has successfully been using since 2020. Internal documents reflect Meta's concern that universally verifying advertisers would cannibalize revenue from its existing practice: charging advertisers up to $349.99 per month for the option to display a "Verified for Business" badge.

9. As Meta has divested itself from anti-scam efforts, it has continued to rake in profits from scam advertisers. Meta lumps its $7 billion of annual revenue from scam ads into a category

it calls "violating revenue" and treats potential penalties from regulators as no more than a cost of doing business. In 2024, when Meta "anticipate[d] penalties of up to $1 billion," it concluded that "those fines would be much smaller than Meta's revenue from scam ads."

10. Consistent with this approach, Meta sets "revenue guardrails" through which it seeks to protect the profits it makes from scam advertisements. Internally, Meta restricts the team responsible for vetting questionable advertisers from taking actions to combat those advertisers if such actions could cost the company more than 0.15% of its total revenue. In other words, Meta's policy is to intentionally limit its internal controls to ensure that "violating revenue" continues to flow. Externally, Meta takes, to borrow its own words, a "reactive only" stance on scam enforcement by focusing its anti-scam efforts on near-term regulatory action. "Keep engaging with regulator on extension," advises one internal document, suggesting that Meta is aiming to drag out its non-compliance for as long as possible.

11. Even so, Meta falsely assures the public that it is "constantly" and "aggressively" fighting scammers. And Meta falsely promises—in its contracts with consumers and legitimate advertisers—that it doesn't allow scams and other deceptive content on its platforms.

12. For example, even though Meta tracks "violating revenue" and prohibits anti-scam staff from cutting too much into its bottom line, a Meta spokesman said this in November 2025: "We *aggressively fight fraud and scams* because people on our platforms don't want this content, legitimate advertisers don't want it *and we don't want it either*." And Meta continues to characterize scam prevention as its "*top* priority."

13. Even after Meta had laid off one anti-scam team in 2023, disbanded another in 2024, and refused to implement universal advertiser verification, the company posted in December 2025 that "we're *expanding* our advertiser verification efforts."

14. Even as Meta provides ad-creation tools that rapidly generate deceptive text and images and has vouched for Business Partners that loan "clean" accounts to scam advertisers, Meta makes this statement on its online "Scam Prevention Hub": "We are *constantly working to improve ways of detecting and blocking accounts* that purposefully deceive, misrepresent, defraud and exploit people for money or property."

15. And even as reports of scams languish unaddressed—in the case of some "Scammiest Scammers," for over six months at a time—Meta's online "Transparency Center" maintains this spurious claim: If posted content violates Meta's standards, "Meta *will* remove it." What's more, Meta claims, "We remove content that goes against our policies *as soon as we become aware of it*."

16. Meta's misrepresentations to consumers and legitimate advertisers, as well as its material contributions to the creation of scam ads, have violated and continue to violate the False Advertising Law (Bus. & Prof. Code, §§ 17500 *et seq.*) and the Unfair Competition Law (Bus. & Prof. Code, §§ 17200 *et seq.*). To redress and punish Meta's previous and current violations of law—and to protect consumers and legitimate advertisers throughout the State—the People seek (1) an order declaring unlawful and enjoining Meta's false and deceptive advertising and its unfair, unlawful, and deceptive business practices; (2) an order requiring Meta to pay any restitution authorized by law; and (3) a judgment requiring Meta to pay civil penalties and any fees or costs permitted by law.

II. JURISDICTION AND VENUE

17. This Court has original jurisdiction over this action pursuant to article VI, section 10 of the California Constitution.

18. This Court has personal jurisdiction over Defendants pursuant to Code of Civil Procedure section 410.10 because Defendants' principal place of business is in California, and Defendants regularly engage in business in California and, specifically, in Santa Clara County.

19. Venue is proper in this Court pursuant to section 393(a) of the Code of Civil Procedure because wrongful acts and violations of law that occurred in Santa Clara County form part of the cause upon which the People seek recovery of penalties imposed by statute.

III. PARTIES

A. Plaintiff

20. Plaintiff the People of the State of California (the "People" or "Plaintiff"), acting by and through County of Santa Clara County Counsel Tony LoPresti, brings this suit pursuant to sections 17200 *et seq.* and 17500 *et seq.* of the California Business and Professions Code.

B. Defendants

21. Defendant Meta Platforms, Inc., formerly known as Facebook, Inc., operates the world's largest group of social networking sites. These social networking platforms include Facebook and Instagram, which are accessible via a webpage and via mobile applications. Meta is incorporated under the laws of the State of Delaware, with its principal place of business in Menlo Park, California. Meta's actions complained of herein took place, primarily or in their entirety, within the State of California.

22. Defendant Instagram, LLC is a wholly owned subsidiary of Meta Platforms, Inc. Instagram is organized as a Limited Liability Company in Delaware with its headquarters in Menlo Park, California. Instagram, LLC operates the Instagram social media platform.

23. This complaint refers to Defendants collectively as "Meta" or the "Company."

IV. FACTUAL ALLEGATIONS

24. The allegations herein are based on the investigation of the undersigned counsel and review of publicly available documents.

A. Meta Knows Scam Ads Are Rampant on Its Platforms but Chooses Profits Over Proven Scam-Prevention Measures

1. Meta's Platforms Are the Venue of Choice for an Epidemic of Online Advertising Scams

25. Online scams are an increasingly significant threat to consumers in California, the United States, and worldwide. According to the FBI, online crime caused a record $16.6 billion in losses for Americans in 2024. Of those losses, 83 percent—or approximately $13.8 billion—resulted from Internet-enabled scams, ranging from complex investment scams to simple non-delivery fraud. California residents reported the most losses—over $2.5 billion—and California ranked number one out of all states in the number of complaints submitted to the FBI's Internet Crime Complaint Center.

26. Online scams can hit vulnerable populations particularly hard. Across the country, victims over the age of 60 reported losing over four times as much as the nationwide average. And California again ranked number one out of all states in the number of complaints received by residents 60 and over, who suffered over $800 million in losses. In addition, according to the Pew

Research Center, "Black, Hispanic and Asian adults are more likely than White adults to have had multiple forms of these frauds happen to them," and "those with lower incomes (26%) are more likely than those in upper-income households (15%) to say they have lost money" to an online scam or attack.

27. Meta is a major vehicle for—and contributor to—this deluge of online scams that are deceiving ordinary consumers and disadvantaging legitimate advertisers in California and across the globe.

28. Meta owns and operates several of the world's largest social media platforms, including Facebook, Instagram, and WhatsApp. These platforms have billions of users who access the platforms multiple times daily. Users don't have to pay to access the platforms; instead, they agree that Meta can show them "personalized" ads that businesses and individuals pay Meta to curate and deliver based on users' personal data.

29. Indeed, in discussing Meta's business model, it is commonly said that "the users are the product." That is, by attracting a vast audience about whom Meta has amassed detailed data concerning their characteristics and interests, Meta has created the preeminent platforms for selling advertising.

30. Such advertisements generate the overwhelming majority of Meta's revenues. For example, Meta's 2025 Form 10-K submission to the U.S. Securities and Exchange Commission reports about $201 billion of total revenue for 2025, of which over $196 billion—or nearly 98 percent—is advertising revenue. And, while Meta doesn't disclose the total number of ads it shows its 3.56 billion "daily active people," it reported in April 2026 that total "ad impressions"—that is, displays of ads to individual users—were up by 19 percent year-over-year.

31. This massive advertising enterprise has become a major venue for online scammers. According to a *Reuters* report, an internal Meta presentation in May 2025 estimated that Meta was involved in *one third* of all successful Internet scams in the U.S. *Reuters* further reported that Meta "internally estimates that its platforms show users 15 billion scam ads a day," resulting in an estimated $7 billion in revenue for Meta annually.

32. The scam ads on Meta platforms are pervasive and widely varied, ranging from complex financial scams to deceptive ads touting products that will never be delivered.

33. For example, an internal Meta document from 2022, as disclosed by *Reuters*' reporting, reflects that "Meta discovered a six-figure network of accounts pretending to be members of the U.S. military deployed in war zones" that "were sending millions of messages a week trying to charm Facebook users into losing their money." Along with scams that used the identities of members of the military, Meta knew about "a torrent of fake accounts pretending to be celebrities or represent major consumer brands [that] were bamboozling users worldwide."

34. And the scams are not limited to impersonations of celebrities and military personnel. Indeed, there are numerous examples of scammers impersonating businesses large and small on Meta's platforms. For example, investment advisory firm Capital Wealth Planning, LLC, based in Florida, was forced to issue a press release in June 2024 to warn the public that scammers impersonating that firm were soliciting investors on Meta's WhatsApp platform. The firm notified the Company, which did not rectify the situation; in December 2024, the Washington State Department of Financial Institutions issued a public warning about these scams. In February 2025, the same Washington agency issued another public warning that scammers on WhatsApp were impersonating three other investment firms.

35. These are not isolated examples of scams. In June 2025, a bipartisan coalition of 42 state attorneys general sent a letter to Meta requesting "immediate action to address widespread investment scams on Facebook and WhatsApp." And, in April 2026, multiple attorneys general issued alerts warning residents about the prevalence of fraudulent investment scams on Meta platforms.

36. In May 2025, the *Wall Street Journal* described Meta as "a cornerstone of the internet fraud economy, according to regulators, banks and internal documents" it reviewed. According to that report, ads on Meta platforms "accounted for nearly half of all reported scams on Zelle for JPMorgan Chase between the summers of 2023 and 2024," and other banks offering Zelle report similar experiences. Similarly, in January 2025, the Managing Director of the UK Payment Systems Regulator reported that "Meta platforms (Facebook, Instagram, WhatsApp)

feature as the top three platforms being targeted by fraudsters to carry out the most common type of [authorized push payment] scam – purchase scams."

37. Other sources similarly track the multitude of scammers on Meta platforms that have not been blocked by the Company. For example, Gary Warner, director of intelligence at the cybersecurity firm DarkTower, tracks thousands of Facebook groups dedicated to luring people into cryptocurrency investment scams as well as groups that purport to be community dating resources where scammers are lurking, as reported by *Wired*. Such groups are often engaged in so-called "pig butchering" or "confidence" scams, through which a target is first allowed to profit from purportedly legitimate solicitations in order to "fatten" them or win their trust before they are scammed for a large amount. The amounts ultimately taken from the victims of such scams are often significant, reaching six or seven figures.[1]

38. The scam ads Meta permits on its platform also include ads for dangerous health products that Meta expressly represents are prohibited by its advertising guidelines. For example, an April 2026 report published by a leading not-for-profit Internet research organization, Reset Tech, documented the proliferation of ads purporting to sell "miracle cures" for incurable diseases such as diabetes on Facebook. The report, which collected over 350,000 "clickbait cure" ads on Facebook based on an extensive collection and analysis of hundreds of thousands of such advertisements shown on the platform between 2020 and 2026, detailed the extensive proliferation of such ads and Meta's knowledge of them.

[1] The impact on victims of such scams can be financially and emotionally debilitating. For example, ABC7 News reported on two retirees in California who fell prey to scams perpetrated on Meta platforms and lost $500,000 and $1 million, respectively, which both scam victims described as their life savings. Both scams began on Facebook and moved to WhatsApp. In the case of an elderly widow in San José, both ABC7 News and Yahoo! Finance report that scammers "took nearly $1 million of her money." As is common in "pig-butchering" scams, the scammer began with a $15,000 "test" trade on a crypto platform that appeared to generate substantial profits for the widow. She was then told to invest $490,000 from her IRA, and later to add still more money to unlock funds when the account was "frozen." The victim ultimately drew down retirement accounts and took out a second mortgage, sending the scammer nearly $1 million in total. According to ABC7 News, the scam emptied her retirement savings and put her home at risk, leaving her with "almost nothing to live on."

39. In short, Meta's platforms are the preferred hunting grounds for online scammers of all stripes, including scam advertisers.

2. Meta Tracks Scam Ads and the Billions in Revenue They Generate

40. Meta is well aware of the volume of scam ads on its platforms because it tracks these ads closely—along with the revenues they generate.

41. As described above, Meta itself has determined that its platforms show users some 15 billion scam ads each day. What's more, Meta has determined that its platforms are uniquely hospitable to scam ads: In April 2025, according to a *Reuters* report, Meta reviewed discussions among online scammer communities and internally concluded that "[i]t is easier to advertise scams on Meta platforms than Google." In fact, by Meta's own account, new legitimate advertisers on its platforms are outnumbered by new scam advertisers: An article in *The Wall Street Journal* reports that "[a]n internal analysis from 2022 . . . found that 70% of newly active advertisers on the platform[s] are promoting scams, illicit goods or 'low quality' products."

42. Both Meta's employees and Meta's leaders understand the ubiquity of scam ads on Meta platforms. Meta platforms are so rife with scam advertisers that Meta staff have produced an internal report of the "Scammiest Scammers"—a profile of each week's most-complained-about advertisers. And, on information and belief, Meta's executive leadership is regularly apprised of this scam-ad epidemic through Meta's periodic "Long-Range Plan" document. Shared exclusively with Meta CEO Mark Zuckerberg and a small cadre of senior executives and Board members, this Long-Range Plan sets forth the percentage of ads identified as illicit that have been shown to consumers, as well as the revenues generated by such ads.

43. Meta tracks the revenue derived from policy-violating ads—including the premiums charged by Meta for showing users ads it has identified as fraudulent or likely to be fraudulent—and labels this funding stream "violating revenue." A 2024 internal document reviewed by *Reuters* reflects Meta's estimate that scam ads annually generate about $7 billion in "violating revenue."

44. Meta's incentive to preserve its "violating revenue" steers its approach to scam prevention. A 2025 internal document reviewed by *Reuters* highlights Meta's "concern[] that abrupt reductions of scam advertising revenue could affect its business projections."

3. Meta Has Restricted, Rejected, and Dismantled Proven Scam-Prevention Strategies to Preserve Revenues

45. The limiting principle on Meta's scam-prevention efforts is simple: Protect the Company's bottom line. Consistent with this principle, an internal document from 2022 acknowledges Meta's "lack of investment" in building scam-detection tools. Instead, Meta has actively restricted, rejected, and dismantled proven strategies to combat scam ads.

46. For example, Meta has set strict "revenue guardrails" on the Company's scam-prevention efforts. According to *Reuters*' review of internal Meta documents, in the first half of 2025, the team responsible for vetting questionable advertisers was not allowed to take actions that could cost Meta more than 0.15% of the Company's total revenue—or about $135 million of the $90 *billion* Meta generated in that period. "Let's be cautious," advised the manager overseeing that scam-prevention team. "We have specific revenue guardrails."

47. These "revenue guardrails" have stymied scam-prevention efforts. For instance, *Reuters*' review of a May 2025 internal Meta document discusses how Meta identified 800 Chinese advertising accounts that, in just one month, had generated $28 million in "violating revenue." More than 75% of that spending came from accounts enjoying Meta's "Business Partner" protections (described in more detail below). When a staffer asked colleagues if Meta intended to punish the Chinese advertising partners who controlled the accounts, they were told no on the ground that "the revenue impact is too high." Although Meta did shut down a handful of these accounts that human reviews had found to be overwhelmingly running banned ads, it did so only after concluding that the accounts were responsible for just $2.8 million of the policy-violating ads. Meta staff further noted that the scammers could soon return to Meta platforms through other accounts, and that it was therefore "likely" that even that fraction of lost "revenue will return."

48. In addition to setting "revenue guardrails" on its anti-scam work, Meta treats potential penalties from regulators as no more than a cost of doing business. Internal Meta

documents reflect that Meta balances the cost of scam prevention—including regulatory fines likely to be imposed for failing to implement adequate scam-prevention measures—against the advertising revenue that Meta would lose if scam-prevention measures or regulatory compliance reduced the number of scam ads on Meta platforms. For example, according to *Reuters*' review of an internal Meta document from 2024, Meta weighed the $1 billion it anticipated in annual penalties against the $3.5 billion it would earn every six months from scam ads; "those fines," Meta concluded, "would be much smaller than Meta's revenue from scam ads." Accordingly, "[r]ather than voluntarily agreeing to do more to vet advertisers, the same document states, the company's leadership decided to act only in response to impending regulatory action."

49. In keeping with this decision, Meta tailors its scam-prevention efforts not to protect the public, but to head off immediate actions from regulators. In October 2024, Meta executives proposed to CEO Mark Zuckerberg a "moderate" approach to scam enforcement by focusing on countries where they feared "near-term regulatory action," according to a *Reuters*-reviewed internal document. *Reuters* further reported that this "moderate" approach defined scam-prevention goals in terms of total revenue:

> Meta executives in charge of enforcing the integrity of the company's platforms settled on trying to reduce the percentage of revenue attributable to scams, illegal gambling and prohibited goods from an estimated 10.1% in 2024 to 7.3% by the end of 2025. By the end of 2026, Meta aims to further cut that figure to 6%, and then to 5.8% in 2027.

By using these metrics to evaluate scam-prevention efforts, Meta could "succeed" simply by increasing its overall revenue—and without reducing the number of scam ads.

50. Meta has also developed strategies to mislead and stall regulators. For instance, *Reuters* reported—based on a review of internal Meta documents—that Meta "sought to make problematic ads less 'discoverable' for Japanese regulators" in 2024. Specifically, after determining that regulators were searching Meta's "Ad Library" for examples of problematic ads, Meta staff "identified the top keywords and celebrity names that Japanese Ad Library users employed to find the fraud ads," then "ran identical searches repeatedly, deleting ads that appeared fraudulent from the library and Meta's platforms." While that process did result in the removal of some problematic ads, it also had the misleading effect of "mak[ing] the search results that Meta

believed regulators were viewing appear cleaner than they otherwise would have." Meta later included this "search-result cleanup" strategy in its "general global playbook" to evade regulatory scrutiny worldwide. That "playbook" also includes instructions for delaying regulators, like "[k]eep engaging with regulator on extension."

51. Meanwhile, Meta has declined to implement universal advertiser verification—a proven, cost-effective process that would require Meta to verify the identities of all advertisers on its platforms. Google implemented universal advertiser verification in 2020 and, within five years, was verifying 90 percent of advertisers on its platforms; by contrast, in 2024, only 55 percent of Meta's ad revenue came from verified advertisers. A *Reuters* report explains that, instead of implementing universal verification, Meta has adopted what it calls a "reactive only" stance, under which it will implement universal verification "only if lawmakers mandate it"—and will otherwise continue to implement its playbook to dodge and hinder regulatory scrutiny.

52. Rejecting universal advertiser verification marks just another way in which Meta has prioritized its bottom line over scam prevention. According to a *Reuters* report, Meta calculated that universal advertiser verification would cost roughly $2 billion in direct expenses to implement on a global level, and it could be implemented in any of the countries where Meta operates in less than six weeks. Meta also determined "that unverified advertisers are disproportionately responsible for harm on Meta's platforms" and that implementing universal verification would "reduce scam activity." But the Company estimated that universal advertiser verification would eliminate almost 5 percent of total advertising revenues. Meta thus decided against implementing universal advertiser verification. Beyond the risk of lost advertising revenue from scammers, Meta was concerned that implementing free universal advertiser verification would cannibalize revenues from its "Verified for Business" verification product, through which Meta charges advertisers up to $349.99 each month for the right to display a badge confirming that Meta has authenticated the account.

53. Reporting by *The Wall Street Journal* in 2025 confirms that Meta has deprioritized scam-prevention efforts, including advertiser verification, to avoid losing revenue:

> Documents reviewed by the Journal show that Meta has deprioritized scam enforcement in recent years, emphasizing the avoidance of erroneous ad takedowns

> over safety concerns. The company has also been cutting costs and shifting resources to other issues in the reshuffling.
>
> The company abandoned plans for advertiser verification requirements similar to what it mandates for political ads, people familiar with the matter say, on the grounds that it worried about losing revenue from marketers unwilling or unable to pass identity checks.

54. Worse yet, Meta has rolled back effective scam-prevention efforts by laying off or disbanding entire anti-scam teams.

55. For example, in 2023, Meta laid off the entire team investigating complaints raised by advertisers regarding scams that impacted legitimate brands. Meta's investment in and focus on developing AI and virtual-reality offerings apparently hampered the efforts of the remaining scam-prevention staff, who—according to a *Reuters* report—were "ordered to restrict their use of Meta's computing resources" and "merely to 'keep the lights on.'"

56. Similarly, in late 2024, Meta disbanded an entire team that was focused on preventing scams originating in China.

57. In early 2024, Meta had identified scammers in China as a particularly significant source of scams on Meta platforms. According to an internal 2024 presentation reviewed by *Reuters*, "Meta believed China was the country of origin of roughly a quarter of all ads for scams and banned products on Meta's platforms worldwide." Meta consequently designated China the top "Scam Exporting Nation." Meta knew that Chinese "scam exports" on its platforms targeted many consumers outside of China, including in California and the rest of the United States. And Meta knew that these scam ads were lucrative: Internal Meta documents reflect Meta's determination that more than $3 billion in ad revenue—about 19 percent of the Company's annual ad sales to Chinese companies—was generated by ads for scams and other prohibited content in 2024.

58. In response to the spread of Chinese scam ads, Meta created a special team to focus on fraud originating in China. By the second half of 2024, that team had reduced problematic ads from Chinese businesses to roughly 9 percent of the Company's China ad revenue.

59. This successful effort eliminated over $1 billion in Meta's revenue. Thereafter, documents described by *Reuters* indicate that the team was suspended and then terminated at Meta

CEO Mark Zuckerberg's behest. Specifically, a 2024 document states, "As a result of Integrity Strategy pivot and follow-up from Zuck," the special team was "asked to pause" its scam-prevention efforts. Internal documents further reflect that "after Zuckerberg's input . . . Meta disbanded its China-focused anti-scam team. It also lifted a freeze it had introduced on granting new Chinese ad agencies access to its platforms. One document shows that Meta *shelved yet other anti-scam measures* that internal tests had indicated would be effective." By early 2025, Meta appears to have abandoned efforts to further reduce Chinese frauds on its platforms. An internal February 2025 document described by *Reuters* reveals that Meta determined to simply accept the higher level of fraud emanating from China and "maintain the % of global harm" coming from China rather than trying to reduce that fraud, as it had publicly stated it was committed to doing. By mid-2025, scam ads had "climbed back to about 16%" of the ad revenue the Company generated in China.

60. Meta's treatment of Chinese scam advertisers led Propellerfish, a consultant retained by Meta, to warn Meta in 2024 that "'Meta's own behaviour and policies' were fostering systemic corruption in the Chinese market for ads targeting users in other countries," as *Reuters*' review of Meta's internal documents reflects. Propellerfish concluded that Meta was "more tolerant of illicit practices in China" than other major online platforms were, with scammers viewing Facebook's enforcement efforts "as inconsistent" compared to TikTok's "stricter" protocols and the identity checks required by Google.

61. In sum, for Meta, scam prevention is ancillary to revenue protection. When scam-prevention strategies threaten revenue, Meta is not afraid to purge them.

4. Instead of Preventing Scams, Meta Uses Its Ad Auction System to Profit From and Promote Them

62. As recent reporting by *Reuters* makes clear, "Meta is earning a fortune on a deluge of fraudulent ads." The Company not only identifies scam ads that it nonetheless runs on its platforms, but, according to *Reuters*, "its responses to suspected rogue marketers" also include "charging them a premium for ads."

63. Advertisers must pay to compete in the online auction process by which ads are placed on Meta platforms.

64. In 2024, Meta began charging extra to run ads that it had already determined were likely scams. Based on its review of internal Meta documents created between 2021 and 2025, *Reuters* reported the following about this new surcharge:

> A cache of previously unreported documents reviewed by *Reuters* also shows that the social-media giant for at least three years failed to identify and stop an avalanche of ads that exposed Facebook, Instagram and WhatsApp's billions of users to fraudulent e-commerce and investment schemes, illegal online casinos, and the sale of banned medical products. . . . Much of the fraud came from marketers acting suspiciously enough to be flagged by Meta's internal warning systems. **But the company only bans advertisers if its automated systems predict the marketers are at least 95% certain to be committing fraud, the documents show. If the company is less certain – but still believes the advertiser is a likely scammer – Meta charges higher ad rates as a penalty, according to the documents.** . . . Before the bidding, the company's automated systems calculate the odds that an advertiser is engaged in fraud. Under Meta's new policy, likely scammers who fall below Meta's threshold for removal would have to pay more to win an auction.

(Emphasis added.) On information and belief, internal Meta documents further indicate that Meta can adjust the number of illicit ads that are shown to consumers—for example, by raising the 95-percent threshold—and has the ability to do so in order to smooth earnings or hit specific revenue targets.

65. Meta internally refers to the premium charged to run scam ads as "penalty bids." While the Company has tried to spin this policy as an effort to reduce scam ads, that claim is belied by the fact that ads subject to "penalty bids" have already been identified by Meta as likely scams even before those advertisers bid in the ad auction. To prevent fraud, Meta need only reject those scam ads. Instead, Meta runs ads it has deemed likely to be scams. By charging an extra "penalty bid" to run such ads, Meta is not combating scams but facilitating, promoting, and profiting from them.

66. Take, for example, Meta's treatment of Beijing Tengze Technology Co. Ltd. According to a *Reuters* report, in 2024, Meta determined that over 50 percent of ads by Beijing Tengze violated Meta's "rules against deceptive practices." At that time, Beijing Tengze was one of Meta's "top 200," a designation shared by major corporations such as American Express and BMW. Rather than block Beijing Tengze from placing fraudulent ads, Meta started charging

Beijing Tengze a premium to push its scam ads on consumers—effectively taking a cut of Beijing Tengze's proceeds from scamming consumers on Meta platforms. Consistent with Meta's refusal to take even basic steps to verify its major advertising customers, *Reuters*' investigation determined that the purported address for Beijing Tengze—one of Meta's top advertisers worldwide—did not even exist. The majority owner of Beijing Tengze controlled another company that also advertised on Facebook and Instagram, also lacked a valid address, and stated in its job postings for social media advertising that it would prioritize candidates with experience distributing black-market goods in Europe and the United States.

67. Another aspect of Meta's ad auction process further facilitates and promotes scam ads: the assignment of a "quality" value. As has been widely reported, Meta's complex auction process is not based simply on an advertiser's financial bid to run ads. Rather, Meta's process incorporates what it has referred to as a "quality" component of the auction bid. That component, which is determined and applied by Meta, reflects factors such as the relevance of the ad to the intended audience and how well the ad flows alongside user-generated content. For example, if an advertiser bids $2 to place an ad and Meta assigns that advertisement a quality value of $2, the advertiser's total bid would be $4, and that bid might displace a competing bid by an advertiser that offered $3 but had a quality component of only $0.50. Meta's explanation for this system is that it encourages and rewards high-quality, relevant ads that will enhance the experience of Meta users and increase user interaction with Meta platforms.

68. However, because scam advertisers are permitted to compete with legitimate advertisers, the inclusion of a "quality" component ultimately increases Meta's scam-ad revenue, the likelihood that scam ads reach consumers on Meta platforms, or both. While Meta's process for determining the "quality" component of a bid is not transparent (and has been described by *Wired* as a "black box"), only two possibilities exist: Either (1) Meta is assigning scam ads zero or negative quality value, reflecting that scam ads lack relevance, good flow, or other features that would enhance the experience of Meta users, or (2) Meta is rewarding scam ads with a positive quality value. If Meta assigns scam ads zero or negative quality value, Meta is effectively determining that they are scams but choosing nonetheless to run those ads if the scammers bid

higher prices (e.g., to outbid a legitimate ad assigned a quality value of $3, a scammer whose ad has $0 quality value must increase the financial component of their bid by more than $3). This acceptance of scam advertisers' bids, of course, boosts Meta's profits. Conversely, if Meta instead assigns scam ads positive quality value, Meta is increasing scammers' total bids and thereby raising the likelihood that scam ads will be shown to consumers. Whether the quality value Meta assigns to a particular scam ad is zero, negative, or positive, the net impact across Meta platforms of permitting millions of scam advertisers to participate in the auction process is a significant increase in Meta's advertising revenues.

69. By design, each aspect of Meta's ad auction process plumps its bottom line—all the more when more advertisers, especially scam advertisers, participate. By bidding in Meta's ad auctions, scam advertisers drive up the financial bids placed by legitimate advertisers and therefore the price of placing legitimate ads. In addition, however Meta treats the quality component of a scam advertiser's bid, that decision ultimately extracts higher financial bids from scam advertisers, requires legitimate advertisers to make higher financial bids than they otherwise would to remain competitive against scammers, or both. Through its ad auction process, Meta thus facilitates and promotes scam ads, all while legitimate advertisers edged out by scam advertisers—and later consumers exposed to scam ads—pay the price.

5. Meta Fails to Respond to Scams Reported by Users and Government Regulators or Identified by Its Own Staff

70. On top of snuffing out scam-prevention measures, letting scam advertisers bid for ad placement, and thereby flooding its platforms with scam ads, Meta also fails to remove ads flagged by users and even its own staff.

71. Despite their ubiquity and risks to both consumers and legitimate advertisers, Meta deems scam ads a "low severity" problem that merely results in a poor "user experience," according to *Reuters*' review of Meta's internal documents. Those same documents reportedly confirm both Meta's "lack of investment" in scam detection, as mentioned above, and the Company's direction to staff to narrowly focus on "fraudsters masquerading as celebrities and

usurping major brands" because those "impersonation scams" risk upsetting public figures and might impact advertising revenue.

72. Not coincidentally, then, Meta roundly fails to address scams reported by its users. A 2023 internal Meta document reviewed by *Reuters* indicates that most scam reports submitted by users of Facebook and Instagram go unresolved. While users that year filed roughly 100,000 valid scam reports every week, the Company improperly rejected—or simply ignored—96 percent of such reports.

73. Meta users of all kinds have reported scams to no avail. For example, a recruiter for the Royal Canadian Air Force relayed to *Reuters* that she had filed multiple reports with Meta after her Facebook account was hacked and scammers began using an image of her to perpetrate a scam. Meta took no action in response to her reports, and at least five military colleagues of hers were ultimately defrauded of thousands of dollars because they trusted that they were dealing with someone they knew, rather than scammers.

74. Meta has also ignored scam reports from law enforcement. A recent *Reuters* report provides a list of 146 examples of scams targeting Meta users in Singapore that Singapore police provided to Meta. The Company determined that, while about a quarter of the ads violated Meta's express policies, the remainder "violate the spirit of the policy, but not the letter," according to an internal presentation. The scams that Meta concluded did not violate its fraud policies, and which Meta did not address, included deceptive ads offering 80-percent discounts on a designer fashion brand, fake concert tickets, and ads for jobs posted by scammers impersonating major corporations.

75. This determination—that a scam ad can "violate the spirit of the policy, but not the letter"—highlights that Meta controls the definition of "fraud" on its platforms. Meta can therefore manipulate its purported success in combating fraud—and misstate its commitment to doing so—by defining common scams as being non-fraudulent. The *Reuters* report cites another such example reflected in internal Meta documents, which detail a case of $250,000 in "scam crypto ads" purportedly posted by the Prime Minister of Canada. Meta's conclusion in that case was emphatic: "Current policies would not flag this account!"

76. And Meta users are not alone in having their concerns overlooked; Meta also refuses to promptly remove from its platforms even those scammers that the Company's systems and employees have identified as violating its policies. According to a 2025 *Reuters* investigation, more than six months after a Meta employee's profile of the "Scammiest Scammers," two such scammers remained active on Meta platforms.

77. A 2024 internal Meta document reviewed by *The Wall Street Journal* reveals that Meta would not remove certain scam advertisers until they had accrued "between eight and 32 automated 'strikes' for financial fraud," or "between four and 16 strikes" where Meta employees "personally escalate the problem." Meta employees interviewed by *The Wall Street Journal* have said that "Meta is reluctant to add impediments for ad-buying clients who drove a 22% increase in its advertising business last year to over $160 billion. Even after users demonstrate a history of scamming, Meta balks at removing them." In the same vein, internal Meta documents cited by *Reuters* reveal that scammers that generated significant advertising revenue—labeled "High Value Accounts" by Meta—could remain on Meta platforms even after being flagged for promoting scams over 500 times.

78. Further, even when Meta does respond to scam reports, it has tended to do so by taking down individual ads rather than banning the accounts that publish them. In the case of "clickbait cure" ads, this tack has enabled scammers to continue publishing deceptive ads for health products because many such ads are generated by networks of accounts that can quickly replace any removed ads. As the head of research products at Reset Tech explained to *The New York Times*, "[t]he next day and the next day, they just launch 100 new ads." While Meta represents that it prohibits ads that "[p]romote claims . . . to cure, heal, or eliminate . . . incurable diseases," Meta had failed to remove approximately ***one third*** of all such ads flagged by the Reset Tech researchers by the time their report was published in April 2026. And, for the period from 2023 to 2026, Facebook deplatformed just 5,339 out of 22,320 health-scam advertising pages for not following its advertising standards—a fact the researchers concluded "suggests systemic gaps in enforcement and lack of oversight of problematic campaigns."

79. Meta is slow to act even when it learns that ads it affirmatively verified and authorized turn out to be scams. Meta requires political advertisers to undergo a "special authorization process" that purports to verify "authenticity and legitimacy." The Tech Transparency Project ("TTP") found that Meta expressly approved 63 scam advertisers that collectively ran more than 150,000 political ads, for which they spent $49 million on Facebook and Instagram. Many of these ads used deepfake videos of President Trump, Elon Musk, Senators Bernie Sanders and Elizabeth Warren, Representative Alexandria Ocasio-Cortez, and White House Press Secretary Karoline Leavitt to sell fictitious government benefits, fake stimulus checks, and fraudulent investment products. By affirmatively approving these scam advertisers, Meta conferred on them a veneer of legitimacy. After approving them, Meta allowed these advertisers to run scam ads for days or weeks before taking any enforcement action. Even after Meta had removed individual ads for violating its "unacceptable business practices" policy (discussed below), nearly half of those advertisers (30 of 63) continued to run advertisements, with six such accounts paying Meta over $1 million each before being disabled. One advertiser, "Senior Health Daily USA," ran 59 identical versions of the same scam ad; Meta removed more than three quarters of them but continued to allow the advertiser to re-upload the same ad. TTP concluded that "Meta is allowing this activity even though it prohibits scams and says it invests in scam prevention to keep users safe."

As the foregoing examples illustrate, scam reports—whether made by Meta users, government actors, or Meta staff—are in many cases a futile enterprise. Meta systematically fails to address them in a prompt or meaningful way.

B. Meta Actively Contributes to the Creation, Optimization, and Targeting of Scam Ads

80. The proliferation of scams on Meta platforms does not result solely from Meta "looking the other way" or failing to adequately police fraud. To the contrary, Meta actively participates in, assists, and encourages the creation, placement, and targeting of scam ads. Through its AI tools, for example, Meta participates directly in the creation, editing, optimization, and targeting of scam ads in ways that vastly enhance the effectiveness of the fraud, while reducing

the costs to scammers. Meta also affirmatively facilitates scam advertising by promoting and providing special protections to supposedly "vetted" business partners that make no secret of offering services to support scam advertisers. And Meta uses its algorithms and other technology to target scam ads to vulnerable users who are most likely to engage with them. In these ways, among others, Meta contributes to and enhances the production of scams on its platforms.

1. Meta Creates, Modifies, and Optimizes Scam Ads Through Proprietary Tools, Including Artificial Intelligence

81. According to *Reuters*, Meta offers AI tools that improve scam ads. These AI tools generate text, enhance images, determine target audiences, and can create and push out ads with unprecedented efficiency. Meta knows, or reasonably should know, that these tools can aid scammers in creating and optimizing misleading ads, accelerating and expanding their distribution, and increasing consumer engagement with scams. Worse still, Meta's AI tools can even make ads *more* misleading.

82. Meta offers advertisers a host of specific tools, many of which leverage advanced artificial intelligence, to help advertisers create, refine, and improve their ads. For example, among many other AI products, Meta's "Advantage+ creative" tool helps advertisers—including scammers—create, refine, and improve their ads:

> When you turn on Advantage+ creative in Meta Ads Manager and Meta Business Suite, your images and videos are optimized to versions your audience is more likely to interact with. . . . Enhancements on images and videos may vary depending on who they are shown to and which optimization is used to improve ad performance. The media and text you upload may be adjusted to help improve ad performance while maintaining the core message of your campaign. If the branding feature is on, we'll try to use your brand preferences in some enhancements.

83. Advantage+ creative can improve ads, and make users more likely to engage in them, by adding AI-generated images, animation, backgrounds, music, and video effects, or simply by improving ad quality by adjusting brightness and contrast or touching up images. The tool will even draft and manipulate the language used in ads. Meta offers that Advantage+ creative provides both "Text generation (AI)" and "Text improvements (AI)," as follows:

> Text generation is a generative AI feature available in Meta Ads Manager, Facebook Page and Meta Business Suite. The text generation feature allows you to create diverse text variations that could help increase stronger customer resonance. The feature can generate up to 5 variations of primary text and headline, and

> generate your text variations using personas. If the branding feature is on, we'll try to use your brand preferences in some enhancements.
>
> . . .
>
> Text improvements is a generative AI feature designed to surface key information about your ad upfront and enable people to better understand your key selling points. When you toggle on this feature, keywords and phrases will be taken from your original ad copy and displayed directly or adjusted to fit better on or around your ad creative, such as text overlays, footers, prominent headlines and more.

84. Advantage+ creative and similar tools can also make ad creation more efficient. Meta provides a "bulk edit" feature so that advertisers—including scammers—can use Meta's powerful tools to enhance multiple ads simultaneously. Another Meta tool, "Dynamic ads," enables advertisers "to automatically promote your entire product catalog across Facebook, Instagram and Audience Network without having to create thousands of individual ads. Dynamic ads capture the intent signals that customers show on websites and apps to ensure the right products are connected to the right people."

85. In addition to Advantage+, Meta also offers an "Ads Manager" tool, which it describes as "an all-in-one tool for creating ads, managing when and where they'll run, and tracking how well your campaigns are performing towards your marketing goals." Meta touts that advertisers can use Ads Manager "to create ads from existing posts published on your Facebook Pages." Using that tool, advertisers—including scammers—can specify their "ad objective," including options such as "Engagement to create ads that click to message, ads that send people to an online destination, app ads and call ads" and "Leads to create ads that send people to an online destination, app ads and call ads." Ultimately, having Meta generate an ad from an existing post on platforms such as Meta and Instagram is as simple as using "the dropdown menu to select Use existing post" and then "[s]elect[ing] the post you want to use to create an ad."

86. Meta not only provides tools for advertisers to create their own ads, but will create ads itself with elements provided by the advertiser, using a tool called "dynamic creative." Meta explains: "When you use dynamic creative in Meta Ads Manager, you can upload multiple creative elements, like images and headlines, which are automatically combined to generate different ad variations for your audience."

87. Another Meta tool, the "flexible ad format," will also create ads using Meta's own data analysis to determine which ad components will appeal to which users:

> The flexible ad format is designed to help you automatically optimize your ad format to show people what we predict they're most likely to respond to based on the specific placement and audience. When you select Flexible as your ad format, you can select up to 10 images and videos in a single ad campaign, and the ad delivery system will automatically determine what media or media combination, such as single image, video or carousel, to show to people.

88. Meta has offered AI tools that generate advertising text and enhance ads since at least 2023. For example, Search Engine Land announced in October 2023 that "Meta's first generative AI-powered tools for advertisers are here" and described the Meta tools "designed to maximize productivity, personalization and performance." These included: a background-generation tool that "creates multiple backgrounds to complement the advertiser's product images"; an image-expansion tool to more efficiently "adjust creative assets" for different formats; and a text-variation tool used "to generate multiple versions of ad texts based on their original copy, and to highlight the selling points of their products/services."

89. The website for Core, a marketing communications company, discussed Meta's 2023 announcement, noting that Meta "has been pushing advertisers to test out its AI-based ad creation elements, with these features becoming more integrated into the ad setup process than ever before." Core also noted that "more than 4 million Meta advertisers are now using at least one of the tech firm's generative AI tools."

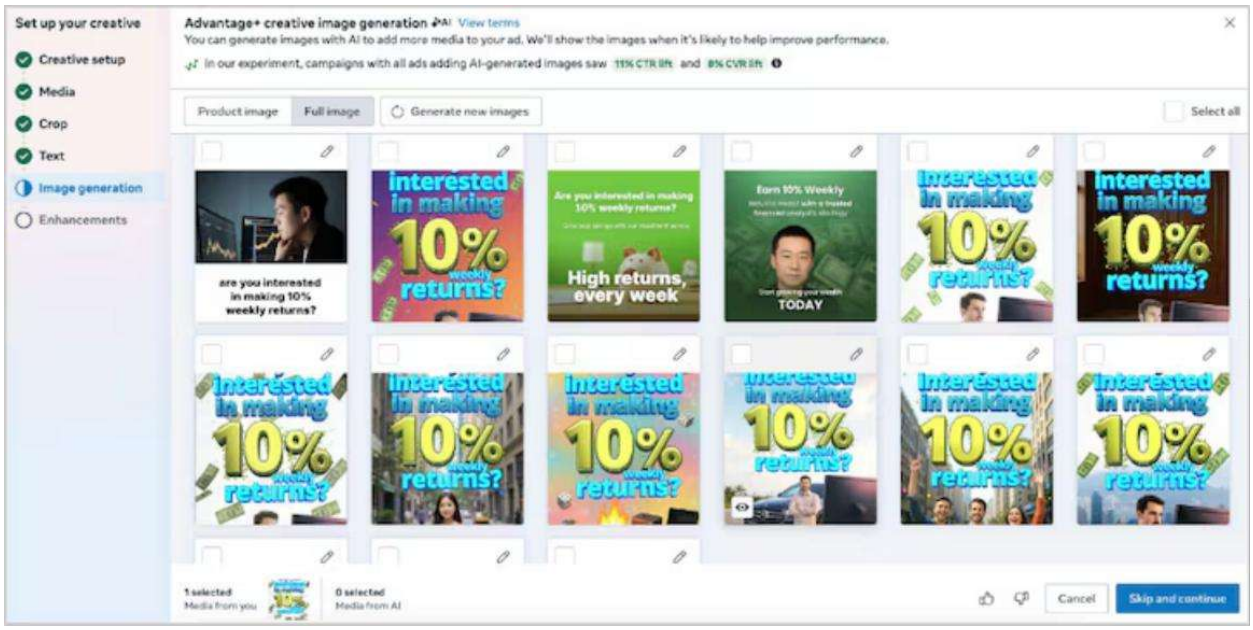
90. Indeed, the number of advertisers using Meta's tools to generate ads is massive and growing. In a December 2024 website post, Meta touted, "Even at this early stage, more than a million advertisers used our generative AI (GenAI) tools to create more than 15 million ads in a month."

91. More recently, on April 29, 2026, *The New York Times* reported on the extent to which Meta creates, optimizes, and targets ads on behalf of its advertising clients: "The emerging A.I. systems are helping companies automate their marketing. . . . The technology is also making the ads more effective, tech companies and brands say." Meta's AI tools are also more proactively steering ads to groups of users. As *The New York Times* reports, rather than advertisers identifying

target customers, Meta is now "using A.I. to recommend customers the brands should be going after."

92. As Meta knows, or reasonably should know in light of its extensive tracking of scam-ad volume on its platforms, these powerful AI tools can be used by scammers to create, improve, and increase consumer engagement with scam ads. But even worse, as a *Reuters* reporter discovered, Meta's tools can make problematic ads even *more* misleading.

93. A *Reuters* reporter tested out Meta's AI features by attempting to create a scam ad on Meta's platforms. According to the article detailing his experience, "Meta's AI systems offered to improve a *Reuters* reporter's advertisements touting investment returns that were too good to be true." That article included the below sample image of Advantage+, which states that "[y]ou can generate images with AI to add more media to your ad. We'll show the images when it's likely to help improve performance."



94. The *Reuters* reporter further detailed his experience having Advantage+ materially modify and improve his scam ads to increase user engagement:

> A feature called Advantage+ used AI to generate alternates of my ads that might be more enticing. Meta Chief Executive Mark Zuckerberg earlier this year noted how effective such tools could be. "We're gonna be able to come up with, like, 4,000 different versions of your creative and just test them and figure out which one works best," he told an audience at a San Francisco conference in May.

> In my case the system suggested 10 variants that featured new visuals, including AI-generated people of different ethnicities. It also suggested different text: "Tired of living paycheck to paycheck?" one asked. "Break the cycle and start earning a steady weekly income with our proven system."
>
> Instead of asking me to choose one, Meta suggested I authorize all of the alternates. Its platform would then test each variant, directing my money to those that performed best. I declined. My ads felt scammy already, and some of the claims featured in Meta's ads violated Reuters policy against making false statements.

95. Meta, too, knows that its AI tools may generate misleading content. In the terms governing use of its generative AI tools, Meta acknowledges that use of those tools may result in output that is "inaccurate, incomplete, misleading, offensive, and/or inappropriate" and disclaims any warranties regarding the accuracy and reliability of such outputs. Meta also purports to wash its hands of any liability associated with use of its AI-generated content—while simultaneously asserting ownership rights over the (potentially misleading or inaccurate) advertising outputs created by its generative AI products.

96. That Meta's own systems assist in creating, refining, and optimizing deceptive ads—the content of which Meta purports to own, at least in part—means that Meta itself not only gives a platform to scams and intentionally limits its efforts to prevent fraud, but *actively contributes* to the creation and development of scam ads that target its own users.

2. Meta Promotes "Vetted" Business Partners That Expressly Facilitate Fraud

97. Meta has also facilitated and encouraged scams on its platforms by promoting and providing special protections for supposedly "vetted" business partners that publicly and expressly offer services to help scammers place deceptive ads on Meta platforms.

98. As of at least December 2025, Meta was working with over 2,000 "business partners" that offered support to advertisers. Meta vouches for these partners, saying "Meta Business Partners are trusted experts who enable businesses to grow" and "Meta Business Partners are companies Meta has vetted for their technical skills and services, and their unique ability to help businesses grow." Some of these partners are known as "Badged Partners."

99. In addition to "vetting" the partners that it recommends to advertisers, Meta offers its business partners tools and resources to help them advance the ad campaigns of the advertisers

they assist. For example, Facebook's webpage describing the business partner program states: "Join Meta Business Partners and get access to time-saving tools, resources, insights and training to help your clients grow and succeed" and "Joining Meta Business Partners means access to benefits that can help you become an expert in driving client success across Meta technologies."

100. In truth, some partners "vetted" by Meta, including Badged Partners, have offered services to assist scammers in placing illicit ads. Moreover, Meta has known, or reasonably should have known, that these Business Partners assist scammers because the Business Partners openly advertise that they do so. For example, some of Meta's business partners advertise that they offer "black hat" services, "ad account rentals," and "high-limit, pre-approved accounts." Such services, and offers for "[w]hitelisted ad accounts," are means by which scammers can access "clean" Meta accounts for purposes of placing illicit ads and bypassing Meta's nominal fraud prevention mechanisms. The terms "white hat" and "black hat" are standard industry terms for services that facilitate ads to advance fraud, scams, or other prohibited content.

101. According to *Reuters*, these Business Partners "promise customers an edge – access to special ad accounts given leeway by Meta's enforcement systems. Those accounts are rented out by big Chinese advertising agencies that are the foundation of Meta's ad business in China. They enjoy special protections from the social media giant."

102. Within Meta, the China market is unique from other markets, because advertisers in China must work through a series of advertising agencies. As explained by *Reuters*:

> In most of the world, advertisers on Facebook and Instagram buy ads through a business profile that is linked to advertisers' accounts and related pages they control. But because businesses can't readily access the platforms in China, Meta pays the 11 large Chinese ad agencies – known as resellers – to enlist advertisers and run ads for them on so-called 'agency accounts.'
>
> Meta pays a roughly 10% commission to agencies for ads purchased through these accounts and grants them special protections. For instance, under a system known as 'whitelisting' or 'mistake prevention,' Meta doesn't immediately remove ads purchased via top-tier agencies when they're flagged by automated systems for breaking Meta's advertising rules, internal documents say. Such rules ban the advertising of scams, illegal goods and services, and certain other products such as sex toys.
>
> Instead, suspect ads remain active as they undergo a secondary review by a human. If Meta's staffers are busy, that might take days – or never happen at all. And in the meantime, Meta continues to show the ads.

103. Accordingly, Meta's process for selling ads in China expressly facilitates the placement of scam ads that target consumers worldwide, with Meta paying agencies to place ads that violate Meta's own policies. Meta internally documented the fact that its policies facilitated and promoted scams on Meta platforms, as in one document that observed, "Unfortunately the added time for secondary review is adequate for scammers to accomplish their objectives by gaining massive impressions." And the harm is felt globally. Indeed, as mentioned above, Meta refers to China as the top scam exporting nation, and China is the country of origin for more than a quarter of all ads that violate Meta's policies worldwide.

104. Meta's "vetted" business partners have not concealed their practices from Meta. For example, *Reuters* reports that Yinolink, one of Meta's Chinese business partners, touted on its website "80% lower chance of suspension than other regular agents," assuring scammers that Yinolink could help them evade scrutiny on Meta platforms.

105. Facebook's own webpage identifying its "vetted" business partners described one partner, Digital Pyramid LLC, with terms that expressly offered services intended for scammers:

> Digital Pyramid LLC is a High Tier Meta Partner Agency specialized in ad account rentals and high-performance advertising solutions. We provide Whitelisted ad accounts with high-trust scores, ensuring seamless campaign management and best Scaling.

106. Digital Pyramid's website touted that advertisers can "Get your hands on the best ad accounts with complete security setups" and provided pricing for "BH Advertising" – referring to "black hat" advertising services, which Digital Pyramid said are "Perfect for High Risk Advertisers."

107. Similarly, Facebook's description of its "vetted" business partner Mythic Edition / GDE Commerce included a reference to providing "Ad account Unbans," meaning an offer to assist advertisers that had been banned by Meta for running prohibited ads, such as frauds and scams. The website link for Mythic Edition directed to a Discord server rather than a traditional corporate website.

108. Orange Trail, another of Meta's "vetted" business partners as of at least December 2025, offers on its website "pre-vetted" ad accounts so that advertisers can advertise on Meta "Without Bans."

109. Other Meta business partners, such as Ronin Global and Ronin Gold, offer "[h]igh limit, pre-approved accounts," services that are valued by scammers whose ads violate Meta's policies. Indeed, the description of Ronin Global on Facebook's directory of "vetted" business partners said that Ronin Global "empowers advertisers with premium accounts."

110. The ease with which these "vetted" business partners facilitate the placement of fraudulent ads was demonstrated by a *Reuters* reporter, who used such partners to place his own scam ads. That reporter "clearly [disclosed] that I wanted to run banned cryptocurrency ads" and found that Meta's "vetted" business partners—and Meta itself—were ready, willing and able to assist him:

> I wasn't surprised to see agency accounts available on shady digital forums, where online marketers openly discuss ways to sell black-market products. It was more of a shock to see them for sale in Meta's own partner directory, a listing of companies that Meta said had been "vetted for their expertise." I was also surprised that once I found agencies happy to run my fake ads, Meta's systems offered to use artificial intelligence to improve them.

111. One such partner that *Reuters* contacted was Bluefocus Agency, whose website states "We've spent years building a robust relationship with Facebook" and yet offers a tutorial on "How to Advertise Illegal Products on Facebook."

112. Based on his personal experience, that *Reuters* reporter wrote: "Though described in the directory as 'trusted experts' with status as a Meta 'Badged Partner,' some of the agencies actively recruit businesses looking to run banned advertisements."

113. After being contacted by the *Reuters* reporter investigating Meta's business partner, Meta removed the directory identifying those partners and providing links to their websites. But the program itself remains live on the Facebook website.

114. As set forth above, Meta has curtailed scam prevention efforts in order to maximize its advertising revenues. This curtailment has extended to programs that were successful in

preventing scams by its Chinese business partners. Based on its review of internal Meta documents, *Reuters* reported that:

> In 2023, as part of an earlier effort to address fraud, Meta stopped verifying new Chinese ad agency partners because of the 'high harm' these intermediaries were causing, one document says. But Meta lifted the moratorium after its 2024 'pivot' in order to 'unlock' revenue.
>
> By late 2024, lower-tier Chinese ad agencies were once again gaining access to verified accounts on Meta's platforms. Of the annualized $240 million in advertising from newly verified resellers that year, half violated Meta's safety rules, Meta determined. 'We are seeing harm from these newly verified agencies,' the document says.

115. *Reuters* further reports that internal documents from May 2025 show Meta identified 800 Chinese advertising accounts that had generated $28 million in ads that violated Meta's rules in just one month. More than 75% of the spending came from accounts enjoying Meta's partner protections. When a staffer asked colleagues if Meta intended to punish the Chinese advertising partners that controlled the accounts, they were told no on the ground that "the revenue impact is too high." While Meta did shut down a handful of the accounts that human reviews found to be overwhelmingly running banned ads, it did so only after concluding that the accounts were responsible for just $2.8 million of the harmful ads and the scammers would likely return to Meta platforms through other accounts, so it was "likely" that even that "revenue will return."

3. Meta Steers Fraudulent Ads to the Most Vulnerable Victims

116. Meta uses algorithms and other advanced, AI-driven technology to select which advertisements are shown to which users. Those algorithms take into account the ads that a given user has previously engaged with, including by clicking on those ads. Accordingly, as Meta itself has recognized, a user who clicks on a scam ad is more likely to be shown additional scam ads because Meta itself will select those ads for that user.

117. Meta has long touted its ability to select which users will be shown which ads. For example, in 2018, CEO Mark Zuckerberg testified before U.S. Senate committees that:

> What we allow is for advertisers to tell us who they want to reach, and then we do the placement. So, if an advertiser comes to us and says, all right, I am a ski shop and I want to sell skis to women, then we might have some sense, because people shared skiing-related content, or said they were interested in that. They shared whether they are a woman, and then we can show the ads to the right people. . . .

118. As *Reuters* reported, internal Meta documents "further note that users who click on scam ads are likely to see more of them because of Meta's ad-personalization system, which tries to deliver ads based on a user's interests."

119. Among the powerful tools Meta touts to advertisers to enhance their advertising campaigns is its AI-driven "Andromeda" tool that selects which ads to show individual users. A December 2024 post on Meta's website describes the benefits Andromeda provided in targeting ads to specific users:

> AI plays an important role in Meta's advertising system by leveraging the power of machine learning (ML) to predict which ads a person will find most interesting. This helps people learn about a business or product they are interested in while helping an advertiser meet their objectives such as increasing brand awareness, acquiring new customers, and driving sales.
>
> Retrieval is the first step in our multi-stage ads recommendation system. This stage is tasked with selecting ads from tens of millions of ad candidates into a few thousand relevant ad candidates. In the following stage, larger and more sophisticated ranking models predict people and advertiser value ***to determine the final set of ads to be shown to the person***. (Emphasis added.)

120. Meta further stresses that "Andromeda improves performance of Meta ads system by delivering more personalized ads to viewers and maximizing return on ad spend for advertisers."

121. Roughly a year after the post touting Andromeda's advanced AI-driven methods of targeting ads to Meta users, a November 2025 post described an even more advanced Meta tool for directing ads to particular users, Meta's "Generative Ads Model" or "GEM," which Meta described as "The Central Brain Accelerating Ads Recommendation AI Innovation." The post provided an in-depth discussion of how GEM directed ads to the users that advertisers most want to target. Among other things, the post explains that GEM is able to "learn from a much longer history of user organic and ad interactions," and thus can "more effectively uncover patterns and relationships, resulting in a deeper and more accurate understanding of the user's purchase journey."

122. The post concluded by naming GEM "The Future of Foundation Models for Ads Recommendations," which it explained as follows: "The future of ads recommendation systems will be defined by a deeper understanding of people's preferences and intent, making every

interaction feel personal. For advertisers, this translates into one-to-one connections at scale, driving stronger engagement and outcomes."

123. These technologies learn from users' history of engagement with ads and other content, and they use that knowledge to rank and choose ads to display to individual users, with the aim of increasing "ad conversions" (e.g., purchases, sign-ups). Accordingly, Meta is more likely to show a scam related to cryptocurrency to a user who has engaged with fraudulent content related to cryptocurrency, and is more likely to show a scam for nutritional supplements to a user who has engaged with fraudulent content related to nutritional supplements.

124. The technology Meta uses to target and facilitate scams in this way has grown increasingly powerful. Reporting on Meta's use of AI tools in digital advertising, *The New York Times* wrote that "the real business breakthroughs have come from targeting" because Meta "is collecting deeper insights into users' interests, which improves the companies' ability to target ads. And it is reducing advertising costs, which frees up money for bigger campaigns." While "[i]t used to be that an advertiser would say, for example, 'I want to target women in New York between the ages of 24 and 35.' Now it's the opposite: Meta . . . [is] using A.I. to recommend customers the brands should be going after."

125. By leveraging this advanced technology to direct scam ads to the users most likely to be taken in by those ads, Meta is engaging in the scam, not acting merely as a passive publisher of advertisements, and enabling scammers to reach more people, more quickly and cheaply, who are more likely to be deceived.

C. Meta Deceives the Public and Breaks Its Promises to Prioritize Safety, Security, and Scam Prevention

1. Meta Misrepresents Its Efforts to Prevent Scams on Its Platforms

126. Meta has made, and continues to make, statements related to its efforts to combat scam advertising that are false, misleading, and likely to deceive reasonable consumers and legitimate advertisers.

127. "*Top Priority*." Meta characterizes protecting consumer safety by combating scam ads as a "top priority" that it pursues "aggressively." For example, Meta's "Scam Prevention Hub"

webpage assures the public that "[a]t Meta, your safety and security are our top priority." In its 2023, 2024, and 2025 Securities and Exchange Commission Form 10-K submissions, Meta states that it is making "significant investments in privacy, safety, security, and content and advertising review efforts" to combat "improper advertising practices." In January 2025, Mark Zuckerberg represented to the general public that although Meta would be making some changes to its content moderation practices in light of the 2024 election, Meta would "continue to focus" its systems on addressing what he called "high-severity violations" of Meta's policies, which he defined to include "fraud and scams." In November 2025, Meta spokesman Andy Stone assured members of the public: "We aggressively fight fraud and scams because people on our platforms don't want this content, legitimate advertisers don't want it and we don't want it either." And a December 2025 Meta post entitled "Scams Are Bad for Business: Our Ongoing Efforts to Fight Fraud" also described Meta's approach to scam reduction as "aggressive."

128. But behind the scenes, and contrary to its public representations, Meta prioritizes profits over safety. As explained, despite making the above assurances, Meta tracks its "violating revenue" streams and prohibits its scam prevention teams from cutting too much into its bottom line by setting "revenue guardrails" that prohibit those teams from taking actions that could cost the company more than 0.15% of its revenue. Instead of making significant investments into combating scam ads and treating them as a "high-severity" violation of Meta's policies, as it publicly vows, Meta's internal documents acknowledge a "lack of investment" in scam detection and deem scam ads a "*low* severity" problem that merely impacts "user experience." And instead of living up to its public commitment to fight scam ads through "aggressive" efforts, Meta welcomes these ads, charging scam advertisers a surcharge to post ads that Meta knows are likely to be fraudulent, misleading, or deceptive. On information and belief, Meta can even adjust the flood of scam ads it allows on its platforms in order to smooth its earnings or hit specific revenue targets.

129. *Immediacy and Reliability*. Meta publicly characterizes its approach to removing scam ads and scam advertisers from its platforms as dependable and immediate. On its Transparency Center webpage, Meta hosts "Community Standards" that "outline what is and isn't

allowed on Facebook, Instagram, Messenger and Threads." Meta states that the Community Standards "apply to everyone, all around the world, and to all types of content, including AI-generated content." The Community Standards expressly prohibit "Frauds, Scams, and Deceptive Practices." The Community Standards provide:

a. "We do not allow: Content that attempts to scam or defraud users and/or businesses."

b. "We aim to protect users and businesses from being deceived out of their money, property or personal information. We achieve this by removing content and combatting behaviors that purposefully employ deceptive means – such as wilful [sic] misrepresentation, stolen information and exaggerated claims – to either scam or defraud users and businesses, or to drive engagement."

c. "We do not allow content that is designed to deceive, mislead or overwhelm users in order to artificially increase viewership."

130. Additionally, Meta's "Unacceptable Business Practices in Advertising" policy, which it also provides to the public on its Transparency Center webpage, states: "Advertisers can't run ads that promote products, services, schemes or offers that use identified deceptive or misleading practices, including scams to take money from people or access personal information. We do this to protect people from being taken advantage of by advertisers." Meta's "Account Integrity" policy states: "We restrict or remove accounts that are harmful to the community. We have built a combination of automated and manual systems to restrict and remove accounts that are used to egregiously or persistently violate our policies across any of our products." And Meta's "Advertising Policies" state: "Our policies prohibit ads promoting products, services, schemes or offers using deceptive or misleading practices, including those meant to scam people out of money or personal information," and "[a]ds must not violate our Community Standards."

131. In the "Enforcement" section of the Transparency Center webpage, under the heading "Taking action," Meta represents: "We remove content that goes against our policies as soon as we become aware of it." Likewise, under the heading "Taking down violating content,"

Meta states: "If your content goes against the Community Standards, Meta will remove it." Under the heading "Our policies" on the Transparency Center webpage, Meta states: "Our policies define what is and isn't allowed on Meta technologies. If content goes against our policies, we take action on it." Meta even states that it goes beyond removing content that clearly violates its policies by seeking to reduce the prevalence of "problematic content" that "doesn't quite meet the standard for removal under our policies." According to Meta, "[t]his means we remove harmful content that goes against our policies [and] reduce the distribution of problematic content that doesn't violate our policies." Last, on its Scam Prevention Hub webpage, Meta states that its automated systems "often" ban scam accounts "without a recent user report. This means our automated systems are able to stop abuse even before it is reported."

132. These representations assure readers, including members of the public who use Meta's social media platforms, legitimate advertisers, and government regulators, that Meta is committed to taking proactive and swift action to detect and address scam ads. But Meta's actual approach to removing scam ads and scam advertisers from its platforms is neither dependable nor immediate. As explained above, Meta eschews proactive scam detection measures, and worse still, it allows scam ads and scam advertisers to fester on its platforms for long periods even after receiving reports of fraud from users, government actors, and its own employees. For example, in 2023, an internal Meta analysis found that Meta improperly rejected or ignored 96% of a sample of roughly 100,000 valid scam reports submitted by users. A 2024 internal Meta document reveals that Meta generally does not remove scam advertisers from its platforms until they accrue "between eight and 32 automated 'strikes'" for posting scam content. Indeed, the document shows that Meta tracks the amount of advertising revenue a scam advertiser generates, and "High Value Accounts" can remain on Meta's platforms even after being flagged over 500 times. Additionally, after police in Singapore provided Meta with a list of 146 examples of scams targeting the country's users, Meta concluded that 77 percent of the scams only violated "the spirit of the policy, but not the letter." In contravention of Meta's suggestion that it removes scam ads from its platforms even when they fall short of the formal standard for removal, deceptive ads flagged by the Singaporean police that Meta did not act on included "too good to be true" offers of 80% off a

designer fashion brand, promotions for fake concert tickets, and job ads posted by entities falsely claiming to be major tech companies. And even the most egregious scammers stay on Meta's platforms long after Meta learns of their wrongdoing: a 2025 *Reuters* investigation found that more than six months after a Meta employee profiled the "Scammiest Scammers" on Meta's platforms, two such scammers remained active.

133. *Constant Improvement*. Meta claims to be "constantly" improving the processes and technologies it uses to combat scam advertising. On its Scam Prevention Hub webpage, Meta states: "[W]e are constantly working to improve ways of detecting and blocking accounts that purposefully deceive, misrepresent, defraud and exploit people for money or property." An October 2024 Meta post states: "Scammers are relentless and continuously evolve their tactics to try to evade detection, so we're building on our existing defenses by testing new ways to protect people and make it harder for scammers to deceive others." A December 2025 Meta post states that, as part of its "ongoing work" to combat scams, "we continue to deploy a range of product updates to bolster our detection efforts. For example, we're using the latest advancements in AI to help us detect scams, and . . . we're expanding our advertiser verification efforts to verify the authenticity of the people and organizations that run ads on our platforms." "The spike in scams is playing out across the internet," the December 2025 post says. "No one likes it. Not the people who use our services. Not advertisers. And certainly not us. . . . Every day we find new ways to stop them and take them down." The post further states: "Our continued development of new product features and tools helps protect individual accounts and legitimate businesses against scams."

134. In May 2025, a Meta spokesperson told a *Wall Street Journal* reporter that the company is "working to address 'an epidemic of scams,'" and "[a]s this scam activity has become more persistent and sophisticated, so have our efforts." And Meta's 2024 and 2025 Form 10-K submissions to the Securities and Exchange Commission assert that it "maintain[s] advertising policies to protect the security and integrity of our platform and comply with global content, security, and integrity obligations" and makes "ongoing efforts to enhance enforcement against

ads and marketers which violate our advertising policies" even though such efforts "adversely affect our revenue."

135. But, as described above, Meta has actually rolled back and blocked internal efforts to advance the processes and technologies it uses to detect and combat scam advertising. For example, in 2023, Meta laid off the entire team investigating scam ads that were hurting legitimate brands. In 2024, Meta disbanded a China-focused anti-scam team, leading to a surge in scam ads from China on its platforms. Additionally, internal Meta documents show that Meta shelved multiple anti-scam measures that internal tests indicated would be effective in combating scam ads. And, despite its public pledges to "detect[] and block[]" scam ads, Meta has refused to implement universal advertiser verification—a proven, cost-effective tool that Google has been successfully using since 2020 to combat scam advertising—apparently based on concerns that adoption of the tool would cannibalize revenues, according to internal Meta documents.

136. *Coordination with Government, Law Enforcement, and Industry Peers*. Meta characterizes itself as a leader in the scam prevention space that coordinates closely with law enforcement and industry peers. For example, Meta's Director and Global Head of Security Policy and Counter-Fraud, Nathaniel Gleicher, wrote in a summer 2025 post on LinkedIn: "Thank you Stop Scams UK for convening this discussion! It's incredibly encouraging to see leaders from across the financial sector, technology sector and government coming together to discuss what we can do to tackle scams together. We are continuing to press to stop scammers on our end, and are excited to work together with our counterparts across society to increase deterrence against scammers and protections for consumers." A Stop Scams UK post further quotes Gleicher as saying: "At Meta, we are committed to creating a safe and secure online environment for all our community. . . . Scams are a society wide problem which requires industry, government and others to work together, and we will continue to expand and evolve our collaboration to stop fraudsters in their tracks."

137. In addition, a March 2026 Meta post touts Meta's participation in the Industry Accord, which it describes as a "landmark voluntary agreement" between it and other technology companies like Amazon and Google that "sets out a framework to implement best practices for

multi-sector and stakeholder collaboration on the transnational threat of scams." The post includes the following quotation from Gleicher: "Our work to combat scams focuses on strengthening defenses on our platforms to stay ahead of scammers. Just as critical to our strategy is supporting efforts that drive collective action across sectors and industries to stop scams at its source. Scammers are growing more sophisticated, and they exploit gaps between companies and platforms — which is why tackling global online fraud demands a united, collective response. We look forward to working with the other Accord signatories to enable a stronger global defense to protect people across apps and services."

138. Contrary to these representations, Meta has refused to adopt industry best practices, including universal advertiser verification, in spite of the fact that Google has been using the tool to great effect since 2020. And Meta has recognized in internal documents that "[i]t is easier to advertise scams on Meta platforms than Google." Put another way, even though Meta recognizes that scam advertisers "exploit gaps between companies," and it has seen that dynamic play out through its refusal to adopt universal advertiser verification, Meta chooses to maintain those gaps while claiming to members of the public that it is playing a leading role in closing them.

139. And, far from collaborating with law enforcement, internal Meta documents indicate the company seeks to obfuscate the extent of the "scam ad" problem and take corrective steps only when necessary to avoid near-term regulatory enforcement action. For example, internal Meta documents reveal that Meta seeks to make scam ads "less 'discoverable'" for regulators by identifying keyword searches performed by regulators and scrubbing the results to reduce the "prevalence *perception*" of scam ads. In other words, Meta takes down scam ads that regulators are most likely to find in their search results to reduce regulators' perception of the prevalence of scams on Meta's platforms, but it does not meaningfully change the *actual* prevalence of these ads—for example, by blocking the scam advertiser or otherwise stopping generation of new scam ads. Meta includes this "search-result cleanup" strategy in the "general global playbook" it uses to evade regulatory scrutiny. The same playbook includes instructions for resisting government efforts to convince Meta to adopt universal advertiser verification by, among other things, seeking delay through repeated requests for extensions.

140. Additionally, Meta has confined its attempts to address scams to steps that minimally impact its revenue: As explained above, after identifying 800 Chinese advertising accounts whose ads had violated Meta's rules, Meta shut down just a handful, and only after concluding it was "likely" that even that fraction of impacted "revenue will return," as Meta did not take any structural steps to address the underlying problem. Worse, as reported by Reset Tech, when Meta responds to scam reports, it typically does so by taking down individual ads rather than banning the accounts that publish them. In the case of misleading ads related to public health topics, this tactic has enabled scammers to immediately resume publishing those ads—"[t]he next day and the next day, they just launch 100 new ads." In sum, Meta's approach to addressing scam advertising does not align with its representation that it acts as a leader in collaborating with government actors to take down scammers. To the contrary, at the end of the day, Meta treats potential regulatory penalties as no more than the cost of doing business, stating in 2024 when it anticipated penalties of up to $1 billion dollars that such a fine "would be much smaller than Meta's revenue from scam ads."

141. *Comprehensiveness.* Meta characterizes its scam prevention efforts as "comprehensive" and "extensive." For example, Meta's Terms of Service provide:

> We work hard to maintain the security (including the availability, authenticity, integrity, and confidentiality) of our Products and services. We employ dedicated teams around the world, work with external service providers, partners and other relevant entities and develop advanced technical systems to detect potential misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community, including to respond to user reports of potentially violating content.

Meta's Scam Prevention Hub and "Unacceptable Business Practices in Advertising" policy include the following statement: "We take a comprehensive approach to making our technologies a safer place." On its Transparency Center page, Meta's introduction to its Advertising Standards further provides, "When advertisers place an order, each ad is reviewed against our policies." Additionally, an October 2024 Meta post assures members of the public that Meta's "ad review system" uses "automated technology . . . to review every ad" it runs on Facebook and Instagram for policy violations, "including scams." According to Meta's Business Help Center, which is a publicly available site targeted toward advertisers, "human reviewers" also "manually review ads"

in some cases. And a December 2025 Meta post on Facebook states: "[W]e're highlighting our extensive work to combat scams on our platforms." In the same post, under the heading "Our Comprehensive Approach to Aggressive Scam Reduction," Meta states that its "multi-layered approach to combating scams includes: using automated, technical defenses to help protect people on our apps; disrupting criminal scam networks; working with partners across the industry and in law enforcement; and raising awareness about ways to spot and prevent scams."

142. Instagram, LLC maintains its own separate contract with users, the "Instagram Terms of Use." The Instagram Terms of Use contain parallel contractual promises regarding the safety and integrity of Instagram's platform. For example, the Instagram Terms of Use promise that: "We also have teams and systems that work to combat abuse and violations of our Terms and policies, as well as harmful and deceptive behavior. We use all the information we have—including your information—to try to keep our platform secure." The Instagram Terms of Use further promise that "[a]utomated technologies also help us ensure the functionality and integrity of our Service."

143. Notwithstanding these strong representations, Meta has in actuality been laying off the "dedicated teams" assigned to work on scam prevention efforts, rolling back and refusing to adopt the processes and technological tools developed and tested by those teams, and setting "revenue guardrails" that prevent those teams from doing their job by prioritizing profits over protecting the public from scams. Meta has also been concealing the extent of the "scam ad" problem from regulatory agencies; refusing to adopt best practices used by industry peers; and improperly rejecting or ignoring "scam ad" reports submitted by users, victims, and people whose likenesses are being appropriated to scam others, including military officials. Moreover, in spite of Meta's assertion that it reviews every ad for violations of its anti-scam policies, Meta in fact posts ads that it knows are likely to be fraudulent, misleading, or deceptive if the scam advertiser pays an extra surcharge.

144. *Us vs. Them*. Meta characterizes scam advertisers as an outside foe it works hard to combat. For example, an October 2024 Meta post refers to Meta's efforts to combat scam ads as "building on our existing defenses," and leaders within Meta have stated that "[s]cams are a

society wide problem which requires industry, government and others to work together, and we will continue to expand and evolve our collaboration to stop fraudsters in their tracks."

145. But Meta participates in the creation and optimization of scam ads. Scam advertisers have access to Advantage+ creative, a suite of Meta-designed tools that create ads with minimal user input, including generating original text and images. As explained, a *Reuters* reporter trying out those tools declined to post the variants of his ad that they produced, on the ground Meta's adjustments made the variants materially more misleading than his original drafts. Moreover, Meta also facilitates scam advertising by promoting supposedly vetted Business Partners that have helped scammers—including many of the Chinese advertising accounts mentioned above—perpetuate scams. As the aforementioned *Reuters* reporter put it:

> I wasn't surprised to see agency accounts available on shady digital forums, where online marketers openly discuss ways to sell black-market products. It was more of a shock to see them for sale in Meta's own partner directory, a listing of companies that Meta said had been "vetted for their expertise." I was also surprised that once I found agencies happy to run my fake ads, Meta's systems offered to use artificial intelligence to improve them.

146. *Ad Targeting*. Meta's Terms of Service promise users that Meta will use its ability to direct ads to particular users to ensure that they see content—and specifically ads—that are of interest to them. Specifically, under the heading "The services we provide," Meta's contract with users promises that:

> 1.2 Connect you with people and organizations you care about:
>
> We help you find and connect with people, groups, businesses, organizations, and others that matter to you across the Meta Products you use. Stronger ties make for better communities, and we believe our services are most useful when people are connected to people, groups, and organizations they care about.
>
> . . .
>
> 1.4 Help you discover content, products, and services that may interest you:
>
> We show you personalized ads, offers, and other sponsored or commercial content to help you discover content, products, and services that are offered by the many businesses and organizations that use Facebook and other Meta Products.

147. Meta uses its ability to direct ads to particular users to ensure that scam ads are sent to the consumers most likely to be harmed by the ads. Meta itself has recognized that, if a consumer previously clicked on a scam ad, the consumer is more likely to be shown additional

scam ads in the future. Moreover, while it used to be that an advertiser would ask Meta to target its ads toward, for example, women in New York between the ages of 24 and 35, Meta now uses artificial intelligence to suggest to advertisers which customers they ought to target. This process means that Meta plays a material role in ensuring that, for example, scam advertisements likely to deceive an elderly person reach an audience of elderly consumers likely to engage with the scam ads, and scam advertisements likely to deceive a young person reach an audience of young consumers likely to engage with the scam ads, *even if the scam advertiser did not ask Meta to do so*. Such conduct is far afield from legitimate efforts to connect a consumer with content that may be of interest to the consumer.

148. In sum, in light of Meta's conduct, its statements—ranging from representations that it treats combating scam ads as a top priority, to representations that it removes scam ads as soon as it becomes aware of them, to representations that it is constantly improving its processes and technologies for combating scam advertising—are false, misleading, and likely to deceive reasonable consumers and legitimate advertisers.

2. Meta Breaks Its Promises to Users and Advertisers

149. Meta provides Terms of Service, formerly referred to as a Statement of Rights and Responsibilities, that apply to Facebook and certain other Meta platforms and that constitute a contract with the users of those platforms, and with advertisers on those platforms. Meta also maintains a separate contract with Instagram users, the "Instagram Terms of Use." Both the Meta Terms of Service and the Instagram Terms of Use incorporate as part of the contract related Meta policies and terms, including, but not limited to, Meta's Community Standards, AI Terms of Service, Community Payment Terms, and Privacy Policy.

150. Meta has breached these contracts by failing to make good on its promises to take meaningful action to combat scams and protect consumers and legitimate advertisers from deceptive ads, as discussed above in Section IV.C.1. In addition to constituting contractual promises to Meta users and advertisers, the below statements by Meta also constitute false and misleading statements that were likely to deceive users and advertisers, particularly as read together with the misrepresentations set forth above.

151. Among other things, Meta's contracts include promises about Meta's extensive efforts to prevent and combat fraud. For example, Meta's Terms of Service provide:

> We work hard to maintain the security (including the availability, authenticity, integrity, and confidentiality) of our Products and services. We employ dedicated teams around the world, work with external service providers, partners and other relevant entities and develop advanced technical systems to detect potential misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community, including to respond to user reports of potentially violating content. If we learn of content or conduct like this, we may take appropriate action based on our assessment that may include - notifying you, offering help, removing content, removing or restricting access to certain features, disabling an account, or contacting law enforcement.

152. Similarly, the Terms of Service promise that "we develop automated systems to improve our ability to detect and remove abusive and dangerous activity that may harm our community and the integrity of our Products."

153. The Terms of Service also specifically promise users that Meta will use its ability to direct ads to particular users to ensure that they see content – and specifically ads – that are of interest to them. Specifically, under the heading "The services we provide," Meta's contract with users promises that Meta will:

> 1.2 Connect you with people and organizations you care about:
>
> We help you find and connect with people, groups, businesses, organizations, and others that matter to you across the Meta Products you use. Stronger ties make for better communities, and we believe our services are most useful when people are connected to people, groups, and organizations they care about.
>
> 1.4 Help you discover content, products, and services that may interest you:
>
> We show you personalized ads, offers, and other sponsored or commercial content to help you discover content, products, and services that are offered by the many businesses and organizations that use Facebook and other Meta Products.

154. The Instagram Terms of Use contain parallel contractual promises regarding the safety and integrity of Instagram's platform. For example, the Instagram Terms of Use promise that: "We also have teams and systems that work to combat abuse and violations of our Terms and policies, as well as harmful and deceptive behavior. We use all the information we have—including your information—to try to keep our platform secure." The Instagram Terms of Use

further promise that "[a]utomated technologies also help us ensure the functionality and integrity of our Service."

155. The Instagram Terms of Use further state: "We use data from Instagram and other Meta Company Products, as well as from third-party partners, to show you ads, offers, and other sponsored content that we believe will be meaningful to you. And we try to make that content as relevant as all your other experiences on Instagram." The Instagram Terms of Use further promise that "[w]e show you relevant and useful ads."

156. Meta's contracts refer readers to a number of webpages that provide a host of terms governing the contracts. Among other things, those webpages commit Meta to preventing fraudulent ads and other scams on its platforms, and to removing ads and other content that violate its policies and standards.

157. For example, Meta's Community Standards, which are incorporated by reference into its contracts with users and advertisers, promise that: "when we limit expression, we do it in service of one or more of the following values" which include:

> Authenticity: We want to make sure the content people see is authentic. We believe that authenticity creates a better environment for sharing, and that's why we don't want people using our services to misrepresent who they are or what they're doing.

158. Meta commits that "Our Community Standards apply to everyone, all around the world, and to all types of content, including AI-generated content." Among other content prohibited by the Community Standards are "Fraud, Scams, and Deceptive Practices." Under that heading, Meta expressly prohibits ads that attempt "to scam or defraud users by misrepresenting the identity of the poster," including by "falsely claiming to represent, or speak in the voice of, an established business or entity" and represents that "We do not allow: Content that attempts to scam or defraud users and/or businesses." Meta expounds upon those commitments as follows:

> We aim to protect users and businesses from being deceived out of their money, property or personal information. We achieve this by removing content and combatting behavior that purposefully employs deceptive means - such as wilful [sic] misrepresentation, stolen information and exaggerated claims - to either scam or defraud users and businesses, or to drive engagement. This includes content that seeks to coordinate or promote those activities using our services.

159. Meta also states that it will "restrict or remove accounts that are harmful to the community. We have built a combination of automated and manual systems to restrict and remove accounts that are used to egregiously or persistently violate our policies across any of our products." With regard to scams and frauds, Meta makes express commitments to users:

> We do not allow content that is designed to deceive, mislead or overwhelm users in order to artificially increase viewership. This content detracts from people's ability to engage authentically on our platforms and can threaten the security, stability and usability of our services. We also seek to prevent abusive tactics, such as spreading deceptive links to draw unsuspecting users in through misleading functionality or code, or impersonating a trusted domain. Online spam is a lucrative industry. Our policies and detection must constantly evolve to keep up with emerging spam trends and tactics. In taking action to combat spam, we seek to balance raising the costs for its producers and distributors on our platforms, with protecting the vibrant, authentic activity of our community.

160. The contracts also include express provisions, designated "Advertising Policies," that detail the categories of advertisements that are prohibited on Meta's platforms. Specifically, Meta represents that "Our Advertising Standards provide policy detail and guidance on the types of ad content we allow, and the types of ad content we prohibit." The Company's advertising policies "are guided by our company's core values and the following principles:"

> Protecting people from fraud or scams: Our policies prohibit ads promoting products, services, schemes or offers using deceptive or misleading practices, including those meant to scam people out of money or personal information. . . .
>
> Promoting Transparency: We strive to make advertising more transparent and to give people more information about the ads they see. Our Ad Library offers a view of all ads currently running across our apps and services. . . .
>
> We use automated and, in some instances, manual review to enforce our policies. Beyond reviewing individual ads, we also monitor and investigate advertiser behavior, and may restrict advertiser accounts that don't follow our Advertising Standards, Community Standards or other Meta policies and terms. . . .
>
> Ads must not violate our community standards.

161. Meta's Advertising Standards include a separate "Unacceptable Business Practices in Advertising" policy that provides: "Ads must not promote products, services, schemes or offers using deceptive or misleading practices, including those intended to scam people out of money or personal information."

162. That policy also includes Meta's "Guidelines for Ads" which provides that:

> Ads can't:
>
> Use deceptive or exaggerated claims about the success of a product or service to mislead people into purchasing or sharing sensitive information
>
> Use deceptive or exaggerated claims about health-related benefits of a product or service to mislead people into purchasing or sharing sensitive information
>
> Use the image of a famous person and misleading tactics in order to bait people into engaging with an ad
>
> Promise financial benefits by misrepresenting an entity, industry association or news outlet to mislead people or ask them to share sensitive information

163. Meta concludes its "Unacceptable Business Practices in Advertising" policy by promising that, with regard to "scams," "we take a comprehensive approach to making our technologies a safer place."

164. For the reasons discussed in Section IV.C.1 above, Meta has failed to deliver on these promises and frustrated the rights of consumers and legitimate advertisers to the benefits of their contracts. Despite Meta's contractual promises that it will take a "comprehensive" approach to platform safety, maintain teams and systems to fight scams, and take action to address misleading advertising, in fact Meta has prioritized its own profits and failed to adopt and maintain meaningful systems to prevent and remove the scam ads that Meta knows to be rife on its platforms. As such, Meta has breached its contracts with consumers and legitimate advertisers and violated the covenant of good faith and fair dealing implied by law into every contract.

D. The Impact of Meta's False and Deceptive Statements and Deceptive, Unlawful, and Unfair Business Practices

165. Billions of users of Meta's platforms have been and continue to be exposed to scam ads due to: (a) Meta's misrepresentations about the safety of its platforms and its commitment and efforts to combat and prevent fraud, which falsely provide consumers with comfort and assurance that they will be protected from scam advertising; (b) Meta's multiple decisions to limit, cancel, or disregard programs and tools proven to limit or prevent scams; (c) Meta's policy and practice of sharing in the proceeds of scams by running ads it deems likely to be fraudulent in exchange for an added payment from the scammers behind those ads—which announces to scammers that

Meta's platforms are open for fraud, at the expense of the public, so long as Meta gets its piece of the proceeds; (d) Meta's promotion of supposedly "vetted" business partners; and (e) Meta's provision of AI tools to develop scam ads, which means that Meta is itself editing and refining scams placed on its platforms, as well as targeting the ads at the consumers most likely to be harmed by them. The scope of the impact to the public is massive. Scammers have reaped billions of dollars from consumers—some of which have flowed directly to Meta as profits—by using Meta platforms to perpetrate their scams.

166. These impacts result from conduct within California that impacts users of Meta's Facebook and Instagram platforms who are located both within and outside California.

167. Meta's misconduct has also impacted legitimate advertisers on Meta's platforms. Among other things, by allowing scammers to place bids to show billions of dollars' worth of scam ads to consumers, Meta has introduced vastly more competition into the advertising auctions, resulting in higher prices. That is, for a legitimate advertiser to win an auction, that advertiser needs to outbid hordes of scammers competing for the same slot. The inclusion of a massive volume of scam ads in the advertising auctions necessarily causes a material increase in advertising prices for legitimate advertisers. While Meta reaps billions of dollars in additional profits by inflating prices, legitimate advertisers suffer. Moreover, a winning bidder's ad necessarily displaces the losing bidder's ad. Each of the billions of dollars of scam ads placed on Meta platforms therefore displaces the ads of legitimate advertisers. In addition, the prevalence of scam ads on Meta platforms impacts consumer trust in the reliability of all advertising encountered on those platforms. This lack of trust negatively impacts legitimate advertisers, which are already paying a premium to reach Meta's billions of users. Meta's actions therefore harm legitimate advertisers by forcing them to pay higher prices, depriving them of ad slots, and reducing the effectiveness of the advertisements they are able to place on Meta's platforms.

168. These legitimate advertisers include numerous California businesses, including those located in Santa Clara County. These impacts result from conduct within California that impacts advertisers located both within and outside California.

169. Meta's conduct has also facilitated and promoted a wave of scams predicated on impersonation. Countless scams use the names and likenesses of celebrities, financial professionals, military personnel, and other respected people to advance their scams. These innocent individuals and businesses are thus associated with egregious scams. Many suffer reputational harm and/or are forced to spend time addressing victims of fraud who contact them after suffering losses.

V. CAUSES OF ACTION

CAUSE OF ACTION I

For Violations of the False Advertising Law,
Bus. & Prof. Code, §§ 17500 *et seq.*

170. The People reallege and incorporate by reference each and every paragraph set forth above as if fully set forth herein.

171. The False Advertising Law (FAL), codified at Business and Professions Code §§ 17500 *et seq.*, makes it unlawful for a business to make, disseminate, or cause to be made or disseminated to the public "any statement, concerning . . . real or personal property or . . . services . . . which is untrue or misleading, and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading."

172. As alleged above, Meta has engaged in and continues to engage in, and/or has aided and abetted and continues to aid and abet, acts or practices that violate the FAL through (1) Meta's statements falsely advertising to consumers and legitimate advertisers the safety and security of its platforms and Meta's efforts and commitment to combating fraud, scams, and deceptive advertising practices on its platforms, and (2) Meta's participation in and contribution to the creation, optimization, and targeting of false and misleading advertisements on Meta platforms.

173. As alleged above, Meta knows—and has known for years—that its platforms expose consumers to billions of false and misleading advertisements each day. Despite that knowledge, Meta has rolled back and declined to adopt effective measures to prevent false and misleading advertisements and has otherwise prioritized profits over efforts to combat false and misleading advertisements. Nonetheless, Meta falsely assures consumers and legitimate

advertisers that its platforms are safe and secure, that it will not tolerate fraud, scams, and deceptive practices, and that Meta is "constantly" and "aggressively" combating fraud. Meta's false and misleading statements to consumers and legitimate advertisers include those set forth above.

174. Meta made, and continues to make, these false and misleading statements to market its platforms and services to consumers and legitimate advertisers. Meta's statements, separately and collectively, are likely to deceive consumers who use, or are considering using, Meta platforms and legitimate advertisers who compete, or are considering competing, to place legitimate advertisements on Meta platforms. Based on, among other things, Meta's tracking of scam advertisements and awareness of its own decisions not to implement fraud prevention measures, Meta knew, or at a minimum should have known, that its statements were false, misleading, and likely to deceive reasonable consumers and reasonable legitimate advertisers.

175. Meta's false and misleading statements were, and continue to be, widely disseminated through Meta's websites and the websites of Meta's platforms, and through other forms of mass media, including those set forth above.

176. Meta is also liable for violating, and/or aiding and abetting violations of, the FAL by directly participating in, contributing to, encouraging, and/or assisting in the creation, optimization, and steering of the millions of false and misleading advertisements placed on Meta platforms, including Facebook and Instagram. As alleged above, Meta's participation, contribution, encouragement, and assistance include, but are not limited to:

a. Creating, optimizing, and enhancing false and misleading advertisements through Meta's sophisticated AI tools, including Advantage+ creative and other tools;

b. Promoting and providing special protections to Business Partners purportedly "vetted" by Meta that have actively solicited and helped advertisers place false and misleading advertisements on Meta platforms; and

c. Using sophisticated algorithms to steer false and misleading ads to the consumers most likely to be harmed by them, targeting such consumers using Meta's extensive data about every user of its platforms.

177. As alleged above, Meta knows or should know that its platforms expose consumers to billions of false and misleading advertisements each day and that these advertisements are likely to deceive, and in fact have deceived, reasonable consumers. Meta also knows, or by the exercise of reasonable diligence should know, that its AI tools contribute to the creation and optimization of false and deceptive advertisements; that its vetted Business Partners have solicited and facilitated false and deceptive advertising; and that its algorithms steer false and misleading advertisements to target vulnerable consumers. These vulnerable consumers include many senior citizens who use Meta's platforms—particularly Facebook—and many minors who use Meta's platforms—particularly Instagram.

178. Meta participates in, contributes to, encourages, and/or assists in the creation, optimization, and steering of false and deceptive advertisements on its own platforms in order to maintain and/or increase its advertising revenues, which include billions of dollars from scam ads. These advertisements are, and have been, widely disseminated on Meta's platforms and are likely to deceive, and have in fact deceived, reasonable consumers.

179. The proliferation of fraudulent advertisements on Meta platforms materially impacts the pricing of advertisements on those platforms, thereby increasing the costs incurred by legitimate advertisers. Meta's platforms price advertisements using a complex auction mechanism. Advertisers bid to place their ads on the platforms, and the proliferation of fraudulent ads representing billions of dollars in advertising dollars inflates the price of the ads purchased by legitimate advertisers. Had Meta not facilitated and promoted the proliferation of scam ads, and had it combatted and prevented scams as it represented it would, legitimate advertisers would not incur such inflated advertising costs.

CAUSE OF ACTION II

For Violations of the Unfair Competition Law,
Bus. & Prof. Code, §§ 17200 *et seq.*

180. The People reallege and incorporate by reference each and every paragraph set forth above as if fully set forth herein.

181. The Unfair Competition Law (UCL), codified at California Business and Professions Code §§ 17200 *et seq.*, prohibits "any unlawful, unfair or fraudulent business act or practice," as well as "unfair, deceptive, untrue or misleading advertising" and any act prohibited by the FAL.

182. As alleged above, Meta has engaged in and continues to engage in, and/or has aided and abetted and continues to aid and abet, acts and practices that violate the UCL.

183. Acts Prohibited by the FAL. As alleged in Cause of Action I, Meta has engaged and continues to engage in acts that violate the FAL. These acts also constitute a violation of the UCL under Business and Professions Code section 17200.

184. Unfair, Deceptive, Untrue, or Misleading Advertising. As alleged in Cause of Action I, Meta has engaged and continues to engage in, and/or has aided and abetted and continues to aid and abet, advertising that is unfair, deceptive, untrue, and/or misleading through (1) Meta's statements falsely advertising to consumers and advertisers the safety and security of its platforms and Meta's efforts and commitment to combating fraud, scams, and deceptive advertising practices on its platforms, and (2) Meta's participation in and contribution to the creation, optimization, and steering of false and misleading advertisements on Meta platforms. Meta's unfair, deceptive, untrue, and misleading advertising is likely to deceive reasonable consumers and advertisers, as alleged above, and violates the UCL.

185. Unlawful Business Acts and Practices. Meta has violated and continues to violate the "unlawful" prong of the UCL through unlawful business acts or practices that include, but are not limited to:

a. Meta has engaged and continues to engage in acts that violate the FAL, Bus. & Prof. Code, §§ 17500 *et seq.*, as alleged in Cause of Action I;

b. Meta has violated and continues to violate the Consumer Legal Remedies Act, Civ. Code, §§ 1750 *et seq.*, by knowingly participating in, contributing to, encouraging, and/or assisting in the creation, development, and targeting of advertisements that:

1. Pass off goods or services as those of another, in violation of Civ. Code, § 1770(a)(1);
2. Misrepresent the source, sponsorship, approval, or certification of goods or services, in violation of Civ. Code, § 1770(a)(2);
3. Misrepresent the affiliation, connection, or association with, or certification by, another, in violation of Civ. Code, § 1770(a)(3);
4. Represent that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that the person does not have, in violation of Civ. Code, § 1770(a)(5);
5. Represent that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, when in fact they are of another, in violation of Civ. Code, § 1770(a)(7);
6. Advertise goods or services with intent not to sell them as advertised, in violation of Civ. Code, § 1770(a)(9);
7. Represent that the consumer will receive a rebate, discount, or other economic benefit, when the earning of the benefit is contingent on an event to occur subsequent to the consummation of the transaction, in violation of Civ. Code, § 1770(a)(17);
8. Otherwise constitute unfair methods of competition or unfair or deceptive acts or practices prohibited by Civ. Code, § 1770.

c. Meta has engaged and continues to engage in conduct that systematically breaches its standard contracts with consumers and legitimate advertisers.

In its form agreements, Meta promises consumers and legitimate advertisers that it doesn't allow scams and other deceptive content on its platforms. Meta systematically breaches that promise, including by, among other conduct identified above, posting scam ads despite knowledge the ads are likely to be false, misleading, and/or deceptive. Meta's conduct is and has been a substantial factor in consumers and legitimate advertisers experiencing harm, including consumers being exposed to scam ads and legitimate advertisers being forced to pay artificially inflated rates to place their advertisements on Meta's platforms.

d. Meta has engaged and continues to engage in conduct that violates the covenant of good faith and fair dealing implied by law into every contract, thereby frustrating the rights of consumers and legitimate advertisers to the benefits of their agreements with Meta. In prioritizing profits over both consumer safety and advertisement auction fairness, Meta has not acted in good faith. Its actions have harmed consumers by depriving them of the benefit of a safe and secure platform and harmed legitimate advertisers by depriving them of the benefit of a fair auction process.

e. Meta has engaged and continues to engage in acts or omissions that constitute negligence and defective product design (collectively, "design defects"), in violation of common law and/or statute. (See *Barker v. Lull Engineering Co.* (1978) 20 Cal.3d 413, 418; Civ. Code, § 1714(a).) Two Meta products are defective in design: (1) a product to protect users from fraud, scams, and deceptive practices in digital advertising on Meta's Facebook, Instagram, and WhatsApp platforms, which Meta designed and disseminated for public use by consumers (the "Scam Ad Prevention Product"); and (2) an advertising product—one of the world's largest advertising platforms—that is comprised of several automated systems for the creation, modification, pricing, review, and steering of advertisements,

as well as the blocking of scam ads that would otherwise compete with legitimate ads (the "Advertising Product").

1. Meta's Scam Ad Prevention Product is an example of a class of competing products offered by several companies to prevent scam ads and other deceptive content on social media platforms. Meta's Scam Ad Prevention Product is defective in design because it does not comply with the standards articulated by Meta and it harms consumers because: (1) the design defects result in platforms that do not perform as safely as an ordinary consumer would expect them to perform; (2) the benefits of the design do not outweigh its inherent risks; and (3) Meta, owing a duty of reasonable care to consumers using its platforms, has breached that duty and harmed those consumers by exposing them to scam ads because of these design defects. These design defects include, but are not limited to, the following:

    i. Designing the Scam Ad Prevention Product to apply a surcharge to ads identified as likely to be scams;

    ii. Declining to implement proven, cost-effective fraud prevention processes, including universal advertiser verification;

    iii. Terminating scam-prevention programs and staff that had proven effective at protecting consumers from scams; and

    iv. Incorporating into the Scam Ad Prevention Product the consideration of the advertising revenue impact of scam-prevention mechanisms.

2. Meta's Advertising Product is an example of a class of competing products offered by several companies to advertisers and advertising

agencies as a tool to create and distribute advertisements through websites, social media platforms, and mobile applications. Meta touted the ability of its Advertising Product to deliver ads to millions of users, narrowly targeted by location, demographic, and topical interests, among numerous other factors. Meta's Advertising Product is defective in design because it does not comply with the standards articulated by Meta and it harms consumers because: (1) the design defects result in the proliferation of scam ads that compete with legitimate advertisements; (2) the benefits of the design do not outweigh its inherent risks; and (3) Meta, owing a duty of reasonable care to advertisers using its platforms, has breached that duty and harmed those advertisers because of these design defects. These design defects include, but are not limited to, the following:

i. Designing the Advertising Product to provide advanced tools used for the creation, optimization, and steering of scam ads;

ii. Declining to implement proven, cost-effective scam-prevention processes that would reduce the number of scam ads competing with legitimate ads on Meta platforms;

iii. Vouching for Business Partners that openly offer services to help scam advertisers;

iv. Terminating scam-prevention programs and staff that had proven effective at reducing the number of scam ads competing with legitimate ads on Meta platforms; and

v. Prioritizing ad revenue from scammers over scam-prevention mechanisms that would reduce the number of scam ads competing with legitimate ads on Meta platforms.

3. Meta's acts and omissions as described above also constitute general negligence, in violation of the duty of reasonable care that Meta owes to consumers and legitimate advertisers on its platforms.

186. As discovery continues, the People reserve their right to add additional predicate violations of law under the "unlawful" prong of the UCL.

187. Unfair Business Acts and Practices. As alleged above, Meta systematically breaches its standard contracts with consumers and legitimate advertisers and violates the covenant of good faith and fair dealing implied by law into those agreements. That conduct violates the "unfair" prong of the UCL.

188. In addition, Meta's business acts and practices as described in this Complaint are unfair and violate the UCL because the harm they cause to consumers and legitimate advertisers greatly outweighs any benefits associated with those practices. Meta's practice of prioritizing profits over safety—and providing false assurances while quietly dismantling and declining effective scam prevention measures—causes significant harm and offers no countervailing benefit to consumers, legitimate advertisers, or the general public. Meta's business acts and practices as described in this Complaint also offend established public policy, as embodied in numerous laws and policies including, but not limited to, the laws identified above; the Elder Financial Abuse statute, Welf. & Inst. Code, § 15610.30; Right of Publicity, Civ. Code, § 3344; laws related to transparency regarding social media terms of service, Bus. & Prof. Code, §§ 22675 *et seq*.; the Unruh Civil Rights Act, Civ. Code, §§ 51 *et seq.*; and the common law and/or statutory Duty to Warn.

189. As discovery continues, the People reserve their right to add additional unfair business acts or practices under the "unfair" prong of the UCL.

190. Deceptive Business Acts or Practices. Meta has violated and continues to violate the "deceptive" prong of the UCL through the following business acts or practices that are likely to deceive reasonable consumers and advertisers:

a. As alleged in Cause of Action I, Meta has made and continues to make statements falsely advertising to consumers and advertisers the safety and security of its platforms and Meta's efforts and commitment to combating fraud, scams, and deceptive advertising practices on its platforms.

b. As alleged in Cause of Action I, Meta has participated in and contributed to, and continues to participate in and contribute to, the creation, development, and steering of false and misleading advertisements on Meta platforms.

c. As alleged above, Meta systematically breaches its contracts with consumers and advertisers in which Meta promises that it doesn't allow scams and other deceptive content on its platforms. Yet, through its statements in the media, on websites, and on its own platforms, Meta falsely assures consumers and advertisers that it is making good on these promises—all the while knowing that its platforms expose users to billions of scam ads every day, that it has rolled back and declined to implement effective scam-prevention measures, and that it allows likely scam advertisers to compete in ad auctions in exchange for an extra fee. Meta's systematic breach of contractual promises, while falsely assuring that it upholds those promises, is likely to deceive consumers and legitimate advertisers, in violation of the UCL "deceptive" prong.

191. As discovery continues, the People reserve their right to add additional deceptive business acts or practices under the "deceptive" prong of the UCL.

VI. PRAYER FOR RELIEF

THE PEOPLE pray that the Court:

1. Declare that Defendants have engaged in, and/or aided and abetted, false and misleading advertising in violation of the False Advertising Law and unlawful, unfair, and deceptive business acts and practices in violation of the Unfair Competition Law.

2. Enjoin Defendants from performing or proposing to perform any further false or misleading statements in violation of the False Advertising Law, pursuant to Business and Professions Code section 17535, and any acts in violation of the Unfair Competition Law, pursuant to Business and Professions Code section 17204.

3. Order Defendants to pay civil penalties for each act of false and misleading advertising, pursuant to Business and Professions Code sections 17500 and 17536, and for each act of unlawful, unfair, and deceptive business acts and practices, pursuant to Business and Professions Code section 17206.

4. Order Defendants to pay civil penalties for each unlawful, unfair, or deceptive business act or practice perpetrated against senior citizens or disabled persons, pursuant to Business and Professions Code section 17206.1.

5. Order Defendants to pay restitution in an amount to be determined according to proof pursuant to Business and Professions Code sections 17500 and 17535 and Business and Professions Code sections 17200 and 17203.

6. Order Defendants to pay treble the amount of all relief awarded by the Court, pursuant to Civil Code section 3345.

7. Order Defendants to pay reasonable attorneys' fees and the costs of the suit.

8. Provide such further and additional relief as the Court deems proper.

DATED: May 11, 2026

Respectfully submitted,

By: /s/ Tony LoPresti

TONY LOPRESTI (SBN 289269)
County Counsel
KAVITA NARAYAN (SBN 264191)
Chief Assistant County Counsel
MEREDITH A. JOHNSON (SBN 291018)
Lead Deputy County Counsel
LAURA S. TRICE (SBN 284837)
HANNAH M. GODBEY (SBN 334475)
BILL NGUYEN (SBN 333671)
Deputy County Counsels

OFFICE OF THE COUNTY COUNSEL
COUNTY OF SANTA CLARA
70 West Hedding Street, East Wing, 9th Floor
San José, CA 95110-1770
Telephone: (408) 299-5900
Facsimile: (408) 292-7240
Email: tony.lopresti@cco.sccgov.org
kavita.narayan@cco.sccgov.org
meredith.johnson@cco.sccgov.org
laura.trice@cco.sccgov.org
hannah.godbey@cco.sccgov.org
bill.nguyen@cco.sccgov.org

BERNSTEIN LITOWITZ BERGER & GROSSMANN LLP

AVI JOSEFSON
MICHAEL D. BLATCHLEY
TAL E. AVRHAMI
CAROLINA YU
1251 Avenue of the Americas
New York, New York 10020
Telephone: (212) 554-1400
Facsimile: (212) 554-1444
Email: avi@blbglaw.com
michaelb@blbglaw.com
tal.avrhami@blbglaw.com
carolina.yu@blbglaw.com

JONATHAN D. USLANER (SBN 256898)
ANYA FREEDMAN (SBN 275213)
MATTHEW ARROW (SBN 338273)
2121 Avenue of the Stars, Suite 2575
Los Angeles, California 90067
Telephone: (310) 819-3481
Email: jonathanu@blbglaw.com
anya@blbglaw.com
matthew.arrow@blbglaw.com

RENNE PUBLIC LAW GROUP, LLP

LOUISE RENNE (SBN 36508)

JONATHAN V. HOLTZMAN (SBN 99795)
JAMES ROSS (SBN 149199)
350 Sansome Street, Suite 300
San Francisco, CA 94104
Telephone: (415) 848-7200
Facsimile: (415) 848-7230
Email: lrenne@publiclawgroup.com
jholtzman@publiclawgroup.com
jross@publiclawgroup.com

BISHOP PARTNOY LLP

ROBERT E. BISHOP
FRANK PARTNOY
1717 K Street, NW Suite 900
Washington, DC 20006
Telephone: (202) 787-5769
Email: bobby@bishoppartnoy.com
frank@bishoppartnoy.com

Counsel for Plaintiff the People of the State of California