Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

**SUPERIOR COURT OF THE STATE OF RHODE ISLAND**
**FOR THE COUNTY OF PROVIDENCE**

| | |
|---|---|
| STATE OF RHODE ISLAND, by and through PETER F. NERONHA, ATTORNEY GENERAL,<br><br>*Plaintiff*<br><br>v.<br><br>META PLATFORMS, INC. and INSTAGRAM, LLC,<br><br>*Defendants*. | C.A. NO.: |

# COMPLAINT

The State of Rhode Island, by and through its Attorney General, Peter F. Neronha, ("Rhode Island" or "State"), brings this action pursuant to his statutory authority against Meta Platforms, Inc. and Instagram, LLC (all defendants collectively, "Defendants").

## INTRODUCTION

1. In 2025, Meta Platforms, Inc. ("Meta"[1]) earned $200.97 billion in revenue, virtually all of which came from paid advertising. Indeed, Meta operates one of the largest advertising systems in the world, selecting and distributing ads in users' feeds on Facebook and Instagram, in their Messenger inboxes, and on WhatsApp. Globally, more than one-quarter of digital ad spending goes to purchase ads on Meta.

2. Meta's platforms help create, serve, and refine billions of advertisements each day through a sophisticated, algorithmically driven system designed to target users based on their

[1] Throughout the Complaint, Meta includes both Meta Platforms, Inc. and Instagram, LLC.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

behavior, interests, and vulnerabilities. In doing so, Meta can take advantage of its sophisticated ad software, its trove of user data, and its monitoring of users' on-platform and off-platform activities. In the case of scams, that means users, including those over age 60, who are most susceptible to ads for fraudulent investments, health cures, and romance, among many others, are especially targeted.

3. Meta knew that an unconscionable share of its advertising revenue—reportedly projected internally to represent 10% of its 2024 revenue, or about $16 billion—came from advertisements for restricted goods (like weapons and explosives, drugs and paraphernalia, tobacco, medical devices, counterfeit or stolen goods, or recalled products) or sought to defraud consumers, including Rhode Island consumers.

4. Rather than address this fraud, Meta knowingly helped create and optimize these ads to ensure that they were as effective as possible and then lied about them, misrepresenting to the public its commitment to prevent fraud on its platforms.

5. Meta represents to the public that it detects, blocks, removes, and "aggressively" combats fraud and scams on its platforms and removes deceptive advertising from its platforms. Meta tells the public that it was "always working to find, remove, and disrupt scammers" and that scams were contrary to the "foundation" of its advertising business.

6. In reality, Meta has knowingly distributed to unsuspecting users large volumes of fraudulent advertisements. Internally Meta projected billions of dollars in revenue from scam advertisements, tolerated likely fraudulent ads unless its systems reached an extreme certainty threshold, and charged suspected fraudsters higher rates rather than excluding them—earning even more money from ads it considered likely to be fraudulent—all at the expense of Rhode Island consumers who it exposed, and continues to expose, to harm. Contrary to its public statements,

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

Meta didn't take steps to vet advertisers or enforce standards because, in the words of one employee, "[redacted]"

7. In addition, to protect its advertising revenue and (falsely) project an image of constant growth, Meta knowingly tolerated millions of fake accounts, which it (falsely) reported publicly as users of its platforms. Among other harms, these fake accounts helped legitimize and distribute fraudulent ads as scammers created and leveraged these accounts to engage with their other accounts to both make their ads appear mainstream and to boost their distribution by Meta's algorithm.

8. Meta's internal long-range planning documents show that the company [redacted].[2] When it was too successful, Meta dissolved the internal team that had removed scam ads originating from China, where many of the scam ads originated.

9. In addition to misrepresenting its own efforts and commitment to address scam ads, Meta failed to warn users about the fraud that it knew proliferated on its platforms.

10. Online scams are big business. According to data released by the Federal Trade Commission ("FTC") in 2025, 30% of people who reported losing money to a scam reported that the fraud began on social media—more than any other medium. Collectively, these victims were defrauded of more than $2.1 billion, a figure that no doubt fails to capture a significant volume of

[2] [redacted]

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

fraud that goes unreported. Facebook accounted for the greatest share of these scams, followed next by Meta's other platforms, WhatsApp and Instagram.

11. According to data released in June 2026 by the Associated Press-NORC Center for Public Affairs Research, 58% of adults report that they are the target of scam attempts each day. And, "[m]ore people who report scam attempts see them on Facebook than any other social media platform." With Instagram and WhatsApp occupying the next two slots, Meta's platforms collectively account for 78% of all online scams and far outpace the next most prevalent source—TikTok—at 9%.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

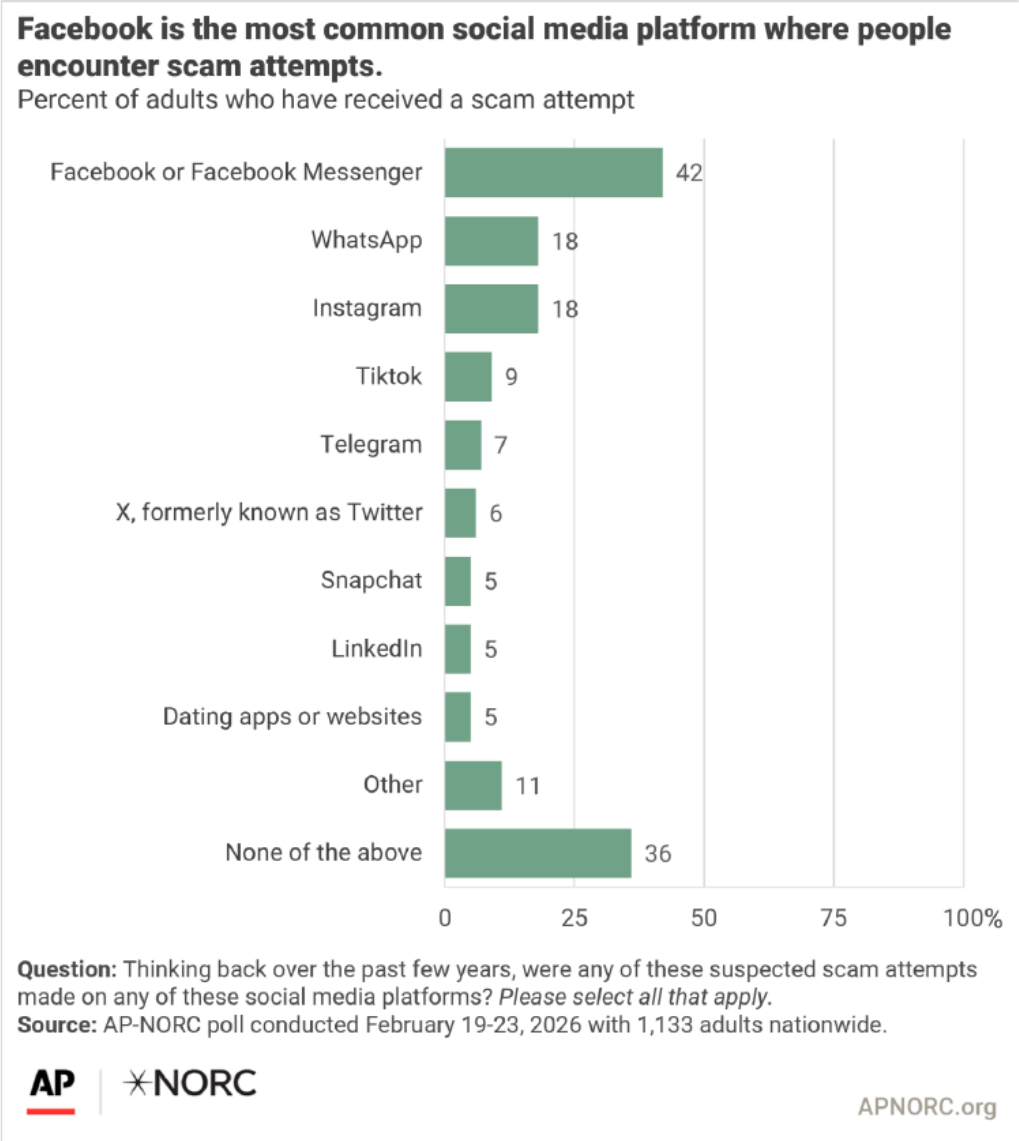



**Figure 1**

12. Publicly available reports from law enforcement have demonstrated that older adults are especially susceptible to fraud. The FBI has found that older adults are attractive scam targets because they often have accumulated savings, may be more trusting, and may be more likely to engage with unsolicited communications. In 2025, victims over 60 experienced more than $7.7 billion in losses. The FBI reported 2,700 fraud complaints from Rhode Island residents in 2025, amounting to $71,960,439 in fraud losses, including 581 complaints from residents over 60.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

13. The FTC likewise repeatedly identified older adults as a population experiencing enormous fraud losses, which have grown substantially in recent years. According to the agency, older adults may be more susceptible to fraud because of cognitive decline, social isolation, lack of financial literacy, loneliness, and other risk factors.

14. The Attorney General ("State" or "Rhode Island") brings this action under the Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1, *et seq.*, to remedy Meta's unfair, false, misleading, and deceptive acts and practices and to protect Rhode Island consumers. The State seeks civil penalties for each of Meta's violations of law and injunctive relief to require Meta to live up to its commitments and address, rather than profit from, the scam ads that it develops and delivers on its platform.

15. This action arises from the gap between what Meta tells consumers about fraud on its platforms and how Meta actually operates its advertising system to facilitate and amplify fraud. It is particularly important as Meta has denied it has any duty to address the legion of "third-party scam advertisers" that operate on its platform.

16. Meta's treatment of scam ads shares much in common with Meta's treatment of child safety and well-being issues, which the State has pursued and resolved through separate litigation. In both cases, Meta decided to under-resource enforcement and to tolerate, rather than ban, bad actors and refused to put in place policies that would more effectively safeguard users or to honestly disclose to the public the dangerous conduct on its platforms. In both cases, Meta acted to create the appearance that it was protecting its users, while prioritizing its own profits over their safety. Although these similarities reveal a familiar playbook in Meta's operations, Meta's inaction against fraudulent ads harms wreaks financial havoc on different constituencies.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

## JURISDICTION AND VENUE

17. This Court has subject-matter jurisdiction pursuant to R.I. Gen. Laws §§ 8-2-14 and 6-13.1-5.

18. This Court has personal jurisdiction over Defendants because Defendants transact business in Rhode Island and/or have the requisite minimum contacts with Rhode Island necessary to constitutionally permit the Court to exercise jurisdiction, with such jurisdiction also being proper under Rhode Island's long-arm statute, R.I. Gen. Laws § 9-5-33.

19. Specifically, this Court has personal jurisdiction over Meta Platforms, Inc., as it has purposefully availed itself of this forum by conducting business in Rhode Island and by causing harm as a result of its actions. For at least 10 years, Meta has systematically served the Rhode Island market by offering its platforms to Rhode Island residents. Meta advertises its products extensively in Rhode Island, through television and Internet advertisements, as well as other mediums directed to or available to Rhode Island residents. Meta also sells ads to Rhode Island businesses and to other third parties that are intended to reach customers in Rhode Island. By virtue of its advertising and the actual conduct of its business within Rhode Island, Meta intended that its products would be used and would create effects specifically within Rhode Island. Rhode Islanders have complained about scams on Meta's platforms. The effects and harms described in this Complaint all arise out of or are related to this conduct, and the harms described herein occurred within Rhode Island.

20. Venue is proper in this Court pursuant to R.I. Gen. Laws §§ 8-2-27 and 6-13.1-5(b).

## PARTIES

21. The State of Rhode Island is a sovereign state of the United States. Peter F. Neronha is the duly elected Attorney General and is the chief law enforcement officer and attorney for the

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

State. The Attorney General brings this action on behalf of the State in accordance with his statutory and common law authority.

22. Defendant Meta Platforms, Inc., d/b/a Meta, and formerly known as Facebook, Inc. and TheFacebook, Inc., is a multinational technology company incorporated in Delaware, with a principal place of business in Menlo Park, California.

23. 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.

24. Meta, through itself and/or its subsidiaries, develops, designs, markets, and operates social media platforms and services including Facebook, Instagram, Messenger, and WhatsApp (collectively, Meta's "platforms"). Meta earns substantially all of its annual revenue, which was $200.97 billion in 2025, by selling advertising.

25. For purposes of this Complaint, Meta includes its wholly-owned subsidiaries Instagram, LLC; Facebook Holdings, LLC; Facebook Operations, LLC; Meta Payments, Inc.; and Meta Platforms Technologies, LLC.

26. As detailed in the allegations below, Meta is engaging, has engaged, and continues to engage in unfair, false, misleading, or deceptive acts or practices in Rhode Island. Meta has conducted this activity on its own and/or through its subsidiaries over which it exercises complete control and dominion, and over which Meta's executive officers and directors have direct oversight. Because Meta and its subsidiaries operate as a common enterprise, each of them is jointly and severally liable for the acts and practices alleged below. All references to Meta in this Complaint shall refer to and are meant to include both Meta and its above-named subsidiaries and platforms, including Facebook, Instagram, and WhatsApp.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

## FACTUAL ALLEGATIONS

### A. Meta Engages in Trade and Commerce in Rhode Island

27. Meta engages in trade and commerce in Rhode Island. Meta opens accounts for Rhode Island users, provides them with access to its platforms, collects extensive personal data on them, and delivers them targeted advertising. Meta also sells and delivers ads for Rhode Island advertisers.

28. Meta operates at least three online platforms that are relevant to this action: Facebook, Instagram, and WhatsApp. All three platforms are offered to and used by Rhode Island consumers in the course of Meta's commercial activities.

29. Meta does not generally charge users a monetary fee to use its products; instead, it monetizes users' private data by actively harvesting it and using it to sell advertising. Meta generates "substantially all of [its] revenue from selling advertising placements to marketers." An essential part of Meta's advertising sales is the number and level of engagement of its users and the data Meta gathers from its users, which allows Meta to target and deliver ads to its users, including, in all respects, Rhode Island users. Meta discloses in its financial statements that "[t]he size of our user base and our users' level of engagement across our products are critical to our success. Our financial performance has been and will continue to be significantly determined by our success in adding, retaining, and engaging active users of our products that deliver ads, particularly Facebook and Instagram."

30. Ad impressions are the number of views of ads that Meta shows to users on its platforms. As a rule, the more views ads receive, the more revenue Meta receives. Meta maximizes the number of ad impressions by collecting data from their users and then monetizes that data by using it to target advertisements to demographics or individuals with characteristics that advertisers want to reach.

31. Meta's Terms of Service for its Facebook and Instagram products make that value-exchange: instead of paying with currency, users of Facebook and Instagram provide their demographic and usage data to Meta, which, in turn, Meta uses on an aggregate basis to entice advertisers to pay Meta to place advertisements on Meta's platforms that are targeted to specific audiences. As Meta advises in its Facebook Terms of Service, "we don't charge you to use Facebook or the other products and services covered by these Terms . . . [i]nstead, businesses and organizations, and other persons pay us to show you ads for their products and services."

32. Meta's Instagram Terms of Use contain a similar disclosure, confirming the same *quid pro quo,* noting that "[i]nstead of paying to use Instagram . . . you acknowledge that we can show you ads that businesses and organizations pay us to promote . . . We use your personal data, such as information about your activity and interests, to show you ads that are more relevant to you" and provide data on the ads' performance to advertisers.

33. Meta executives have confirmed the importance of collecting users' data in order to deliver targeted advertisements. In a January 30, 2019 earnings call CFO David Wehner stated: "In terms of our ability to continue to grow the advertising business, it's about working to develop the best – the best products we can to enable advertisers to achieve their end business results. Targeting obviously is very important in that."

34. Meta advertises its ability to target advertisements to potential advertisers, including on its website where it promotes that advertisers are able to reach the people that conform to the specific "traits . . . interests, gender, or location and use ad targeting to find the people most likely to take action."

35. Meta's ability to collect and aggregate data and to enable advertisers to incorporate the collected data into a targeted advertising strategy are key to the price and scale of Meta's ad

sales. Meta's digital ad model differs from traditional advertising, in which advertisers place their advertisements on billboards, in magazines or on television with broad distribution that includes both consumers who may be interested in the product and consumers who may not be interested.

36. Companies that seek to advertise on Meta "do not have long-term advertising commitments." They "will not continue to do business with [Meta], or they will reduce the budgets they are willing to commit to [Meta], if [Meta] do[es] not deliver ads in an effective manner." Thus, the *quid pro quo*—consumers providing their data in return for access to Meta's platforms—has been key to Meta's extraordinary advertising revenue.

37. Meta had specific knowledge not only of users in Rhode Island, but that ads on its platforms were distributed to users in Rhode Island. Indeed, Meta collects and publishes data in its Ad Library that breaks down the distribution of its ads by state.

38. Meta's platforms engage in other forms of commerce in Rhode Island besides advertising. For example, Facebook includes a feature called "Facebook Marketplace," which facilitates the sale of goods and services via the Facebook platform by permitting users to post the digital equivalent of classified advertisements on Facebook. Meta charges and collects a fee when items are sold on its Marketplace, including in Rhode Island. Additionally, Meta offers users, including users in Rhode Island, the opportunity to monetize their account(s) in order to sell subscriptions or permit advertisements to be placed on their pages.

39. A significant number of Rhode Island residents use Meta's products.

### B. Meta Plays an Active Role in Creating and Distributing Ads, Including Ads for Fraud and Scams

40. Meta does not simply host ads paid for by third parties; Meta is an active collaborator in creating and distributing ads on its platforms. Through its advertising tools, Meta works with fraudulent actors to generate ads rapidly, cheaply, and effectively and to get an ever

and ever better return from their efforts.

41. Ads Manager is the integrated commercial ad system through which advertisers create, target, deliver, measure, and optimize paid advertisements across Meta's platforms. Through Ads Manager, Meta sells its ad services, determines the final format and presentation of ads to maximize their appeal, selects the users who will receive the ads based on the advertisers' goals, measures the ads' performance, and optimizes delivery of the ads to users most likely to act on them.

42. In other words, advertisers supply basic inputs: text and images for their ads, as well as the advertisers' goals and audience. Based on its default settings, Meta's Ads Manager applies the "creatives," assembling inputs into finished ads and helping to determine how they will appear. That includes rewriting text, adding visuals, and generating versions of ads for different users in order to maximize the likelihood that Meta's audience will engage with the ads.

43. Meta's automated tools, including "dynamic creative," can be used by an advertiser to create up to 1,000 ads and are designed to alter the appearance, emphasis, format, and presentation of an ad; highlight key phrases; create videos from images; add soundtracks; personalize ad appearance based on viewers' response; and use generative artificial intelligence—all to optimize ads for engagement and maximize their performance.[3] Meta's Business Help Center advises, "[w]hen 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."

[3] As another example, Meta promotes: "Dynamic creative uses ad components like images, videos, and text and combines them in ideal ways for your audiences."

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

44. Advertisers also can take advantage of Meta's Advantage+, which allows them to tap Meta's "advanced ad technology to determine the most relevant ad variation for each person. We will automatically adjust your ad creative when it's likely to improve performance." This could include "applying compositional changes to creative, adding music," modifying images, adding text overlays, and "pick[ing] the version each member of your audience is most likely to respond to." Ads Manager also offers text generation, a generative AI feature that allows advertisers "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."

45. Reuters reporter Jeff Horwitz found that Meta not only accepted his obvious scam ads (described below) but then helped him optimize an ad, promising 10% weekly investment returns. As he described the experiment:

> 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.
>
> I clicked publish.
>
> Within 20 minutes, my ads' status began shifting from "In Review" to "Active." After four days, my ads had logged well over 100 clicks. I received more than three dozen inquiries via my website and Facebook Messenger.

46. Mark Zuckerberg has openly promoted Meta's role in catapulting advertisers into the market with Meta's ad tools. At a conference in 2025, Zuckerberg asserted that "Meta's ad tools, several of which have generative AI capabilities, are sophisticated enough already that the

company doesn't even recommend that customers specify the demographics they'd like to target. Meta's tools can find interested users better than human marketers can…." This applies not only to the audience, but the ad itself: "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."

47. Meta also offers a flexible ad format, which, as marketed to advertisers, "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." Meta continued:

> **Automatic optimization:** The ad delivery system can automatically optimize the ad format for you and show what it predicts is the best format, such as single image, video and carousel, to your audience. This is useful if you don't have a strong preference in ad formats.
>
> **Ad creation with less effort:** You don't need to select different ad formats for different ad placements, as it'll be selected for you based on what the ad delivery system determines people are most likely to respond to. You also don't need to create more ads per ad set to test different formats.

Perhaps in response to litigation, Meta announced that this tool would not be available after March 2026.

48. Through each of these tools, Meta contributes to creating and frequently determines what ads on its platforms will look like.

49. Meta's Ads Manager also directs who will see ads and how those ads will perform. Through its Experiments tools, Meta provides testing and performance tools that allow advertisers to refine advertisements over time and increase their return. Meta identifies the highest-performing version of an ad based on metrics like the click-through or conversion rates and works (through its AI) with advertisers to test and adapt the ad's content, audience, and placement.[4]

[4] Meta's ad tool "starts by prioritizing your suggestions to create the broadest possible audience, then evolves your audience in real time to find more relevant customers."

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

50. Meta also allows advertisers to target their advertisements to specific age groups such as selecting users who are 65+, among other demographic attributes including gender and education level. Advertisers can also target ads by user interests, including categories related to retirement planning, personal finance, investment products, health and wellness. Thus, an advertiser can seek to reach users age 60+ who have shown an interest in investing, Medicare-related topics, and/or retirement. Meta promises: "Once your ad starts running, our system will learn who is engaging with it and, over time, narrow your audience so you reach more of the right people."[5] Meta will also target ads based on users' behavior on the platform, such as whether they have engaged with similar ads in the past. Thus, users most susceptible to engaging with and responding to scam ads will receive more of them.

51. As with creating ads, Meta is not merely executing the wishes of advertisers who have chosen their target audiences. Meta has developed and deploys extremely sophisticated, highly engineered generative AI models, trained on and powered by its massive data collection, to identify the users most likely to be moved to action by any particular ad—including scam ads.

52. Meta delivers ads through an auction system that is not merely a pricing mechanism, but a means of boosting the sale and distribution of ads that maximize users' expected engagement. Meta runs an instant auction every time there is an opportunity to show an ad—when a user opens Facebook or Instagram or scrolls through the user's feed. Each ad that targets a group that includes the user enters the auction. Ads with the highest total value score "win" and are offered to the user in a ranked order that Meta assigns.

---

[5] In the same vein: "You decide who sees your ad and where. Create the online audience based on the traits of who you want to see your ad, and narrow down your ad's audience by interests, gender or location and use ad targeting to find the people most likely to take action. Once your ad starts running, our system will learn who is engaging with it and, over time, narrow your audience so you reach more of the right people."

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

53. An ad's score or ranking is based on:

- The advertiser's bid for specific results, such as the user clicking on the ad or purchasing the advertised good or service. The advertiser can set the bid manually or can rely on Meta's automated system to optimize its bid;
- Estimated action rates, or Meta's prediction of how likely a specific user is to take the advertiser's desired action based on user feedback. Thus, a fraud or scam ad that is likely to entice its audience into a sale is more likely to be shown;[6] and
- Ad quality or user value, which measures how engaging and high-quality the ad is.

Thus, if a user is eligible to see a clothing ad, a mortgage ad, and a scam investment ad, Meta will evaluate the available ads and predict how likely the user is to engage with each one, delivering the most engaging ads first.

54. According to an internal record, as of 2025, advertisers pay between [redacted] per click for ad placements.

55. Meta's ad auction facilitates fraud by design in two important respects. First, as noted above, by favoring highly-engaging ads, Meta puts a thumb on the scale in favor of ads employing the hallmarks of fraud—a false sense of urgency (limited-time or limited-supply offers, for example), highly attractive returns (10% weekly investment returns) or celebrities (often impersonated). [redacted] As one Meta employee noted, these auction adjustments "[redacted]."

[6] Complaints are likely to dampen an ad's score, but the fact that many consumers will not report fraud undermines the effect of this factor.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

56. Meta designs and implements an algorithm to optimize distribution of ads. As described above, based on how an ad performs, Meta automatically adjusts ad delivery to "people who are more likely to interact with it" and reallocates the advertisers' ads purchases to the ads that perform better. Upon information and belief, Meta makes use of its extraordinary collection of user data—obtained through its *quid pro quo* with users—to personalize and target ads to an unprecedented degree.

57. Meta also supplies advertisers with detailed performance analytics showing which audiences generated the greatest engagement, leads, or conversions and enables advertisers to use that information to refine and scale future campaigns.

58. In sum, fraudulent advertisers do not simply upload a finished ad for Meta to distribute. Meta's advertising infrastructure transforms the fraudster's inputs—images, videos, text, budgets, and targets—into paid advertisements and campaigns that Meta both develops and implements. *In short, Meta materially participates in the fraudulent advertising that occurs on its platforms.*

59. Meta's ad-creation and -optimization tools have enabled its platforms to operate as consumer fraud engines on an unprecedented scale. Fraudulent ads depend for their success on appearing legitimate and tailored to the consumer. They are designed to incite action by creating a sense of exigency, emotional manipulation, or enticing results—whether for good health, investment returns, or desired goods. They are built to win Meta's ad race. By improving the appearance of these ads, generating or altering creative elements, and optimizing ads toward versions users are more likely to engage with, Meta's tools also can make fraudulent ads more urgent, persuasive, and effective. They maximize the likelihood that susceptible users will get and act on fraudulent ads.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

### C. Meta Has Long Know that Scam Ads Proliferate on its Platforms

60. Meta recognized—internally—that its ad optimization/distribution system meant that users who engage with fraud ads are more likely to receive more of them. That is true even (in fact, especially) when [redacted], according to a Meta internal analysis:

a. [redacted]

b. [redacted]

c. [redacted]

In other words, earlier or contemporaneous engagement signals (when a user interacts with an ad by clicking it, dwelling on it, viewing the linked website, or commenting on it) are treated as positive signals that prompt Meta's ad delivery system to serve that user more similar ads. [redacted] and thus the user continues to receive similar (fraudulent) ads.

61. For a number of Meta's users, [redacted]

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

62. In early 2023, Meta acknowledged that [redacted]

63. A Pulitzer Prize winning series of articles by Jeff Horwitz described, based on Meta internal documents and sources, an "epidemic of scams," which Meta knowingly facilitated and tolerated." According to Reuters' coverage, Meta projected in 2024 that revenue from ads for scams or restricted goods would account for about 10% of Meta's annual revenue, or $16 billion.[7] Meta also knew that it showed users an estimated 15 billion ads showing signs of fraud *every day*. Ads that "present higher legal risk" (such as those that impersonate a consumer brand or public figure) alone yielded $7 billion in annual revenue for the company.

64. An April 2025 internal presentation by Meta integrity personnel titled [redacted] acknowledged [redacted] According to [redacted] affecting [redacted], and found that [redacted].[8] Moreover, Meta found that in [redacted] of the Meta-involved scams, [redacted]:

[7] According to the article, while Meta spokesman Andy Stone called the 10% figure "overinclusive," he "declined to provide an updated figure."
[8] As noted in the presentation, [redacted]

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

65. The presentation continued: In addition,

**Figure 2**

66. Reuters' reporting also described that:

a. Ads for fraud and scams are so prevalent and effective that, between 2023 and 2024, Meta's platforms are reported to have accounted for almost half

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

of all scams on the payment platform Zelle involving JPMorgan Chase customers.

b. As of at least late 2024, Meta permits companies between four and 32 strikes for financial fraud before they are prohibited from advertising on the platform. "High Value Accounts" were allowed more than 500 strikes.

c. Meta estimated that regulation in Europe and Britain that would hold Meta responsible for consumers' losses from scams would cost the company up to $9.3 billion—a measure of the magnitude of scams on its platforms.

67. In fact, Meta internal documents reveal that Meta actively discouraged employees [redacted] (emphasis added). Once again, Meta chose the path that ensured that it protected its revenue, rather than its users.

68. Data from other countries confirm that this is a Meta-wide problem. In Britain, the Payment Systems Regulator found last year that Meta's platforms were involved in 54% of all payment scams in 2023, with "a devastating impact left on victims."

69. Litigation against Meta has provided additional insight into the extent of this fraud. In a class action recently filed against Meta in the Northern District of California, plaintiffs alleged that scammers in China used the name and image of a senior Bank of America executive and Meta's Ad Manager tools to create and distribute ads on Facebook and Instagram that lured users into scam stock trades on WhatsApp. The ads, which plainly violated Meta's published policies,

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

promised daily returns of 30% to 40%. Investors claimed to have lost more than $300 million, all told.

70. In denying Meta's motion to dismiss, the Court summarized the role of Meta's Ad Manager:

> If a user [advertiser], for example, tells the tool that he is interested in an ad promising astronomical weekly investment returns, Advantage+ Creative will spin up a slew of ads that include the provided language and other language, images, and videos it decides will be effective in promoting the user's chosen message. In fact, a journalist from Reuters ran an experiment in which he told Advantage+ Creative that he wanted an ad asking users if they were "interested in making 10% weekly returns." Advantage+ Creative generated a slew of ads saying just that *and* new ads with language like "Tired of living paycheck to paycheck? Break the cycle and start earning weekly income with our proven system." The reporter did not come up with that (patently fraudulent) language; it was all Meta. (internal citations omitted; emphasis in original).

71. The Court also cited examples of ads that were so facially fraudulent that Meta must have been aware of their content. For example, the Court observed that the below ad promises "*daily* potential returns that are roughly three to four times the average *annual* return of U.S. equity markets, all for free. Even a cursory look would warrant suspicion that the ad is fraudulent. Meta cannot, with a straight face, claim otherwise."

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

**Figure 3**

### D. Despite its Public Representations, Meta's Leadership Chose Not to Aggressively Address Ads for Frauds and Scams on Its Platforms

72. The more ads Meta sells and the more users engage with those ads, the more money Meta makes. In fact, according to a document reviewed by Reuters, Meta estimated potential fines of up to $1 billion as "the cost of any regulatory settlement involving scam ads," which was negligible next to the $3.5 billion Meta would earn every six months from scam ads.

73. To provide just one example, Meta--internally—identified [redacted]

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

[redacted] In roughly five weeks in December 2025 and January 2025, these [redacted]

74. While Meta continued to make billions from scam ads, it treated scams as a low priority for enforcement. Reuters cited to a "lack of investment," at least as of 2022, and a shift to automated tools to identify fraudulent ads, which resulted in a nearly 50% drop in scams that Meta was able to review on Facebook Groups. While the article notes that resources were shifted to concerns like human trafficking, Meta's trillion-dollar market capitalization does not require a this-or-that trade-off in keeping its users safe.

75. In early 2023, Meta acknowledged the impact of ongoing layoffs on its scam enforcement, instructing teams, according to another internal document reviewed by Reuters, to do what they could to "keep the lights on." [9]

76. Following an October 2024 memo to prepare for a meeting with Meta CEO Mark Zuckerberg, it was decided, according to Reuters' coverage, that Meta would "act only in response to impending regulatory action."

77. In 2025, Meta was willing to [redacted] as a result of curbing fraudulent ads.[10] Its advertising "[redacted]" protected Meta's profit metrics—not Meta's users. Meta laid out that it would [redacted]

[9] Meta's spokesperson acknowledged layoffs but claimed that enforcement staff had been added in recent years.

[10] Meta spokesperson Andy Stone did not deny the figure but offered that it came from a "[redacted]"

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

78. Meta—privately—published the "Scammiest Scammer" of the week, acknowledging the most egregious advertisers. When Reuters checked five of those accounts, two were still active six months later.

79. The weekly scam shout-out highlights the failings in Meta's ad enforcement and the disparity between its public statements and its internal efforts and knowledge. In particular, Meta acknowledged that [redacted]:

- Episode 2 of the Scammiest Scammer detailed an advertiser that ran a [redacted] DPA is another Meta advertising product that generates different ads for different users based on their online interactions. Meta recognized that [redacted]. Internal comments described this [redacted]
- The scam featured in Episode 3 targeted Brazilian users with pages [redacted]
- Episode 5 analyzed a [redacted]

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

[redacted]

- As described in Episode 7, in September 2023, a single user [redacted] because Meta policies permitted it to "[redacted]" (emphasis added). Because Meta protected this advertiser's account from removal, it was allowed to spend [redacted].

- Episode 9 detailed an ad account engaged in "[redacted]"

80. Despite having this detailed insight into the deficiencies in its enforcement policies and efforts, Meta did not disclose these gaps to consumers, continued to falsely portray the efficacy of its advertising policies, and failed more broadly to disclose the known, unaddressed prevalence of scam ads on its platforms.

81. Perhaps because of its understaffing, according to the same Reuters report citing a 2023 document, Meta ignored or erroneously rejected 96% of the 100,000 valid fraud reports it received from users each week. Meta aimed to reduce its misses to 75% of reports. The same Reuters article described a military recruiter whose hacked account was used for a crypto scam.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

She and others reported the fraud more than 100 times, but by the time Meta responded, four of her colleagues had been scammed.

82. Internally, Meta identified military impersonation scams as a [redacted] According to a Meta document, the [redacted] Yet, in 2022, Meta [redacted] Meta claimed that it was [redacted]

83. [redacted] Meta's guardrails seemed to work to protect its revenue, not its users.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

84. Likewise, Meta has erred on the side of protecting fraudulent advertisers, rather than consumers. Meta acknowledged—internally—that deploying [redacted]. In other words, Meta set an extraordinarily low tolerance for false positives: the company required that [redacted] could be legitimate businesses wrongly caught in the crossfire**.** In drawing this line, Meta chose to tolerate a massive volume of scams reaching its users to avoid inadvertently removing even a [redacted] share of legitimate advertisers.

85. According to reporting, at lower levels of confidence that an ad was fraudulent, Meta merely charged a premium for the ad instead of removing it. While higher prices may sideline or shrink the distribution of some fraud ads, Meta *chose to allow* and aid the substantial volume of fraud ads that continued to reach its users. Rather than categorically rejecting these ads, as its policies and public statements indicated it would, Meta put consumers at risk while its fraud surcharge fed its bottom line, replacing some of the revenue from lost ad sales.

86. Reuters reported the example of Beijing Tengze Technology Co. Ltd, which was one of Meta's top 200 advertisers, alongside blue-ribbon companies such as American Express. (See discussion of China ads below.) Meta determined that more than half of Beijing Tengze's ads violated its ad rules. Had Meta conducted even the most rudimentary investigation, it would have found, as Reuters did, that Beijing Tengze's address "did not exist." But rather than bar Beijing Tengze's ads from its platforms, Meta charged Beijing Tengze a premium for its ads; rather than stopping these scams from proliferating, Meta chose to profit—even more—from them. According to Reuters, the principal owner of Beijing Tengze controlled another Facebook and Instagram advertiser, the address for which led to a vacant office that had been vacated after the company failed to pay rent. That company publicly posted job listings that indicated it would

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

prioritize candidates with experience distributing black-market goods in Europe and the United States.

87. In addition to knowingly permitting fraudulent advertisers, Meta chose to remove only the specific ads it identified as fraudulent, rather than consistently fanning out to remove similar ads or all ads from the same advertiser. Thus, the same (or nearly identical) scam ad continued to run even after one version was removed. Meta has the tools to identify ads that are identical or similar to ads it removes and can enforce its policies at the level of bad actors, not just bad ads, but chooses not to deploy these tools against scam ads.

### E. Meta Refused to Implement Advertiser Verification Despite Knowing it Would Dramatically Reduce Scam Ads

88. In April 2020, Google announced that it would begin requiring that advertisers verify their identity by providing "personal identification, business incorporation documents or other information that proves who they are and where they operate. Beginning this summer, users will start to see disclosures that list this information about the advertiser behind the ads they see."

89. As Google also explained at the time, "This change will make it easier for people to understand who the advertiser is behind the ads they see from Google and help them make more informed decisions when using our advertising controls. It will also help support the health of the digital advertising ecosystem by detecting bad actors and limiting their attempts to misrepresent themselves."

90. Meta acknowledged—internally—that Google's rules "[redacted]." Elsewhere, Meta acknowledged [redacted] and that, while Google accounts were [redacted]

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

[redacted] In a 2022 presentation, Meta identified its deficiencies in comparison to Google: [redacted] In contrast, "[redacted]"

91. Meta's advertiser verification program is voluntary and fee-based. Except in limited circumstances, even now, an advertiser can open an account and place ads on Meta's platforms by providing an email or phone number, a name, and a birth date. Meta does not require documentation of the advertiser's business or location. In the absence of verification requirements, not only can a scam advertiser open for business quickly and without barriers to entry, but a banned advertiser can reappear in the time it takes to provide a new email address or phone number.

92. Meta knew that advertiser-verification requirements had reduced scams [redacted] in markets where they were implemented and that the same requirements could be implemented in other markets in as little as four to six weeks.[11] Meta also observed that [redacted] Meta also knew that its limited or targeted enforcement efforts (as opposed to

[11] However, ads were not eliminated, but relocated: [redacted]

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

universal verification) would not impact its revenue because "[redacted]"

93. According to internal documents reviewed by Reuters, Meta estimated that it would cost $2 billion to implement advertiser verification—just over 1% of Meta's advertising revenue.[12]

94. Verification would have an even bigger impact on Meta's revenue. Responding to Reuters' report that verification would [redacted] and [redacted]. In the same document, Meta estimated that approximately [redacted].

95. This was not far from other internal estimates. In 2022, Meta observed: [redacted]

96. Meta had encountered problems with fraudulent political ads in the 2016 presidential election. Meta subsequently informed Congress that Russian-sponsored trolls buying ads with rubles were able to impersonate Americans and spread disinformation. In the wake of the election, Meta implemented "know your customer" rules for political ads, which required a

[12] Internally, Meta did not [redacted].

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

verified U.S. address and identification and made the advertiser's details visible to viewers. The same fix was not applied to other ads.

97. After Google's announcement that it would verify all advertisers, in 2018-2019, Meta [redacted]. Meta planned to announce its commitment to universal verification of advertisers but then pulled back. In an internal review of the Reuters article, Meta acknowledged that [redacted] Meta internal documents waffled between [redacted] Meta employees also pushed the company to [redacted] as well. This was despite the fact that the [redacted]

98. Instead of universal verification, which Meta rolled out in certain smaller markets, [redacted]—though the State easily identified scam ads in these areas. While Meta also [redacted]

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

99. In contrast to its public representations about its aggressive actions to prevent fraud, Meta chose to leave one of the most effective—and revenue-disruptive—options on the table.

### F. Meta Continued to Serve Known Scam Ads from Lucrative China-Based Advertisers without Adequate Safeguards to Protect Consumers

100. Meta's decision to accept unverified ads from China (or "GCR," Greater China Region) also contributed to the high prevalence of fraud on its platforms. According to Reuters, 10% of Meta's revenue, or $18 billion in annual sales, stems from ads by businesses in China. But, by early 2024, Meta had identified scammers in China as also a particularly significant source of scams on Meta platforms. [redacted]. Even more concerning, [redacted]

101. According to an internal Workplace post from December 2025, China "planning" or ad agencies, which bought or placed ads for China businesses, [redacted] Meta had found that [redacted]. But for reasons that are not explained, [redacted]

102. China planning agencies—many of which are recommended by Meta as "badged partners"— immediately pass go and never land in jail. They skip Meta's enforcement reviews and can instantly access an unlimited ad spending limit, enabling them to quickly advertise at a massive scale—facts that Meta nowhere acknowledges in its advertising policies, transparency webpages, and blog posts. Meta pays a commission to the ad agencies for the ads purchased by

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

their clients and protects them from enforcement. For instance, as described in [redacted], Meta applies a [redacted], which means that Meta does not remove agency ads that its automated review identifies as potentially fraudulent unless a human reviewer—if available—confirms that the ad violates Meta's policies. In the meantime, the flagged ad remains on Meta's platforms.

103. Ad agencies in China like Blue Focus blatantly market their availability for such purposes, advertising that it provides access to "whitelisted" accounts that can "scale your advertising efforts on Facebook without limitations or the risk of being banned." Blue Focus promises that its ad accounts "can bypass the new account approval process. You can start running ads immediately without the usual waiting period associated with standard accounts." The agency openly promotes its ability to work around Meta enforcement: "If your Facebook Agency Ad Account is disabled, we will immediately work with Facebook to appeal the suspension and account. … For cases of permanent disablement, we will promptly allocate your budget to another account so you can continue advertising without wasting time waiting." This is confirmed by Meta's own recognition among GCR ads of "[redacted]"

104. Likely scam ads placed by Blue Focus, such as the one below, continue to appear on Facebook:

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

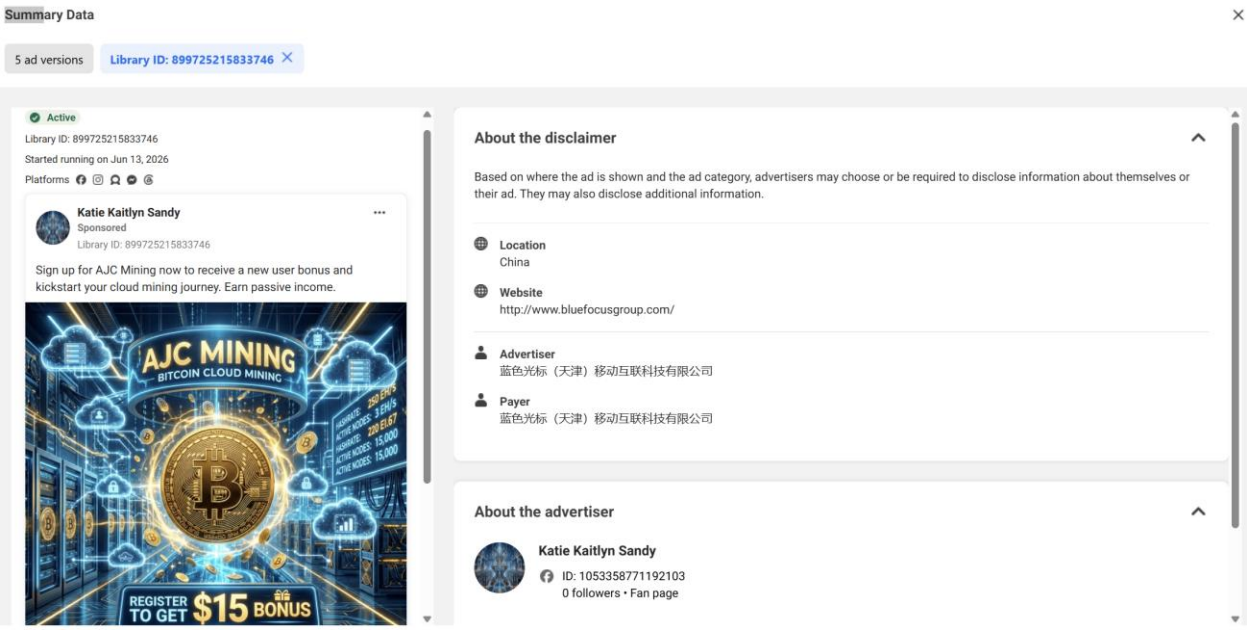



**Figure 4**

105. Moreover, an Integrity review from October 2024 documented that Meta still had "[redacted]" The presentation also identified difficulties "[redacted]." Additional issues known to Meta at the time making advertisers in China particularly dangerous for its users included "[redacted]."

106. It is therefore no surprise that, [redacted]

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

[redacted] There were also ongoing enforcement deficiencies. [redacted]

107. In fact, Meta knew that its policies and enforcement with respect to ads originating in China facilitated consumer fraud. A March 2025 report by an outside consulting firm, [redacted] confirmed the "[redacted]" arising from "[redacted]"

108. In the below slide summarizing "[redacted]" which, as Meta knew, makes it easier for scammers to bypass Meta's detection.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

[redacted] [13]

**Figure 5**

109. [redacted] concluded that "[redacted]." Another slide in the report compared [redacted]:

[13] "SMB" refers to small and medium-sized businesses.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

**Figure 6**

110. For businesses, participants surveyed by described using (all of which are possible because of Meta's lack of advertiser verification), . The presentation concluded that " " Notes related to meetings between and Meta expressly acknowledge that Meta had

111. Indeed, recognized that the core of the problem was Meta's decision to allow

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

112. also provided Meta This is a marked contrast with Meta's claim of aggressive enforcement.

113. Meta also acknowledged—internally—that 's assessment recognized that Meta was more than . In an internal chat assessing the Reuters' article, Andy Stone, Meta's Vice President of Communications, acknowledged that

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

114. A follow-up research note from May 2025 likewise confirmed [redacted]:

[redacted]

**Figure 7**

115. Per Reuters, Meta created a special team to focus on fraud originating in China. It worked—for a time. [redacted] According to Reuters, "As a result of Integrity Strategy pivot and follow-up from [Zuckerberg]," the team that carried out that work was directed to pause its efforts and was eventually eliminated.

116. According to internal documents reviewed by Reuters from the same time, Meta identified 800 Chinese advertising accounts that had generated $28 million in ads that violated Meta's rules in a single month—75% of which were from Meta's trusted or badged partners. Yet Meta declined to enforce against the ad agencies on the ground that "the revenue impact is too high." While Meta ultimately shut down a fraction of the worst actors, which were responsible for just $2.8 million of the harmful ads, Meta expected that the scammers would re-appear through other accounts, so it was "likely" that even that "revenue will return."

117. When Meta chose to under-enforce against fraud ads and to permit advertisers from China to operate in a framework that fostered scams, it not only allowed those ads to be posted to its users, it processed those ads through its optimization machinery, shaping and directing them in

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

a manner *designed* to increase the likelihood that those ads would ensnare Rhode Island and other consumers.

118. To be clear, this Complaint does not seek to hold Meta liable for its failure to remove content created by third party, scam advertisers. Instead, the State seeks to hold Meta responsible for the gap between Meta's public statements regarding its treatment of fraudulent ads on its platforms and its internal knowledge about its advertising ecosystem that Meta knowingly hyper-charged through its design, distribution, and optimization tools and Meta's own conduct in facilitating fraudulent ads.

**G. Meta Subverted and Ignored Regulators and Enforcement Authorities**

119. Meta not only aided and concealed the prevalence and efficacy of scam ads on its platforms, but it actively worked to conceal its conduct from regulators and undercut requirements to safeguard consumers. As Reuters reported, Meta drafted and implemented a "global playbook" that laid out steps to disarm regulators and dodge verification requirements. "Beginning one year ahead of expected regulation, the playbook advises, Meta should tell the local regulators it will create a voluntary verification process. When doing so, the documents add, Meta should ask those authorities for time to let the voluntary measures play out. To buy yet more time, and further gauge reactions from regulators, after six months, Meta should agree to verify 'new and risky' advertisers, the playbook continues." Meta acknowledged this as "[redacted]" Regardless of its timing, Meta's strategy was to do just enough to avoid regulation, but not to protect its users.

120. In lieu of regulation, Meta announced an Industry Accord Against Online Scams and Fraud. In a March 2026 public post, Meta described the compact as a

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

"landmark voluntary agreement … to combat the escalating global threat of online scams." Meta explained: "Our work to combat scams focuses on strengthening defenses on our platforms to stay ahead of scammers." Meta promised consumers that it would provide warnings and employ advanced scam detection, and promoted its investments to stay ahead of the curve on fraud:

> Scammers are constantly evolving their tactics — and so are we. Every day, criminals use increasingly sophisticated measures to defraud people on our platforms and across the internet. That's why we're announcing new investments in advanced AI, tools for people to spot and avoid scammers, and partnerships with law enforcement and industry peers for offline enforcement.

121. [redacted]:

[redacted]

122. In November 2025, US Senators Hawley and Blumenthal called on FTC and Securities & Exchange Commission to investigate Meta for its "facilitation of and profiting from criminal investment scams, fake government benefits schemes, deepfake pornography, and other fraudulent activities." The Senators pointed out that, despite Reuters' coverage, "[e]ven a short review of Meta's Ad Library at the time of this letter shows clearly identifiable advertisements for illicit gambling, payment scams, crypto scams, AI deepfake sex services, and fake offers of federal benefits, advertisements that often falsely appear to link to legitimate sites. Further, despite the company's rules against nudity, advertisements for pornographic and sexually explicit material, and which often lead to malware, are widespread on Meta's products." (citations omitted).

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

123. In the wake of the Reuters coverage and other public calls for change, Meta announced a handful of actions to address scammers on its platforms. However, the underlying engine creating and powering scam ads has not changed and continued evidence of scam ads confirms that the problem persists, as described below.

### H. Fraud Ads Remain Widespread on Meta's Platform, Contradicting its Public Representations

124. Even now, Meta continues to generate and distribute ads that show the hallmarks of fraud involving investment opportunities, cryptocurrency, and health cures, among others, and violate Meta's ad policies, as the Attorney General's Office found.

125. This occurs despite Meta's policies against ads offering investment opportunities "where returns on investment are guaranteed or risk-free"; "where returns on investment or compensation is partly or fully based on recruitment of others to participate in the scheme"; that offer "opportunities of unrealistic financial reward for unclear or minimal effort"; that claim "quick returns" or the opportunity to "get rich quick,"; or that claim a small investment can be turned into a large amount through "flipping" or a "trick."

126. Moreover, while specific ads may be removed, others quickly reappear, capitalizing on Meta's low barriers of entry and reaching consumers in the interim.

127. The examples below are just that—examples—and the State found many comparable examples.

128. For example, the ad below has dozens of active versions in Meta's Ad Library:

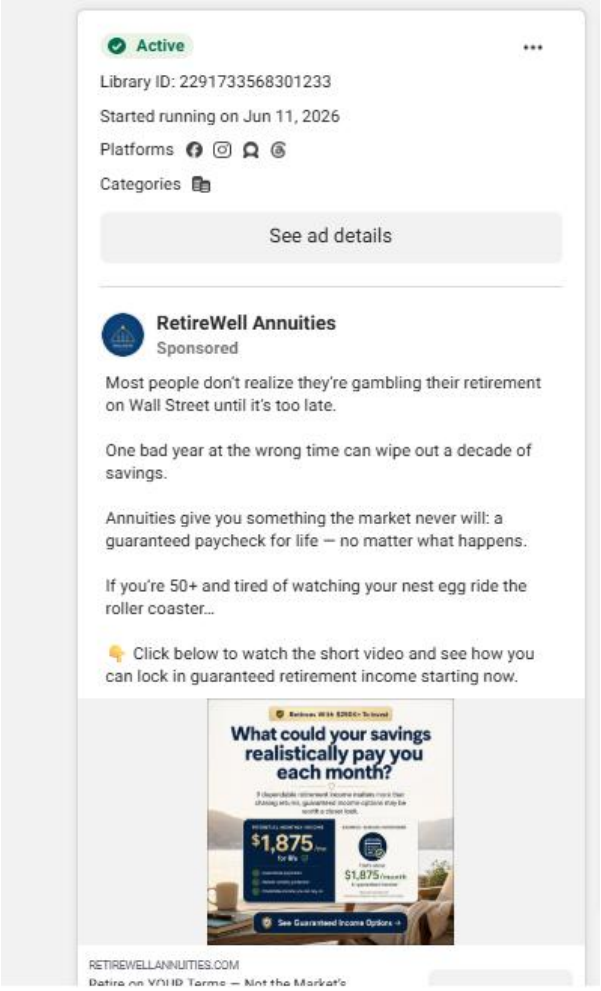



**Figure 8**

The ad promises to "Turn your savings into guaranteed lifetime income. 💰 Fixed & indexed annuities | Tax-deferred growth | Zero market risk." The phone number provided is fake—and is even used on government websites as an example of how to spot phishing emails.

129. The ad below for an AI trading technology leads to a website with a "limited time offer" of a license for $397 and highlights a graphic suggesting continuous profits.

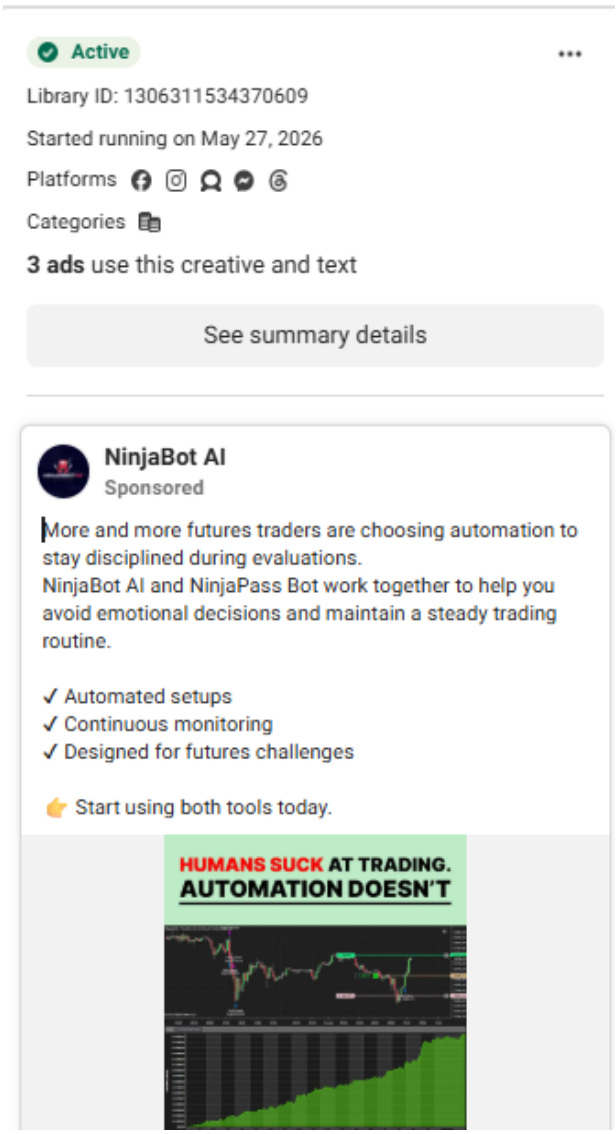



**Figure 9**

Reddit posts indicate that the advertiser uses WhatsApp, Telegram, and dating sites for viral advertising, another red flag. Other consumers complain that they have not been able to withdraw money they invested.

130. The ad below for "Aicommerce" suggests multi-level marketing, promising training on AI services, which can then be marketed to businesses, in return for a large up-front investment. The advertiser claims to need to work only 4-hours a day from Italy and to have grown his wealth from nothing to $6 million.

**Summary Data**

**2 ad versions**

**About these ads**

Advertisers often use the same image or video and text to create ad campaigns with different start dates, locations or budgets. This section contains the collective data for **2 ads**.

**2 ads** Any filters you applied to the search results are also applied to this group of ads. To adjust the filters, go back to the search results

Active

Library ID: 3129154663946288

Started running on Jun 22, 2026

Platforms

See ad details

**Peter Szabo of Aicommerce**
Sponsored

$0 → $6M in 12 months.

That's how much my AI company made last year.

But honestly? The revenue isn't even the best part.

The best part: I work ~4 hours a day, and I'm writing this from Italy, where I'm spending the next two months with my family.

And right now, my team and I are building these exact same semi-passive, cash-flowing AI mini stores for everyday people — done-for-you in the next 30 days.

The vast majority of our clients started out as burnt-out corporate employees grinding 60+ hours a week just to get by.

They went to college. They're not technical. Most of them figured they had no shot at building anything real online.

Active

Library ID: 819879231059074

Started running on Jun 22, 2026

Platforms

See ad details

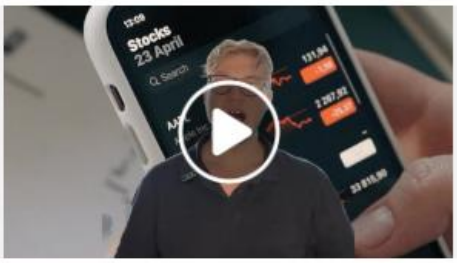
**Peter Szabo of Aicommerce**
Sponsored

$0 → $6M in 12 months.

That's how much my AI company made last year.

But honestly? The revenue isn't even the best part.

The best part: I work ~4 hours a day, and I'm writing this ...




VIDEO.AICOMMERCE.CO
$0 - $500K/mo with AI

Learn more

**Figure 10**

One review of Aicommerce describes a consumer's experience:

> Aicommerce / Leadevo / Fanbasis is a multi-layered corporate shell game run by Peter Szabo. They hide behind a fake 90-day refund guarantee and then move the goalposts. In their reply to my previous review, they actually claimed that investing $12,000 OVER 5 MONTHS was "insufficient spend" to hit their advertised promises of $29,000 a month. They run your credit card under completely different company names (like Fanbasis) so you can't track the billing, forge accounts in your name to fight bank disputes, and then blame the victim when their system fails. Total scam.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

131. Wealth Automators claims to allow consumers to set up Amazon, Wal-Mart, TikTok, and eBay stores that "sell on autopilot through AI automation." The ad text promotes an investment opportunity for those with "$25,000+ in Liquid Capital" who want "Stable, Reliable Income." It's simple, the ad assures consumers: "You invest, we do EVERYTHING else." An accompanying video ad sets the price of the "investment" at $35,000 and promises that consumers will not be billed until their stores become profitable. The FTC has taken enforcement action against similar fraudulent schemes.

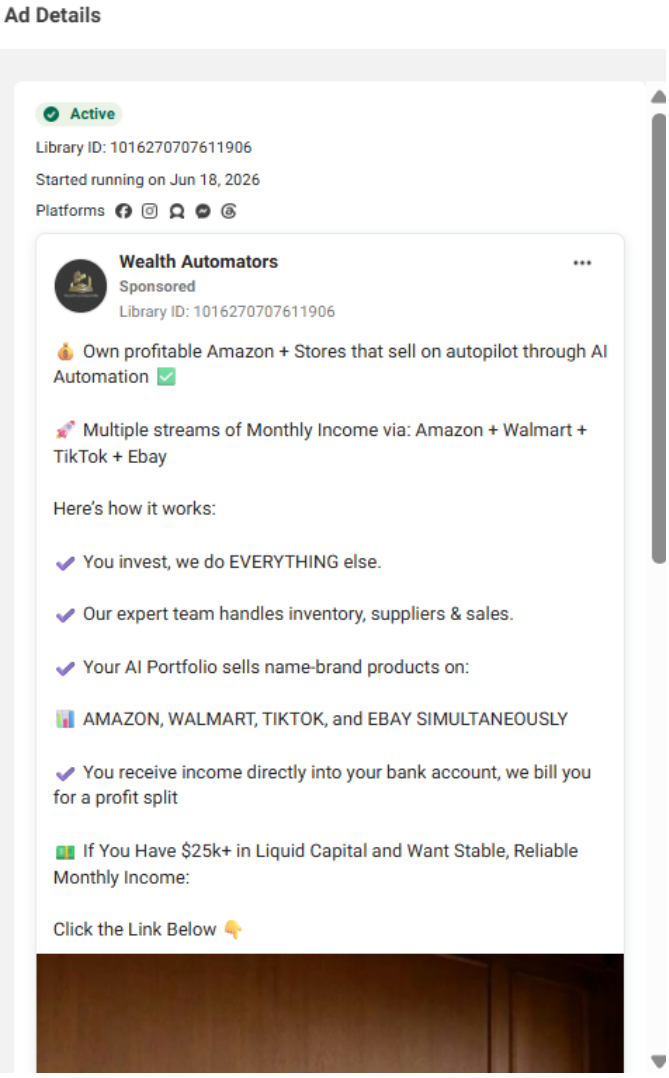



**Figure 11**

132. An ad featuring an image of Elon Musk above the New York Times logo promoted the opportunity for $31,000 in returns in one month through "Elon Musk's New Investment Platform," which was tested by the "NYT News Team."

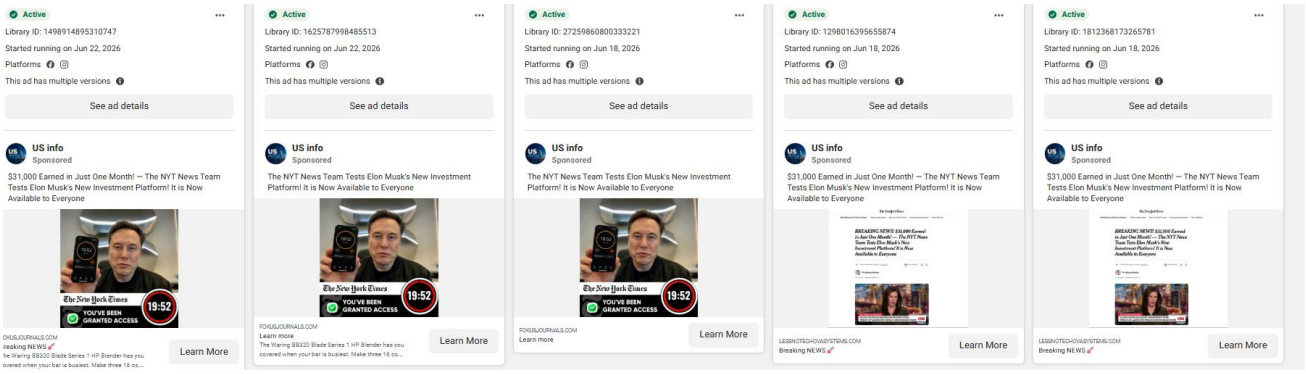



**Figure 12**

The URL address directed consumers to commercial sweepstakes or marketing links.

133. An ad for Maga Vault, five versions of which appear in the Meta Ad Library as running since July 7, promotes "Trump gold bars" using a deepfake video of the President urging viewers to buy and warning that supply is running out:

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

**Figure 13**

This ad has between 350,000 and 400,000 impressions, including, upon information and belief, consumers in Rhode Island.

134. The Attorney General's investigation also found numerous ads violating Meta's ad policies for health and wellness advertising or that otherwise showed signs of fraud. The ad below, for example, promised to reverse Alzheimer's in 45 days. This contravenes Meta's representation that it does not "allow advertisers to run ads" that include claims "to cure, heal, or eliminate … incurable diseases" including Alzheimer's.

**Figure 14**

135. There were more than 2,000 versions of this ad active in the Meta Ad library. They used fake references to CNN Health or 60 Minutes and impersonated celebrities including Meryl Streep (above), Morgan Freeman, Dolly Parton, and Dr. Oz to promote a "honey and cinnamon" cure to Alzheimer's. The ads trace back to a much smaller network of Facebook accounts and URLs. The comments are clearly fabricated and are included in identical threads, and the same names and wording appear across the distinct ads. Yet these ads proliferate on Meta's platforms.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

136. Many ads also violate Meta's prohibition on ads that "[e]mploy clickbait tactics in a health ... context, such as sensational language with exaggerated or extreme claims ...." For instance, the below ad encourages consumers to ignore a doctor's recommendation to start dialysis, noting that the author, with stage 3 kidney disease, refused dialysis despite being told by her doctor that she was "Playing Russian Roulette with Her Life."

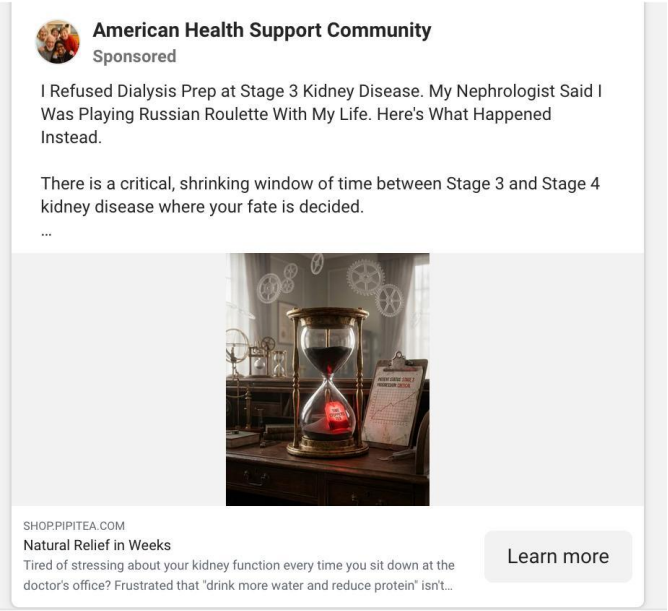



**Figure 15**

137. Another ad similarly urges consumers to ignore medical advice, instead touting the use of "Height Gummies" that caused a teen to grow 4 inches:

Active

Library ID: 2259679131525198

Started running on Jun 16, 2026

Platforms

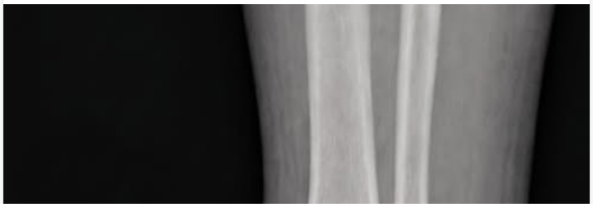
This ad has multiple versions

**Youth Growth Finds**
Sponsored
Library ID: 2259679131525198

My son's height was 5'6" at age 15. Dr. Martinez didn't ask if I wanted a specialist referral. She told me. "We're referring to endocrinology. Today. Your previous doctor should have done this two years ago."

Dr. Patterson's retirement letter came on a Tuesday.

Standard form letter. "After 32 years of practice, I'm stepping away ...



No Fillers. No Random Nutrients. Pediatric Growth Specialist Formulated.

Research-grade framework. Exact specifications used in adolescent growth studies. Nothing added to cut costs. Everything mapped to bone building, hormone production, sleep optimization, immune support, or activation.

Try Treunil Height Gummies for 60 days.

👉 https://treunil.com/products/treunil

Measure your son weekly. Same wall. Same time. Same method.

If you don't see growth - if you're not satisfied for any reason - full refund. No questions asked. Zero risk.

You're being pressured.

Your doctor wants a specialist referral. Maybe immediately. Maybe with threats about non-compliance and documentation.

You have two choices.

One path: Make the appointment. Start the evaluation process. Accept the bone age scans showing plates closing. Watch months pass waiting for appointments. End up on hormone therapy at $30,000 per year or be told it's too late. Just like my nephew. Years of process. Stuck at 5'2" anyway.

Another path: Try a supplement actually formulated with all five systems at clinical doses. Track his height. Bring results to your doctor.

I chose the second path.

Jake grew four inches. His doctor monitors him quarterly. No

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

**Figure 16**

138. Others who have tested Meta's platforms have come to similar conclusions about the pervasiveness of scam ads on them. The Tech Transparency Project ("TTP") examined political ads in Meta's ad library (which are retained for much longer periods than other ads). In an October 2025 report, Meta Awash in Deepfake Scam Ads, "TTP identified 63 scam advertisers who have collectively run more than 150,000 political ads on Meta platforms, spending $49 million." The advertisers, who were often the top political ad spenders on Instagram for various periods in 2025, ran ads targeted at seniors and claimed to offer Medicare or Social Security benefits. According to TTP, "[a]ll of the 63 scam advertisers showed they had ads removed by Meta within the past 12 months for violating the company's policies …"

139. Many of the ads identified by TTP ran in Rhode Island and targeted seniors. One ad sponsored by the Relief Eligibility Center in April 2025 announced: "BREAKING NEWS: Trump's First order in office is to give every American $5,000," urging people to claim the benefit "before the deadline this Sunday at midnight." It showed an image of Elon Musk and a U.S. Treasury stimulus check, followed by a manipulated video of Musk on the Joe Rogan podcast promising $5,000 in "direct stimulus checks."

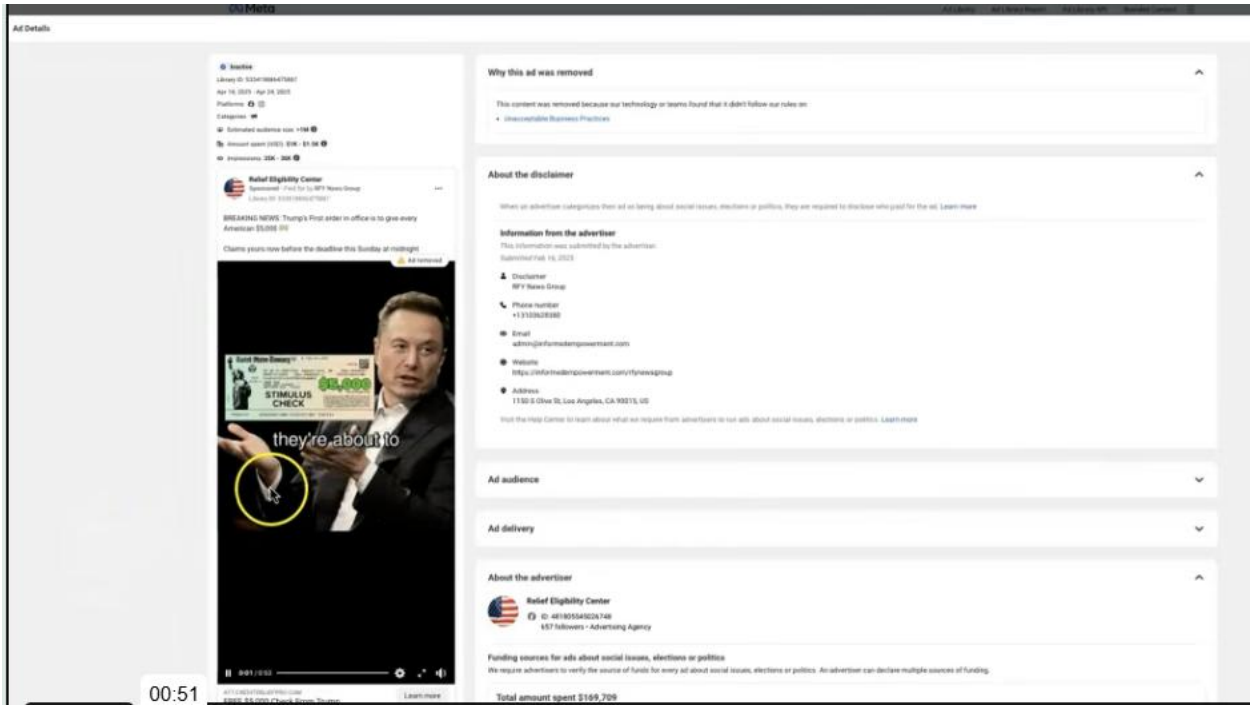



**Figure 17**

As TTP pointed out, no such promise was ever made, and its "act quick" message is a further red flag of potential scams. The ad targeted users 65 and older, including Rhode Island users, contained no disclosure of its AI-generated content, as Meta purportedly requires, and ran for a week before Meta removed it for violating its ad policies.

140. TTP also pointed out Relief Eligibility Center, which has run numerous similar ads, was in the top 1% of Meta advertisers running "social issues, political and election" ads during the 90-period from April 3 to July 1, 2025. The account spent $141,368 on ads in that time frame, outspending corporate advertisers like UBS and Uber.

141. TTP highlighted similar ads also targeting seniors that were distributed to Rhode Island consumers and promoted investment scams. This included ads from America's Secret Fund, Alternative Health Remedies, Patriot Reset, Patriotic Savants, and Smart Patriotic Plays, which ran numerous versions of each ad and collectively spent millions of dollars on Meta ads. All of

these advertisers are tied to Paradigm Press, which identifies itself as part of the Agora Companies. TTP, using the same information available to Meta, noted that Agora was described by *Forbes* as "hawking bad financial and health advice on Facebook," and noted that it had previously been sued by the FTC, Securities and Exchange Commission, and two state attorneys general.

142. Another ad promising a free Gulf of America tumbler, also distributed to Rhode Island residents, led consumer respondents to believe they were only paying for shipping and handling but then enrolled them into a monthly subscription service without their knowledge. The TTP report identifies numerous similar advertisers that peddled schemes to Rhode Island consumers (among others). Some of these advertisers spent more on Meta ads over a several year period than large brands like Walmart or Pfizer. The fraudulent nature of these ads is confirmed, according to TTP, by hundreds of consumer complaints to the Better Business Bureau.

143. A report released in May 2026 chronicled the Center for Countering Digital Hate's ("CCDH") investigation of "How Meta Helps Medicare Scammers Target Seniors." Applying guidance from the FTC, the Centers for Medicare & Medicaid Services ("CMS"), and AARP, CCDH identified 93,779 Medicare scam ads from Meta's Ad Library. These ads also violated Meta's Advertiser Standards on Fraud, Scams and Deceptive Practices, promoting fabricated or misleading "free benefits"; falsely presenting the advertiser as a government entity or implying government endorsement; using fake AI-generated endorsements from politicians or celebrities;

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

and imposing fabricated deadlines for enrollment:

The table below outlines examples of policy-violating ads that were approved by Meta.

| | |
|---|---|
| | **1. Offering 'free benefits' that are fabricated or misleading**<br>While benefits like "grocery cards" or "Flex cards" are genuine Medicare Advantage benefits that apply in certain scenarios, this tactic involves presenting them in a way where key details are misleading or entirely false. Examples include over-stating their value, saying that they can be spent on "anything", that they are available to everyone on Medicare, or presenting them as a government transfer like stimulus checks.[37]<br>🚫 Breaches Meta's policies banning "misleading schemes that promote free products or services".[38] |
| | **2. Falsely presenting the advertiser as a government entity**<br>This tactic involves advertisers falsely presenting themselves as a government entity, including by using official-sounding domain names like "govmedplan.com" or by encouraging people to ring a phone number that is implied to be a Medicare or government call center.[39]<br>🚫 Breaches Meta's policies banning "falsely claiming to represent, or speak in the voice of, an established business or entity, in an attempt to scam or defraud".[40] |
| | **3. Falsely implying the endorsement of government officials**<br>This tactic involves implying the benefits on offer have been endorsed by a politician by presenting the politician or government official as a supporter or creator of the benefit. Ads using this tactic often show the President signing a bill, implying that they've created a new benefit. Some use explicit statements like "Biden approves Flex Card".[41]<br>🚫 Breaches Meta's policy on using "the image of a famous person and misleading tactics in order to bait people into engaging with an ad".[42] |
| | **4. Using fake AI-generated endorsements**<br>This tactic involves creating deepfake videos or deepfake voice impressions of famous individuals such as politicians or celebrities to create fake endorsements. Ads deploying this tactic often depicted politicians such as Joe Biden or Donald Trump to dupe users into engaging.[43] Others depicted celebrities such as Oprah Winfrey, Brad Pitt, Steve Harvey, Ellen DeGeneres or Dave Ramsey.[44]<br>🚫 Breaches Meta's policies on using "the image of a famous person and misleading tactics in order to bait people into engaging with an ad".[45] |
| | **5. Stating fabricated deadlines for enrollment**<br>This tactic involves creating fake time pressure by fabricating a deadline after which 'free' benefits will no longer be available or by saying users must apply before funds run out. While Medicare Advantage plans do technically have specific enrollment periods, this tactic employs arbitrary deadlines, such as claiming viewers "have only 12 hours left" to enroll.[46]<br>🚫 Breaches Meta's policies banning "misleading schemes that promote free products or services".[47] |

**Figure 18**

144. An example of one of the Medicare scam ads shows President Biden describing legislation establishing Medicare Flexible Spending Cards that would provide eligible citizens

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

$2880 to help "pay for your everyday expenses like rent, groceries, and bills." The ad urged consumers to respond "now because the deadline is this Friday and the funds are limited."

| | | |
|---|---|---|
| | "Would $2880 help you pay for your everyday expenses like rent, groceries, and bills? Because of the economy, we just passed this legislation to get Medicare Flexible Spending Cards into the hand of American seniors over the age of 64. All you have to do is call our Medicare Help Centers to find out how you can claim your flex card. Do it now because the deadline is this Friday and the funds are limited."[53] | ✅ Offering 'free benefits' that fabricated or misleading<br>✅ Falsely presenting the advertiser as a government entity<br>✅ Falsely implying the endorsement of government officials<br>✅ Using fake AI-generated endorsements<br>✅ Stating fabricated deadlines for enrollment |

**Figure 19**

145. In all, ads from the top thirty scammers generated "215 million impressions on their ads in the last year, nearly six times as many as all previous years on record" and an estimated $14.3 million in revenue for Meta, "$12 million of it in the past twelve months alone"—belying the contention that Meta has improved its enforcement efforts. Consumers over the age of 65 viewed these ads more than 185 million times. Meta knew about these scam advertisers because it had previously taken down others ads they purchased: "The scam advertisers in our dataset had, on average, 151 ads taken down for policy violations; one had 1,335.… Removed ads were replaced with near-identical copies. Disabled accounts launched new ones."

146. CCDH also explained, as described above, that "Meta's targeting tools allow advertisers to reach specified audiences based on criteria including age. This can work in two ways: they can either set a minimum age 'control' which means that ads will be restricted to a specific age group, or an 'audience suggestion,' which expresses a priority for a certain age group.

CCDH's analysis also revealed that Meta fails to implement its publicly promoted policies regarding its ad standards by initially approving these ads and then failing to "act on ads before they amass impressions and ad spend," "act on content it already found to be violative," and "act on scammers repeatedly violating its policies."

147. Also using data from Meta's Ad Library, CCDH analyzed the state-by-state viewership of ads from the top 30 Medicare scammers. These ads generated 105,886 impressions in Rhode Island, 66,467 of which were by consumers 65 and over.

148. Another research survey, published in February 2026, analyzed more than 14 million ads viewed more than 10 billion times on Meta's platforms in the United Kingdom and European Union. Nearly one-third of those ads (4.5 million), resulting in 304 million impressions, showed red flags of being associated with e-commerce scams, phishing campaigns, malware, and other consumer scams. Half of those ads came from just 10 advertisers, which makes clear that enforcement aimed at even the worst offenders would have a dramatic impact on Meta's fraud ecosystem.

### I. Meta Also Openly Distributed Violating Ads for "Nudification" Apps

149. Nudification apps are deepfake AI applications that digitally undress people (including minors) or create nonconsensual nude images from existing, non-nude images. Because they appear real, they have caused tremendous trauma to their subjects, and they have allowed users to create and distribute illegal content and to sextort their subjects.

150. In June 2025, Meta announced that it was "Taking Action Against 'Nudify' Apps." Meta noted that it had "developed new technology specifically designed to identify these types of ads – even when the ads themselves don't include nudity – and use matching technology to help us find and remove copycat ads more quickly" and that it has "strict rules against non-consensual

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

intimate imagery – whether it's real or AI-generated – including the promotion of nudify apps."

151. Contrary to Meta's public statements, and without disclosure to its users about the proliferation of these ads or Meta's failure to prevent ads for nudification apps, Meta continued to approve ads for nudification apps, permitted them to stay up for substantial periods without detection despite overt signs of their purpose, and allowed them to reappear as identical or obviously similar ads for the same apps even once removed. The State found numerous examples of ads for nudification apps that Meta promoted despite its policy barring such ads. "Try AI Magic Now" offered nude images of young women. Captions promised users could "Create whatever you like, exactly as you please." Others promoted the ability to transform regular images of young women into sexually explicit photos and videos, as below.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

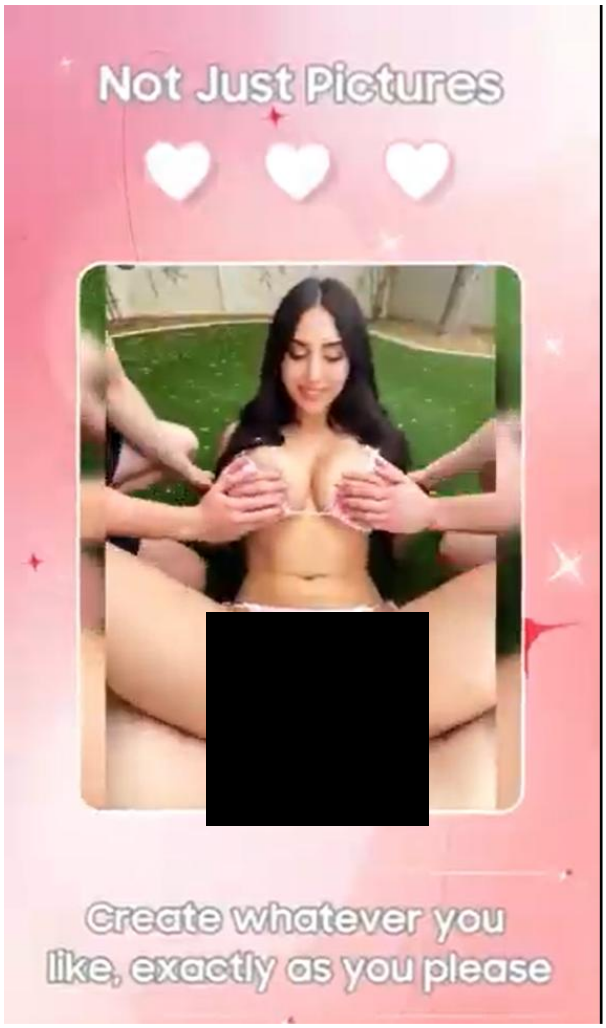



**Figure 20**

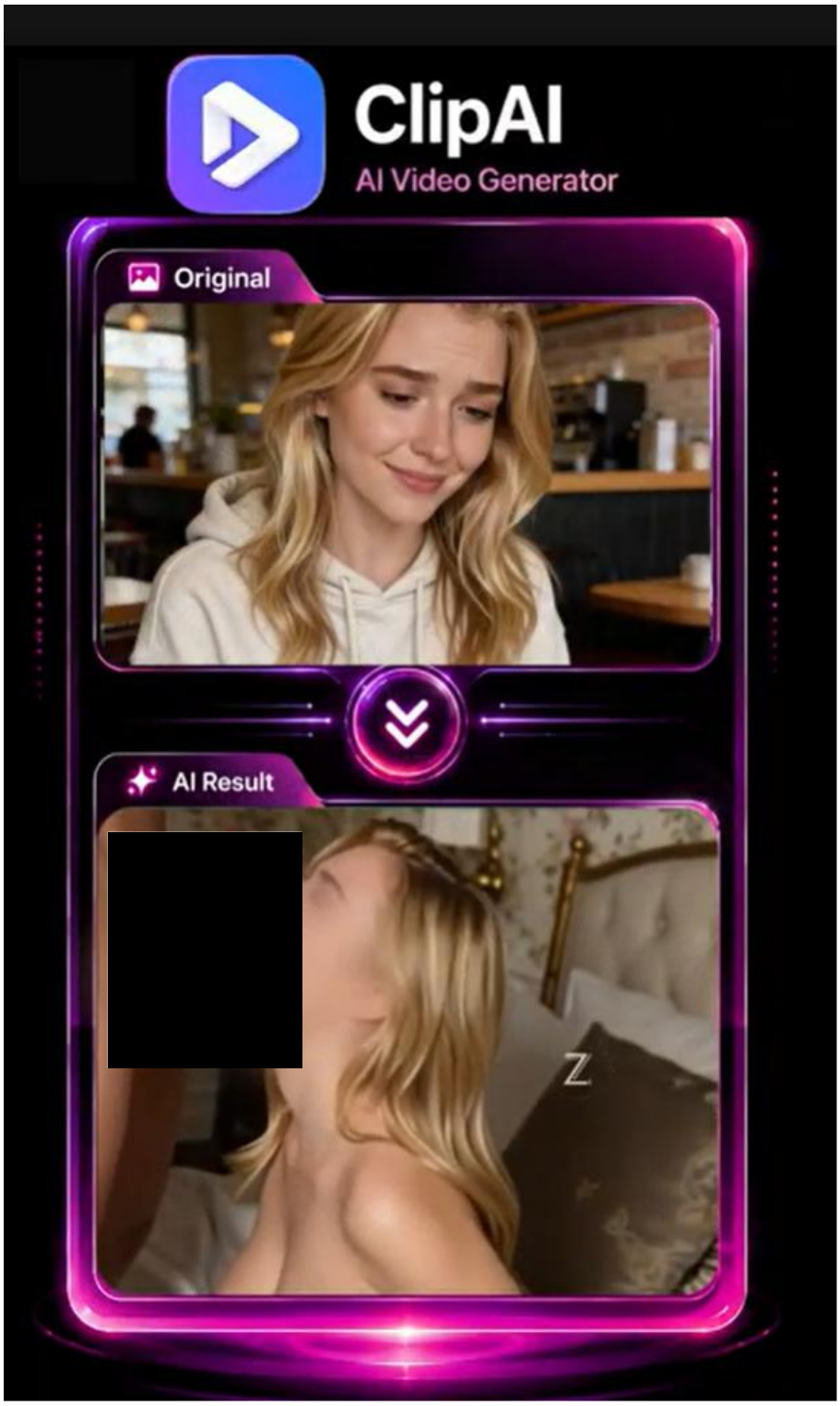



**Figure 21**

The ads ultimately direct the user to an Apple or Play Store URL to download the apps.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

### J. Financial Institutions Warned Meta About the Prevalence of Scam Ads and Urged Meta to Take Action to Rein Them In

152. Meta internal documents acknowledge [redacted] In January 2025, Meta had [redacted] the extent of the fraud on Meta's platforms.

153. In March 2025, [redacted]

154. In providing background on the issue, [redacted] In a separate August 2023 document, [redacted]

155. [redacted]

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

156.

157. Meta's fraud claim rates were , and

[14] A May 2025 document notes

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

[redacted] expected to reject [redacted]. At the end of June, [redacted] estimated that [redacted]. Again, [redacted] In July, [redacted] [redacted] also expressed concern that Meta's plan to [redacted] (which Meta continues to permit) would make it "almost impossible to police imposter ads": "They will need to catch the bad actors at sign-up or not catch them at all."

158. [redacted] had consistently tied the proliferation of fraud on Meta's platforms to its lack of advertiser verification, as well as its failure to act on consumer complaints. In 2024, [redacted] personnel described [redacted] According to the document, [redacted] Nearly a year later, [redacted] complained that [redacted]

159. Over time, [redacted] reiterated its requests, calling on Meta to [redacted]

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

160. [redacted][15]

161. [redacted]

[15] [redacted]

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

[redacted] Indeed, Meta did not roll out more (though still limited) warnings until March 2026.

162. [redacted] (emphasis in original).[16]

[16] [redacted]

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

163. Scammers set up accounts using —the types of ads purportedly banned and removed by Meta. Impersonation, a frequent subject of the concerns raised to Meta, is used to leverage the bank's credibility and build consumers' trust. And while not every impersonating account purchased ads, the same fake accounts (which Meta failed to act on, per below) functioned across ads, messaging, and off-platform payment channels as parts of a connected fraud funnel.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

164. Observing that [redacted] another 2023 document described [redacted]. Even though [redacted]

165. By November 2023, [redacted] concluded that [redacted] and impersonation accounts remained visible [redacted]. Even when [redacted] While [redacted] could use Meta's [redacted]

166. Deficiencies in Meta's ad and account policies and infrastructure allowed these campaigns to proliferate and persist. [redacted]

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

167. Like tried raising these issues directly with Meta. A November 2024 email from Although Yet, in mid-2025,

168. Contrary to Meta's claim that it took vigorous action against fraud on its platforms, in December 2023, Perhaps it should be no surprise that

169. While the presentation noted that the —an apparent reference to Meta's Ad Library.

170.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

[redacted][17]

171. Meta was on notice of similar impersonation frauds affecting other financial institutions. Australian regulators sued Meta in March 2022 and accused Meta of knowingly permitting ads for fraudulent cryptocurrency investments that misappropriated celebrities' identities.

172. A 2024 Wall Street Journal article described how scammers used Facebook ads to impersonate well-known investors and direct victims into WhatsApp groups promoting investment schemes that caused millions of dollars in losses. Investment firm Pershing Square identified more than 90 ads impersonating Bill Ackman, many of which "remained visible for weeks" after being reported. Nine victims sent Facebook a letter documenting 21 reports of fraudulent ads, but Facebook advised them that the ads did not "go against our standards."

173. Mark Zuckerberg described 2023—the year the banks' fraud reports seemed to explode—as Meta's "year of efficiency." As part of that push for "efficiency," Meta dramatically reduced its trust and integrity staff, harming consumers while further enriching the company.

### K. Meta's Knowing Tolerance of False Accounts Helped Propel Scam Ads and Boosted Meta's Profits

174. Meta has repeatedly claimed to have impossibly high numbers of users—numbers in excess of the actual populations in key demographic segments.

175. Meta's own internal analysis has long shown this. A May 2021 internal Meta

---

17 [redacted]

presentation disclosed by the Wall Street Journal found that the tally of Facebook users in their 20s active in a given month "often exceeds the total population of Americans their age," while a related internal study of approximately 5,000 recent account sign-ups found that 32%-56% were opened by existing users. Emails revealed in litigation brought by a class of advertisers alleging that Meta overstated its reach to users also showed that Meta executives were actively discussing this problem in 2017 and 2018, with the product manager responsible for the Potential Reach tool (which estimates the maximum number of unique people within the advertiser's targeting parameters available to be shown an ad) admitting that part of Meta's revenue was "revenue we should have never made given the fact it's based on wrong data."

176. Outside researchers had reached the same conclusion. In 2017, Pivotal Research used Ads Manager to document huge discrepancies in the "potential reach" in young users. Facebook claimed to reach 41 million U.S. 18–24-year-olds and 60 million 25–34-year-olds. That year, census numbers reflect only 31 million and 45 million individuals, respectively, in these age groups. Related research by the Video Advertising Bureau found that Facebook's potential reach exceeded census population in every state and, by even more dramatic numbers, in every major US city.

177. The flagship social science studies of Facebook, published in *Nature* and *Science* in 2023, revealed enormous churn in Facebook's user base, even as the company elsewhere claimed saturation of the U.S. market. That is significant because if everyone is already using Facebook, there would be no need for (or ability for) people to replace departing users.

178. Fake accounts are a key means by which scams are delivered to users. Fake accounts themselves create and buy scam ads and defraud Meta's users. Moreover, fake accounts are used to manufacture engagement, and engagement, per both Meta's ad auction and algorithm,

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

alters the visibility of content or accounts. Fraudsters use fake accounts to promote scam ads and accounts (opening, clicking through, liking, and sharing these ads, for example). This faux-engagement is "counted" by Meta's algorithm and boosts the distribution of these ads. Alongside the reach driven by gaming Meta's algorithm, coordinated activity among such fake accounts can help manipulate real users by simulating apparent real activity (e.g., the number of viewers or commenters) to make the fraud more credible.

179. In one internal document, Meta recognized that approximately [redacted] of [redacted] and this percentage rose to [redacted]

180. To maintain the illusion of its reach and growth, Meta chose policies that enabled fraudulent accounts to remain on the platform at massive scale. First, Meta did not act to remove known fake accounts, allowing their direct (ad) and indirect (engagement) fraud to continue. Second, Meta failed to put in place verification requirements for new users that would make it harder for fake accounts to be created in the first instance. Both of these operational decisions fostered fraud on Meta's platforms, allowed it to persist, and amplified it.

### L. Meta Deceptively Represents That It Prohibits Fraudulent Advertising and Protects Users

181. Notwithstanding its own design and operational decisions and despite readily available evidence of widespread scams created and disseminated through its ad tools, Meta makes repeated public representations that it prohibits fraudulent conduct and protects users from scams on its platforms. Set out below are illustrative examples of those statements.

182. On its public "scam protection" webpage, Meta claims that it "aggressively combats scams on and off our platforms through a multi-layered approach: automated defenses, disrupting criminal networks, and cross-industry partnerships."

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

183. Meta promises users that it "uses detection technology and products to combat scams and protect people on our platforms;" employs "trained investigators focused on disrupting scam networks and making our systems more resilient to them in the future;" and takes a "comprehensive approach to making our technologies a safer place." Meta further lays out its use of "artificial intelligence and review teams to detect, review, and take action on millions of pieces of content every day on Facebook and Instagram," and states that WhatsApp "uses machine learning to tackle fake accounts, fraudulent activity and bulk messaging." Meta describes the number of scam ads removed and notes that the vast majority were proactively detected, creating the impression that Meta is vigilantly searching for and removing the scam ads it finds.

184. Similarly, presenting its "Policies Against Scams and Fraud," Meta represents that it is "constantly working to improve ways of detecting and blocking accounts that purposely deceive, misrepresent, defraud and exploit people for money or property …. This means our automated systems are able to stop abuse even before it is reported." Meta further states that it is "always working to find, remove, and disrupt scammers targeting people on our platforms."

185. Meta publicly shares its advertising policies, which lay out in detail the kinds of scams it prohibits: for example, ads that impersonate celebrities or established businesses, using "misleading tactics to bait people into engaging with the content in an attempt to scam or defraud" or offer "opportunities of unrealistic financial reward for unclear or minimal effort."

186. Meta also describes "How Meta tackles scams":

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

**How Meta tackles scams**

Our approach on Facebook and Instagram.

**Remove**
We remove scams when they go against our policies.

**Reduce**
We limit the reach of suspicious content by reducing its visibility.

**Inform**
We show warnings and safety tips to help people stay safe.

**Improve**
We work with industry partners to stay ahead of scam trends.

**Figure 22**

187. Meta's Community Standards webpage describes a long list of specific types of ads that Meta claims unqualifiedly that "We do not allow," such as: "Content that uses deceptive tactics to mislead people or businesses for commercial or financial gain" though loan, gambling, investment or financial, inauthentic identity (such as romance or charity), government grants, insurance, job, debt relief, credit repair, and giveaway frauds and scams.

188. Meta not only describes this content generically but adds language that indicates Meta actively enforces its prohibitions.[18] Thus, Meta advised, for example: "When advertisers place an order, each ad is reviewed against our policies. Our Advertising Standards also provide guidance on advertiser behavior that may result in advertising restrictions being placed on a Business Account or its assets (an ad account, Page or user account)." Meta also promised: "We use machine learning classifiers to review every ad that runs on our platforms for violations of our

[18] *See e.g.:* "Note: We also look for other signals to determine if an entity is posting legitimate, non-fraudulent content, such as when it is a verified entity and a bank or financial institution." (with respect to investment, insurance, and debt relief/credit repair fraud and scams); "Note: We also look for other signals to determine if an entity is posting legitimate, non-fraudulent content, such as when it is a verified entity" (with respect to job scams).

ad policies, including scams. This automated process includes analysis of the different components of an ad, such as the text, image or video." Furthermore, in distinguishing ads that are age-gated (certain weight loss ads) and content that Meta only "may remove" (such as surveillance devices or recruitment for class action lawsuits), Meta suggests that all other deceptive ads are removed when detected.

189. Until September 2026, when it revised its website, Meta promised that "to protect users and businesses from being deceived out of their money, property or personal information," it "remov[ed] content and combat[ed] 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 these activities using our platform."

190. Repeatedly, in its publicly available Form 10-k securities filings, Meta promised that it is making "significant investments in privacy, safety, security, and content and advertising review efforts" to "combat illegal activities."

191. In a January 2025 announcement, Mark Zuckerberg promised that, even with other changes to Meta's content moderation, the company would continue to focus on high severity violations, including "fraud and scams."

192. After Reuters' reporting and litigation against it, Meta has re-emphasized its deceptive statements. A Meta spokesperson offered: "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." In December 2025, Meta also published a blog post, "Scams Are Bad for Business: Our Ongoing Efforts to Fight Fraud," which again asserted that Meta took a "comprehensive" and "aggressive" approach to reducing scams.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

193. Especially in light of its affirmative misrepresentations regarding the zealousness and efficacy of its efforts to address fraud and scam ads, Meta's failure to disclose the ongoing prevalence of frauds and scams on its platforms also was misleading.

194. Meta's false, misleading, deceptive, and unfair conduct not only injures Rhode Island consumers, but impacts legitimate businesses and public figures whose identities and brands are misused and creates a marketplace in which legitimate advertisers must struggle to compete with dangerous and unfounded schemes.

## CAUSES OF ACTION

### COUNT ONE
### Violation of the Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-2
### Deceptive Acts and Practices
### (All Defendants)

195. The State re-alleges and incorporates herein by reference each of the allegations contained in the preceding paragraphs.

196. Section 6-13.1-2 prohibits deceptive acts or practices in the conduct of any trade or commerce.

197. Meta has engaged in trade or commerce in Rhode Island.

198. A deceptive act or practice is "(1) a representation, omission, or practice, that (2) is likely to mislead consumers acting reasonably under the circumstances, and (3) the representation, omission, or practice is material." *Long v. Dell, Inc.*, 93 A.3d 988, 1003 (R.I. 2014).

199. Defendants' misrepresentations, omissions, and practices were material and likely to mislead consumers. "[E]xpress representations that are shown to be false are presumptively material." *Id*.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

200. Meta has engaged in false, misleading, or deceptive acts and practices under the Deceptive Trade Practices Act through the conduct laid out above and below.

201. Meta falsely represents that certain types of ads are prohibited—investment scams, certain health products, or nudification apps, for example, creating the misleading impression that Meta enforces its policies to prevent these ads.

202. Meta has publicly represented to consumers, regulators, advertisers, and the public that it actively detects, prevents, removes, and suppresses fraudulent and illegal activity on its platforms. Meta has repeatedly claimed that it uses advanced technology, artificial intelligence, automated systems, human reviewers, and sophisticated enforcement mechanisms to identify and remove scam advertisements and protect consumers from fraud.

203. Among other misleading statements, Meta has represented that it "uses detection technology and products to combat scams and protect people on our platforms" and has taken a "comprehensive approach" to addressing fraud and deceptive conduct.

204. Meta has further represented that it effectively employs machine-learning systems, automated detection tools, and specialized review teams to identify fraudulent content, remove scam advertisements, prevent repeat offenders from advertising, and protect consumers from deceptive practices. Meta has also represented that it blocks accounts that "deceive, misrepresent, [or] defraud;" 'aggressively" and proactively identifies and removes scam advertisements before users encounter them; and that the vast majority of its enforcement actions occur before users report the offending content. These representations were and are material because the misrepresentations are express, and because reasonable consumers would consider a platform's ability and willingness to protect users from fraud important when deciding whether to use the platform and whether to trust ads displayed there.

205. At the same time it made these representations, Meta knew that fraud and scam advertising was widespread on its platforms, that fraudulent advertisers generated substantial revenue for the company, that its policies and enforcement efforts were not only insufficient to address fraud, like that originating from China or from the fake accounts it allowed to persist, but facilitated scams against its users.

206. Despite possessing such information, Meta's public statements omitted critical facts necessary to make those statements not misleading. Meta failed to disclose to its users the true magnitude of fraudulent advertising shown to users on its platforms; the extent to which it permitted high-probability and repeat scam advertisers to continue to purchase ads; the fact that it permitted suspected fraudulent advertisers to continue purchasing ads, often at a premium; that it targeted those ads to the most susceptible users, and the substantial revenues Meta derived from such advertising.

207. Further, Meta deceptively represents that, consistent with its "strict rules," its technology removes ads for nudification apps and prevents them from reappearing, and failed to disclose that ads for nudification apps are readily available on its platforms.

208. By omitting these and other material facts, Meta's representations that it detects, removes, and aggressively combats scams are materially misleading. Through its public statements, enforcement reports, platform policies, and representations, Meta created the overall impression that ads displayed on Facebook and Instagram were subject to meaningful and effective screening for fraud. That is not accurate.

209. Investigations by the Attorney General's Office and by outside organizations identified numerous fraudulent ad campaigns that remain active on Meta's platforms despite obvious warning signs, including impersonations of public figures, false Medicare or Social

Security benefit offers, investment scams, health supplements or treatments, and other deceptive schemes.

210. A reasonable consumer exposed to Meta's representations regarding scam prevention would not have expected Meta to continue accepting payment for, helping to create, distributing, optimizing, and amplifying such ads.

211. Government agencies, researchers, and consumer-protection organizations have publicly documented for years that older adults suffer disproportionately severe losses from fraud schemes.

212. Meta nevertheless provided advertisers with audience-selection, targeting, optimization, ranking, and performance-measurement tools capable of identifying and reaching older users, including, specifically, users over the age of sixty.

213. Scam advertising campaigns on Meta's platforms specifically targeted seniors and promoted purported Medicare, Social Security, retirement, and investment-related opportunities, as well as health cures and supplements. These advertisements generated millions of impressions.

214. Meta's representations regarding fraud prevention were therefore particularly misleading because Meta knew that vulnerable populations, including older consumers, were being exposed to—and targeted for—precisely the categories of scam advertisements that Meta publicly claimed it was preventing.

215. Meta's acts and omissions had the tendency and capacity to mislead reasonable consumers.

216. Upon information and belief, Defendants' wrongful conduct is ongoing.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

**COUNT TWO**
**Violation of the Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-2**
**Unfair Acts and Practices**
**(All Defendants)**

217. The State re-alleges and incorporates herein by reference each of the allegations contained in the preceding paragraphs.

218. Section 6-13.1-2 prohibits unfair acts or practices in trade or commerce. In determining whether an act or practice is unfair, the Rhode Island Supreme Court held the following factors apply: "(1) Whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, or otherwise—whether, in other words, it is within at least the penumbra of some common-law statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; and (3) whether it causes substantial injury to consumers (or competitors or other businessmen)." *Long*, 93 A.3d at 1000. An act or practice must not satisfy every factor to be unfair; it may be unfair because it meets one factor to a great degree or two or three factors to a lesser degree. *Id*. at 1001.

219. Meta has engaged in trade or commerce in Rhode Island.

220. Meta has engaged in unfair acts and practices through conduct, as described in this Complaint, that is unconscionable, offends public policy, and is immoral, unethical, oppressive, and/or unscrupulous.

221. Meta's conduct is unfair in that it takes advantage of vulnerable consumers, including seniors. By misleading Rhode Island consumers about the prevalence of fraud and scam ads on its platforms, and by participating in helping to design, target, and optimize fraud ads to make sure that they are effective as possible and that they reach users most likely to engage

with and act on them, Meta left Rhode Island consumers without the ability to protect themselves from bad actors on its platforms.

222. Meta's conduct in allowing fraudsters to continue to operate on its platforms, and to not ban suspected scam ads, but charge more for them; to maintain policies and constrain its enforcement and to tolerate fake and fraudulent accounts in order to protect its revenue at the expense of its users; and to conceal its conduct from regulators is fundamentally unfair, unethical and unscrupulous. The same is true of the assistance Meta provided to optimize and amplify scam ads. Meta acted with callous disregard for the safety and well-being of its users, despite at least one major competitor verifying ads more stringently and in a commercially viable manner, in order to retain and increase its own profits. Meta undertook this course of action knowing at least one major competitor had chosen to verify ads more stringently and therefore knowing there was a commercially viable alternative manner in which to conduct its business.

223. Meta was aware of, but did not disclose, the scale of scam ads on its platforms, and, instead, knowingly and purposely misled consumers and regulators about the extent of fraudulent ads on its platforms and its efforts to rein in that fraud, depriving consumers of the ability to protect themselves.

224. Meta's conduct violates established public policy, including public policies providing heightened protection to older consumers as reflected, for example, in the Elder Adult Financial Exploitation Prevention Act, R.I. Gen. Laws ch. 19-34, and the Senior Savings Protection Act, R.I. Gen. Laws § 7-11.2.

225. Meta has caused substantial harm to consumers that was not reasonably avoidable by consumers and is not outweighed by countervailing benefits to consumers or competition. Scam ads on Meta's platforms include fraudulent investment opportunities, health remedies, and

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

other deceptive offers. Rhode Island consumers exposed to and deceived by these advertisements, including consumers over the age of 60, suffer financial losses and other harms.

226. Meta enabled scam advertisers to target seniors. Based on its own optimization and analytic tools and its collection of data on ad distribution and impressions, Meta knew that certain fraud ads were primarily directed at users who were 65 and older.

227. Upon information and belief, Defendants' conduct is ongoing.

**COUNT THREE**
**Unjust Enrichment**

228. The State realleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

229. Meta has received and retained substantial revenues derived from advertisements that promoted fraudulent schemes, deceptive offers, impersonation scams, fake investment opportunities, false Medicare and Social Security benefit offers, ineffective or dangerous health supplements or treatments, and other unlawful or deceptive conduct directed at consumers, including consumers in Rhode Island.

230. Meta did not merely provide a neutral infrastructure for fraud on its platforms. Instead, Meta knowingly provided design assistance, audience-selection tools, targeting capabilities, optimization systems, delivery services, analytics, and related services that enabled advertisers to identify, engage, and repeatedly solicit users likely to respond to fraud ads.

231. Meta collected advertising fees from advertisers promoting such schemes—to the tune of billions of dollars.

232. Meta knew that fraud was rampant on its platforms but not only developed and applied policies that protected fraudulent actors and reined in its own enforcement efforts, but misled consumers about the prevalence of such fraud and its efforts to address it.

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

233. Meta further knew that older adults represented a frequent target of fraud schemes. Government reports, law-enforcement warnings, academic research, and consumer-protection publications for years have identified older adults as particularly vulnerable to certain forms of financial fraud and scam advertising.

234. Despite that knowledge, Meta accepted and retained advertising revenues generated by fraud advertisers and continued designing, optimizing, and targeting fraud ads to increase their reach and effectiveness.

235. Meta's retention of such revenues was unjust because those revenues were derived from advertising campaigns that deceived consumers, extracted money from consumers through fraud, and caused substantial consumer injury.

236. The benefits retained by Meta were directly connected to the unlawful or inequitable conduct alleged herein because Meta's compensation increased as fraudulent advertisers purchased additional ads, showed them to a larger audience, and increased their engagement.

237. Allowing Meta to retain revenues earned from the creation, targeting, optimization, distribution, and amplification of fraudulent advertising would be inequitable and contrary to principles of justice and equity.

238. Meta has been unjustly enriched at the expense of Rhode Island consumers and the public through its receipt and retention of revenues generated from fraudulent advertising campaigns.

## PRAYER FOR RELIEF

WHEREFORE, the State prays for judgment against Defendants as permitted by Rhode Island law, as follows:

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

A. An Order and Judgment against Defendants, and in favor of the State, for each violation alleged in this Complaint;

B. Declaration that Defendants' acts and practices alleged herein are unfair and deceptive and constitute unfair methods of competition in violation of R.I. Gen. Laws § 6-13.1-2;

C. An injunction pursuant to R.I. Gen. Laws § 6-13.1-5(a) permanently enjoining Defendants from engaging in unfair and deceptive acts and practices;

D. Consumer restitution pursuant to R.I. Gen. Laws § 6-13.1-5(c) to Rhode Island consumers affected by Defendants' unlawful acts and practices;

E. Civil penalties pursuant to R.I. Gen. Laws § 6-13.1-8 for each and every violation of the Deceptive Trade Practices Act against Defendants;

F. Disgorgement of Defendants' unjust enrichment, benefits, and ill-gotten gains, plus interest, acquired as a result of the unlawful conduct alleged herein;

G. Appointment of a receiver, auditor, or monitor to ensure Meta's compliance with relief ordered by the Court;

H. Costs, filing fees, pre- and post-judgment interests, and attorneys' fees; and

I. All other relief deemed just by this Court.

**JURY TRIAL DEMANDED**

The State hereby demands a jury trial on all causes of action for which a jury is available under the law.

Dated: October 22, 2026

**PETER F. NERONHA**
**ATTORNEY GENERAL OF RHODE ISLAND**

By: */s/ Sarah W. Rice*
Sarah W. Rice (Bar No. 10588)

Case Number: PC-2026-05842
Filed in Providence/Bristol County Superior Court
Submitted: 10/22/2026 11:09 AM
Envelope: 5893726
Reviewer: Alexa G.

*Assistant Attorney General*
Marisa-Lyn Menna (Bar No. 11281)
*Special Assistant Attorney General*
150 South Main Street
Providence, RI 02903
Telephone: (401) 274-4400
Fax: (401) 222-2995
srice@riag.ri.gov
mmenna@riag.ri.gov

Linda Singer *(Pro Hac Vice to be submitted)*
Motley Rice LLC
401 9th Street NW, Suite 630
Washington, DC 20004
Telephone: (202) 386-9626
Fax: (202) 286-9622
lsinger@motleyrice.com

*Counsel for the State of Rhode Island*