

Filed Under Seal

Exhibit 1

**IN THE UNITED STATES DISTRICT COURT FOR
THE NORTHERN DISTRICT OF CALIFORNIA**

PEOPLE OF THE STATE OF CALIFORNIA,
et al.,
Plaintiffs,

v.

META PLATFORMS, INC, et al.,
Defendants

IN RE: SOCIAL MEDIA ADOLESCENT
ADDICTION/PERSONAL INJURY
PRODUCTS LIABILITY LITIGATION

THIS DOCUMENT RELATES TO:
4:23-cv-05448

MDL No. 3047

Case No. 4:23-cv-05448-YGR

Judge: Hon. Yvonne Gonzalez Rogers

Magistrate Judge: Hon. Peter H. Kang

TRIAL REPORT OF TIM ESTES
March 20, 2026

I. Summary of Opinions

1. The following opinions detail my conclusions based on my professional training and experience, the relevant standards in the tech industry, the relevant literature, and my extensive review of documents and testimony in this case:

2. As confirmed by the U.S. Surgeon General and my own experience and education on these issues, the Defendants' social media platforms can contribute to a wide range of harms in kids, including anxiety, depression, sleep disruption, negative body image, eating disorders, and self-harm, as well as structural changes to the brain. They have also become hunting grounds for predators seeking to sexually exploit children.

3. Meta could have (and should have) greatly reduced these harms and risks with technological solutions that were readily available to them. As outlined below, these solutions were technically feasible and in many cases had been implemented by other companies in other contexts. But Meta either did not implement them, waited unreasonably long to implement them, or implemented them in ways that were predictably ineffective.

4. **Opinion 1:** Meta should have implemented systems to help parents and guardians protect children from the potential harms of their platforms. One of the most basic ways to protect children from adult-oriented platforms is a system of age verification and Verified Parental Consent (VPC). This ensures that children or minors under a designated age are not able to set up an account without some form of adult consent and supervision. It also allows the platform to exclude the youngest and most vulnerable children altogether. Meta could have, and should have, set up an age verification and VPC system. In public statements, Meta stated that children under 13 are not allowed on their platforms. In practice, however, Meta's age verification systems were either non-existent or broken. Meta allowed millions of pre-teens to use its addictive platforms and collected data from them without obtaining any form of VPC, in violation of industry standards and regulations.

5. **Opinion 2:** Meta claims that age checks and VPC were not feasible or would have created unreasonable privacy risks are incorrect. Effective, privacy-friendly ways to check age and

or credit card verification for every user would invade privacy or exclude people without IDs, and that kids would always find a way around restrictions.⁵⁶

72. As outlined below, robust systems for online age checks and parental consent were readily available during that time period and are available today. Standard tools include credit card verifications, ID scans, and AI age estimators (among others). These tools were widely in use in other industries, including (for example) by video game console manufacturers and mobile operating system developers. Platforms like Microsoft's Xbox Live, Nintendo's online network, Sony's PlayStation Network, Apple's iOS ecosystem, and Google's Android system have been successfully verifying parent permission and supervising child accounts for more than a decade. In short, age verification and parental consent online has been the norm across much of the tech and media industry.

73. Meta's failure to implement effective age checks and parental consent was not reasonable and not in-line with industry standards, including the standards set for children under the age of 13 by COPPA.

A. Widely Available Age Verification Tools

74. Modern digital platforms have had a rich toolkit of age verification methods at their disposal for many years that do not unnecessarily harvest personal data. Examples of such technologies include the following:

1. Credit Card and Payment Verification (2010 to present)

75. One of the oldest and simplest methods to verify age is the credit card check. Credit cards (as well as debit cards in adult-controlled contexts) serve as a proxy for adulthood because minors generally cannot obtain one independently. As early as 1999, the U.S. FTC explicitly endorsed "the use of a credit card . . . in connection with a monetary transaction" as an approved

⁵⁶ See, e.g., How Do we Know Someone is Old Enough to Use Our Apps?, Meta (July 27, 2021) <https://about.fb.com/news/2021/07/age-verification/>.

115. While Meta denied or downplayed what was happening on their platforms, internal records indicate a gap between their public stance (“we don’t allow under-13s, problem solved”) and private reality (“millions of kids are here and driving our metrics”). This is most troubling because it may lull regulators and parents into a false confidence that the issue is being handled.

116. By reviewing the timeline and evidence, it becomes apparent that by 2010, the existence of effective parental consent systems was widely known and their efficacy demonstrated. This set an industry standard: a reasonable company in the online services space that knows it has children on its platform should implement verifiable parental consent and age gating as other responsible companies have.

117. Social media companies failed to adopt these reasonable measures. They had ample examples to emulate – whether by integrating a credit card verification on sign-up, implementing a parent-managed sub-account system, or partnering with app stores to enforce parental approval (as Meta belatedly suggested in 2023) – but did not follow them.

E. Meta’s Experts’ Opinions Are Built on a Theoretical Façade, Not Based in Reality

118. Despite addressing different technical domains, the expert reports submitted by Meta are built upon a shared set of flawed premises. While authored by different individuals, these defense reports present the same flawed narrative, they describe a sanitized, theoretical world of social media safety that is irreconcilable with the reality revealed by Defendants’ own internal documents, audits, and executive testimony. They collectively paint a picture of responsible companies grappling with unforeseeable challenges. The factual record, however, reveals a consistent pattern of inaction and misdirection. Moreover, the challenges these companies faced were foreseeable and addressable.

The undersigned hereby certifies their understanding that they owe a primary and overriding duty of candor and professional integrity to help the Court on matters within their expertise and in all submissions to, or testimony before, the Court. The undersigned further certifies that their report and opinions are not being presented for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation.

Dated: March 20, 2026



Timothy W. Estes