Three Keys to Defeating Class Certification in Pixel Cases

Individual questions predominate on issues of (1) information shared, (2) consent, and (3) Article III standing.

Jul 08, 2026

Categories:

Publications

Authors:

Wendy L. Llewellyn-Langford
Michael R. McDonald

A judge in the Northern District of California declined to certify a class of Capital One website users who claimed that tracking technologies embedded on its website, including Meta Pixel, unlawfully collected and shared their personal financial information with third and fourth parties for marketing and sales purposes. The court held that the plaintiffs did not demonstrate that common questions predominate over individual inquiries regarding (1) what information was allegedly shared; (2) whether putative class members either expressly or impliedly consented to sharing their information; and (3) Article III standing, as the plaintiffs failed to present a method of proof by which harm on a class-wide basis could be shown.

Complaint

The plaintiffs alleged that they applied for credit cards — which required supplying private and financial information — through the Capital One website, which, unbeknownst to the plaintiffs, contained embedded third-party tracking technologies that they claimed unlawfully sent their information to third parties, to be used for targeted advertisements and other marketing efforts. The plaintiffs alleged the information shared with those third parties (and ultimately other fourth parties) included employment information, bank account information, citizenship and dual citizenship status, credit card preapproval and eligibility, credit card approval and eligibility, existing user or customer status, browsing activities (including viewed pages and content), and credit card application status.

The single remaining named plaintiff — Williams — alleged that she applied for a credit card with Capital One through the website, was not approved, and was shortly afterward "constantly bombarded

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons

with credit card advertisements," to the point that she blocked Capital One on social media "due to the bombardment of targeted advertising." The complaint initially alleged 17 causes of action that included violations of state and federal privacy and other laws, but only six counts remain: negligence, violation of the California Consumer Privacy Act, unjust enrichment, violation of the California Invasion of Privacy Act, and two counts for violation of the federal Electronic Communications Privacy Act.

Motion for Class Certification

The plaintiff sought to certify two national classes of Capital One website users and two California subclasses. Capital One opposed, arguing that (1) the plaintiff did not identify a common question of fact; and (2) individual questions predominate the class.

Assessing Rule 23(a)(2) commonality and Rule 23(b)(3) predominance together, the court noted that the plaintiff identified 12 categories of data that constitute the "personal and financial data" underlying her claims, including hashed names, hashed email addresses, hashed phone numbers, obfuscated banded FICO scores, obfuscated banded income segments, citizenship status, country of origin, employment status, type of bank account, type of credit card, obfuscated value of credit card to Capital One, and the results of the application process. However, the court noted that "not every application Plaintiff submitted resulted in a transmission of information via the technologies at issue," that "consumers' various browsing habits and browser settings can influence what information is shared and when," and that "[t]he parties dispute which information was shared regarding even the named Plaintiff in this action." The latter issue, in the court's view, would necessitate "individualized inquiries . . . to determine whether, and if so, what information was sent for any particular individual through a particular technology."

Rather than applying to all prospective plaintiffs on a class-wide basis, "Plaintiff's privacy claims here depend on an individualized assessment of each prospective plaintiffs' interactions with the tracking technology and the amount and type of information included on their credit card application." Accordingly, because the

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

plaintiff was unable to show that Capital One "transmitted each category of 'personal and financial data' for each putative class member in a uniform manner to third-parties," the plaintiff failed to show that common questions would predominate over individual inquiries.

Similarly, the court determined that the issue of whether putative class members consented to disclosure of their information would also require individualized inquiries that would predominate over common questions because consent is "intensely factual" and requires "consideration of the circumstances." More specifically, the court noted that (1) express consent would require determining to which of multiple Capital One privacy disclosures putative class members were exposed; and (2) implied consent would require evaluating to which of the various disclosures each putative class member was exposed, as well as whether that individual knew about and consented to sharing information based on that disclosure.

Finally, the court pointed to its May 22, 2026, order dismissing one of the other named plaintiffs —Ingraham — for lack of Article III standing because, unlike Williams, he failed to demonstrate an actual expectation of privacy due to his submission of two additional applications for credit cards on Capital One's website after filing this lawsuit. The court noted it "would need to engage in this same, fact-intensive inquiry for each prospective plaintiff," which would also include determining "what, if any, data was shared, how that data was shared, for what purpose the data was shared, and the nature of that data shared with respect to each plaintiff" to determine standing for both the statutory and common law claims, and that the plaintiff had not demonstrated a method capable of showing that "harm" on a class-wide basis. Accordingly, issues of Article III standing provided an additional ground on which the court denied class certification.

Takeaway

This decision provides three key areas on which defendants can focus in order to defeat class certification in Pixel and other tracking technology cases:

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

- Lack of uniformity in information allegedly shared with third parties for each individual website user, whether because information transmitted by the tracking technology varies, or because a user's browser or device affects which information is picked up by the tracking technology;
- Differences in privacy policies and disclosures to which users have expressly consented, and the subjective nature of determining whether users have impliedly consented; and
- Differences in proofs required to determine harm, and thus Article III standing, for each individual user.

For more information about this holding and its implications for other claims involving website tracking tools, please contact the authors or any attorney with FBT Gibbons' Class Actions team.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons