KRIEG DEVAULT

Insights

CIPA "Pen Register" Demand Letters Target Financial Institution Websites

June 29, 2026

By: Brett J. Ashton and David A. Bowen

This is a follow up to our April 20, 2026 client alert, "*Latest Developments in Meta Pixel Class Action Litigation Impacting Financial Institutions,"* in which we reported that website-tracking litigation against financial institutions had expanded geographically and diversified into newer theories, which included "pen register / trap-and-trace" claims under the California Invasion of Privacy Act ("CIPA"). In that alert, we flagged the November 2025 decision in *Camplisson v. Adidas America, Inc.* where the court held that software-based trackers collecting IP addresses and device identifiers can qualify as pen registers under CIPA's "intentionally broad language."

Since then, this theory has moved to the forefront. Plaintiffs' counsel are sending pre-litigation demand letters with fully drafted complaints attached, relying specifically on CIPA's pen register and trap-and-trace provisions, Cal. Penal Code §§ 638.50(b) and 638.51(a). This follow-up focuses on that pre-litigation activity, the legal theory supporting it, and the practical steps financial institutions should consider now.

Key Takeaways

- **A new wave of demand letters is arriving with draft complaints.** Plaintiffs' counsel are presenting these as ready to file if the matter is not resolved, pressuring institutions to quickly assess and respond. CIPA's private right of action allows statutory damages of$5,000 per violation.
- **Out-of-State institutions targeted**. The demand letters are being sent to institutions with no operations in California, with the claim based solely on an alleged visit to the institution's website.
- **The legal theory recasts routine web trackers as "pen registers**." Plaintiffs allege pixels, tags, scripts, and analytics tools that transmit IP addresses and other routing/signaling data to third parties function as pen registers or trap-and-trace devices.
- **Courts are split.** Several federal district courts in California have allowed these claims to survive the pleadings stage, while California state courts and other federal courts have been more skeptical and have dismissed or narrowed the theory. Outcomes remain uncertain.
- **Proactive remediation remains the best defense**. A current tracking inventory, a consent management platform that actually blocks non-essential transmissions until opt-in, accurate disclosures, and disciplined vendor management materially improves an institution's defensive posture in avoiding or defending a claim.

Background

The new demand letters follow a familiar template, but with a sharpened legal focus. Counsel identifies an institution's public-facing website, documents the third-party tracking technologies firing on it (commonly pixels, tags, and analytics or advertising scripts from vendors such as Meta, Google, LinkedIn, TikTok, and similar providers), and asserts that those technologies operate as pen registers or trap-and-trace devices under CIPA.

The core factual allegation is that, on page load (before the visitor interacts with a cookie banner or provides any affirmative consent) the website automatically transmits "addressing" or "signaling" information, including the visitor's IP address and device or browser identifiers, to one or more third parties. Plaintiffs allege this information is used for analytics, advertising, retargeting, and profiling, and that the institution had the technical ability to prevent or delay these transmissions but did not. The demands typically contend that no court order authorized the "installation or use" of these technologies and that no valid prior consent was obtained.

These demands are notable because they often arrive with a draft class-action complaint ready to file if the matter is not resolved by the deadline. As in prior cases, the named plaintiff may be a non-customer who merely visited the public website. The demand letters are also being directed to institutions with no operations in California, with the asserted nexus resting solely on a California resident's alleged visit to the website of an out-of-state institution. Although the demands may include claims for negligence, unjust enrichment, invasion of privacy, and state wiretap or consumer-protection violations, the pen register theory is increasingly the lead count because it supports a straightforward statutory-damages calculation.

Plaintiffs' Legal Theory

CIPA's pen register provisions were enacted against the backdrop of telephone-era surveillance. Section 638.50(b) defines a "pen register" as a "*device or process"* that records or decodes "dialing, routing, addressing, or signaling information" transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of the communication. A "trap and trace device" is defined as the inbound counterpart, capturing incoming source information. Section 638.51(a) makes it unlawful to install or use a pen register or trap-and-trace device without first obtaining a court order, subject to certain exceptions (most relevantly, *where the consent of the user has been obtained*).

Plaintiffs fit modern web technology into this framework as follows:

- "**Device or process**." Plaintiffs lean heavily on the word "process," arguing that software-based trackers (i.e., scripts and tags) are a "process" even if they are not a physical device.
- **"Routing, addressing**, **or signaling information**." Plaintiffs characterize IP addresses, device and browser identifiers, and similar metadata as "addressing" or "signaling" information rather than communicative content.
- **No court order, no consent**. Plaintiff's falsely assert that unless a court authorized the tracker, Section 638.51(a) is violated each time the technology fires if no affirmative consent preceded the transmission. In reality, a court order is not required if consent is given by the consumer.

CIPA's civil remedy, Cal. Penal Code § 637.2, provides statutory damages of $5,000 per violation (or three times actual damages, whichever is greater), together with injunctive relief and costs. Plaintiffs commonly also seek attorneys' fees. Aggregated across the volume of California visitors to a financial institution's website, the theoretical exposure is substantial. Several federal district courts in California have allowed pen register claims to advance past the pleadings stage, reasoning (as in *Camplisson*) that the statutory language is broad enough to reach software trackers and whether a given technology qualifies is a fact question unsuitable for resolution at the pleadings stage. Other courts, including a number of California state courts, have been more skeptical, treating pixel outputs as behavioral analytics data rather than routing or signaling information, questioning whether IP-based transmissions fall within the statute, or otherwise dismissing or narrowing the claims.

What Should Financial Institutions Do Now?

The pen register theory remains novel, and we continue to believe that many of the underlying claims are vulnerable on the merits, particularly in venues that have read CIPA's definitions more narrowly. But the landscape has become measurably more plaintiff-friendly, the demand letters now arrive with complaints in hand, and the statutory-damages framework creates settlement pressure independent of how a case might ultimately be resolved. For financial institutions, proactive review and mitigation represent sound risk management. The stronger an institution's tracking inventory, consent controls, disclosures, vendor management, and arbitration infrastructure, the better positioned it will be to defend against, or avoid becoming the next target of, these demands.

Krieg DeVault's Financial Institutions attorneys are actively monitoring developments in website-tracking litigation and are available to provide guidance on how best to protect your institution against these risks.

Disclaimer: The contents of this article should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult with counsel concerning your situation and specific legal questions you may have.