Insights

Latest Developments in Meta Pixel Class Action Litigation Impacting Financial Institutions

April 20, 2026

By: Brett J. Ashton and David A. Bowen

On January 13, 2025, we published a client alert in which we warned that the plaintiffs' bar had begun adapting theories used in a wave of healthcare website-tracking class actions to target financial institutions, and highlighted a then-recent putative class action against a small Indiana-based community financial institution as an indicator that institutions of every size were at risk. In the fifteen months since that alert, the trend has continued and expanded to a degree that warrants this follow-up.

In Gassman v. Guardian Credit Union, No. 2:25-cv-00176-BHL (E.D. Wis. Mar. 31, 2026), the court allowed nine claims to survive the pleadings stage of a putative class action alleging unauthorized website tracking and sharing of customers' personal and financial information. Critically, the court held that the credit union's defense that its use of common web-analytics pixels was lawful, anonymized, and disclosed in its privacy policy raised factual disputes that could not be resolved at the pleading stage. This decision highlights the growing risks these cases pose to financial institutions where courts are permitting claims to advance beyond the motion-to-dismiss stage, exposing defendants to costly discovery and potential class-wide litigation.

Website-tracking class actions have become a nationwide concern for financial institutions and other companies with California and Florida leading the number of cases filed. More than 1,000 lawsuits asserting violations of the California Invasion of Privacy Act ("CIPA") alone were filed in 2025, and an increasing number of similar cases are being filed in other states. Named defendants range from the nation's largest banks to community financial institutions, like the credit union in *Gassman*, with a modest online footprint.

Financial institutions that do not specifically target customers in a certain state, and that have no physical presence in that state, remain at significant risk of being named in Meta Pixel-type lawsuits. Plaintiffs often aren't even customers of the financial institution, rather individuals asserting they accessed the financial institution's website and suffered damages. This is not a theoretical concern. Plaintiffs' firms are currently sending demand letters and filing putative class actions against institutions with no operations, branches, or marketing presence in the plaintiff's state of residence. The reasons that these claims are reaching out-of-state institutions include, among others:

- **Customer access from other states.** Plaintiff attorneys claim that a state's wiretap, eavesdropping, or consumer protection law applies if a resident of that state accesses an institution's public website from within that state, even if the institution has no physical presence there.
- **Digital operations.** The proliferation of online accounts and digital loan applications means that even institutions with a narrow geographic focus are routinely transacting with residents of other states.

- **Jurisdictional theories.** Plaintiffs contend that the interactivity of a website, the placement of cookies onto users' devices within the forum state, or the institution's purchase of targeted advertising directed at residents of that state are sufficient to establish the "minimum contacts" required for personal jurisdiction. However, courts continue to differ in their interpretations of this matter.
- **Forum shopping.** Plaintiffs' attorneys often file in states with stricter laws than the federal Wiretap Act, which prohibits intercepting wire, oral, or electronic communications without consent from at least one participant to the communication. States like California, Florida, and Illinois require consent from all parties involved in a communication.

The central fact pattern in these cases remains consistent with our initial alert. Plaintiffs allege that the institution utilizes website tracking software from vendors such as Meta, Google, LinkedIn, TikTok, and similar providers, resulting in the transmission of visitor data to third parties without sufficient notice and consent. The array of claims includes negligence, negligence per se (based on purported violations of the Gramm-Leach-Bliley Act ("GLBA"), Section 5 of the FTC Act, or applicable state privacy laws), breach of contract, unjust enrichment, bailment, conversion, invasion of privacy, and violations of state wiretap, eavesdropping, and consumer protection statutes, as well as claims under the federal Electronic Communications Privacy Act and Computer Fraud and Abuse Act.

What *has* changed is number of claims directed at out-of-state institutions (as mentioned above) and types of claims being made. We are now seeing significant activity in several newer categories:

- **Broken or defective cookie banner cases.** A rapidly growing category of suits alleges that a website's cookie banner offered users the ability to reject non-essential cookies but that, on the back end, third-party tracking technologies continued to fire despite a "Reject All" or opt-out election. Plaintiffs argue that this gap between the banner's promise and the website's behavior constitutes a misrepresentation as well as violations of privacy law. In December 2025, the U.S. District Court for the Northern District of California's decision in Wiley v. Universal Music Group, Inc., No. 25-cv-03095-PCP, 2025 WL 3654085 (N.D. Cal. Dec. 17, 2025) dismissed multiple claims at the pleadings stage but allowed the plaintiff's privacy and unjust enrichment claims to survive. This decision highlights that courts may treat any undisclosed override of cookie opt-out selections as an egregious privacy violation that financially benefits the company collecting the data without authorization.
- **Pen register / trap-and-trace theories.** Plaintiffs increasingly rely on federal and state laws prohibiting the use of a "pen register" or "trap and trace device" without a court order. A pen register records outgoing dialing, addressing or signaling information from phones and electronic devices, while a trap and trace device records incoming source information like caller IDs or IP addresses. Neither captures the content of calls or messages. Defendants have repeatedly argued that these terms are limited to telephone surveillance devices, but some courts have rejected that argument in a growing line of cases, most prominently in a November 2025 decision out of the U.S. District Court for the Southern District of California (Camplisson v. Adidas America, Inc. No. 25-cv-00603-GPC-KSC, 2025 WL 3228949 (S.D. Cal. Nov. 18, 2025). The court denied the motion to dismiss and held that software-based trackers collecting IP addresses, device identifiers, and similar data can qualify as pen registers under CIPA's "intentionally broad language." Other courts have interpreted the definition more narrowly, viewing pixel outputs as behavioral analytics data rather than routing signals.

- **Session replay cases.** Plaintiffs are still focusing on cases involving session replay vendors that capture mouse movements, keystrokes, scrolling, and form submissions. The Northern District of California's decision in Torres v. Prudential Financial, No. 22-cv-07465-CRB, 2025 WL 1135088 (N.D. Cal. Apr. 17, 2025) limited CIPA Section 631 liability stating that session replay data is not "read" while it is "in transit." This provides a defense for institutions that can demonstrate user actions such as clicks, keystrokes, and mouse movements are only accessible after transmission, once the software has stored and reassembled the information.
- **VPPA-adjacent cases.** Where the institution's website hosts video content, like financial education, product explainers, branded marketing, plaintiffs have leveraged the federal Video Privacy Protection Act ("VPPA"). The VPPA prohibits a video tape service provider from knowingly disclosing a consumer's personally identifiable information without consent. Federal courts in Michigan and New York recently reached different conclusions on whether sharing Meta Pixel data on video-viewing activity can violate the VPPA.

What Should Financial Institutions Do Now?

The geographic expansion of Metal Pixel/website-tracking litigation combined with aggressive cross-border filing strategies means that every financial institution with a public-facing website should treat these claims as a top-tier litigation risk, regardless of charter type, asset size, physical footprint, or whether the institution actively markets into the states where suits are being filed. The following actions are recommended:

- **Audit website tracking technology.** Maintain a current inventory of every pixel, tag, SDK, cookie, session replay tool, chat widget, and AI chatbot on each public-facing and authenticated page, together with the specific data transmitted to each third-party recipient.
- **Review and update privacy policies and website disclosures.** Privacy policies should accurately state the categories of tracking technologies in use and the categories of third parties receiving visitor data. Generic boilerplate can be fatal to a defendant's motion-to-dismiss.
- **Implement (and test) conspicuous, persistent consent mechanisms.** A prominent cookie banner/consent management platform that actually blocks non-essential cookies, pixels and scripts form activating until affirmative consent is captured is still an effective defense. The platform should log consent on a per-visitor basis. Critically, institutions should regularly test the platform to ensure that "Reject All" and granular opt-out elections are honored on the back end. Cases involving "broken cookie banners" have become a rapidly expanding category of legal filings, as discrepancies between the banner's stated commitments and the website's actual practices invite litigation
- **Review vendor agreements.** Vendor contracts with Meta, Google, LinkedIn, Snap, HubSpot, Microsoft, TikTok, chat providers, session replay vendors, and AI chatbot vendors should be reviewed for indemnification, cooperation, data-use limitation, deletion, and audit clauses.
- **Strengthen arbitration and class-action waiver provisions.** Online-banking terms of use, account agreements, and website terms should include individual-arbitration and class-waiver provisions drafted to cover non-customer website visitors to the maximum extent permitted by applicable law. The enforceability of such clauses against mere website visitors is an open and actively litigated question but drafting for the best possible outcome remains advisable.

- **Pay heightened attention to high-exposure jurisdictions—even without operations there.** Institutions with *any* direct or indirect exposure to California or Florida—whether through customers, operations, marketing reach, digital account opening, or membership fields—should prioritize taking the defensive steps recommended above. The absence of a branch in a given state is no longer a reliable defense.

While we continue to believe that many of the underlying claims in these website-tracking cases are meritless, the legal landscape has become measurably more plaintiff-friendly since our original alert. Courts are increasingly rejecting defense-friendly readings of legacy wiretap statutes, plaintiffs are successfully pleading around one-party consent rules, and the plaintiffs' bar is openly targeting institutions with no operations in the forum state. The stronger an institution's disclosure, consent, vendor-management, and arbitration infrastructure, the better positioned it will be to defend against—or avoid becoming the next target of—these claims.

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.
