ALFA International
THE GLOBAL LEGAL NETWORK

2026 Business Litigation Practice Group Seminar

June 3-5, 2026

Fees, Feeds, and Phone Calls:

Navigating Modern Consumer Compliance Risks

Megan Stumph-Turner
BAKER STERCHI COWDEN & RICE LLC
Kansas City, Missouri
mstumph@bakersterchi.com

Matthew Burke
YOUNG MOORE AND HENDERSON, P.A.
Raleigh, North Carolina
matthew.burke@youngmoorelaw.com

The Pitfalls of Pixels

Lawsuits are on the rise related to pixel tracking technologies such as Meta Pixel and Google Analytics, and consumer-facing businesses must take note. As digital platforms become more personalized and data-driven, businesses are faced with navigating a growing web of privacy laws and legal risks that accompany these tools.

The newest wave of consumer litigation impacting the financial services industry is "pixel" litigation, wherein plaintiffs allege that tracking technologies—often deployed by third-party platforms such as Meta, Google, or other analytics providers—transmit user data without adequate notice or consent.

When embedded in a financial institution's website or customer portal, these technologies may capture not only general browsing activity, but also potentially sensitive information such as personal identifiers, account-related data, and user behavior patterns. The extent of data captured—and whether it is actually disclosed to third parties—remains a key factual battleground in these cases.

Plaintiffs have asserted a range of legal theories, including invasion of privacy, violations of state wiretapping statutes, and consumer protection claims. These complaints often reference statutes such as the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA), though those statutes generally do not provide private rights of action. Instead, plaintiffs frequently rely on state-law UDAAP or consumer protection statute-based claims to seek damages.

A significant driver of this litigation trend is the use of state wiretapping laws, most notably the California Invasion of Privacy Act (CIPA), with plaintiffs arguing that pixel technologies operate as unauthorized interception tools when embedded on websites. These claims often hinge on whether a third party (e.g., Meta or Google) is deemed to have "intercepted" a communication in transit.

In addition, plaintiffs have increasingly asserted claims under the Video Privacy Protection Act (VPPA), particularly where websites include video content and tracking technologies that may disclose user viewing behavior to third parties.

Narrow Victory for a Financial Institution

In *Stevens v. TD Bank* (June 2025), a federal court dismissed pixel-related claims alleging violations of GLBA. The court's decision turned on the plaintiff's failure to specifically allege what personal financial information was captured or how any alleged disclosure resulted in concrete harm.

While the decision provides a helpful defense roadmap, it is likely to be narrow in impact. Plaintiffs are expected to refine their pleadings to include more detailed allegations regarding data capture, transmission, and injury. As a result, defendants should not assume that similar claims will be dismissed at the pleading stage going forward.

Regulatory Trap or Relief?

California Senate Bill 690 (SB 690) has been proposed to amend CIPA by creating a limited safe harbor for businesses that use tracking technologies for a "commercial business purpose," provided those uses comply with the California Consumer Privacy Act (CCPA).

The bill is intended to address the recent surge of wiretapping lawsuits that characterize routine website tracking as unlawful interception. However, SB 690 has not yet been enacted and will not be reconsidered until at least 2026, with any potential effective date likely in 2027 or later.

Even if enacted, SB 690 would not provide a blanket safe harbor. Its protections would depend on strict compliance with CCPA requirements, including:

- Clear and accurate privacy disclosures
- Consumer rights mechanisms (including opt-outs)
- Limitations on cross-context behavioral advertising without appropriate consent

Moreover, the scope of key terms—such as "commercial business purpose"—would likely be subject to further litigation, creating continued uncertainty for businesses relying on the statute.

A Cautionary Tale: Healthcare Sector Settlements

Although arising in the healthcare context, recent pixel-related settlements provide a cautionary example for consumer-facing businesses. Cases involving Adena Health and The Christ Hospital resulted in multimillion-dollar settlements resolving allegations that patient data was shared with third parties such as Meta and Google through tracking technologies embedded on patient portals.

These lawsuits asserted claims including negligence, unjust enrichment, and violations of federal and state wiretapping laws. They underscore the significant exposure that can arise when sensitive personal data is alleged to have been disclosed without adequate consent.

Given the parallels between protected health information and nonpublic personal financial information, similar legal theories may be applied to other enterprises. In particular, the use of tracking technologies on authenticated pages—such as account dashboards, loan application portals, or payment interfaces—may present heightened risk.

Practical Considerations for Consumer-facing Businesses:

In light of the evolving litigation landscape, consumer-facing businesses should consider proactive risk mitigation steps, including:

- Conducting comprehensive audits of all tracking technologies (pixels, SDKs, cookies) across web and mobile platforms
- Avoiding or strictly limiting deployment on authenticated or customer-specific pages
- Implementing robust consent management mechanisms, including opt-in where required
- Ensuring that privacy disclosures accurately reflect actual data collection and sharing practices
- Reviewing third-party vendor agreements to address data use restrictions, confidentiality obligations, and indemnification

Coordinating between legal, compliance, and IT teams to ensure alignment between technical implementation and legal disclosures

Conclusion

Pixel tracking litigation represents a rapidly evolving area of legal exposure for businesses operating in a digital-first environment. While cases such as *Stevens v. TD Bank* demonstrate that not all claims will succeed, courts are continuing to grapple with how legacy privacy and wiretapping statutes apply to modern web technologies.

Pending legislation such as SB 690 may offer some relief, but it is unlikely to eliminate risk entirely. In the near

term, companies should expect continued litigation activity, increasingly sophisticated pleadings, and a patchwork of judicial interpretations.

Dialing Up Risk: Current TCPA Litigation and Regulatory Trends

The Telephone Consumer Protection Act (TCPA) remains a significant source of litigation risk for consumer-facing businesses across industries, with 2025–2026 marking a period of notable regulatory shifts, judicial reevaluation, and expanding theories of liability.

A Turning Point: Courts Reconsider Longstanding FCC Interpretations

Recent decisions have begun to reshape the TCPA landscape by limiting judicial deference to the Federal Communications Commission (FCC). Courts are increasingly interpreting the statute independently rather than relying on prior FCC guidance. This shift introduces substantial uncertainty, as long-standing assumptions—particularly around consent requirements—are now being revisited on a case-by-case basis.

In a significant 2026 appellate decision, the Fifth Circuit held that the TCPA requires only "prior express consent," rejecting the FCC's long-standing requirement of prior express written consent for certain telemarketing communications. *Bradford v. Sovereign Pest Control of TX, Inc*. This ruling signals a potential split in authority and underscores that consent standards—historically viewed as settled—are now in flux.

In doing so, the court rejected the Federal Communications Commission's (FCC) longstanding interpretation, concluding that the statute's text draws no distinction between written and oral consent and that "express consent" may be conveyed in either form. The ruling is among the first to directly address FCC interpretations of the TCPA following the Supreme Court's decision in Loper Bright Enterprises, which directs courts to interpret statutes independently rather than defer to agency guidance.

Consent Under Scrutiny: Revocation and One-to-One Requirements

Consent remains the central battleground in TCPA litigation, but the rules governing consent are evolving rapidly.

FCC rules that took effect in April 2025 clarify that consumers may revoke consent through any reasonable means, including replying "STOP" to a text message. Businesses must honor such requests within a defined timeframe, increasing operational and compliance demands across marketing, customer service, and IT systems.

At the same time, a proposed "global revocation" rule—which would require businesses to treat a single opt-out as applying to all communications—has been delayed until at least January 2027, reflecting industry concern and ongoing regulatory reconsideration.

Separately, the FCC's attempt to impose stricter "one-to-one consent" requirements, particularly in lead-generation contexts, has faced legal challenges and partial rollback. This has created continued ambiguity around whether consent obtained through third parties or comparison-shopping websites is sufficient for downstream outreach.

New Technology, Same Old Statute: AI and Expanding Liability Theories

Plaintiffs are increasingly testing how the TCPA applies to emerging technologies, particularly AI-driven communications and automated outreach tools. Courts and regulators are evaluating whether:

- AI-generated or synthetic voices qualify as "artificial or prerecorded" voices under the statute

- Modern messaging platforms fall within evolving definitions of autodialers
- Misdirected communications—such as calls or texts to reassigned numbers—trigger strict liability

Regulators have already indicated that AI-generated voices used in robocalls fall within TCPA restrictions, and plaintiffs' attorneys are actively expanding liability theories to encompass new forms of digital engagement.

For consumer-facing businesses that rely on automated communications for marketing, customer engagement, appointment reminders, or account notifications, these developments present heightened and evolving risk.

Regulatory Fragmentation and Increased Enforcement Risk

The TCPA enforcement landscape is becoming increasingly fragmented. While federal priorities continue to evolve, state attorneys general and private plaintiffs are driving much of the enforcement activity, often pursuing aggressive interpretations of the statute and parallel state consumer protection claims.

This creates a complex compliance environment in which businesses must navigate:

- Federal statutory requirements
- FCC rulemaking and guidance
- Diverging court interpretations
- State-level enforcement trends

The result is a patchwork of obligations and risk exposures that vary by jurisdiction and communication method.

Practical Considerations for Consumer-Facing Businesses

In light of these developments, businesses should reassess their TCPA compliance frameworks with a focus on:

- Consent capture and documentation, including clear records of how and when consent was obtained
- Revocation mechanisms, ensuring opt-outs can be processed easily and honored promptly across all communication channels
- Use of automated and AI-driven technologies, including whether disclosures and consent practices adequately address these tools
- Third-party vendor and lead-generation practices, particularly where consent is obtained indirectly
- Reassigned number risk mitigation, including number validation and database scrubbing
- Cross-functional coordination, aligning legal, marketing, and technology teams to ensure compliance in practice—not just on paper

Conclusion

TCPA litigation is entering a period of heightened uncertainty and transformation. Courts are reexamining foundational principles, regulators are recalibrating rules, and plaintiffs are advancing novel theories tied to emerging technologies.

For consumer-facing businesses, TCPA compliance is no longer a static exercise. It requires continuous monitoring, operational discipline, and a proactive approach to managing risk in an increasingly complex and unsettled legal landscape.

Junk Fee Litigation and Regulatory Trends

FTC "Junk Fee" Rule Enforcement (Post–May 2025)

The Federal Trade Commission's Rule on Unfair or Deceptive Fees, effective May 12, 2025, prohibits "drip pricing" and requires businesses in live-event ticketing and short-term lodging to disclose the total price—including all mandatory fees—upfront. Despite potential shifts in federal leadership, bipartisan scrutiny of hidden fees signals that enforcement is likely to remain active and sustained.

State-Level "Patchwork" Litigation

States are moving more aggressively than the federal baseline. Jurisdictions including California, Minnesota, Massachusetts, and Connecticut have enacted or expanded "junk fee" laws in 2025, many of which impose broader "all-in" pricing requirements. These statutes are fueling class action litigation under state UDAP frameworks, particularly where businesses fail to present a complete price at the outset.

Restaurant and Hospitality Service Fees

Recent legislation has provided partial clarity for restaurants—such as California SB 1524—which generally permits service charges if they are clearly disclosed. However, litigation trends in 2025–2026 show continued exposure where restaurants fail to prominently list these charges on menus or online ordering platforms.

Merchant Surcharges vs. Hidden Fees

While credit card surcharging is now permitted in most states, risk arises when these charges are framed as mandatory or are disclosed only at the end of a transaction. The central legal question in current litigation is whether the fee is genuinely avoidable (e.g., by paying with cash) or functions as a disguised mandatory charge.

Rise in Class Action Activity

Plaintiffs' firms are increasingly targeting digital interfaces—particularly e-commerce and booking platforms—where mandatory fees are introduced late in the checkout process. These cases often hinge on whether the initial advertised price is misleading under federal or state consumer protection laws.

Significant Legal Developments & Enforcement Trends

State AG Enforcement (2025): Attorneys General in Maryland and Pennsylvania reached settlements with auto dealerships over undisclosed "sales commission" fees and add-on products.

Texas Settlement: The Texas Attorney General secured a $9.5 million settlement with an online hotel booking platform for failure to disclose mandatory fees upfront—underscoring the financial exposure tied to non-compliance.

Card Fee Litigation (2025–2026): Ongoing challenges to the multibillion-dollar Visa / Mastercard interchange fee settlement continue, with merchant groups arguing it does not adequately address excessive swipe fees. Federal court review is expected to extend into 2026.

Illinois Surcharge Ruling (2026): In February 2026, a federal court upheld an Illinois law prohibiting the assessment of swipe fees on sales tax and gratuities—a notable development in the ongoing tension between merchants and payment processors.

Best Practices to Mitigate Risk

Audit Digital Checkout Flows: Ensure advertised prices reflect the true, all-in cost from the outset; avoid introducing mandatory fees only at the final stage.

Use Conspicuous Disclosures: Clearly and prominently disclose any mandatory service charges—especially in restaurants and hospitality—on menus, websites, and booking interfaces.

Track State Law Variations: For multi-state operators, compliance should be calibrated to the most restrictive jurisdictions (e.g., California), rather than relying solely on federal standards.