Shumaker

JULY 23, 2026 | PUBLICATION

Client Alert: Federal Court Declares Vivek Shah a Vexatious Litigant: What It Means for Businesses Facing CIPA Demands

INDUSTRY SECTOR

Technology

SERVICE LINE

Data Privacy
Technology

RELATED PROFESSIONALS

Brian C. Focht

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

A federal court has imposed a pre-filing order against the most prolific individual CIPA plaintiff. The order has important limitations. Businesses should understand both the development and its boundaries.

Demand Letters Everywhere, Businesses Strike Back

As we discussed in a previous Client Alert, businesses across the country have been receiving demand letters and draft complaints from Vivek Shah alleging that their websites violate the California Invasion of Privacy Act (CIPA). We have been closely tracking this dramatic increase in demands and assisting clients in responding.

On July 20, 2026, a federal court entered an order declaring Mr. Shah a vexatious litigant and requiring him to obtain the court's permission before he files a new lawsuit in the federal court for the Central District of California (the Order).

This is a meaningful development. Although it does not resolve the underlying legal questions or eliminate the risk of future demands, the Order provides useful context for any business evaluating how to respond to a Shah demand.

The Order

Judge. R. Gary Klausner of the United States District Court for the Central District of California, issued the Order in *Shah v. Crain Communications, Inc.*, Case No. 2:26-cv-03070-RGK-CTS on July 20, 2026.

In reaching its decision, the court applied a four-factor test to determine whether Mr. Shah meets the standard of a "vexatious litigant," which requires: (1) notice and opportunity for the litigant to be heard; (2)

an adequate record for review; (3) substantive findings of frivolousness or harassment; and (4) narrow tailoring. The court found all four factors satisfied.

Key findings from the court's analysis:

- Shah has filed at least 29 lawsuits from 2021 to 2026.
- In the past seven months alone, Shah filed seven nearly identical CIPA complaints against different defendants. None advanced past the initial pleading phase. All were dismissed voluntarily by Shah or dismissed by the court at the infancy of the case. *Notably, the court did not include in the Order whether any of those voluntary dismissals were the result of a settlement between the parties or, as the court appears to conclude, so that Shah would not be required to defend against a motion to dismiss.*
- Many complaints were template versions of Shah's own prior filings or near-copies of pending class action complaints filed by others.
- The court found that Shah's "record of: (a) seeking out CIPA violations and submitting enough search queries in an attempt to establish the amount in controversy for subject matter jurisdiction; (b) voluntarily dismissing cases upon a defendant's motion to dismiss; and (c) failure to try any CIPA (or other claims in the above record) on the merits, strongly indicates that Plaintiff's purpose is to harass defendants into coercive settlements—rather than seek redress from the judiciary in good faith."
- The court cited the California Court of Appeals: "A party who repeatedly files baseless actions only to dismiss them when challenged is no less vexatious than the party who follows the actions through to an adverse completion."
- The court noted that Shah is "well-acquainted with industry practices that may violate his privacy" and "has the means and knowledge to verify if a website is actively transmitting his search queries to a third party without his consent," making repeated claims of the same avoidable injury suspect. Essentially, the Order makes the argument that if a user expects their personal information will be shared with third parties when they visit a website, they have no expectation of privacy and thus cannot be injured. The result: Shah must obtain pre-filing permission before filing any new civil action in the Central District of California asserting claims under CIPA (Cal. Penal Code § 630, et seq.) or related consumer digital privacy statutes.

What the Order Does Not Do

This order has clear boundaries that businesses should understand:

- The order applies only to the United States District Court for the Central District of California.
- The order covers only claims arising under CIPA or related digital privacy statutes.
- The order does not prevent Shah from filing CIPA lawsuits in California state court, where many (if not most) CIPA claims are filed.
- The order does not prevent Shah from filing in any other federal district court.
- The order does not limit his ability to initiate or participate in arbitration.
- The order does not bar him from filing non-CIPA, non-privacy claims in the Central District of California. *Notably, only 15 of the 29 listed cases involved CIPA and/or digital privacy law violations, according to the Order.*
- Demand letters are not affected by this order. Shah may continue to send pre-litigation demands regardless of the pre-filing restriction.

In practical terms: the order narrows one avenue of litigation in one court. It does not remove the underlying risk.

Signs of a Shifting Tide or Setbacks that will be Reversed on Appeal?

Shah's recent losses in other proceedings suggest that judicial and arbitral decision-makers are increasingly skeptical of serial CIPA claims:

Shah v. TalentBridge, Inc. (Case No. 2:26-cv-00222-AH-SSCx, C.D. Cal.): Shah's First Amended Complaint was dismissed. The case is now on appeal before the Ninth Circuit.

Shah v. Pashion Footwear, Inc. (Case No. 2:26-cv-05124-PA-AS, C.D. Cal.): An arbitrator dismissed Shah's CIPA and Electronic Communications Privacy Act (ECPA) claims. Shah filed a petition to vacate the arbitration award in federal court but voluntarily dismissed it.

However, it is impossible to know for certain whether these recent losses are a true sign of change. The TalentBridge matter, along with several of the cases listed in the Order, are on appeal. Both the California Court of Appeals and the Ninth Circuit have proven to be receptive to allowing these types of claims to proceed. The vexatious litigant finding is expected to be appealed as well.

The legal landscape remains unsettled. Businesses should not treat these developments as a reason to defer compliance or refuse to take Shah's demand letters seriously.

Status of the Underlying Case

The vexatious litigant order has no direct bearing on *Shah v. Crain Communications, Inc.*, the very case in which the motion was brought. The court explicitly stated that the pre-filing order "does not place restrictions on the present case pending in this Court."

Briefs have just been submitted in connection with Crain Communications' pending Motion to Dismiss. That case will continue to develop and may produce further judicial guidance on the viability of CIPA website-tracking claims. However, given the judge's demonstrated skepticism of Mr. Shah's allegations of invasion of privacy, I expect the court to dismiss the matter and for Mr. Shah to appeal.

Practical Guidance: A Two-Pronged Approach

As we have detailed in previous client alerts, every response is situation-specific. However, companies that have received demand letters or are facing claims from Mr. Shah should take those claims seriously. Our advice generally comes down to a two-pronged approach:

Prong One: Compliance

Address the website activity behind the claim. The objective is to bring the website into compliance with applicable law and reduce the risk of a repeat demand from a different claimant.

Practical steps include:

- Conduct a technical audit of all third-party scripts, pixels, tracking tools, chat functions, search bars, and analytics currently active on the website.
- Identify which tools receive user input (search terms, form entries, chat messages) and determine where that data is transmitted.
- Remove or disable tools that are outdated, duplicative, improperly configured, or no longer necessary.
- Confirm that consent mechanisms (cookie banners, opt-in flows) actually prevent data collection until the visitor makes a selection. A banner that loads after scripts have already fired provides limited

protection.
- Apply heightened protections to sensitive pages: search fields, login pages, checkout pages, patient portals, job applications, and financial forms.
- Ensure your privacy notice accurately describes the tools in use, the information collected, and the third parties that receive it. An inaccurate privacy notice can increase risk rather than reduce it.

Prong Two: Response Strategy

The second prong concerns how the business communicates with Mr. Shah or other claimants.

Key principles:

- Avoid impulsive, overly eager, or hostile communications.
- Do not ignore a demand, but do not pay without investigation.
- Route all communications through legal counsel.
- Preserve evidence of the existing website configuration before making any changes.
- Document the current state so the business can later establish what the website did and did not do during the relevant period.

An informed, measured response, either through counsel or thoroughly reviewed by counsel, is generally more effective than paying it without analysis or uncoordinated communication between your company and Mr. Shah.

How We Can Help

Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line is ready to assist with both prongs of this approach.

On the legal side, we will review demand letters and draft complaints, evaluate the strength of the allegations, communicate with the claimant, negotiate resolutions, and defend against litigation. We have successfully negotiated outcomes ranging from reduced settlement amounts to complete withdrawal of the demand.

On the compliance side, we will assist you by conducting technical website audits, identifying problematic scripts and tracking configurations, and updating your privacy notice and cookie consent mechanisms. The end goal is to bring your website(s) into compliance both to help resolve the current dispute and to reduce the risk of future claims.

Contact Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line to discuss your situation.