

Customisation's new blind spot: generative AI and secondary liability for user-uploaded content

6 min read | 09 September 2026

 Dana Justus  Ivy Estoesta

Sterne, Kessler, Goldstein & Fox PLLC



Shutterstock/wk1003mike

Generative AI is weakening the customer assurances that customisation businesses have long relied on to avoid IP liability, making robust contracts and consistent enforcement more important than ever.

Customisation is everywhere in modern commerce, and many companies offering it carry more legal risk than they realise.

Apparel companies embroider customer logos onto jackets and shirts, print-on-demand vendors reproduce user-supplied artwork on mugs and canvases, and promotional companies turn an uploaded file into branded giveaways.

In each case, the company did not create the design; it is simply executing the customer's instructions and trusting the customer's word that the desired outcome does not infringe another company's IP rights.

Companies offering customisation may assume they sit in the same category of protection as an online marketplace, insulated by the familiar safe harbours that shield passive hosts.

In most cases, that assumption is wrong. Their protection rests instead on a different premise: that they can reasonably rely, in good faith, on the customer's representation that it owns or is authorised to use the uploaded content.

Generative AI is quietly eroding that premise, and brand owners and counsel should take notice.

Customisation companies are not marketplaces

When a company takes a customer's uploaded logo or artwork and applies it to products that it manufactures and sells, it is no longer hosting content. It becomes a direct commercial user of that trademark or creative work.

The Digital Millennium Copyright Act safe harbour under 17 USC § 512 and the passive-marketplace framework of *Tiffany (NJ) Inc v eBay Inc* do not reach conduct where the company itself places the design on the product and sells it.

Without that safe harbour, a customisation company's defence depends largely on its customer warranties, indemnities, a documented right to refuse or halt production on IP grounds, and an enforceable click-wrap agreement capturing the individual submitter's representations, warranties, and licence grant at the point of submission.

Any weakness in these provisions can directly impact the company's infringement exposure.

Where the contract layer can come up short

Because the contract layer carries the full weight of an IP infringement defence, any vulnerabilities tend to surface only when a dispute is already underway. Several recurring weaknesses are worth understanding.

A warranty and indemnity that do not match in scope

A warranty may promise only that content clears "trademark rights", while the indemnity reaches all intellectual property. If a rights holder brings a claim based on copyright, trade dress, right of publicity or design patent rights, the company can find the indemnity triggered but the corresponding warranty silent.

Terms built around "logos"

If the operative language is drafted for logo uploads, it may not reach everything else a customer submits (eg, text, names, titles, slogans, mascots and professional

credentials). Each of those can carry third-party rights of its own and would fall outside a logo-focused promise.

Content that never passes through a warranty at all

If the customer's assent is confirmed at one submission point but not another, a category of submitted material might end up with no warranty or licence attached to it, even though it is reproduced and sold like everything else.

A counterparty who may not be who they claim

In group or team orders, the person clicking through the agreement might be claiming to bind an organisation they do not actually represent. If the terms run only against the organisation and the organisation later disavows the submitting user, the company can be left without an enforceable counterparty.

Uncertainty about who actually agreed and to what

A warranty is only as valuable as the ability to show that a specific, identifiable person assented to a specific version of the terms. Where that record is thin, the enforceability of the entire promise becomes contestable.

Each of these issues is easy to overlook in isolation, but any one of them can be the difference between an infringement defence that holds and one that fails.

Often, however, the most significant exposure arises because customisation programmes evolve while the contractual framework does not. A company may believe it has robust customer representations and warranties in place, only to discover during a dispute that certain categories of content, submission channels or users never became subject to those protections at all.

Generative AI's impact

The contract layer was built on a central assumption: the customer is in a position to know and truthfully represent whether they have the rights to use the uploaded content.

Generative AI now erodes that assumption before any rights holder ever objects.

A decade ago, a customer uploading a polished logo most likely obtained it from a designer, employer, school or team, and that provenance itself served as a proxy for authorisation. Today, a customer can generate a professional-looking logo or design in seconds using generative AI, injecting uncertainty into a customisation company's risk assessment.

For example, a customer who asks an AI tool for a "vintage university crest" for a custom baseball hat may receive something that appears original, but may in fact

closely resemble a real university's protected marks, and neither the customer nor the customisation company may recognise the resemblance.

Even when AI-generated output appears entirely original, it may reproduce or closely evoke a protected trademark, copyrighted work or other IP, and the risk is not limited to logos; the same tools can produce the text, names, slogans and mascots that might fall within the contractual gaps discussed above.

These possibilities undermine the reliability of the representation that underpins an IP infringement defence; when a customer does not fully understand the provenance of AI-generated content, the representations underpinning an infringement defence become less reliable.

At the same time, AI dramatically increases the volume of borderline submissions, outpacing any realistic human review process.

The knowledge question, and why enforcement records matter

Secondary liability has always turned on knowledge. Once a rights holder objects to the use of its IP on a product and the company keeps producing it, the good-faith premise collapses and wilful-blindness exposure follows.

The direct-user posture makes this harder, not easier. As the US Supreme Court's [2026 ruling in Cox Communications v Sony Music Entertainment](#) confirmed, even platforms that qualify for safe-harbour protection can lose it through inconsistent or undocumented enforcement. A customisation company that cannot claim that protection in the first place is even more exposed if it is unable to show that it tracked notices, applied its rules evenly and acted on what it learned – regardless of how well its terms read.

Generative AI sharpens that problem from both directions. It makes questionable content easier to create and harder to detect, which cuts against any claim of no reason to know, while multiplying the volume of representations a company is relying on and making each one less trustworthy.

None of these considerations should prompt companies to move away from customisation options, which remain valuable and – when handled thoughtfully – defensible. But it does suggest that companies leaning on the good-faith reliance framework should revisit whether that reliance is still reasonable when the customer may not know what they uploaded thanks to generative AI.

For now, the safest assumption is that customer representations carry less certainty than they once did, and that the gap between what a warranty promises and what it can deliver will only widen as generative AI becomes more pervasive.

Dana Justus

Counsel

Sterne, Kessler, Goldstein & Fox PLLC

djustus@sternekessler.com

Ivy Estoesta

Director

Sterne, Kessler, Goldstein & Fox PLLC

iestoest@sternekessler.com

Copyright © 2026 LBR trading as Centellic Company Number: 03281866 VAT: GB 160 7529 10