ARTIFICIAL INTELLIGENCE + CONSUMER GOODS AND RETAIL

Legal red teaming for retail companies

As AI capabilities continue to expand, so do actions against retailers for alleged misuse of this new technology. Regulators, State Attorneys General, and private litigants are exploring ways to hold retailers to account for perceived misuses of generative AI (GenAI) and large language models (LLMs), spanning issues of consumer protection, fraud, product liability, and data privacy that could affect customer interactions and satisfaction. The use of AI chatbots in retail is becoming more common, but these chatbots can pose significant risks if not properly tested and monitored. Companies that invest proactively in legal and technical testing could avoid far costlier enforcement actions and consumer claims.

DLA Piper's legal red teaming services offer a comprehensive approach to identifying and mitigating legal, compliance, and reputational risks that are not surfaced through traditional technical testing. We have performed legal red teaming for multiple Fortune 100 clients, and, in 2024, the Financial Times described our legal red teaming as the best new service to manage legal risk. By combining legal and technical knowledge, we deliver next-level red teaming protocols under privilege.

The challenge

Traditional red teaming approaches could fall short of emerging standards

Lawmakers around the world are adopting AI red teaming as an industry-standard approach to testing GenAI and LLMs for adherence to safety, fairness, and compliance standards.

100+

Lawyers, data scientists, coders, and policymakers focused on AI worldwide

Gen AI Litigation Powerhouse
BTI Consulting Group 2026

AI Leading Lawyer
Danny Tobey
Band 1
Chambers USA 2025

Spotlight:
Global Market Leaders
Artificial Intelligence
Chambers Global 2025

Innovation in New Services to Manage Risk
Financial Times 2024

Best Use of AI
Law.com 2024

Red teaming typically uses adversarial techniques to uncover flaws and vulnerabilities in an AI system, including harmful or biased outputs, unexpected or undesirable behaviors, limitations, or potential misuse of the system. However, traditional red teaming does not address additional legal, regulatory, and technical complexities that arise when applying LLMs in consumer-facing settings.

Our multidisciplinary approach

Next-level red teaming protocols

Our approach moves beyond traditional red teaming's focus on a narrow range of technical factors, instead addressing the complex web of legal, compliance, and regulatory frameworks that accompany the use of GenAI in consumer-facing applications.

Hybrid attorney and automated approach

We combine attorney experience and automated tools to risk-assess and thoroughly test models from all angles. Our process begins with a collaborative effort between our attorney subject matter experts and technical team to develop a risk taxonomy that identifies areas of potential legal, regulatory, and reputational exposure based on the specific functionality, technological underpinnings, and audience of the AI tool. Our teams then interrogate the model using strategies designed to evaluate areas of potential exposure, particularly seeking to identify problematic patterns of response that elevate legal, compliance, and reputational risk. In addition to deep-dive testing to "depose" the AI tool, we use our own AI technology to exponentially increase testing volume, enabling us to evaluate our clients' AI tools cost-effectively at scale.

Future-proofing innovation

While emerging AI regulations lack clarity, they will likely touch on audits and reporting. We can conduct the forensic audits you need to future-proof against anticipated legislation and policy and ensure you're using AI responsibly and effectively – all under attorney-client privilege.

Remediation and monitoring

Using our combined legal and technical experience, our team translates our findings into actionable mitigation strategies and remediation recommendations. We test remediation efforts to ensure risk reduction and prepare documentation of our findings and recommendations. We regularly work with red teaming clients to develop strategies for spot-testing or ongoing monitoring to mitigate risks associated with changes to the underlying model or model drift. Leveraging our strategic alliance with Scale AI, we can help explore other remediation options, such as finetuning models to mitigate legal risks and conducting technical red teaming for cybersecurity risks.

Risk mitigation under privilege

With a fully integrated legal and technical team under one law firm roof, we can deliver technical red teaming solutions while maintaining a strong argument for attorney-client privilege. This allows us to test and remediate GenAI for the benefit of customers and employees without creating a potentially problematic regulatory or litigation record. Final testing can be performed for a public-facing or regulatory report after development and refinement are completed.

Key benefits for retail companies

Risk identification

Our legal red teaming protocol helps uncover key vulnerabilities in your AI chatbots, including potential consumer protection violations, biases that could affect customer interactions and satisfaction, and data privacy issues. The first wave of chatbot litigation has proven that GenAI outputs can, and often will, end up in publicly filed complaints, making it all the more valuable to pressure test these systems and understand their weaknesses.

Enhanced customer experience

By engaging directly with your AI systems, we can help ensure that they provide accurate and reliable information to customers, enhancing shopping experiences and building trust in your brand.

Regulatory compliance

Our approach includes assessment of compliance with industry-specific regulations and standards – for example, evaluating whether a chatbot appropriately responds to queries identifying a product safety issue or the input of a minor's personal information – helping retail companies adhere to legal and regulatory requirements.

Reputational risk mitigation

We identify and address potential reputational risks, including harmful or offensive GenAI outputs. We have elicited controversial political, social, and brand-related statements from our clients' chatbots that, without appropriate guardrails, could have been headline-worthy.

Tailored solutions

We offer customized red teaming services tailored to the unique needs and objectives of retail companies, ensuring that our solutions are relevant and effective. Our approach takes into account your brand strategy, the type of GenAI tool involved, target user base, and prior regulatory enforcement history, among other factors.

Case study

Legal red teaming of a Fortune 50 retail chatbot

We conducted legal red teaming of a large retail company's first consumer-facing chatbot. Our work helped the client identify key vulnerabilities in the system which, if left unchecked, could have put our client at risk for enforcement activity, private litigation claims, and reputational harm. Our red teaming protocol focused on, and thus helped mitigate, the following potential vulnerabilities:

- Consumer protection risks
- Litigation risk from pricing-related errors and hallucinations
- Data privacy concerns
- Inconsistent safety and defect reporting avenues
- Reputational risks
- Deficiencies in compliance with AI-specific regulations

Getting started

Our solutions are always tailored to your unique needs and objectives. That is why our approach to red teaming starts with a privileged discovery session designed to help us learn about your existing models, identify your definition of success, and develop a bespoke approach and timeline. Our customized red teaming services are specifically tailored to the unique needs and objectives of retail companies, ensuring that our solutions are both relevant and effective.

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa, and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com

Key contacts

Danny Tobey M.D., J.D.
Partner
Chair, AI and Data Analytics
Dallas
T +1 214 743 4538
Email

Ashley Allen Carr
Partner
Austin
T +1 512 457 7251
Email

Barclay Blair
Senior Managing Director
AI Innovation Lead
New York
T +1 512 457 7251
Email

Zev Eigen J.D., Ph.D.
Senior Director,
Data Science
Los Angeles
T +1 310 595 3126
Email

Oct 27 2025 | CGR_S2 Legal red teaming for retail companies_v4LM