



MAYER|BROWN

THE RISKS AND DISPUTES THAT MAY ARISE IN THE NEXT ITERATION OF AGENTIC AI SOLUTIONS

Reginald Goeke



USE OF, AND CONTRACTING FOR, AI AND AGENTIC AI CONTINUES TO INCREASE

89%

- Organizations use AI in at least 1 business function (56% report using AI in 3 or more functions).

44%

- Organizations are scaling the usage of AI systems.

80%

- Organizations are asking their partners for GenAI capabilities and Agentic solutions.

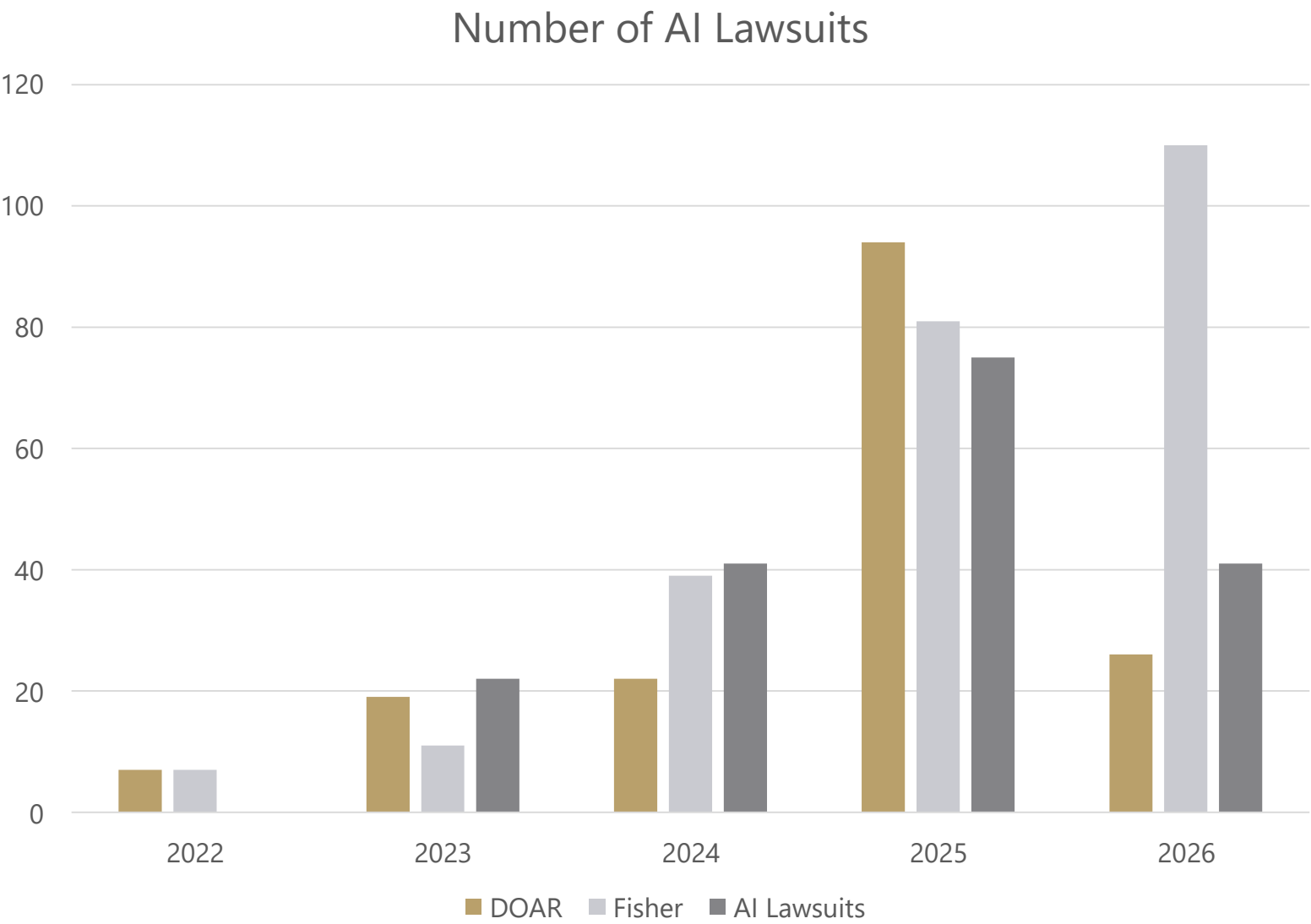
44%

- 44% of outsourcing contracts now include AI components.

31%

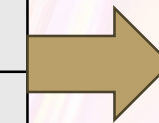
- Organizations with over \$1B in revenue are scaling use of agentic AI; another 16-29% are piloting agentic AI use.

AI-RELATED LITIGATION IS GROWING



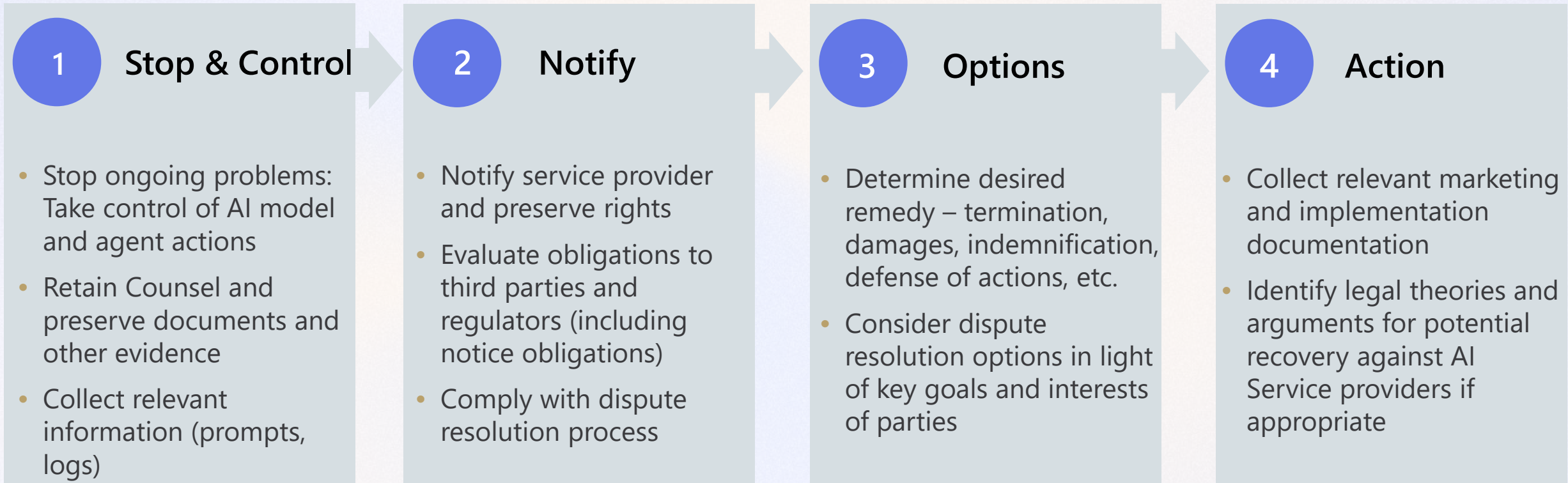
AGENTIC AI PROVIDERS CREATE MANY HURDLES TO CLAIMS RESULTING FROM THE USE OF THEIR TOOLS

	Hurdles to Recovery
Liability Limits	• “As-is” provisions • Highly limited warranty provisions • Liability shifting provisions (based on model use)
Proof Issues	• Proving model was source of error; proving breach of duty/guardrails • Proving company conduct not at fault
Damages Limits	• Limits on consequential and indirect damages • Remedy limits and liability caps
Indemnity Limits	• Limits on indemnity (e.g., for gross negligence) • Limits on amounts and/or provisions regarding defense
Termination / Disputes	• Limited bases for contract termination as of right • Required dispute resolution procedures that create potential procedural hurdles



Risks and liability from Agentic AI use fall on the user

WHAT TO DO WHEN DISPUTES/ISSUES ARISE?





LITIGATION RISKS ARISING FROM AGENTIC AI

- AI failure to perform as promised
- AI causes injuries to third parties
- Disputes over IP rights
- Data Privacy and Security risks
- Regulatory violations

AI FAILURE TO PERFORM

Types of Potential Failures

- Agentic AI error in transactions
- Failure of AI Agent to perform in day-to-day activities
- AI update that degrades performance
- AI infinite loops
- Regulations that preclude use of AI tool

Examples

- Instruction to purchase 10 chairs at \$100 apiece executes as 1 chair bought 1000 times
- Mis-identifying sales opportunities and mis-scheduling meetings
- Failure to address or notify company of customer complaint
- Supplier throttles back capabilities to manage potential risks
- Agentic AIs operate for hours or days, resulting in massive use of AI tokens
- Adoption of regulations that materially limit use of AI tool (such as limits on use for compliance)



AI FAILURE TO PERFORM

Hurdles to Recovery	Potential Responses
Liability / Damages limits	 • Product liability / product design was grossly negligent (circumventing liability limitation) • Fraudulent inducement (AI-washing) (to circumvent warranty, damages limits) • Implied duties not expressly stated in agreement (e.g., duty of good faith)
Proof Issues	 • Evidence demonstrating company properly used models (governance/prompt history) • Seek model logs if possible
Termination limits	 • Claims to permit early termination (e.g., material breach, fraudulent inducement) • Claims to permit rescission (e.g., frustration of purpose)

AI INJURES THIRD PARTIES

Examples of Potential Third-Party Injuries:

- Agentic AI hacks third-party site and extracts proprietary information
- AI agent designed to market product may publish disparaging remarks regarding competitor product
- Automated customer service system induces purchases based on inaccurate representations
- AI agent may access third-party site in violation of user terms precluding agentic access
- AI agent may deny claims (insurance) or loans (housing) based on improper criteria (e.g., discrimination)



THIRD-PARTY INJURIES

Hurdles to Recovery	Potential Responses
Limited warranties / Indemnification / Damages limits	 • Demonstrate model operated outside guardrails promised by AI company • Gross negligence / strict liability claim • Evidence of marketing regarding reliability of model (e.g., fraud, fraudulent inducement claim)
Proof Issues	 • Demonstrate that model was operated as expected and with proper safeguards (governance, prompts, controls)
Disputes over who must / is able to defend	 • Exercise rights under indemnification provisions: – Control defense if possible (and if claim involves regulatory, reputational risk or critical customer risk) – Consider potential arguments about conflicts with vendor indemnitor



IP CLAIMS ARISING FROM AI MODEL ACTIONS

Examples of Potential IP Claims Arising from AI Model Use:

Third-party IP

- Generative AI is trained on unlicensed information and/or creates output that infringes on copyrighted works
- Agentic AI that scrapes third-party web sites may trigger claims of IP theft
- Agentic AI obtains proprietary or trade secret information from third parties, or copies proprietary source code

Disclosure of User IP

- Agentic AI discloses (or is trained on) trade secret or other proprietary information

Dispute over IP Rights

- AI provider with access to company prompts and data creates IP overlapping with the user company's information, or develops a business that impacts the user's business

IP DISPUTES ASSOCIATED WITH AI USE

Hurdles to Recovery	Potential Responses
Limits on IP indemnification	→ • Determine if claim falls within IP indemnification provision • Demonstrate that company conduct does not give defense to IP indemnification
Proof issues (disclosure of information) — e.g., was it model error or user error	→ • Demonstrate model exceeded guardrails • Demonstrate responsible company conduct
Limits on consequential damages	→ • Allege gross negligence • Fraud/Inducement (e.g., marketing regarding model controls and respect of IP)
Proof issues (model provider misuse of user information)	→ • Enforce use restrictions • Audit rights if available



CYBERSECURITY AND PRIVACY CLAIMS ARISING FROM AI MODEL ACTIONS

Examples of Potential Cybersecurity Claims:

Customer Data

- Agentic AI given access to customer information on corporate database discloses that data to third parties through its outputs, shared system logs, or persistent memory (resulting in third-party data breach claims)

Proprietary Information

- Agentic AI accesses and discloses proprietary and/or trade secret data either due to access rights given to AI, or due to AI hacking of systems to which not given authorization

Third-party attacks

- Third parties may engage in code or prompt injection, using AI tool to access proprietary information (e.g., by bypassing authorization checks)
- Similar attack may trap AI model into recursive reasoning loop, triggering continuous calls to paid APIs or deadlocking system resources

CYBERSECURITY ISSUES

Hurdles to Recovery	Potential Responses
Indemnification limits (customer data)	→ • Determine if claim is indemnifiable; demonstrate that company actions did not contribute
Proof issues (leak of proprietary information)	→ • Demonstrate sound governance/operation • Seek logs
Proof issues (third-party attack; duty of care)	→ • Develop expert analysis on reasonable designs for Agentic AI tools • Marketing on AI capabilities (fraud claim)
Liability and damages limits	→ • Product liability/design defect; gross negligence • Fraudulent inducement



REGULATORY VIOLATIONS BY AGENTIC AI

Examples of Potential Regulatory Violations:	
Consumer Protection	• Agentic AI that sells or advertises products in a way that violates consumer protection or safety regulations (deceptive advertising, discriminatory advertising) • Agentic AI that decides loan application or insurance claim in ways that violate consumer protection, discrimination, or health care laws
Antitrust	• Agentic AI conducting sourcing/purchasing and collaborates with other AI on bids, or engages in tit-for-tat strategies that stabilize prices above equilibrium • Agentic AI that shares data with other market participants on costs or prices
Other regulations	• Automated order spoofing (securities regulation) • Use of AI agents for screening, interviewing may violate labor, employment, ADA laws

REGULATORY VIOLATIONS

Hurdles to Recovery	Potential Responses
Limits on liability / company assumption of risk (human in loop)	 • Fraudulent concealment/misrepresentation (marketing materials) • Liability limitation is unconscionable and against public policy
Proof issues (model error or user error; standard of care)	 • Model controls/governance/prompts • Forensic analysis of conduct
Damage limits (regulatory fines treated as consequential damages)	 • Recategorize damages as direct damages (regulatory fine is the immediate, straight-line result of agent going rogue) • Argue that the Agentic AI provider is actually the principal actor to whom responsibility should be assigned

TAKEAWAYS: BE PREPARED FOR AGENTIC AI RISKS

- As agentic AI is increasingly adopted, it will create significant litigation and other risks.
- Service providers will look to deflect and shift that risk to companies deploying the agentic AI (through contractual and other limits).
- Companies should adopt governance, controls, logs, and other tools to demonstrate their own responsible use.
- When issues arise, stop actions and preserve status quo, notifying necessary parties, consider options, and then act.
- Third-party contracts will likely constrain ability to recover, but arguments are available to help obtain contributions from AI provider.