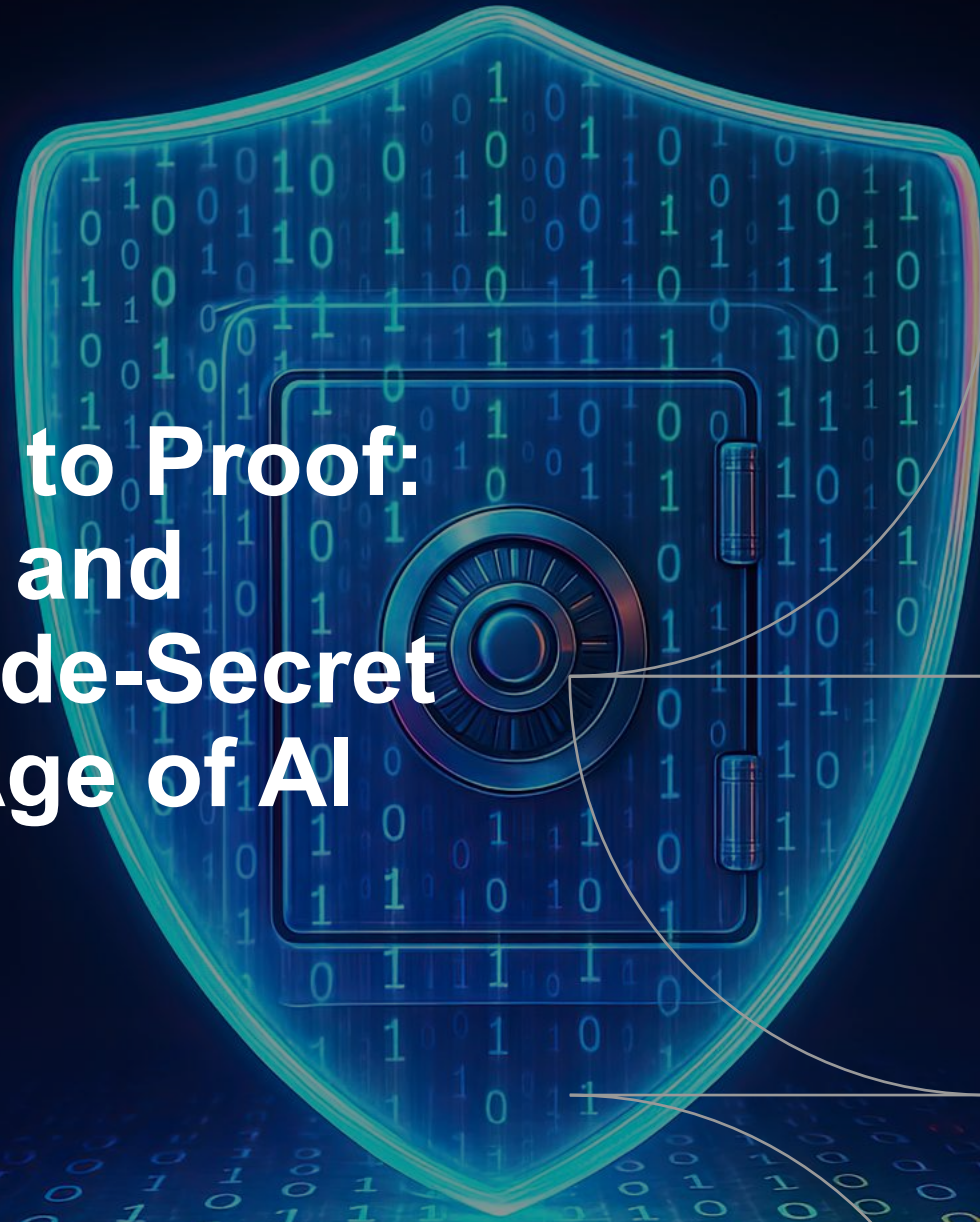




From Prompt to Proof: Investigating and Litigating Trade-Secret Theft in the Age of AI

September 9, 2026



Legal Disclaimer

This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal or expert opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

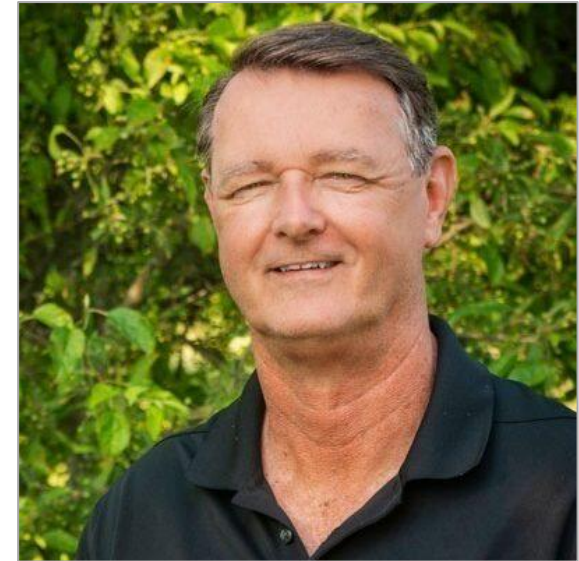
Speakers



Jesse Coleman
Partner
Houston



Gio Perez
Associate
Houston

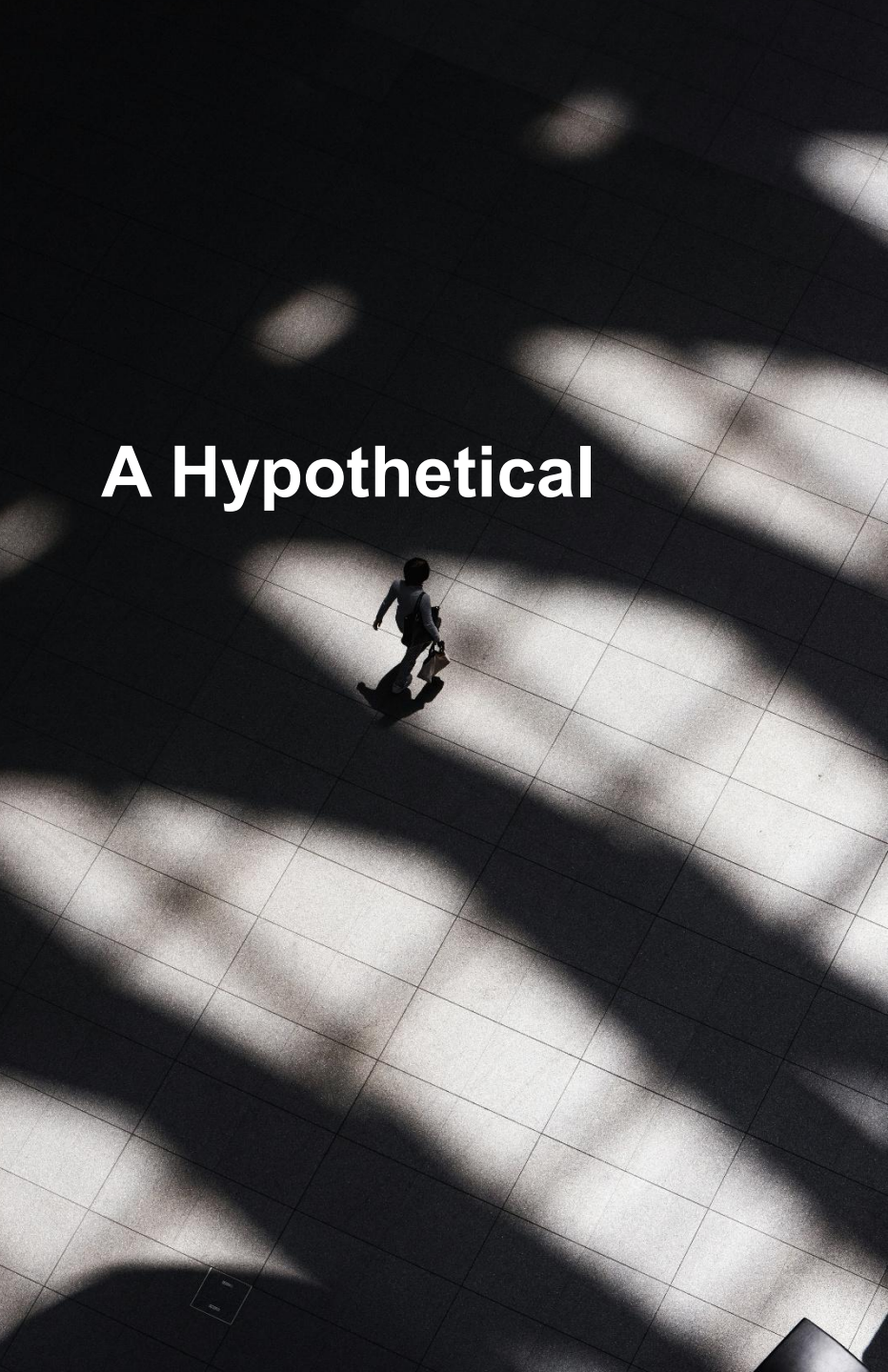


Jim Vaughn
Senior Managing
Director – Digital
Forensics & eDiscovery
iDiscovery Solutions



Agenda

- 1. Legal Framework and Emerging Litigation Risks**
- 2. Governance and Prevention**
- 3. Digital Forensics and Investigation**



A Hypothetical

The Departing Executive

A senior sales executive planning to join a competitor uploads the company's customer list, pricing history, renewal data, and sales notes to a personal AI account.

She asks the tool to identify the 25 most vulnerable accounts, create a competitive pricing strategy, and rewrite the results as a "market-entry plan" that contains none of the source documents' original language.

She deletes the local files and leaves with only the AI-generated plan.

Has a trade secret been misappropriated?

From Shadow AI to Litigation Risk

AI Use Is Expanding Outside Company Controls

68%

Access public GenAI assistants for work through personal accounts

57%

Admit entering sensitive or high-risk information into public GenAI assistants

1,500+

Federal trade-secret cases filed in 2025, an all-time high

Sources: TELUS Digital “AI at Work” survey; Lex Machina 2026 Trade Secret Litigation Report.

What Qualifies as a “Trade Secret” Under the DTSA?

DTSA - 18 U.S.C. § 1839(3).

- **Protectable Information**
 - Financial, business, scientific, technical, economic, or engineering information
 - Methods, techniques, processes, programs, code, designs, plans, and compilations
 - Tangible or intangible, and stored in any form
- **Reasonable Measures**
 - The owner takes reasonable measures to keep the information secret
- **Independent Economic Value**
 - The information derives actual or potential economic value from not being generally known
 - And not readily ascertainable through proper means

Four Categories of AI-Related Trade Secrets

AI Can Receive, Build, Create, and Combine Trade Secrets

1. Inputs Provided to AI

- *A sales team uploads confidential customer pricing and renewal data to identify accounts most likely to leave.*

2. Assets Used to Build AI

- *A company develops a proprietary process for cleaning and labeling data used to fine-tune an industry-specific model.*

3. AI-Generated or Enhanced Assets

- *An AI system analyzes years of testing data and identifies a more efficient manufacturing process, including approaches that consistently fail.*

4. The AI Stack as a Compilation

- *A company combines proprietary data, a third-party model, custom prompts, human review, and internal workflows to produce a unique forecasting tool.*



Does Submitting Information to an AI Tool Destroy Trade-Secret Status?

Not necessarily. It Depends on the Disclosure.

Disclosure to an AI provider is not automatically fatal, but disclosure without appropriate protections may defeat “reasonable measures.”

The Tool

- Was it an approved company tool or personal account?
- Can the provider use, retain, or access the information?
- Could the information reach other users or customers?

The Protections

- Must the provider keep the information confidential?
- Who within the company or provider can access it?
- Can the company monitor and retrieve AI activity?

The Company’s Conduct

- Was the employee authorized to submit the information?
- Did the company communicate and enforce its AI policy?
- Did the company investigate and contain the disclosure?



Case Example: When AI Use Becomes the Disclosure

***Trinidad v. OpenAI, Inc.* (N.D. Cal. Jan. 5, 2026)**

Alleged Trade Secrets

- Plaintiff claimed that OpenAI misappropriated proprietary AI “protocols and frameworks” developed through interactions with ChatGPT.

No Reasonable Measures

- By developing the frameworks through ChatGPT, plaintiff voluntarily disclosed the information to OpenAI.
- OpenAI had no obligation to maintain the information’s confidentiality.
- Ownership of the ideas or resulting output did not establish that the information remained secret.

Terms of Use Controlled the Disclosure

- Accepting OpenAI’s Terms constituted consent to disclosure for the trade-secret analysis, regardless of whether that consent was enforceable as a contractual matter.
- The court dismissed the DTSA claim and the entire complaint with prejudice.

“Because she “disclose[d] [her] trade secret to others who are under no obligation to protect the confidentiality of the information, . . . [her] property right is extinguished.”

Trinidad v. OpenAI Inc., No. 25-cv-06328-JST, 2026 U.S. Dist. LEXIS 1129, at *10 (N.D. Cal. Jan. 5, 2026) (quoting *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984)).

A magnifying glass with a green handle and silver rim is positioned over a stack of papers. The papers are of various colors (white, orange, yellow, red) and are bound with white string. The magnifying glass is focused on the papers, and the text 'AI Raises the Stakes for Trade-Secret Identification' is overlaid on the image.

AI Raises the Stakes for Trade-Secret Identification

“Our AI platform” may not be specific enough.

Name the secret: What, exactly, is protected?

Trace its history: Where did it come from, and how was it protected?

Connect it to value: What competitive advantage and damages are attributable to it?

***Trinseo* Cautionary Tale**

10 asserted → 4 misappropriated → \$75 million verdict vacated

“[W]here a plaintiff alleges multiple trade secrets, the jury must have a reasonable basis to award damages attributable only to the information or technology that actually qualifies as a trade secret.”

Trinseo Europe GmbH v. Brown, 165 F.4th 399, 412–13 (5th Cir. 2026) (footnote omitted).

AI Complicates Proof of Use

The Evidence May No Longer Look Like the Trade Secret

Traditional Use

Trade secret → copied file → same information used by competitor

AI-Assisted Use

Trade secret → summarized, translated, coded, or synthesized → new output or business strategy

The Plaintiff Still Must Prove

- What entered the AI process
- How the information was transformed or used
- What output, value, or competitive advantage resulted

Responding to AI-Assisted Misappropriation

Preserve First. Investigate Quickly. Tailor the Remedy.

Preserve → Investigate → Contain → Remediate

Preserve

Accounts, prompts, files, and logs

Investigate

Input, transformation, output, and use

Contain

Restrict use and segregate affected work

Remediate

Delete derivatives and certify nonuse

Returning the source file may not eliminate the output or the competitive advantage.



Revisiting the Hypothetical

The Departing Executive, Reconsidered

Is it a trade secret?

The customer list, pricing history, and renewal data derive value from not being known — if reasonable measures were in place.

Did the disclosure defeat those measures?

A personal account with no confidentiality obligation, and a provider free to retain or use the information.

Can use be proven?

The plan borrows none of the original language, so proof runs through the input, the transformation, and the resulting advantage.

What does the response look like?

Preserve the account and prompts, investigate, contain, and remediate — deleting the local files does not delete the output.

The market-entry plan may be new. The advantage it carries is not.

AI Controls Across the Employee Lifecycle

Recruiting & Onboarding

- Keep prior-employer information out
- Identify approved AI tools and uses
- Provide role-based training

During Employment

- Define protected AI assets
- Control access, inputs, and integrations
- Require periodic training and certifications

Departure

- Ask about personal AI accounts and AI-derived materials
- Preserve relevant activity before deletion
- Revoke access, tokens, plugins, and API credentials

Policy

Replace a Binary Policy with an AI Use Matrix

Move Beyond “Do Not Use AI”

- **Permitted**

Public information and approved routine uses

- **Controlled**

Internal information with safeguards

- **Approval Required**

Trade secrets, regulated data, and privileged material

- **Prohibited**

Prior-employer data, evasion, and unauthorized agents

AI Vendor Diligence

Know Where Your Data Goes

- **Use:** Training or service improvement?
- **Access:** Who can see the data?
- **Retention:** How long is it kept?
- **Ownership:** Who owns inputs and outputs?
- **Evidence:** What can be preserved and exported?
- **Remedies:** Who bears the risk?

Contracting for AI Use

Key Terms

Ownership: Who owns the inputs, outputs, and custom work?

Confidentiality: Who can access the data, including personnel and subprocessors?

Use: Can the provider use the data for training or service improvement?

Retention: How long are prompts, files, outputs, and logs kept?

Evidence: Can records be preserved and retrieved for an investigation?

Five Prompts, Five Different Risks

1. **“Rewrite this public press release.”**
Low risk: public input and routine drafting
2. **“Summarize this confidential customer complaint.”**
Confidentiality and vendor-retention risk
3. **“Compare our nonpublic price list with the competitor proposal attached.”**
Trade-secret and third-party information risk
4. **“Use these 500 customer files to develop a churn model.”**
Customer-data, access, retention, and output-ownership risk
5. **“I just joined from Competitor X. Build a sales strategy from my former account notes.”**
Potential misappropriation and prior-employer trade-secret risk

A black and white photograph of a heavy metal padlock and chain on a wooden surface. The padlock is a circular, stainless steel model with a keyhole and a small circular mark in the center. It is attached to a thick, dark metal chain that loops around a rough, textured wooden post. The lighting is dramatic, highlighting the metallic sheen of the padlock and the grain of the wood.

Build the Record
before the Dispute

Reasonable Measures Must Be Provable

- **Govern:** Policies, classifications, and ownership
- **Train:** Role-based guidance and certifications
- **Control:** Access, approved tools, and monitoring
- **Document:** Vendor diligence and exceptions
- **Respond:** Preserve, investigate, and remediate



The Hypothetical, Again

What Would Have Changed the Outcome

A use matrix instead of a ban

Customer and pricing data would have been approval-required, not a judgment call made alone.

An approved tool with real terms

No training on customer content, no secondary use, and no personal accounts for company data.

Access and logging

A record of what was uploaded, when, and by whom — evidence that exists before the dispute.

Identification done in advance

The secret named, its history traced, and its value tied to the accounts it protects.

The measures that defeat the claim are the same ones that would have prevented it.

Where the Evidence Resides

Follow the Evidence Across Six Environments

1

Ex-Employer Endpoint

Deleted files, shadow copies, browser, USB and recent-file artifacts

2

Network & SaaS Logs

DLP, proxy, VPN, CRM exports, audit and OAuth records

3

AI Vendor Account

Prompt history, uploads, account activity and login timestamps

4

Personal Devices

Laptop, phone, cloud storage, webmail and messaging

5

New Employer

Email, Teams or Slack, file metadata, CRM and outreach

6

Backups & Immutable Logs

Endpoint backups, SIEM and DLP records that outlast deletion

Start with the most durable sources, then connect the artifacts into a timeline.

Expedited Discovery

Target Preservation, Imaging, and a Narrow Search Protocol

- 1 PRESERVE** Litigation hold and preservation order for the individual and new employer
- 2 IMAGE** Forensic images and targeted examination of relevant personal sources
- 3 OBTAIN** AI-vendor activity, prompts, uploads, metadata and system access logs
- 4 SEQUESTER** New-employer plan and derivatives pending review; certify receipt
- 5 TESTIFY** Limited deposition on inputs, account, outputs, use and current copies

A TRO or preliminary-injunction record should focus on emergency facts, not open-ended review.

Prevent, Detect, Preserve

Controls That Would Have Changed the Outcome

PREVENT	DETECT	PRESERVE
AI acceptable-use policy Prohibit confidential data in personal AI accounts Approved enterprise AI Provide a legitimate tool with appropriate terms Need-to-know access Limit full customer and pricing exports by role	DLP and CASB Flag bulk exports and unsanctioned AI uploads UEBA Detect anomalous downloads before departure Audit logging Record traffic, OAuth grants and file activity	Departure protocol Preserve devices before wiping or reissue Log retention Keep proxy, CASB, SIEM and DLP records Investigation readiness Define owners, escalation and preservation steps

Layer policy, access, monitoring and preservation so the company can act before evidence disappears.

thank you

Jesse Coleman

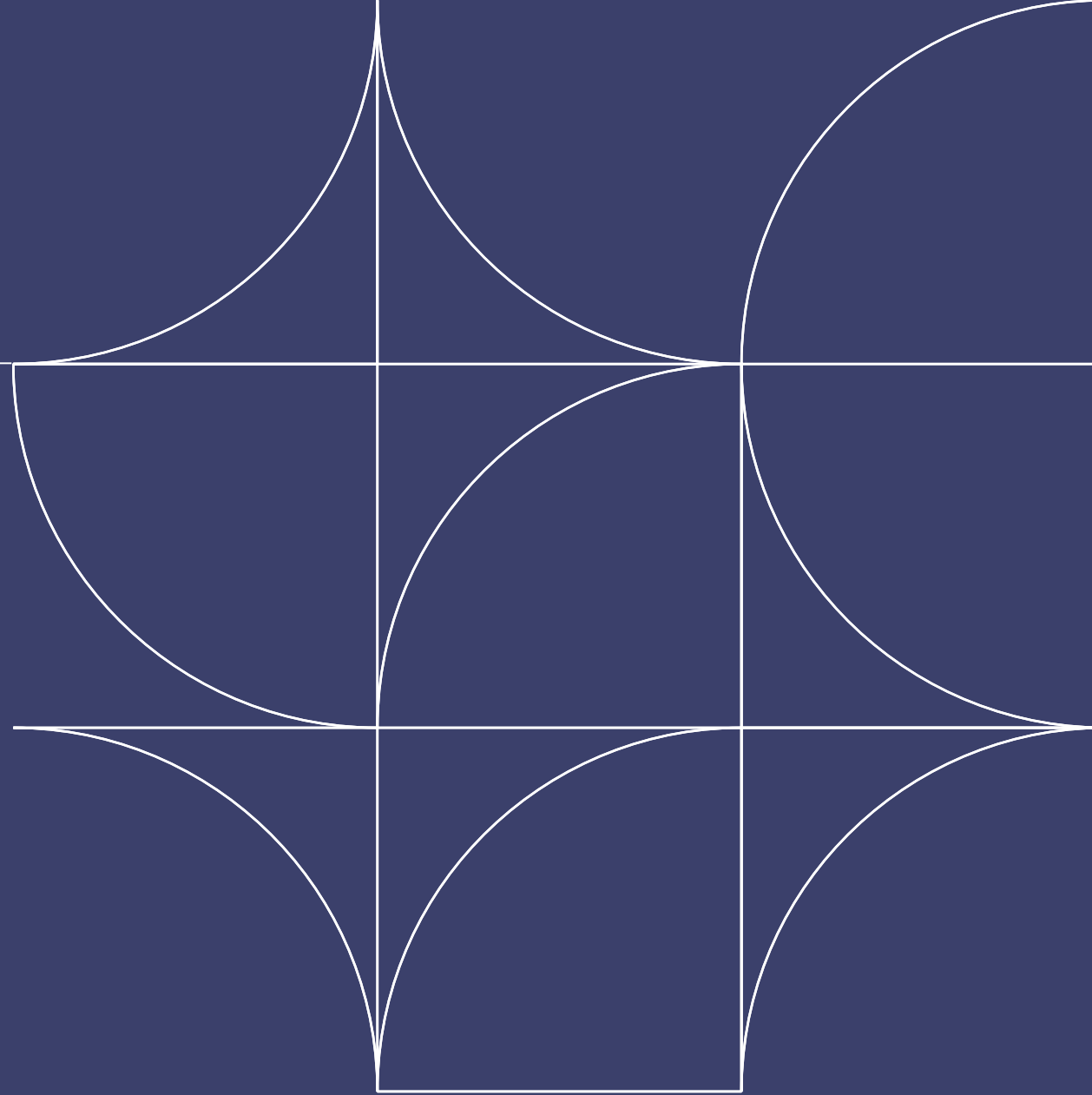
Email: jmcoleman@seyfarth.com

Gio Perez

Email: gperez@seyfarth.com

Jim Vaughn

Email: jvaughn@idsinc.com





VERIFICATION FORM

Please scan the QR code to complete the digital attendance verification form to receive CLE credit for this program.

QR code directs you to our electronic form which can also be found in the calendar invite that was sent to you for this program.

You will need:

1. **Title:** From Prompt to Proof: Investigating and Litigating Trade-Secret Theft in the Age of AI
2. **Date Viewed:** September 9, 2026
3. **Attendance Verification Code:** SS4944

State-specific CLE credit information can be found in the form.