2026 Future Leaders Practice Group Seminar

February 4-6, 2026

Responsible Uses of AI & Cautionary Tales

Bradley Ouambo
Moderator
FRANTZ WARD
Cleveland, Ohio
bouambo@frantzward.com

Theresa Sanders
TAYLOR DAY GRIMM & BOYD
Jacksonville, Florida
tsanders@talordawlaw.com

What is AI

To understand AI and its capabilities, it is helpful to look at its subfields. The subfields include machine learning, knowledge-based systems, computer vision, robotics, natural language processing, automated planning and scheduling, and optimization. These subfields work such that it allows machines to learn from data, make decisions based on existing knowledge, take actions in the physical world with robotics, see and detect the world, understand and communicate in human languages, plan and sequence actions based on desired outcomes, and to optimize its decisions so that it results in the best outcome given the constraints. In practice, a single AI machine generally does a few of these subfields at a human-level or better not all of them.

What “Responsible AI” Means in the Workplace

There are several uses for AI to help your practice and business. AI can be a helpful tool to conduct research, write memos or articles. Ultimately, you want it to align with business goals and values, maintain human accountability, and transparency.

Alignment With Business Goals and Values

- AI tools should solve real business problems (efficiency, accuracy, insight) without undermining legal, ethical, or reputational standards.

- Use cases should be documented and approved, not ad-hoc or “shadow AI” (staff using tools without oversight).

Human Accountability

- AI supports decisions; it does not replace accountability.

- A named human owner is responsible for each AI system’s outputs, data inputs, and downstream impacts.

Fairness, Transparency, and Explainability

- Employees and affected parties should understand AI’s role in decisions (e.g., how recommendations are produced and how to challenge them).

- Avoid opaque “black box” deployments in high-stakes contexts (e.g., lending, hiring, disciplinary decisions) without robust oversight.

Intersection with Data Security and Privacy

Data Classification and Handling

- Map what data is being sent to AI tools: public, internal, confidential, regulated (e.g., PII, PHI, payment data).

- Prohibit or tightly control feeding confidential or regulated data into external AI systems unless contracts and controls explicitly permit it.

Security Principles Applied to AI

- **Least privilege**: AI systems should access only the data required for a given task.

- **Data minimization**: Strip or mask identifiers before using AI where possible.

- **Secure storage and transmission**: Encryption in transit and at rest; secure endpoints; audit logs of who accessed or queried what.

Regulatory and Legal Implications

- Breach notification rules may apply if AI systems mishandle personal or financial data.

- Use of AI must comply with data protection laws (GDPR, CCPA, GLBA, sector-specific regulations) and professional duties (e.g., attorney–client confidentiality).

AI in the Legal Industry: Uses, Benefits, and Risks

Common Applications

Document Review and E-Discovery

- AI assists in identifying relevant documents, categorizing, de-duplicating, and flagging privileged materials.

- Natural language processing (NLP) is used to search large corpora quickly.

Legal Research and Drafting

- AI tools summarize cases, draft memoranda, motions, contracts, and correspondence.

- Chat-based tools help with quick issue-spotting, checklists, and first drafts.

Contract Analysis and Lifecycle Management

- AI extracts key clauses, compares documents to templates, flags deviations from standard terms, and assists with negotiations

Compliance and Risk Monitoring

- Ongoing monitoring of regulatory updates, case law developments, and internal policies; AI flags potential areas of non-compliance.

Potential Benefits in Legal Settings

Efficiency and Cost Savings

- Reduces time spent on repetitive tasks (sorting documents, first-draft research).

- Frees lawyers to focus on strategy, advocacy, and client relationships.

Improved Consistency and Quality Checks

- Standardizes language and clause libraries.

- Helps catch omissions, inconsistencies, and cross-references across large document sets.

Key Risks and Challenges in Legal

Confidentiality and Privilege

- Risk of exposure if client matter details or privileged communications are entered into AI systems that log or train on user data.
- Use of third-party vendors must address confidentiality and privilege (clear contractual terms, data residency, and security controls).

Accuracy, Hallucinations, and Unauthorized Practice

- AI-generated legal arguments or citations can be incorrect or fabricated.
- Relying on AI outputs without verification can lead to sanctions, malpractice risk, or incorrect advice.

Bias and Fairness

- AI used in compliance or risk scoring may reflect biases (e.g., in investigations, enforcement prioritization).
- Inconsistent treatment could create legal exposure and reputational harm.

AI in the Financial Industry Uses, Benefits, and Risks

Common Applications

Fraud Detection and Transaction Monitoring

- Machine learning models detect anomalies in payments, credit card transactions, trading, and account behavior.
- Real-time pattern recognition improves detection compared to static rules.

Credit Scoring and Risk Modeling

- AI models evaluate creditworthiness, default risk, counterparty risk, and portfolio risk.
- Alternative data sources (e.g., behavioral data) may be incorporated—subject to regulatory constraints.

Algorithmic and High-Frequency Trading

- AI-based strategies analyze markets, execute trades, and respond to signals faster than humans.
- AI assists with backtesting and scenario analysis.

Customer Service and Personalization

- Chatbots and virtual assistants handle routine inquiries, provide financial education, and assist with account management.
- Recommendation engines suggest products based on user profiles.

AML (Anti-Money Laundering) and Sanctions Compliance

- AI helps detect suspicious patterns and prioritize alerts for human investigators.

- Entity resolution and network analysis link related parties and transactions.

Potential Benefits in Financial Settings

Improved Detection and Risk Mitigation

- Better fraud, AML, and risk models reduce losses and regulatory exposure.
- More accurate credit models may expand access to credit while managing default risk.

Operational Efficiency

- Automation of routine reviews, alerts triage, and customer inquiries.
- Reduced manual workload and faster decision cycles.

Customer Experience and Financial Inclusion

- Personalized offerings and proactive alerts (e.g., spending alerts, savings nudges).
- AI-based underwriting can responsibly broaden access if carefully designed and monitored.

Key Risks and Challenges in Financial Settings

Model Risk and Systemic Impact

- Flawed or uncalibrated models can misprice risk, misallocate capital, or cause simultaneous market behaviors (e.g., flash crashes).
- Model risk management (MRM) frameworks must include AI/ML-specific practices (validation, challenger models, stress tests).

Bias, Fairness, and Regulatory Scrutiny

- AI in credit, pricing, and marketing must comply with fair lending and anti-discrimination laws.
- Use of proxies for protected classes (zip codes, behavioral signals) can create disparate impacts.

Data Security and Confidentiality

- Financial data is highly sensitive and heavily targeted.
- Misconfigured AI pipelines, data lakes, or third-party services can introduce new attack surfaces.

Explainability and Auditability

- Regulators often require understandable reasoning behind decisions (e.g., adverse action notices in lending).
- Complex models (deep learning) can conflict with explainability requirements unless supplemented with interpretable methods.

Types of Regulations and Governance Surrounding AI Use

External/Legal and Regulatory Frameworks (High Level)

Data Protection and Privacy Laws

- General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA/CPRA), and similar laws: require lawful basis for data use, transparency, purpose limitation, and data subject rights.

- Data processing agreements (DPAs) and cross-border transfer rules apply to AI vendors.

Sector-Specific Regulation

- **Legal**: ethics rules, professional responsibility, confidentiality and privilege duties, rules against unauthorized practice of law.

- **Financial**: banking, securities, and consumer finance regulators (e.g., fair lending, AML, model risk management guidance).

Emerging AI-Specific Rules and Guidance

- Jurisdictions introducing AI acts, algorithmic accountability, transparency, and risk-management mandates.

- Soft law: standards (International Organization for Standardization (ISO) guidelines), regulatory guidance, and supervisory expectations.

Company-Level Governance and Policies

AI Use Policy

- Defines permitted and prohibited uses (e.g., no input of trade secrets or client data into non-approved tools).

- Specifies approved tools, review processes, and escalation paths.

Data Governance and Classification

- Clear rules for what types of data may be used in training, fine-tuning, or prompting AI systems.

- Guidelines for anonymization, pseudonymization, and content redaction before use.

Vendor Management

- Due diligence on AI vendors: security controls, data retention, model training practices, incident response, certifications.

- Contractual clauses covering confidentiality, IP, data location, data controls such as SOC 2/ISO 27001, and audit rights.

Model Lifecycle Management

- Processes for model development, validation, deployment, monitoring, and retirement.

- Periodic performance checks, drift detection, and bias assessments.

Access Control, Logging, and Monitoring

- Role-based access to AI tools and underlying data.
- Logging of prompts, outputs, and administrative actions to support audits and incident investigations.

Self-Imposed Professional and Individual Practices

Professional Judgment and Oversight

- Treat AI outputs as drafts or inputs, not final answers—especially in legal and financial decisions.
- Always perform an independent professional review.

Personal "No-Go" Rules

- Do not enter: client-identifying details, trade secrets, unreleased financials, authentication credentials, or security configs into non-approved tools.
- Avoid using personal consumer accounts for work-related AI tasks.

Documentation and Explainability

- Keep records of when and how you used AI in high-stakes work (e.g., drafting key contracts, risk reports, or legal filings).
- Note assumptions, data sources, and validation steps.

Practical Tips for Leveraging AI Effectively and Securely

Before Using AI: Planning and Risk Assessment

Define the use Case and Risk Level

- Classify tasks as low, medium, or high risk (e.g., brainstorming vs. legal advice vs. credit decisioning).
- Higher risk → stricter review, validation, and approval.

Know Your Tools and Data

- Use only organization-approved AI platforms for work data.
- Understand what the vendor does with your data: training, logging, cross-tenant sharing, retention, and deletion.

Set Clear Guardrails

- Create prompt templates that exclude sensitive details (e.g., use abstract case descriptions instead of names and IDs).
- Configure tools with data loss prevention (DLP), content filters, and access limitations where available.

During Use: Secure and Responsible Practices

Data Hygiene in Prompts

- Redact or mask identifiable details whenever possible.
- Use synthetic or sample data for testing, training, and demos.

Human-in-the-Loop Review

- For legal and financial outputs:
    - Verify numbers, citations, references, and legal authorities.
    - Cross-check key assertions against primary sources.
    - Use AI as a calculator or idea generator, not a decision-maker.

Check for Bias and Completeness

- Ask AI to present alternative scenarios, counterarguments, or diverse perspectives.
- Compare outputs across multiple queries or tools for consistency.

Bringing it Together: A Practical Implementation

Establish an AI Governance Framework

- Cross-functional group (IT/security, legal, compliance, operations, HR, risk) overseeing AI strategy, policies, and risk assessments.

Create an AI Acceptable use Policy and Data Guidelines

- Define what AI tools can be used, bye whom, and for what purposes
- Prohibit data categories and establish data-handling rules
- Require human reviews for high-risk outputs

Pilot and Scale

- Start with lower-risk use cases (summarization, internal knowledge search) in controlled pilots.
- Measure benefits, monitor security events, gather user feedback, and refine processes before expanding to higher-stakes areas.

Integrate with Existing Compliance and Security Programs

- Align AI oversight with existing privacy, cybersecurity, model risk, and internal audit frameworks.
- Ensure legal and financial use cases have additional sector-specific safeguards and documentation.