2025 AI Committee: Foundation for 2026 AI Committee Work

The receivables industry spent 2025 deploying AI at scale. The governance, measurement, and vendor discipline to match that deployment has not kept pace.

By Shantanu Gangal

The Shift That Happened in 2025

In 2025, AI in receivables management moved from exploration to deployment. AI voice agents, predictive scoring models, automated documentation tools, and omnichannel outreach systems entered production at scale across the industry.

The questions at last year's RMAI's Annual Conference were no longer about whether AI belongs in collections. They were about governance, what standards apply, and who is accountable when something goes wrong.

This article covers the state of AI deployment as of mid-2026, the regulatory threads that matter most, and the governance foundations that remain underdeveloped at many organizations.

AI in Action Today

The most visible application is the AI voice agent. Unlike prior-generation IVR systems, these use large language models (LLMs) to conduct natural, adaptive conversations. They can authenticate right-party contact, present account details, negotiate payment arrangements, and process a promise to pay, without a human collector involved.

For large volumes of lower-balance or out-of-statute accounts that are difficult to staff cost-effectively, the operational case is straightforward.

Beyond voice, AI is active across several other functions like real-time agent assistance during live calls; automated call notes and documentation; quality assurance monitoring across 100% of interactions; predictive models that score and triage accounts by contact timing and propensity to pay; and omnichannel coordination across phone, SMS, email, and direct message under Regulation F contact rules.

Taken together, AI is no longer a point tool. It is a layer of decisioning operating across the full collection lifecycle, from the first outreach attempt through the documentation that surfaces in a compliance review.

RMAI AI Committee

In April 2025, a member subgroup was formed to understand these implications in greater detail. The RMAI Board of



Directors established this committee to foster communication and collaboration across RMAI's various committees on AI-related initiatives. Our goal is to ensure alignment, minimize duplication, and encourage coordination as AI continues to impact our industry. The subgroup drew expertise from many of the committees. Members brought in their experience as agencies, debt buyers and technologists. The AI Committee drafted a white paper for members of RMAI as well as generated supporting materials when RMAI directors speak with regulators and legislators.

What Regulators Are Watching

Several regulatory threads are directly relevant to collections operations.

1. **No technology exceptions**: Federal consumer financial protection laws apply to new technologies without exception. The FDCPA, TCPA, and Regulation F apply to AI-driven calls on the same basis as human-initiated contact. That principle has not changed regardless of shifts in any individual agency's enforcement posture.

2. **Explainability pressure**: The Bureau's emphasis on explainability in algorithmic decision-making extends a warning to collections. If an AI system decides which consumer receives which outreach strategy or settlement offer, operators need to be able to explain that decision. Courts have held that using algorithmic tools can itself constitute a policy producing bias under disparate impact theory.

3. **Multi-agency scrutiny**: Regulatory oversight of AI in consumer finance is not concentrated in a single agency. The FTC has become increasingly active on AI-related consumer protection enforcement, particularly around deceptive practices and data misuse. Collections operations that involve AI should be evaluated against the full range of applicable federal and state authority, not any single regulator's current priorities.

4. **State-level legislation**: California's AI Transparency Act takes effect August 2026. Colorado's Consumer Protections for Artificial Intelligence Act is effective June 2026, requiring reasonable care against algorithmic discrimination in high-risk systems. Multi-state operators face an increasingly complex compliance geography.

One data point worth noting is the CFPB's FDCPA annual report documented complaint volumes nearly doubling between 2023 and 2024, from approximately 109,900 to 207,800. Whether AI is contributing to that trend or operating in a pre-existing high-complaint environment is something each organization should examine with its own data.

Where Most Organizations Are Exposed

The central finding from RMAI's AI Subgroup work in 2025 was not about any specific technology. It was about governance. Many organizations deploying AI have not built the internal frameworks to manage it consistently. Three questions expose where that gap typically sits:

- Do you know where AI is operating in your business?
- What decisions is AI authorized to make, and where does human review apply?
- If an interaction produces a complaint or regulatory inquiry, what is your audit trail?

The Subgroup also addressed organizations that have not adopted AI. The conclusion was that a documented AI policy is necessary regardless of whether a company uses or restricts AI.

AI operates upstream in the chain. A creditor's AI-driven account decisioning may determine which accounts reach a collector's portfolio, at what price, and with what prior contact history. Operators who do not use AI directly are still affected by it.

A Consumer-Centric Approach

Ultimately, the promise of AI is a shift from an industry often perceived as adversarial to one that is collaborative, consumer-centric and solution-driven.

Machine learning enables us to engage with consumers in a way that feels personal and respectful. By analyzing consumer behavior, we can determine the best times and channels for communication, ensuring that our outreach is not only effective but also considerate of the consumer's preferences.

What to Ask Before Signing a Vendor Contract

A common concern among collections executives is whether deploying AI means sending sensitive consumer data to external providers. The answer depends on architecture, not technology category.

LLMs process inputs wherever they are hosted. Three deployment models carry different risk profiles:

1. On-premises (AI runs on company-controlled infrastructure, no data leaves the environment)



2. Private cloud (dedicated, logically isolated environment with contractual data handling terms)
3. API-based services (data sent to a third-party's infrastructure, appropriate for some use cases with proper controls, but requiring careful evaluation for non-public personal information)

Vendor due diligence should cover:

1. Where data is processed
2. Whether it is used to train the vendor's models
3. Data retention policies
4. Relevant security certifications such as SOC 2 or ISO 27001
5. Contractual accountability if an incident occurs.

These questions are not specific to AI. They are the same questions any disciplined compliance function should ask of any third-party data processor.

How to Measure Whether AI Is Working

1. **Call duration.** AI-driven collection calls tend to run longer than traditional automated outreach. Industry data from RMAI subgroup discussions indicates this correlates with higher consumer engagement and more completed payment arrangements. Longer calls are also useful evidence when demonstrating consumer benefit to regulators.
2. **Containment rate.** The share of interactions resolved by AI without human escalation or complaint generation is the baseline operational metric. Drops in containment typically indicate edge cases outside the system's training parameters, and those cases warrant review.
3. **Bilingual performance.** For portfolios with Spanish-speaking consumer populations, AI agents that operate in both languages without material performance degradation extend operational reach without proportional staffing increases.

What Sound AI Governance Looks Like

Based on industry practice and RMAI's governance discussions, the following elements constitute a reasonable starting point:

1. **An AI inventory**: a documented list of every AI system in use, its function, its decision scope, and the responsible vendor.
2. **Human oversight thresholds**: explicit rules for when AI must escalate to a human, with documentation that those rules are enforced.
3. **Disparate impact testing**: periodic review of AI-driven outcomes across consumer segments to identify distributional patterns before regulators identify them first.
4. **Vendor contracts**: clear allocation of responsibility for AI performance, data handling, and incident response.
5. **Staff training**: operations, compliance, and legal teams should understand how the AI systems they oversee function, including their known limitations.

AI governance training should not crowd out ethics education. FDCPA compliance and consumer protection obligations are matters of organizational culture, not technology choice. AI changes the delivery mechanism, it does not change the underlying obligations.



Shantanu Gangal
CEO
Prodigal

Shantanu Gangal is the CEO of Prodigal; the leading AI agent for loan collections. A Computer Science engineer and a tinkerer at heart, he is excited to watch the millions of calls AI handles daily and the potential it presents for our industry. Shantanu has been a member of the RMAI Editorial Committee as well as the AI Working Group.