

April 2026

BankNews.com

BANKBEAT

Stepping Into Crypto



*De novos
discussed*

*Marketing
to Gen X*

*Day care is key
bank benefit*



On Topic

By Michael Gentry

The AI governance gap and why it matters

While generative AI systems have begun to reshape how many businesses operate, banks and financials must act more deliberately in their adoption of new technologies. Regulation requires financial institutions to carefully evaluate these tools through existing frameworks. Banks cannot set aside compliance teams and risk management considerations around consumer protection, data privacy and cybersecurity to adopt AI systems.

That measured approach reflects strength, not hesitation. Banks already maintain strong cybersecurity programs, layered controls and employ professionals who manage complex threats every day. These defenses give banks a solid foundation for AI governance, but they do not remove the need for it.

Criminals, by contrast, do not need to convince a committee to adopt a new technology. They increasingly use AI to enhance fraud schemes, exposing banks to losses, regulatory scrutiny and litigation. The increasing use of deepfakes in impersonation scams illustrate the risk. Fraudsters now use AI-generated audio, video and images to impersonate executives, customers and vendors, pressuring employees to authorize wire transfers, change payment instructions or disclose sensitive information. All in, the Federal Trade Commission (FTC) reported that impersonation fraud ranked among the most common fraud categories in 2024, with \$2.95 billion in losses to U.S. businesses and consumers.

This AI adoption by threat actors heightens exposure for financials. Payment systems move quickly. Employees make decisions under time pressure. Remote and hybrid work reduces informal verification. AI-enabled impersonation can exploit these conditions and bypass traditional cybersecurity controls.

AI adoption gap creates a governance gap

This imbalance creates an AI governance gap: banks must operate deliberately, while criminals act without constraint. IBM's 2025 *Cost of a Data Breach Report* illustrates the risk of not investing in AI-specific governance measures. Thirteen percent of surveyed organizations reported breaches involving AI

models or applications. Of those surveyed, 97 percent lacked controls governing internal AI use. Sixty-three percent reported not having an AI governance policy.

Banks can close this gap by extending governance beyond cybersecurity. Technical safeguards remain essential, but they may prevent employees or vendors from introducing unapproved AI into workflows. Without clear rules and oversight, well-intentioned staff may expose data, weaken controls or create new attack paths.

Don't wait on slow, uncertain regulation

When not stalled by political debate, federal regulators are focused on home-grown AI dominance rather than enacting a unified AI regulatory framework. States have moved ahead independently, creating a patchwork of laws that vary by jurisdiction and use case.

Some states have taken broader, risk-based approaches. Colorado's Artificial Intelligence Act, scheduled to take effect in June, imposes consumer-protection obligations on developers and deployers of high-risk AI systems, which will have a direct impact on financials' uses of AI in lending. Other states have targeted specific applications. An Illinois law recently became effective requiring employers to disclose any use of AI in hiring, promotion, discipline or related actions.

But the future of these and other state laws is murky. In December 2025, President Trump issued an executive order seeking to curb state AI laws, directing federal agencies to challenge regulations the administration views as barriers to innovation and domestic competitiveness.

This tension leaves financials operating amid overlapping and unsettled obligations. Waiting for federal clarity invites risk. Organizations that delay assessing and managing AI use will compound the risks brought along by the governance gap and the speed of threat actors' adoption. Internal governance provides the only stable path to control risk while the legal landscape continues to shift.

Here are five practical steps for financials looking to advance their AI governance:

1. Establish a clear AI governance policy tying permissible AI use to existing risk frameworks.
2. Ensure that the governance program is managed by an empowered committee with deep knowledge of those frameworks.
3. Strengthen vendor controls and contractual

On Topic, Continued on page 35

Michael Gentry is a shareholder at Reinhart Boerner Van Deuren. He is part of the firm's Labor and Employment Practice, and a member of Reinhart's Data Privacy and Cybersecurity Group and Artificial Intelligence (AI) Group. Gentry can be reached via email at mgentry@reinhartlaw.com.

Closer, Continued from page 38

“I got a call from [Fishback’s brother] and his son Tom ... and they decided to give me a large sum of money that I could use at [Kids World] in honor of Bob, who was still living at the time,” Poppen said. “That allowed us to do a major playground expansion for our kiddos. That was just money that they freely gave to do that. So they support it not only in words, but in actions. I think that’s what’s allowed it to be so successful.”

Kevin Tetzlaff, president and CEO of First Bank & Trust, agreed with this sentiment. “I was a Kids World parent for years, having had four children part of the program,” Tetzlaff said. “What was clear to me then and continues to drive executive decisions now is that having an onsite childcare center is a unique and valuable benefit for employees of First Bank & Trust that drives job satisfaction and productivity. We’re all extremely proud that our organization prioritizes this family-first concept and that Bob had an intuitive sense of ‘work-life balance’ long before that phrase became corporate-speak.”

In addition to offering daycare services, Kids World also provides a full pre-school with low student-teacher ratios, an in-house nutritionist, homemade meals, field trips and other activities.

While First Bank & Trust has considered replicating Kids World at its other locations, the location in South Dakota has a couple of key features that make the daycare work so well. Brookings is small enough that despite having four bank locations,

none of them are more than one mile away from Kids World. In a bigger city, that commute could detract from the convenience of it. Finances are another factor. Poppen noted how expensive an endeavor it is to start a daycare and that it would be unrealistic to expect the same level of support and commitment across all bank locations.

A number of other companies have reached out to First Bank & Trust expressing interest in setting up something similar at their institution. However, Poppen said, none have replicated it—and their main concerns have to do with financials and staffing.

“That is not an easy thing to do, to staff an early childhood learning center. In full disclosure, [it] is not a money-making profession. You don’t go into it because you’re going to make a ton of money... You have to do things to support the staff to retain them and that’s not always easy, especially if you’re competing with others.”

First Bank & Trust has an advantage over other daycare options in Brookings because Kids World employees receive the same benefit package as the rest of the bank, including health insurance, paid vacation, paid sick leave, 401(k)s and a salary slightly above market rates.

Ultimately, it is evident that Kids World has made a major impact on the First Bank and Trust community. “We always joked in the past that when you found out you were expecting, you called Kids World before you called your spouse,” Poppen said. ♦

On Topic, Continued from page 6

requirements around AI use.

4. Train employees to counter AI-enabled fraud and avoid unapproved tools.
5. Prepare incident response and litigation strategies addressing AI misuse.

Why this matters for bank leadership

AI-enabled fraud already affects financial

institutions. Banks do not lack expertise or infrastructure. They manage complex risks every day. By extending existing safeguards into a clear AI governance framework, banks can prevent rogue AI use, reduce exposure and demonstrate diligence to regulators and courts. Institutions that act now to circumvent the governance gap will stand strongest as AI-driven threats evolve. ♦

Person of Interest, Continued from page 26

own; you have got to have great people around you,” Kooiman said. “I was able to hire some of those people.”

He called his opportunity to work with Raymo, and Platt who served as president of the bank before Kooiman, a “real blessing.” Platt, Kooiman noted, was the person who brought a KSOP to the bank several years ago. A KSOP combines the features of a 401(k) plan with an Employee Stock Ownership Plan. Kooiman said it is a benefit that has made a big difference for many First

State Bank Southwest employees.

Reflecting on his time working with Raymo, Kooiman said “We often said our personalities were so different, but when it comes to banking, we were always on the same page.”

Kooiman said they were unified on an important point. “One thing we stressed at the bank—Gene started it, I continued it, so did Greg and now Mark is—that we stress to the employees: it’s God first, family second and work third, and in that order.” ♦