

The ProSight Journal®

Fall 2026 | ProSightFA.org

ProSight's Model Risk Survey Highlights Core Principles, Common Challenges

Plus:

- AI Data Center Risks and Opportunities for Lenders
- Building a Multigenerational Fraud Strategy





ProSight Annual Conference

Connecting leaders in risk, compliance, and fraud

November 2-5, 2026 | Virtual Conference

Growing Forward: Turning Disruption Into Opportunity

Explore how organizations are addressing evolving risk, fraud, and AI-driven disruption. Hear practical strategies to strengthen resilience, accelerate transformation, and unlock growth in an increasingly competitive environment.

Many sessions will be CPE eligible and regulated per NASBA guidelines, with the opportunity to earn up to 14 NASBA CPE credits. The conference will also be CEU eligible and **has been approved by ABA**

Professional Certifications for 20 CERP, 8.5 CRCM, 6 CAFP, and 1.25 CSOP credits.



7,500+
Attendees



150+
Institutions



75+
Speakers



25+
Sessions

Featured Keynote Speakers



**DANA M.
PETERSON**
The Conference Board



**MAURO F.
GUILLÉN**
Wharton School

Register Today

All-Access Institutional Virtual Passes

To purchase or utilize your all-access institutional pricing, contact your [Relationship Manager](#).

Departments

4 ProSight Welcomes New Members

6 Ask the Workout Window

Features

6 Ask the Workout Window: Using an Article 9 Sale To Maximize Recovery

Jason Alpert explains how an Article 9 sale can maximize a bank's recovery by offering a faster, lower-cost alternative to bankruptcy for disposing of collateral.

11 ProSight's Model Risk Survey Highlights Core Principles, Challenges Amid Shifts in Focus and Regulation

ProSight's survey finds model risk management becoming more targeted while core principles endure amid regulatory change.

MICHAEL BENDER

17 Community Banks Gain Model Risk Flexibility

Community banks gain flexibility to tailor model risk programs under revised guidance, while retaining responsibility for sound oversight.

21 Model Guidance: More Flexibility, Not Less Responsibility

Revised model guidance gives large banks greater flexibility to tailor risk programs while maintaining strong governance, oversight, and accountability.

27 Lender Liability: Where Good Intentions Go Wrong

Disciplined communication, clear boundaries, and consistent loan enforcement can help banks reduce lender liability risks and costly borrower claims.

JASON ALPERT, MARTIN KNAUST

33 AI Data Center Risks and Opportunities for Lenders

AI data centers offer lenders significant growth opportunities but introduce risks tied to energy, technology, customers, and regulation.

AMY SHORT

38 The Issues Management Blueprint

Effective issues management relies on leadership, accountability, prioritization, training, and proactive remediation to strengthen bank risk management.

43 Building a Multi-Generational Fraud Strategy

A multi-generational fraud strategy combines behavioral detection with age-relevant messaging to protect customers of all generations.

CARA WICK

47 Primer: A Look at Credit Risk Insurance

Credit insurance helps banks manage nonpayment risk, expand lending capacity, and protect cross-border receivables, but remains underused in the U.S.

Index to Advertisers

ProSight Annual Conference

Inside front cover • [Visit website](#)

Ask ProSight

Page 5 • [Visit website](#)

ProSight Enterprise Risk Manager

Page 16 • [Visit website](#)

ProSight Internal Audit Conference

Page 26 • [Visit website](#)

ProSight eMentor

Page 37 • [Visit website](#)

ProSight Fraud Alert Network

Page 46 • [Visit website](#)

ProSight Newsletters

Page 51 • [Visit website](#)

ProSight Proudly Introduces New Member Institutions

American Momentum Bank | Tampa, FL

Waterfall Bank | Clearwater, FL

The ProSight Journal®

Executive Editor: Celina Rogers

Editor-in-Chief: Frank Devlin

Senior Editor: Dan Washburn

Senior Editor: Michael Bender

Art Director: Christopher Santoro

Editorial Board

Jason Alpert, Managing Partner, Castlebar Holdings

Matt Bryant (Chair), Director of Credit Risk, Frost Bank

George Buchanan, Chief Risk Officer, Flagstar Bank

Kevin Cavalieri, Retired, M&T Bank

James Clarke, Principal, Clarke Consulting

Fred Daniels, Chief Credit Officer, Citizens Trust Bank

Stephany Head, Founder, OpRisk Associates

Eric Holmquist, Founder, ERM Advantage

Robin Ingari, EVP, Prosperity Bank

Joe Iraci, CEO, Atlas Quotient

Brian Jones, CEO, First National Bank of Elmer

Bart Leahey, Chief Compliance Officer, Frost Bank

James Lentino, Chief Risk Officer, Wintrust Bank

Shelly Liposky, Chief Controls Officer, RBC

Subbu Narayanaswamy, Corporate Risk, Wells Fargo

Kevin Oden, CEO, Kevin D. Oden & Associates

Avani Parekh, Risk Officer, TD Bank

John Soffronoff, Managing Partner, Arcsalus Advisors

Kathy Swift, Nonprofit Development Officer, Heritage Bank

Cara Wick, Global Financial Crimes Executive, Bank of America

Elisabeth Wilson, Senior Risk Advisor, Atlantic Union

Article submissions or comments: Editorial contributions are welcome. All articles submitted become the sole intellectual property of ProSight. Authors have permission to reuse articles in print and on the web, provided they indicate the article was published in The ProSight Journal. For additional information, see Guidelines for Authors at ProSightFA.org. Contact Frank Devlin, fdevlin@ProSightFA.org.

Research, download, photocopy: Individual articles or entire issues can be researched and downloaded. Visit prosightfa.org/industry-insights/the-prosight-journal/. No part of this publication may be reproduced by any technique or process whatsoever without permission.

Advertising: ptaylor@ProSightFA.org



Letters to the editor:

Interact with us: *The ProSight Journal* welcomes letters from our readers. Letters can be emailed to Frank Devlin, Editor-in-Chief, fdevlin@ProSightFA.org. We look forward to hearing from you!



Follow us on LinkedIn:

linkedin.com/company/prosightfa/

The ProSight Journal (ISSN 1531-0558) is published quarterly by ProSight Financial Association ("ProSight"), 222 W. Adams Street, Suite 2300, Chicago, IL 60606, 1-800-844-3637. Copyright © 2026 by ProSight Financial Association. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or use of any information storage and retrieval system, without the prior written permission of ProSight. This publication is designed to provide accurate and authoritative information concerning the subject matter covered, but is not to be construed as rendering legal, accounting, or other professional advice.



Ask ProSight ✨

An AI Powered Research Assistant

Exclusive Member Benefit

Ask ProSight delivers faster access to the information you need and supports more informed decision-making.

Our AI-powered research assistant helps members search our website with ease, providing fast, accurate answers and direct links to reliable, relevant content. Whether you're exploring member benefits, researching educational programs, or looking for guidance on industry topics, Ask ProSight gives you clear, trustworthy results instantly.

Ask your first question today at
ProSightFA.org





Ask the Workout Window

Insights Into Special Assets and Situations From a Workout Leader



Using an Article 9 Sale to Maximize Recovery

In each issue of The ProSight Journal, veteran workout leader Jason Alpert gives advice on thorny workout challenges. Have a challenge you would like Jason to address? Send your question to WorkoutWindow@ProSightFA.org. Please note: Sending a question indicates you approve of the question's publication, without attribution to you, and its use in the development of scenarios, practices, and advice that could be included in the Workout Window or other ProSight content, properties, and platforms.

By Jason Alpert

QUESTION: OUR BORROWER IS a small, branded consumer products company that's out of money. We have a \$4.25 million revolving line of credit (fully drawn and in default) secured by all business assets. The company has real customers and operations, but the assets have minimal value besides some equipment (which we are in first position on), and the guarantors have very limited resources. An interested buyer has emerged (a local entrepreneur), but they want a clean structure and management wants to stay involved. Our chief credit officer suggested a UCC Article 9 sale as a faster, cheaper alternative to bankruptcy. I've never run one and didn't know this was an option to resolve the debt. How does this remedy work?

JASON: An Article 9 sale is essentially a foreclosure under Article 9 of the Uniform Commercial Code, allowing a secured creditor to dispose of its collateral and generally transfer that collateral free and clear of subordinate security interests and liens that are extinguished under applicable law.

Article 9 has been adopted in every state (with some state-specific variations), so it is important to understand the specific laws applicable to your state. Article 9 is unique in that it allows for “self-help” remedies in situations where the lender can physically retake possession of the collateral. A classic example is the borrower who “gives you the keys,” leaving the bank in possession of a facility full of equipment and inventory that it needs to liquidate. It is important to note that Article 9 is a method for perfecting and selling secured personal property collateral. If you cannot obtain possession of the collateral, the first step will be to go through a process such as replevin to obtain a court order allowing for possession by the secured creditor. The exact steps to judicially take possession will vary from state to state.

For the purposes of this exercise, let’s assume the borrower is cooperating and will grant you access to sell, or has turned over the collateral voluntarily. Article 9 has been widely used as a means of disposing of typical personal property collateral such as office furniture, inventory, and equipment, but in recent years it has also started to be utilized more and more as a way of transferring ownership interests, such as a membership interest in an LLC. It is important to make sure that you have a perfected security interest in the type of collateral you want to sell through Article 9. Many form line-of-credit loan documents contain generalized descriptions of personal property collateral and do not always contain a pledge of membership interests.

Even if the company may not be a practical candidate for a Chapter 11 or Subchapter V case, this cost-effective and efficient remedy is a great tool to extract the best value and recovery for the bank.

This is especially true when the company has more value as a going concern than its assets would have in liquidation. Generally, Article 9 sales are faster (the transaction is completed in weeks, not months or years), cheaper (lower attorneys’ fees, no bankruptcy professional fees or court costs), and offer more privacy relative to a Section 363 bankruptcy sale or receivership sale. (The privacy factor can be valuable inasmuch as the company can avoid the reputational challenges within a very public process). It must be noted that while an Article 9 sale is faster and cheaper than a Bankruptcy Section 363 sale (which is the gold standard), it comes at the cost of higher tail risk to the bank and the buyer given that no judge is blessing the sale and providing a rock-solid court order waiving all liens and claims.

It is critical that you engage with your counsel to ensure that the proper process is followed and that every aspect of the disposition—the method, manner, time, place, and terms—is commercially reasonable. The key point is that price alone doesn’t prove reasonableness, but a bad process almost guarantees a fight about the price. In order to build the case that the sale is commercially reasonable, the process must demonstrate that there was a bona fide marketing effort to draw other buyers into the sale. The bank may want to engage a broker or adviser to assist in this process and to maintain a full record of who was contacted, when, what marketing materials were distributed, and the responses that came back from interested parties. Most importantly, the bank must ensure that proper notice of the sale (a reasonable authenticated notification) is provided to the borrower, all guarantors, and all junior lienholders and claimants of record. Additionally, the notice should be sent at least 10 days before the sale to qualify for the statutory safe harbor on timing. So that any unknown claimants receive notice, there should be a public notice run in an appropriate publication (similar to a foreclosure sale). Please note that Article 9 also allows for private sales; the requirement of commercial reasonableness still applies. A classic example would be a commercial condominium foreclosure where



Article 9 has been adopted in every state (with some state-specific variations), so it is important to understand the specific laws applicable to your state. Article 9 is unique in that it allows for “self-help” remedies in situations where the lender can physically retake possession of the collateral.

the operator in the neighboring bay wants to buy the equipment and is in the best position to offer top dollar and move quickly.

While the Article 9 process can seem simple, there are several complexities that the bank must consider and address. The first is the treatment of the guarantors, particularly if the bank is considering pursuing the guarantors for any deficiencies. If the Article 9 process is not followed, the bank’s deficiency claim may be reduced or eliminated, impairing its ability to collect on the guaranty. Certain guaranty agreements contain waivers intended to limit notice and commercial-reasonableness defenses, although the effectiveness of such waivers varies by jurisdiction and should be carefully evaluated with counsel.

Second, the bank needs to understand that an Article 9 sale only wipes out junior security interests, not all liens and claims. It is important that the bank run

lien searches so that tax liens, judgment liens, and landlord claims are known and addressed during the sale. Finally, the sale cannot cleanse the buyer of certain successor liabilities such as product liability, warranty claims, WARN Act exposure, and certain unpaid taxes. If the borrower has these liabilities, expect that the buyer will incorporate these concerns into their final price.

For your specific question, the buyer appears to be interested in the company as a going concern and would like to utilize the Article 9 process to purchase the pledged interests subject to the limitations of Article 9 and any liabilities or claims that are not extinguished through the foreclosure process.

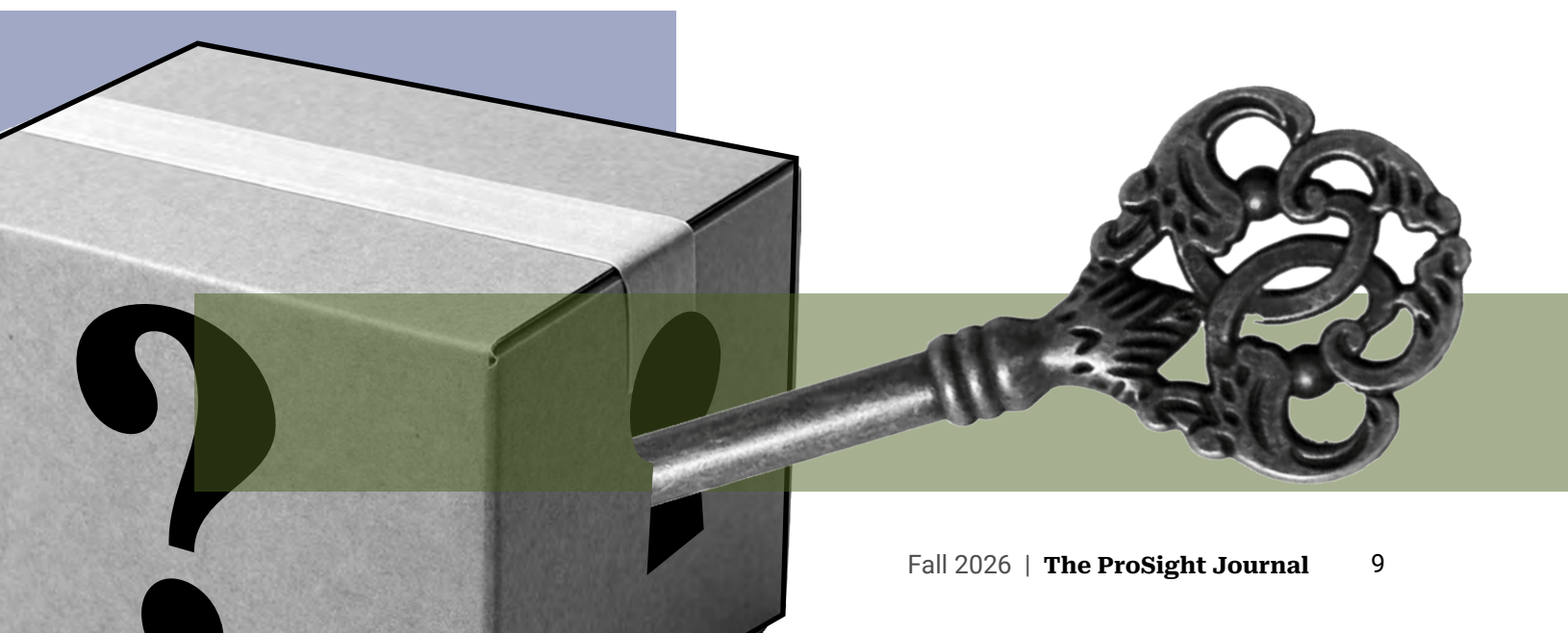
However, the equity structure may preserve many contracts, permits, accounts, and business relationships without requiring traditional asset-by-asset assignments. The buyer must carefully consider

change-of-control provisions, regulatory approvals, anti-assignment clauses, and other contractual restrictions that may still be triggered.

The trade-off is that a buyer of the membership interests takes the company with all its liabilities (trade payables, taxes, and litigation exposure), so—unlike an asset sale—the equity route sacrifices some of the “free and clear” cleansing, and the buyer’s diligence and price will reflect that risk. If the bank does not have a pledge of those interests, then the loan needs to be modified to add the membership interests as collateral. (Note that collateral added on the eve of a sale can itself be attacked as a preferential transfer if a bankruptcy follows within 90 days—another reason the timing recommendation below matters.) The bank should consider a friendly settlement in which it obtains the membership interests as collateral and obtains the cooperation of the borrower and guarantors with the sale in exchange for a release of any deficiency claims after the sale has been consummated. As stated above, the guarantors lack known resources and the price received for the going concern should exceed what the bank would receive in a straight liquidation of the company’s assets. Most importantly, the borrower’s cooperation in providing access to financials, operations, contracts, and other proprietary

information will likely result in a higher price because the transaction is fully transparent to prospective buyers. In the modification or settlement agreement, some practitioners may consider delaying certain releases until after the expiration of the 90-day preference period, subject to advice of counsel. That way, any post-close objections are addressed—and more importantly, the 90-day preference period expires for any subsequent bankruptcy filings by the guarantors or the old borrowing entity.

Sales of membership interests via Article 9 do not trump state laws regarding the transfer of membership interests, because companies are organized and exist under state law. Most operating agreements have transfer restrictions such as consent requirements and rights of first refusal that Article 9 does not override for membership status: the buyer typically receives only the economic rights (distributions) as an “assignee,” not governance or voting rights, unless the other members admit the buyer as a member under the operating agreement. Some jurisdictions’ LLC acts explicitly preserve this distinction even against a secured creditor’s foreclosure sale. In our scenario, this is one more reason the friendly settlement matters: as part of the cooperation package, the members should consent to the transfer (and amend the operating agreement if needed) so the buyer is admitted with full membership rights at closing.

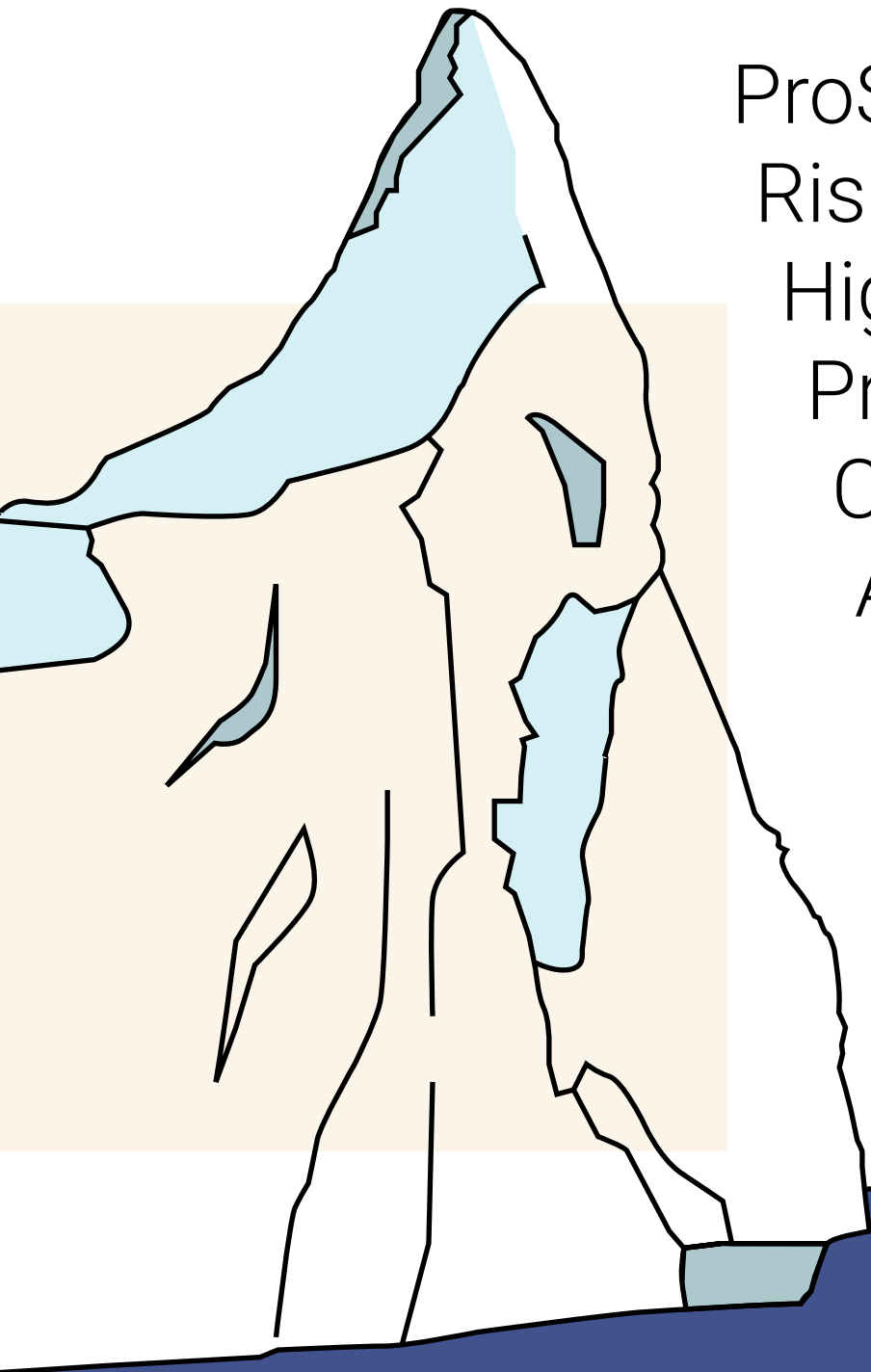


Closing Thoughts

The best solution is not always an Article 9 sale. Banks should compare expected net recovery, timing, execution risk, litigation exposure, and administrative cost against alternatives such as a receivership, note sale, consensual restructuring, bankruptcy sale, or traditional liquidation. If an Article 9 sale is the optimal outcome on an NPV basis compared with the alternatives, then be sure to engage outside legal counsel with experience in Article 9 dispositions. Additionally, the engagement of a broker or sale adviser should be encouraged so that the marketing process can be fully documented and preserved in the event of any objections. A third-party broker can also establish the baseline value for the sale, or an appraisal can be obtained to set expectations, support negotiations, and strengthen the process. An Article 9 sale's speed and cost savings are real. However, the process rewards preparation and documentation and punishes shortcuts. Even if the process is "friendly," the bank cannot treat that as a license to be informal. An Article 9 sale done carelessly can fail and create additional problems. Nevertheless, an Article 9 sale is a very valuable resolution tool and one that more banks should add to their toolbox of solutions.>

Disclaimer: *The Workout Window is neither intended nor to be considered legal advice. As The Workout Window stresses, consult with legal counsel and your institution's management to be sure you are acting within the parameters of your institution's policies and banking law.*

Jason Alpert is managing partner at Castlebar Holdings, a distressed debt fund and financial institution adviser. Jason led and managed workout and special asset teams at major financial institutions for two decades. He is on the editorial advisory council of The ProSight Journal and is an adjunct professor at the University of Tampa. Email Jason at jason@castlebarholdings.com or reach out to him at 813-293-5766.



ProSight's Model Risk Survey Highlights Core Principles, Challenges Amid Shifts in Focus and Regulation

Professionals Assess Practice Under SR 11-7, Durable Themes for SR 26-2

By Michael Bender

THIS YEAR'S ANNUAL Survey on Model Risk Management (MRM) conducted by ProSight Financial Association's Model Validation Consortium explores themes top of mind for model risk professionals as shifting regulatory winds push the MRM discipline in new directions.

Conducted *before* the April release of [Revised Guidance on Model Risk Management \(SR 26-2\)](#), the study describes practice under SR 11-7, elaborating approaches that will be tested as responses to regulators' new tailored, risk-based guidance take shape.



Importantly, it shows how ironclad principles such as effective challenge, independence, and the authority to effect change—reinforced in SR 26-2—endure in institutions as more responsibility for defining and managing overall model risk exposure shifts their way. In the survey, more than half (54%) of respondents said their institutions do very well or extremely well at understanding the importance of MRM independence.

“The foundations of sound model risk management practices endure regardless of a change in emphasis on particular models or the frequency and completeness of assessments,” said Will Kutteh, director of ProSight’s Model Validation Consortium.

Organizationally, most institutions (89%) establish this independence through reporting lines for MRM reporting into an independent control group such as risk management. Gradually, those lines are moving from the deputy or chief risk officer (54% in 2026 vs. 61% in 2025) to the head of enterprise risk management (31% vs. 27%) or operational risk management (9% vs. 5%).

The survey results also expose the challenges, such as third-party model validation, that remain regardless of new approaches to risk assessment. In this year’s survey, for example, just 2% of respondents said vendors do very well or extremely well at describing the black-box components of their models—consistent with 1% and 3% of respondents in the prior two years.

One aspect of MRM sure to change under SR 26-2 is the depth and frequency of model validations, particularly those deemed less risky under current and future classifications. The survey suggests that nearly 1 in 3 institutions do not subject their lowest-risk models to calendar-based validations, indicating a preference for change-driven validations. This trend is likely to



continue under new guidance, with institutions focusing effort on validating Tier 1, or the highest-risk, models while scaling back testing of less critical ones.

That doesn’t mean staffing needs will ease. In the study, respondents at banks of all sizes said they lacked the full-time equivalents needed to achieve their ideal operating state, including for internal and external MRM teams. Most said they needed more non-validation support staff as well.

“As the number and complexity of models grow, institutions need more manpower to responsibly evaluate and report on the risk,” Kutteh said.

Artificial intelligence oversight will take on a new character under SR 26-2, as both generative and agentic AI have been excluded from the new model risk guidance. That’s consistent with prevailing trends in industry practice as more institutions have moved toward recording AI and AI-related systems in separate inventories from other models.

In the 2026 survey, 59% of respondents said their institutions record AI systems separately versus 14% in the 2025 survey. Likewise, 28% now assign policy/framework responsibility to a separate AI committee/working group versus 4% last year.

Cybersecurity models and non-model tools, meanwhile, remain in the model inventory for most institutions (81%), and those models are validated at least most of the time (72%). Still, 78% of institutions rest responsibility for cybersecurity risk with their IT/information security teams.

MRM's Expanding Purview

When it comes to oversight of models and non-models under MRM, institutions are discriminating less among quantitative models, qualitative models, and non-model tools. This year, 60% of respondents said their non-model tool programs sit within their MRM policy/program, versus 38% last year, though they continue to identify them separately (72%) from model inventory. At the same time, more than 70% said they don't distinguish between quantitative and qualitative models in their model inventory, an increase from 55% last year.

In terms of consistency of definitions, institutions have settled these past few years on a set of attributes to describe non-model analytical tools. Those include calculations or logic used for business purposes (72%), the absence of assumptions (49%), and functionality that does not produce estimates or forecasts (68%).

More than half of institutions (62%) survey the enterprise annually to identify new models and verify inventories. For most, the highest-risk models (whether banks use a three-, four-, or five-tier system) sit within Current Expected Credit Losses (CECL) (88%) and asset/liability management (ALM) (80%) processes. For banks with more than \$250 billion of assets, high-risk models are spread across everything from stress testing to market risk.

Validation and Review Cadence

Regardless of the number of rating tiers they maintain, more than 75% of responding organizations review their Tier 1 models annually. More than three-quarters of respondents (82%) said a review can trigger a new finding or issue.

More than two-thirds (68%) said those reviews sometimes trigger a model re-validation. If that trigger rating is severe enough, 40% said that their institutions would pause use of the model until the issue is remediated. Otherwise, about three in four said they conduct full-scope independent validation on Tier-1 models at least every two years.

For lower-tier models, more than half of respondents said they reviewed each tier every 12 months, regardless of the number of tiers they use. About 30% of institutions said they do not validate their lowest-risk models—a practice that may expand under new, more flexible SR 26-2 model risk guidance.

“Model purpose, together with model exposure, determines model materiality,” the letter states. “Bank organizations may deem certain models immaterial ... in those cases, model risk management may consist of identifying those models and monitoring model performance and conditions under which the use of models may



become material to the banking organization in the future.”

For those hoping to expand their model validation capabilities, typical barriers remain. Cost is tops (69%), followed by talent (55%), resources (55%), and technology (18%)—percentages consistent with those in the prior two years.

Model Vendors and the Black Box

When a vendor fails to meet MRM requirements for documentation, validation, or developmental testing, institutions take steps to flag and rectify the situation, including issuing a validation finding (54%), re-evaluating the model’s risk rating (49%), and increasing monitoring frequency (44%). Few, though, stop using the vendor entirely (14%). When asked how many times respondent institutions had terminated a vendor relationship for MRM deficiencies in the past three years, 96% said “zero.”

That’s because the industry has become almost universally dependent on third-party outsourcing for at least part of its model needs. About nine in 10 respondents (88%) said their institutions outsource some part of the model lifecycle to a third party. Even so, the challenge, they say, is that these vendors fall short of expectations in explaining everything from theory and conceptual soundness (61%) to model design and analytics (63%).

And they’re not improving much from previous years, the survey suggests. Vendor contracts often lack language around specific MRM customer obligations. And many third parties don’t provide external, independent validations of their own products.

“Despite raising concerns and pushing back against the opaqueness of third-party MRM

practices, institutions are beholden to their providers because building their own capabilities can be cost-prohibitive,” Kutteh said.

Almost half of respondents (48%) said that 10% or fewer of their model vendors conduct and provide evidence of independent validation, and 85% of organizations said they received validation reports from 50% or fewer of their model vendors. When it comes to documentation, 84% said they ask for more information from the vendor when

“Despite raising concerns and pushing back against the opaqueness of third-party MRM practices, institutions are beholden to their providers because building their own capabilities can be cost prohibitive.”

—Will Kutteh

documentation is deficient, while another 10% accept the vendor's claims that the analytics are valid.

The model risk function continues to play an important role in vendor onboarding generally. While vendor management typically takes the lead (96%), model risk (76%) is also closely involved.

AI: A Special Case

How institutions are to manage AI model oversight going forward remains an outstanding question in SR 26-2. The letter expressly separates generative and agentic AI models from inclusion in model risk inventories, leading some to speculate that further clarity is forthcoming.

The position is consistent with industry practice; almost two-thirds (59%) already record these in separate AI inventories. Generative AI is the most widely used technology (75%), with machine learning (71%) close behind. While banks are enthusiastic about the future potential of agentic AI and agentic workflows, only 11% of respondents said their institutions were using them. Overall, only a third (29%) have reached the “operate and monitor” stage with any AI use case, a state where an AI system is continuously used within a well-structured governance environment.

For now, institutions are parsing the treatment of AI systems. While 44% of respondents said they don't monitor or test individual AI use cases, another 31% said they do it ad hoc. For those AI systems classified as models, 87% of respondent institutions validate them at least sometimes. For those identified as non-model tools, 60% said they are not validating them at all and 40% said they look at them sometimes.

Flagging a potential risk, 42% of respondents said that they never validate AI systems classified in a separate AI inventory, while 38%

said they do only sometimes. In the still-early stages of AI in production, institutions are relying heavily on people to validate results in the field.

Human-in-the-loop review (71%) was by far the most common method institutions use to review and control AI. Some do reasonableness testing (22%), hallucination rate testing (10%), and bias/fairness testing (6%). Explainability (67%) remains the top challenge to validating AI systems—reflecting the black-box nature of large language models.

“Evaluating AI models and applying sound risk assessment principles are still very much a work in progress,” Kutteh said.

Conclusion

As the industry adapts to SR 26-2, the survey findings reveal that model risk management is becoming more targeted in its application while remaining firmly anchored in principles such as independence, effective challenge, and accountability.

Institutions are expanding oversight beyond traditional quantitative models to include non-model tools, cybersecurity applications, and emerging AI technologies, even as resource constraints and vendor transparency concerns persist.

At the same time, organizations continue to rely heavily on third parties and are still working to establish consistent approaches for AI governance and validation. Together, the findings depict an MRM function whose responsibilities continue to broaden and evolve while its core mission—ensuring the sound, controlled use of analytical tools across the enterprise—remains unchanged.>

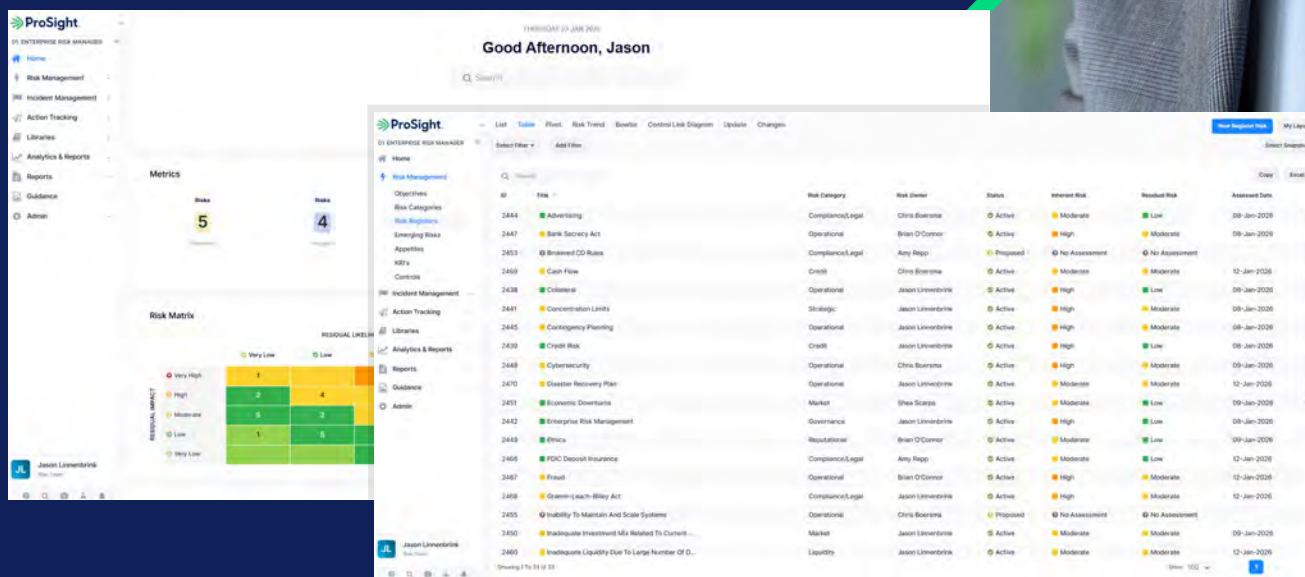


ProSight Enterprise Risk Manager

Your Risk Program Shouldn't
Live in Spreadsheets

Different departments, different terminology, different definitions of high risk. When risk data is scattered across applications, spreadsheets, inboxes, and shared drives, coordinating mitigation takes longer than the mitigation itself, and no one has a current view of where the institution actually stands.

ProSight Enterprise Risk Manager replaces the patchwork with one system built for financial institutions: centralized risk and control registers, structured self-assessments, KRI monitoring, and reporting leadership can act on.



Learn more at ProSightFA.org.

Stay Ahead. Lead with Confidence.



Community Banks Gain Model Risk Flexibility

Revised model risk guidance grants flexibility, but community banks remain responsible for oversight.

COMMUNITY AND REGIONAL banks may have more flexibility under the federal banking agencies' revised model risk management guidance, but institutions under \$30 billion in assets should not assume model risk has disappeared from the regulatory radar.

That was a central message from Kevin Oden, founder and managing partner of Kevin D. Oden & Associates, during a recent ProSight Financial Association webinar examining the implications of the agencies' new model risk management (MRM) guidance for smaller institutions. While the revised framework reduces prescriptive expectations for many banks under \$30 billion, Oden emphasized that regulators continue to expect institutions to manage model risk in a manner consistent with safety-and-soundness obligations.

"The threshold is a soft signal, not a bright line," Oden said.

The revised guidance, issued jointly by the Federal Reserve, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corp. in April, updates the long-standing SR 11-7 framework that has governed model risk management for more than a decade. While the agencies state that the guidance is expected to be most relevant to institutions with more than \$30 billion in assets, Oden stressed that smaller banks remain responsible for understanding and managing the risks associated with the models they use.

“SR 11-7 still provides the foundational conceptual framework for how banks should manage their model risk,” he said.

The guidance changes regulatory expectations for institutions below the \$30 billion threshold, but it does not eliminate them. Oden noted that the revised framework contains explicit requirements for smaller institutions whose activities or model use extend beyond traditional community banking.

“The door is not closed,” he said.

Safety and Soundness Remains the Standard

Oden also stressed that banks under \$30 billion cannot dismantle model risk management programs or stop investing in oversight.

“I’ve heard people say, ‘Well, we’re under \$30 billion, so we don’t need to invest in MRM anymore.’ That is the furthest thing from the truth,” he said.

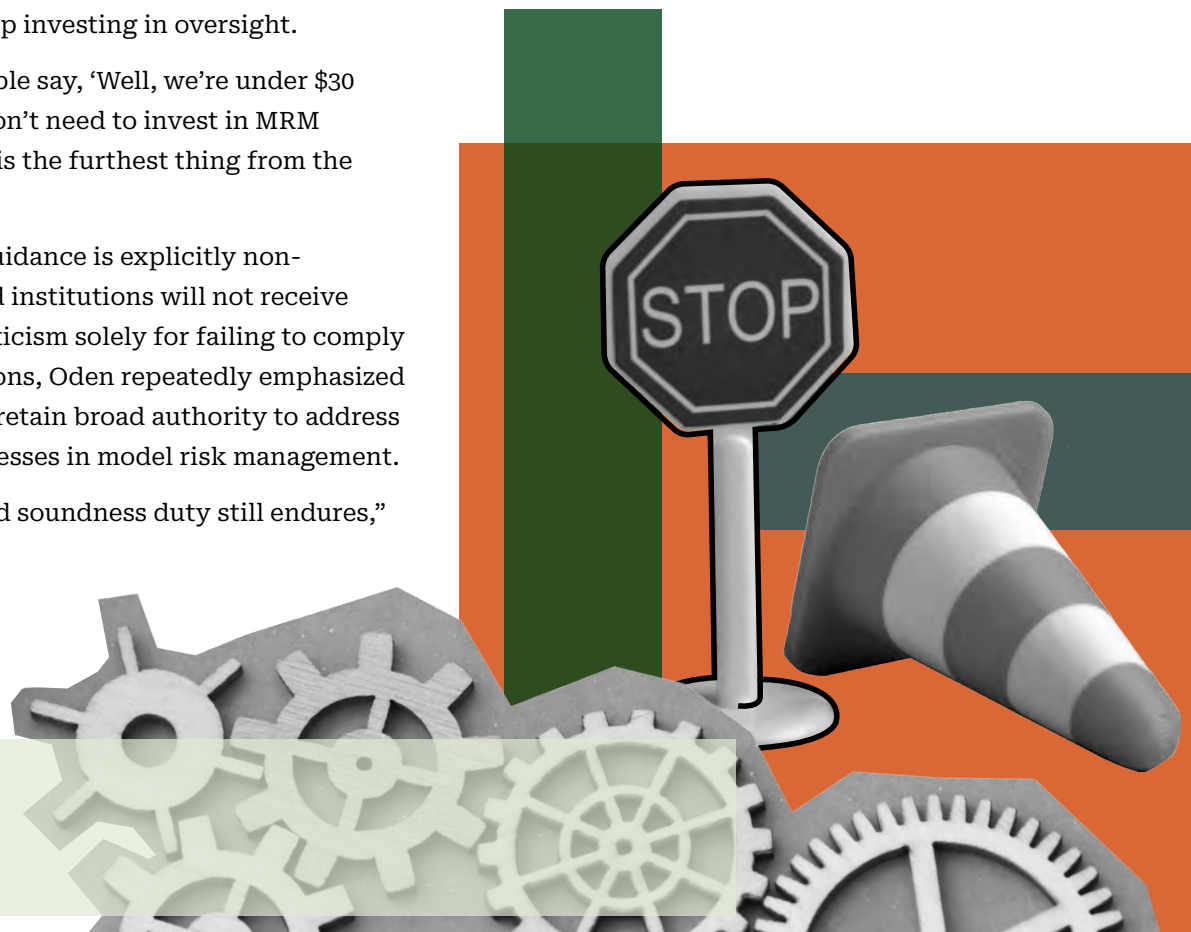
Although the guidance is explicitly non-enforceable and institutions will not receive supervisory criticism solely for failing to comply with its provisions, Oden repeatedly emphasized that regulators retain broad authority to address material weaknesses in model risk management.

“Your safety and soundness duty still endures,” he said.

Examiners retain authority to identify unsafe or unsound practices stemming from poor model risk management, particularly when models influence capital, liquidity, fraud detection, anti-money laundering compliance, credit decisions, or other activities with significant business or customer impacts.

The revised framework may be lighter, Oden said, but responsibilities tied to safety and soundness have not changed.

Will Kutteh, director of ProSight’s Model Validation Consortium, said one model risk manager recently summarized the situation to him succinctly: “Model risk for financial institutions below \$30 billion did not evaporate overnight.”



Not Every Community Bank Faces the Same Expectations

But the new guidance “does give you the ability,” Oden said, to “tailor or right-size your risk management posture around your models to be commensurate with the risk.”

For banks whose model use remains confined to traditional community banking activities, that right-sizing could be significant.

Oden described what he called a “Path A” approach for institutions with no fintech partnerships, no crypto or digital-asset activities, and model use confined to conventional community banking practices. Those institutions still have model risk management responsibilities, but they may be able to reduce work associated with lower-risk and immaterial models.

High-risk models, however, may continue to warrant more frequent review. Oden suggested that institutions consider maintaining validation frequencies of at least every two years for those models while applying more flexible approaches elsewhere.

The key, he said, is documenting the rationale.

“You will need to basically document why you’ve made changes to your program, what activities are in scope and out of scope, and why they’re out of scope,” Oden said.

That documentation trail, he added, will be critical when examiners review an institution’s approach.

Some Activities Trigger Greater Scrutiny

Meanwhile, Oden said, a number of modeling activities remain firmly in regulatory scope regardless of asset size.

Among them are stablecoin and digital-asset activities, complex credit products, capital markets activities, significant fintech partnerships, and certain forms of artificial intelligence and machine learning.

“If you have stablecoin or digital asset activities ... those activities will definitely be in scope,” he said. The same applies to:

- Specialty finance.
- Asset-based lending.
- Structured products.
- Credit modeling beyond conventional underwriting.
- Capital markets activities (including value-at-risk models).
- Valuation models.
- Hedging.
- Counterparty exposure models.
- Fraud detection.
- Bank Secrecy Act and anti-money laundering models.
- Customer analytics.
- Other models tied to regulatory obligations or customer outcomes.

Kutteh said institutions engaged in more complex or nontraditional activities continue to have strong strategic reasons to maintain a solid understanding of the models they rely on.

“There is still strong justification from a strategy perspective in having a good understanding of the models that are in use and they’re using to make these decisions,” he said.

AI Remains a Complicated Area

One area generating confusion involves artificial intelligence.

Oden said banks should distinguish between traditional AI and machine-learning models, which remain within the scope of model risk management, and generative or agentic AI systems, which the revised guidance explicitly excludes.

The distinction matters because some institutions appear to assume all AI-related activities have been removed from model risk management requirements. Oden said that interpretation is incorrect.

Oden added that he expects regulators to issue additional guidance on generative and agentic AI, though no such guidance had been released as of early summer 2026.

A Shift Toward Proportional Oversight

The revised guidance also introduces concepts that many institutions have already been applying informally, including the notion of immaterial risk.

Kutteh said the new terminology provides organizations with greater clarity and may allow some institutions to move away from full validation requirements for the lowest-risk models in their inventories.

The concept aligns regulatory expectations more closely with the actual risks posed by different types of models, he added.

Kutteh also highlighted growing interest in trigger-based or change-based validation approaches: tying validations to material modifications, environmental changes, or other significant events rather than a fixed calendar schedule.

That approach, he said, has the potential to align model risk management workloads more closely with how institutions actually operate and maintain models.

Flexibility Comes With Responsibility

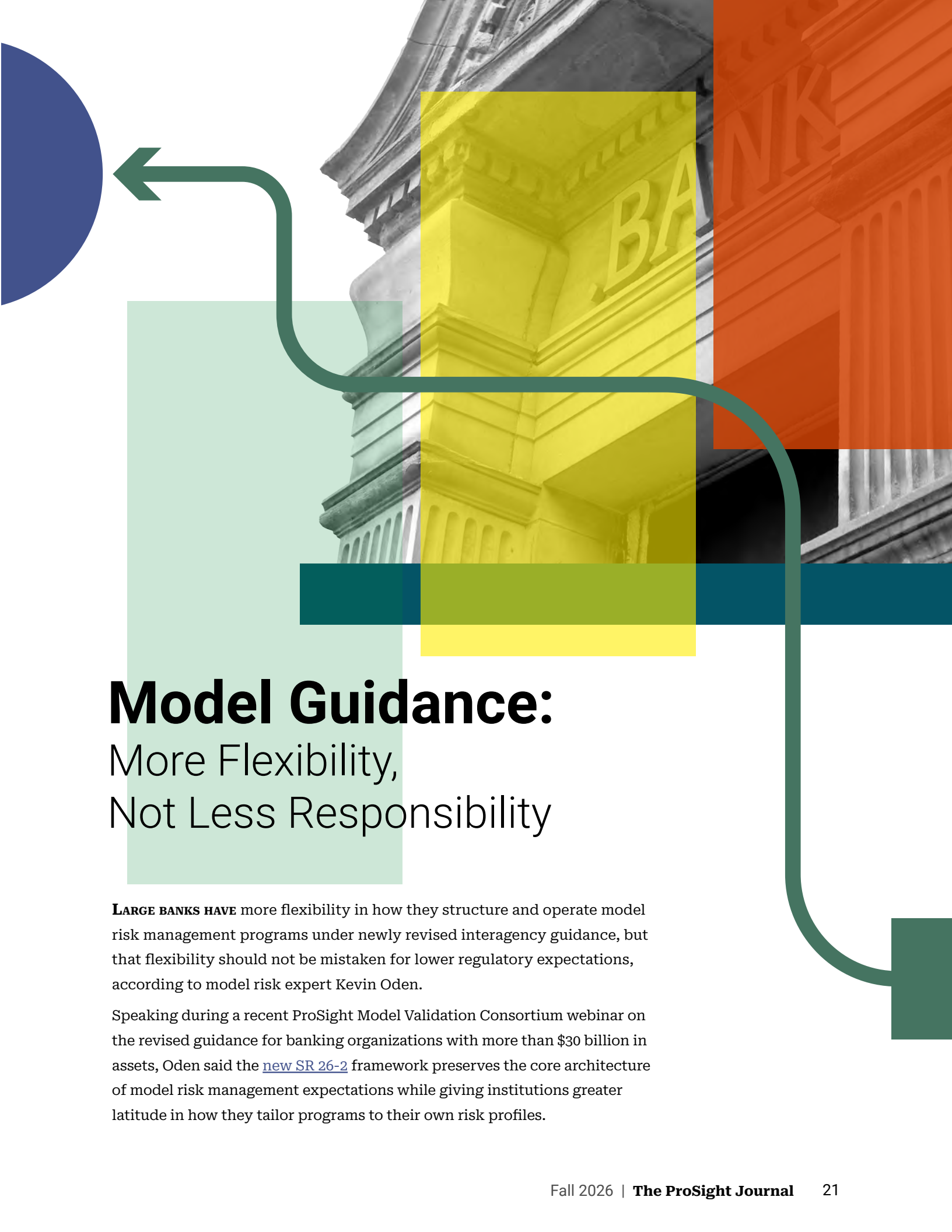
Throughout the discussion, both speakers returned repeatedly to a single theme: flexibility.

The revised guidance gives community banks more discretion in how they structure model risk management programs, allocate resources, and oversee lower-risk models. But that flexibility comes with an obligation to explain and support those decisions.

“With this opportunity for increased flexibility comes the obligation to justify the rationale behind some of those modifications,” Kutteh said.

For many community banks, that may mean fewer validation exercises, streamlined documentation requirements, and more targeted oversight. But it does not mean model risk management has become optional.

For institutions under \$30 billion, the challenge is not deciding whether model risk management still matters. It is determining how much is enough.>



Model Guidance:

More Flexibility, Not Less Responsibility

LARGE BANKS HAVE more flexibility in how they structure and operate model risk management programs under newly revised interagency guidance, but that flexibility should not be mistaken for lower regulatory expectations, according to model risk expert Kevin Oden.

Speaking during a recent ProSight Model Validation Consortium webinar on the revised guidance for banking organizations with more than \$30 billion in assets, Oden said the [new SR 26-2](#) framework preserves the core architecture of model risk management expectations while giving institutions greater latitude in how they tailor programs to their own risk profiles.

Programs built under the old framework “often accumulated process debt,” said Oden, founder and managing partner of Kevin D. Oden & Associates. “This is an opportunity to streamline.”

The revised guidance, issued jointly by the Federal Reserve, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corp. on April 17, replaces several earlier issuances, including the longstanding SR 11-7 framework that has guided model risk management for more than a decade.

While the new guidance retains the familiar three-pillar structure of model development and use, validation, and governance, Oden said the regulatory stance has changed significantly.

“The regulatory posture is principles-based rather than prescriptive,” he said.

That shift is particularly important for institutions above the \$30 billion threshold, where the guidance is expected to be most relevant.

Among the most significant changes, Oden highlighted a move toward a more risk-based approach, a less rigid view of validation independence, a newly codified concept of aggregate model risk, and the explicit exclusion from scope of generative and agentic artificial intelligence.

A Risk-Based Framework

One of the central themes of the revised guidance is flexibility.

“It used to feel like one size had to fit all, whether you were \$100 billion or whether you were \$1 trillion in assets,” Oden said. Under the new framework, he said, expectations are intended to be proportional to the scope and complexity of an institution’s activities.

Banks above \$30 billion in assets remain squarely within the scope of the guidance. However, Oden said the framework gives institutions more room to calibrate oversight based on the materiality and risk of individual models.

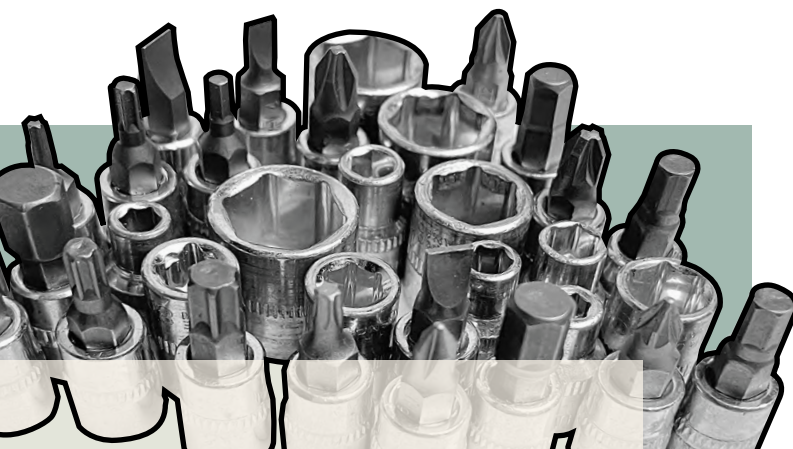
“The framework gives you flexibility, not a pass,” he said.

Low-risk or immaterial models may require less frequent monitoring or less intensive validation than higher-risk models, provided institutions can justify those decisions and maintain appropriate documentation.

“The responsibility for managing model risk remains the same,” Oden said. “It should be commensurate with the risk.”

Will Kutteh, director of the Model Validation Consortium at ProSight Financial Association, said many institutions have already begun exploring ways to create lower-risk categories within model inventories to better align oversight requirements with actual risk.

Organizations have been saddled with applying the same level of rigor to ultra-low-risk models as they do to more consequential models, he said. The revised guidance gives institutions additional support for taking a more differentiated approach.



New Attention to Aggregate Risk

Another significant development is the formalization of a risk framework built around concepts including inherent risk, model exposure, model purpose, materiality, and aggregate risk.

Oden said many institutions already considered these concepts informally, but the revised guidance places them at the center of model risk management.

The addition of aggregate risk may prove especially significant.

Regulators have long asked institutions how they think about model risk across an enterprise rather than within individual models, Oden said. The new guidance explicitly incorporates that concept into the framework.

Aggregate risk includes interactions among models, upstream and downstream dependencies, common assumptions, and shared data sources.

“If every model in your inventory relies on, say, the Secured Overnight Financing Rate, then there is some risk to that data being corrupted,” Oden said.

Exactly how institutions will measure aggregate risk remains uncertain, he acknowledged. Approaches will likely differ from one institution to another before practices begin to converge.

One potential approach is to treat aggregate risk as an overlay that reflects the concentration of assumptions or dependencies across a model inventory. “I think the easiest way to think about that aggregate risk is as an overlay,” Oden said.

Kutteh said aggregate risk is “more closely positioned as one of the building blocks” of model risk under the revised framework. Under

the earlier guidance, he said, it was more closely associated with inventory management and board reporting.

Validation Independence Evolves

Perhaps the most closely watched change for many institutions involves validation independence.

Under the prior framework, regulators frequently focused on organizational structure and separation between model developers and validators. Oden said the revised guidance places greater emphasis on the quality and rigor of validation rather than where validators sit within an organization.

“The quality of the validation process now really depends even more so on rigor and effectiveness rather than organizational structure,” he said.

“If every model in your inventory relies on, say, the Secured Overnight Financing Rate, then there is some risk to that data being corrupted.”

—Kevin Oden

The change could give institutions more latitude in how they structure validation functions, particularly when using third-party support.

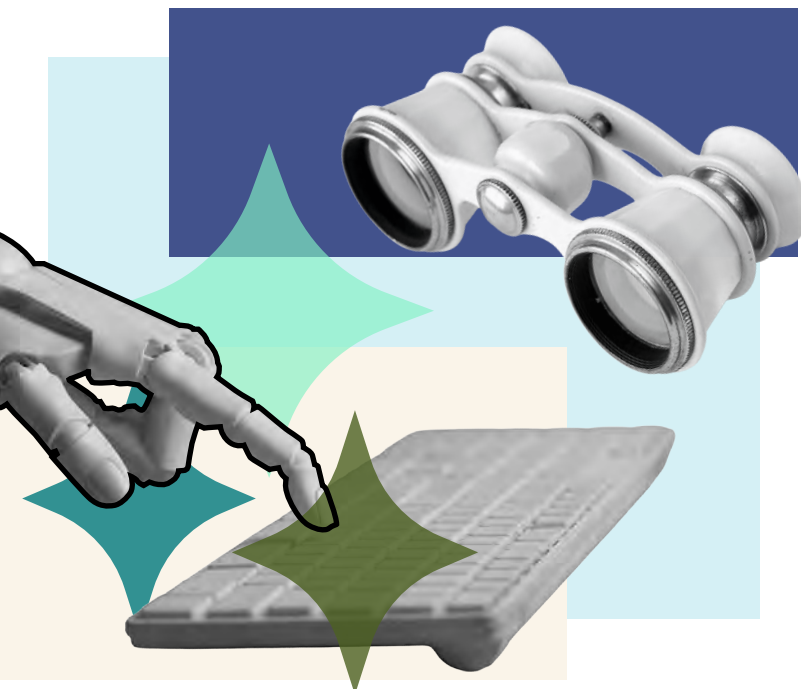
“External and even co-sourced validations can be clearly defensible if you can still prove that effective challenge,” Oden said.

In other words, validators must still have sufficient authority and expertise to challenge model developers and model owners, even if the organizational structure differs from traditional approaches.

The emphasis of validation reports may need to shift accordingly, focusing less on organizational independence and more on demonstrating the rigor of review and challenge.

AI Carve-Out Creates Governance Questions

The revised guidance explicitly excludes generative AI and agentic AI systems from its scope, a decision that has generated considerable discussion among model risk professionals.



Large language models, retrieval-augmented generation systems, and multi-step agentic AI systems are all carved out of the guidance, Oden said.

Traditional machine learning models, however, remain firmly within scope.

“AI and ML models were explicitly pulled into the model inventory,” he said.

Oden said he expects additional regulatory guidance on generative and agentic AI in the future.

In the meantime, institutions may need to establish separate governance frameworks for emerging AI technologies.

“You should consider an AI governance policy,” Oden said.

Potential elements could include alignment with the National Institute of Standards and Technology’s AI Risk Management Framework, AI-specific board reporting, and processes for evaluating AI capabilities embedded in third-party products.

Kutteh said many institutions were already using model risk management frameworks as a foundation for AI governance before the revised guidance was issued.

Now, he said, organizations are increasingly creating dedicated AI governance committees, working groups, or centralized functions that operate separately from traditional model risk programs.

That does not mean model risk management teams will be excluded from AI oversight. Instead, many institutions continue to involve model risk professionals in inventory, assessment, and governance activities as AI programs mature.

A Chance to Right-Size Programs

Despite the flexibility in the new guidance, neither Oden nor Kutteh expects large institutions to make abrupt changes to their model risk programs.

Many banks are already planning updates to model risk management policies this year, Kutteh said, but most appear focused on targeted adjustments rather than wholesale redesigns.

Areas likely to receive attention include policy language, inventory definitions, validation methodologies, and governance structures.

Oden encouraged institutions to review references to older guidance, adopt the new terminology introduced by the revised framework, and reassess inventory classifications.

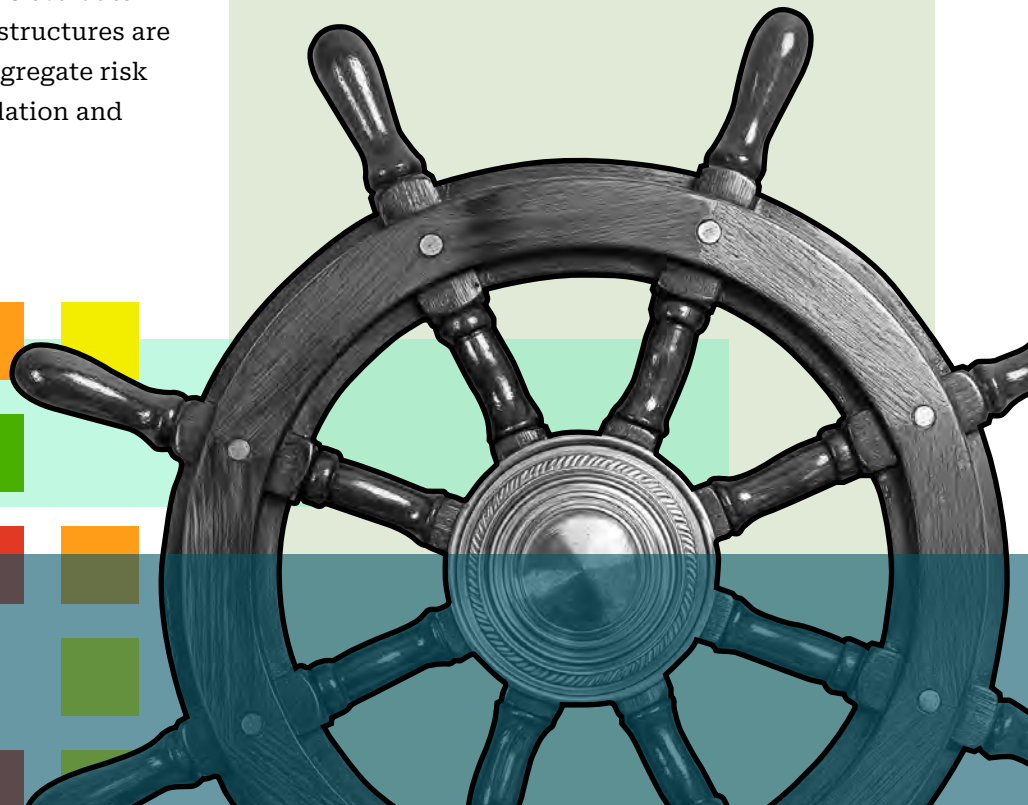
He also suggested that institutions evaluate whether separate AI governance structures are appropriate and consider how aggregate risk should be incorporated into validation and reporting processes.

Most importantly, he said, institutions should view the revised guidance as an opportunity to improve efficiency while preserving sound risk management practices.

“This is an opportunity to right-size, not retreat,” Oden said.

For large banks, the revised guidance may offer more flexibility than the industry has seen in years. But according to Oden, the expectation that institutions actively identify, understand, and manage material model risk remains unchanged.>

Guided by an industry-led Advisory Council, ProSight’s [Model Validation Consortium](#) combines 100+ years of experience in advancing sound risk management principles with deep knowledge and expertise in all phases of model risk management.





NOVEMBER 15-18, 2026 | OMNI FORT LAUDERDALE

ProSight Internal Audit Conference

Navigating Technology, Risk, and Change



300+
Attendees



25+
Sessions



60+
Speakers



120+
Institutions

About the ProSight Internal Audit Conference

Designed for internal audit professionals in financial services, this event delivers education, insights, and networking on today's evolving technology, risk, and regulatory landscape.

Gain practical perspectives on AI, operational resilience, cyber risk, enterprise transformation, and regulatory developments from industry leaders and experienced practitioners.



Opening Keynote:
Erica Orange
Futurist & Author of
"AI + The New
Human Frontier"

Attend to hear her session, "The Future Rewired: Navigating Transformation in a Rapidly Evolving Financial Services Environment"

Advance your professional journey
by earning up to 18 NASBA-approved CPE credits

Benchmark emerging practices
with peers across the financial services industry

Build connections with professionals
driving the future of assurance and risk

Register Today

Reserve your room at the Omni Fort Lauderdale by Friday, October 23, 2026, to secure the group discounted rate.

Lender Liability:

Where **Good** Intentions Go **Wrong**

How routine
banking decisions
can trigger lender
liability and costly
borrower claims.

By Jason Alpert, CRC, and Martin Knaust



The wrong comment made by the relationship manager, the failure of the portfolio manager to issue a default letter, or a simple mistake by loan servicing could all result in harm to the borrower—resulting in a lender liability case.

BANKERS EXPECT TO be repaid on their loans, but what happens if their borrowers have been harmed (or think they have been harmed) by a bank during the origination or servicing of the asset? Lender liability is one of those topics that tends to surface during banker training sessions, legal reviews, or after something goes wrong with a loan and it's transferred to workout. Most bankers understand lender

liability conceptually, but do they appreciate how easily the ingredients for a lender liability claim can develop during the course of a seemingly normal borrower-lender relationship? The wrong comment made by the relationship manager, the failure of the portfolio manager to issue a default letter, or a simple mistake by loan servicing could all result in harm to the borrower—resulting in a lender liability case. It is important for bankers, especially those in a customer-facing role, to understand lender liability and how to avoid it (especially if collecting the loan is proving to be difficult).

At its core, lender liability can be distilled into a simple formula:

(Loan + Duty) x Breach = Damages.

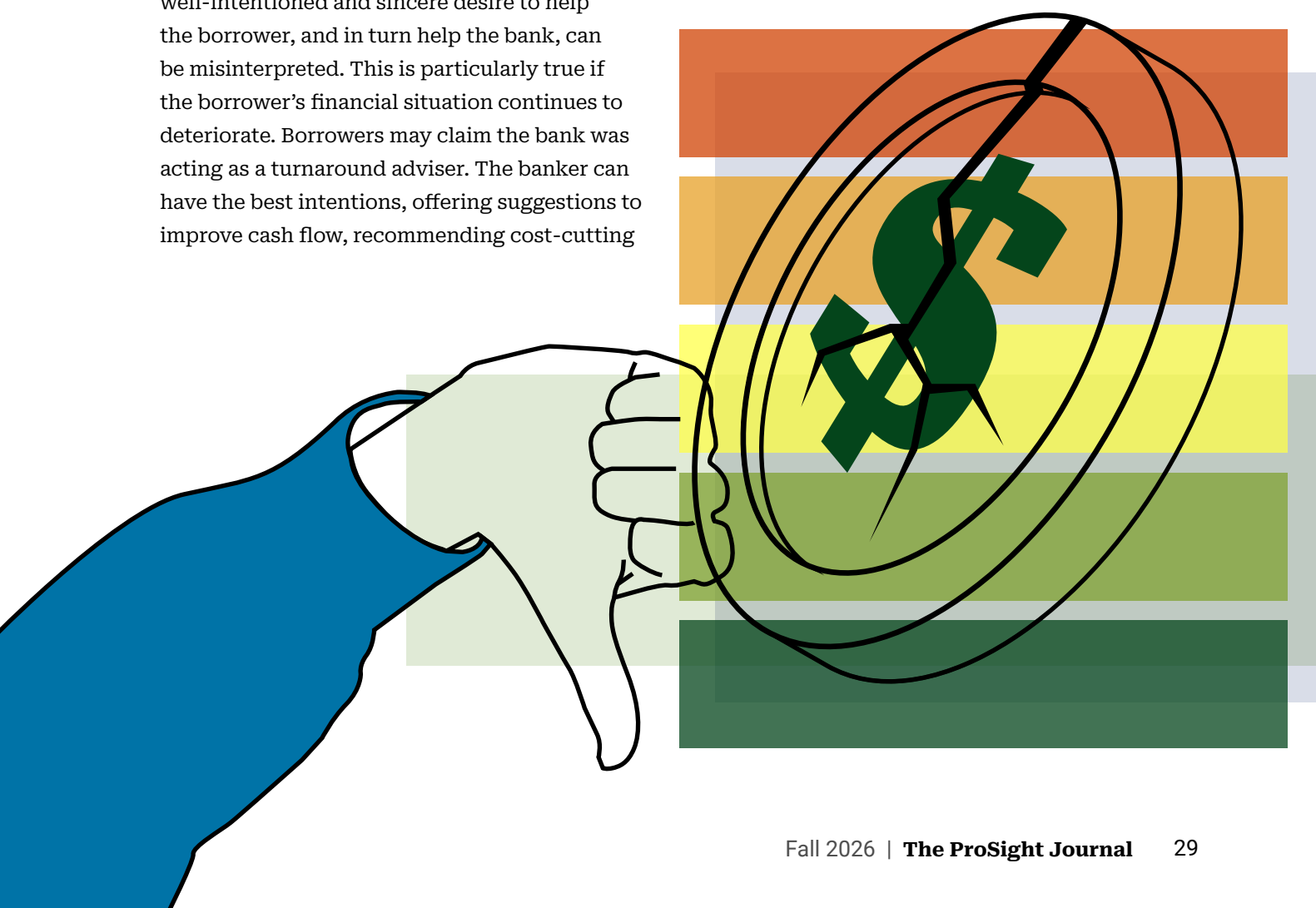
To break down this formula, every lender liability claim starts with a loan or credit and the lender's duties that accompany it. These duties can be generally categorized as contractual, common law, and statutory standards. The contractual standards are the explicit terms outlined in the loan documents and agreements. The common law duties are those such as good faith and fair dealing. Statutory standards include regulatory requirements and other legal obligations. The breach is any act or omission by the bank that violates a duty owed to the borrower, whether by contract, common law, or statute, and is the proximate cause of damage to the borrower. Typically, damages are the money that the borrower has allegedly lost due to the bank's act or omission, and recovery may be sought by arbitration, mediation, or litigation. In that regard, the bank's contract with the borrower may control what remedy the borrower may seek and the method, timing, and venue for pursuing it. Damages are most often compensatory in nature, seeking to make the borrower whole or limiting some or all of the borrower's obligation to repay the loan. In certain circumstances, damages may be more punitive in nature, seeking

to punish specific bad acts. A regulation or statute may also provide for a specific or fixed measure of damages. While the lender liability formula seems simple, the implications and penalties are far-reaching and complex.

A lender liability issue may arise at any point during the life of a loan, but a claim more often arises when the loan is in default or nearly so, with no clear path of returning to fully performing status without significant turnaround. With a performing loan, most communication is structured and limited. With a problem loan, communication becomes more frequent and difficult. Relationship managers often try to stabilize the situation and help their customers by offering guidance, suggesting strategies, and working closely with management. Unfortunately, it is at this point that the traditional lender-borrower boundaries may become unclear, and a banker's well-intentioned and sincere desire to help the borrower, and in turn help the bank, can be misinterpreted. This is particularly true if the borrower's financial situation continues to deteriorate. Borrowers may claim the bank was acting as a turnaround adviser. The banker can have the best intentions, offering suggestions to improve cash flow, recommending cost-cutting

measures, or introducing strategy. But these same suggestions can be cited in claims that a lender directed the borrower on how to operate the business, especially if the moves appear to benefit the lender at the expense of other stakeholders in the business.

For example, consider a lender that strongly encourages a borrower to remove a key salesperson and reduce headcount by 15% to obtain a draw under a line of credit. Now imagine that the salesperson and others who were let go were responsible for major customer relationships now lost to the company—resulting in further financial woes. If that series of events can be construed as part of a quid pro quo for preferential treatment of the bank, the bank could face a lender liability claim—even if the lender's advice appeared to be accepted and enacted by management.



The potential perils of lender liability claims are particularly well illustrated in a case earlier this decade filed by a Texas manufacturer serving the automotive industry. In it, the lender was accused of essentially using its factoring structure to sweep the borrower's collections and exert excessive control over the day-to-day operations of the business, including who could be paid and when. The filing claimed that the lender's actions advanced its own interest to the detriment of the interests and viability of the business as a going concern. As the situation deteriorated, the lender exerted more operational control, and ultimately the business failed. The bankruptcy court found the lender at fault for the borrower's collapse and held it liable to the bankruptcy estate for almost \$17 million, with a separate award to the owner individually. Roughly \$14 million of that amount was for loss of enterprise value and lost business opportunity, not disputed principal.

Most of the landmark lender liability claims emerged in the 1980s, with a general trend of courts since then limiting the scope of lender liability. But the Texas case is an important warning that lender liability claims are still alive and well—and that potential damages can involve more than just the amount of the outstanding loan balance.

When working with the borrower and providing guidance, the lender must be clear that the ultimate business decision is to be made by the owner and management. In both oral and written communications, the lender must qualify any recommendations as just that and make clear that the bank is not requiring the borrower to follow them. The bank must communicate that all its business decisions are made in the context of the overall relationship with the borrower and not limited to any specific borrower action or decision. The lender should avoid tying any specific action (for instance, a renewal or payment modification request) to something the borrower did or did not do. If there is any appearance of a *quid pro quo*, the borrower can make the argument that it only took a specific course because the bank compelled it to do so.

One of the most overlooked drivers of lender liability is the “course of dealing” argument borrowers can assert against a bank. In simple terms, a course of dealing refers to how the lender and borrower actually behave over time, not just what is written and agreed to in the loan documents. This can seem counterintuitive. After all, loan documents are the legal basis for how the loan and relationship are to be governed. However, over the course of a

One of the most overlooked drivers of lender liability is the “course of dealing” argument borrowers can assert against a bank.

relationship, if certain terms in the contract aren't enforced, the bank can lose those rights over time as the borrower can reasonably assert that it relied on the bank's nonenforcement as the new operating paradigm for the relationship. If a lender consistently waives covenants, delays enforcement of a provision, or provides informal assurances, those actions can effectively modify the loan terms. These patterns may create an implied obligation on the part of the bank to act the same way in the future. For instance, assume a real estate loan has a debt service coverage ratio (DSCR) covenant associated with it. However, year after year, the borrower defaults under that loan and the bank, in order to mollify the customer, waives the default each time (or worse, doesn't even notify the borrower they are in default). After a few years, the bank's management or its regulators require the enforcement of the default. But the customer now has an argument that it believed the DSCR was not material to the bank, and it relied on receiving another waiver.

The best practice is to formally notify the borrower of the current default and that any waiver or accommodation of that default is a one-time event that does not permit or waive any future default or enforcement action. Where the bank is granting something of value, whether a waiver, a forbearance, a modification, or simply additional time, it is both reasonable and appropriate to request a release of claims in exchange. That request must be in writing and needs to be supported by identifiable consideration. The release should also cover known and unknown claims through the effective date, and should be joined by any guarantors, who hold claims of their own. It is important to note that such a release is bargained for, not extracted. A bank that withholds funding it is already obligated to advance until the borrower signs a release has not protected itself from a lender liability

claim—quite the opposite. It has created the very claim it was hoping to avoid.

Another area that deserves attention is confidentiality. When borrowers become distressed, lenders often interact with a broader group of stakeholders such as employees, vendors, advisers, brokers, and potential investors. Each of these interactions can create unintended lender liability exposure.

Bankers understand the critical importance of confidentiality; however, when searching for answers or solutions, the lender could accidentally share information with people who do not have a need to know—which could harm the customer. For instance, consider a customer who is not financially astute and directs the bank to get answers from their bookkeeper. During the conversation, the bank shares that the loan is in default and moving to the workout group. The bookkeeper then shares this information with colleagues in the breakroom and employees resign en masse, resulting in the company being unable to staff.

The bank should always obtain written borrower consent regarding who the loan can be discussed with and the scope of information that can be shared. In the event information is to be shared with an outside party who does not have a specific need to know, the lender must ensure that a confidentiality or nondisclosure agreement is executed. Even well-intentioned conversations can create issues if they involve unauthorized disclosure or suggest the lender is acting on behalf of the borrower.

Finally, distressed situations often involve outside professionals who, while valuable, introduce additional complexity. Lenders must be mindful of how these advisers are engaged. The borrower, not the bank, engages, retains, and hires its own advisers. The bank can certainly make recommendations, but it does not control who the borrower selects.

There are situations, such as the engagement of a turnaround professional, where the bank will require the borrower to hire a professional adviser. In those instances, the bank can require a turnaround consultant, but it needs to provide at least three firms acceptable to the lender and allow the borrower to make the choice. That said, the borrower should have the right to hire an advisor not on the lender's list, provided that the adviser possesses the documented expertise and experience the lender requires. This discipline is not limited to turnaround consultants or to distressed credits. Any time a banker recommends a professional, whether an accountant, attorney, appraiser, engineer, or investment banker, the same practice applies: offer several qualified names, document that the borrower made the selection, and have the borrower engage and pay the professional directly. The bank should disclose any business relationship it has with a firm it recommends and should never accept compensation for a referral. A single name offered casually at origination can look very different several years later, when the relationship has soured and the borrower is reconstructing who told it to do what.

In essence, avoiding lender liability boils down to disciplined communication and execution when engaging with the customer. While there are occasional bad acts by the lender during the origination and servicing of the loan, most lender liability claims arise unintentionally

through the bank attempting to help its customer or limit losses to its shareholders. That unintended nature points to a knowledge gap worth addressing. Most banks train extensively on credit, including underwriting, structure, risk rating, and documentation, and very little on what a banker should say and write. Improper or unprofessional communication, a comment made in a meeting, a suggestion that was heard as a directive, or an email written in frustration can have significant implications. The most cost-effective lender liability control banks can adopt is coaching on communication discipline, a clear escalation path to workout and counsel, and this simple standard for correspondence: write every email as though it will be published on the front page of The Wall Street Journal. In cases where there is any hint or claim of lender liability, the bank should proceed very cautiously and research the claim thoroughly. The bank should engage its internal counsel and consider outside counsel if necessary. If an argument can be made that lender liability exists, the bank must make every effort to remediate the situation and sometimes even provide the customer with favorable terms to obtain a waiver of claims and a release in a modification or forbearance agreement.>

Jason Alpert is managing partner at Castlebar Holdings, a distressed debt fund and financial institution adviser. Jason led and managed workout and special asset teams at major financial institutions for two decades. He is on the editorial advisory council of The ProSight Journal and is an adjunct professor at the University of Tampa. Email Jason at jason@castlebarholdings.com or reach out to him at 813-293-5766.



AI Data Center Risks and Opportunities for Lenders

By Amy Short

ARTIFICIAL INTELLIGENCE is transforming industries across the economy, but behind every AI application sits a growing physical infrastructure requirement: data centers. As organizations race to deploy AI-powered tools and services, demand for computing power, storage capacity, and networking infrastructure is accelerating at an unprecedented pace.

For lenders, this rapid expansion potentially presents significant opportunities as well as emerging risks. Financing AI-related data center projects can provide access to a sector with strong long-term growth prospects, but these projects also require careful underwriting due to their substantial capital needs, evolving technology requirements, and increasing regulatory scrutiny.

As banks evaluate lending opportunities tied to AI infrastructure, understanding the fundamentals of the data processing and hosting industry can help identify the possible rewards and risks that deserve closer examination.



The Growth Story Behind AI Infrastructure

The data processing and hosting industry is experiencing strong momentum. The [Vertical IQ Industry Profile](#) for Data Processing & Hosting (NAICS 518210) shows that revenue increased 13.9% year over year in the fourth quarter of 2025, reaching nearly \$114 billion for the quarter. Looking ahead, industry sales are forecast to grow at a compound annual rate of 9% through 2030, more than double anticipated GDP growth.

Of course, AI is a major driver behind this growth. Data centers worldwide are expected to require approximately \$6.7 trillion in capital expenditures by 2030 to meet demand for computing power. Of that amount, AI-focused facilities alone are projected to account for \$5.2 trillion.

The scale of these investments creates opportunities across multiple lending categories, including:

- Commercial real estate financing for data center development.
- Construction lending for new facilities.
- Equipment financing for servers, networking equipment, and power systems.
- Working capital facilities for operators and service providers.
- Treasury management and cash management services.

But demand is being fueled by more than AI applications alone, as we see continued growth in cloud computing, software as a service (SaaS), data analytics, disaster recovery services, and remote work technologies.

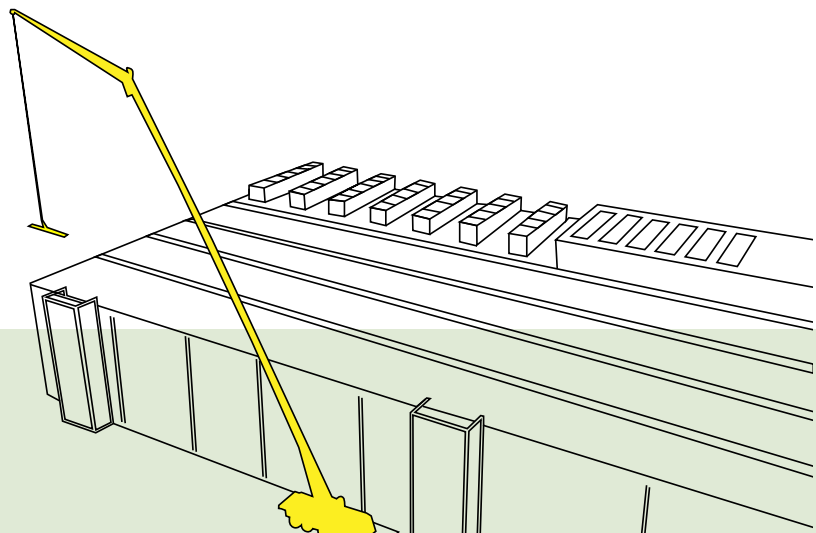
Why AI Data Centers Appeal to Lenders

Several characteristics make the data processing and hosting vertical particularly attractive from a credit perspective.

The industry benefits from recurring revenue streams generated through hosting contracts, cloud services, co-location agreements, and software subscriptions. Many of the industry's customers enter into multi-year service agreements, creating predictable cash flow and high customer retention when service levels are maintained.

The data center industry also demonstrates healthy profitability. According to Vertical IQ's latest financial benchmarks, firms generated median EBITDA margins of 16.2% and after-tax net profit margins of 6.3% in 2024-25.

Additionally, the niche's barriers to entry for competitors are substantial. Successful data center operators require significant investments in infrastructure, specialized technical expertise, cybersecurity capabilities, and reliable power and cooling systems. The industry's credit profile reflects these advantages, earning a "Stable/Satisfactory" industry risk rating and exhibiting lower cyclical sensitivity than many other industries.



A Booming AI Industry ... But Not Without Risks

For lenders, these data points can support attractive financing opportunities when projects are properly structured and sponsors have demonstrable operational expertise. Yet the AI data center niche still exhibits several potential challenges that must be considered by financial institutions.

Energy: A Very Real Risk Factor

While AI is driving major data processing and hosting demand, it is also creating one of the industry's most significant risks: energy consumption (a hot topic in the news lately).

Data processing and hosting centers consumed approximately 4.7% of total U.S. electricity in 2024, according to the Department of Energy's latest figures released in June 2026, and DOE projects that figure could rise to 11.8% by 2030. Total data center electricity consumption increased from 58 terawatt-hours in 2014 to 192 terawatt-hours in 2024 and could reach as much as 649 terawatt-hours by 2030.

The growing strain on power grids and water resources has drawn increasing attention from policymakers. In fact, legislators in 14 states are pursuing measures that would limit or delay new data center construction while studying impacts on communities and grid reliability.

Lenders evaluating new AI data center projects should closely examine:

- Availability and reliability of power and water infrastructure.
- Utility commitments and pricing arrangements.
- Grid capacity in the project location.
- Renewable energy strategies.
- Potential regulatory and permitting hurdles.

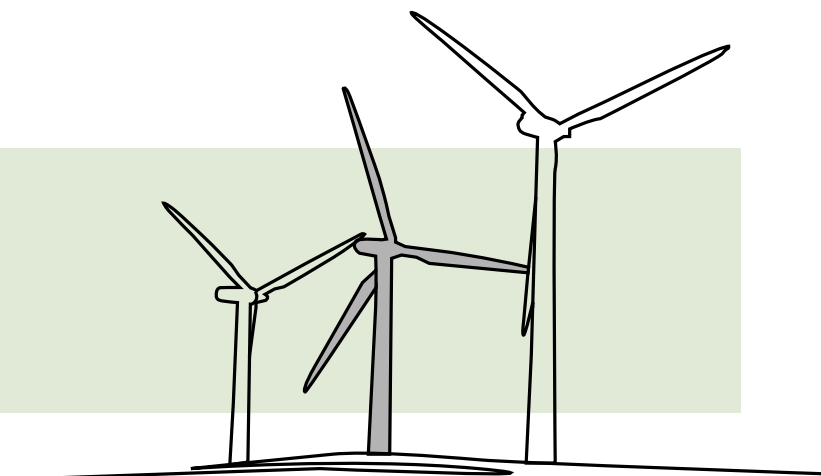
Projects with secured power and water access and strong energy management plans may hold a significant competitive advantage over facilities that face uncertainty around future resource availability.

Technology Obsolescence Concerns Are Also Legitimate

Traditional commercial real estate assets have typically enjoyed long useful lives and relatively stable functionality. But we are seeing that AI infrastructure is different. Rapid technological change is one of the industry's primary risks. Hardware, software, networking technologies, and AI computing architecture continue to evolve at a rapid pace. Data processing and hosting firms must continually upgrade infrastructure and invest in staff training to remain competitive.

For lenders, this means evaluating more than just the real estate itself. Questions worth exploring include:

- How frequently will computing equipment require replacement?
- Does management have a proven upgrade strategy?
- Are capital expenditure projections realistic?
- How dependent is the facility on a specific AI technology platform?



A state-of-the-art facility today could require significant reinvestment within just a few years if technology standards change substantially.

Customer Concentration and Revenue Stability Considerations

Large AI projects often involve relationships with major technology companies or hyperscale cloud providers. While these customers can generate significant revenue, they also can create concentration risks for lenders as they expose operators to revenue disruptions if contracts are not renewed or if customers reduce spending.

Underwriters should assess:

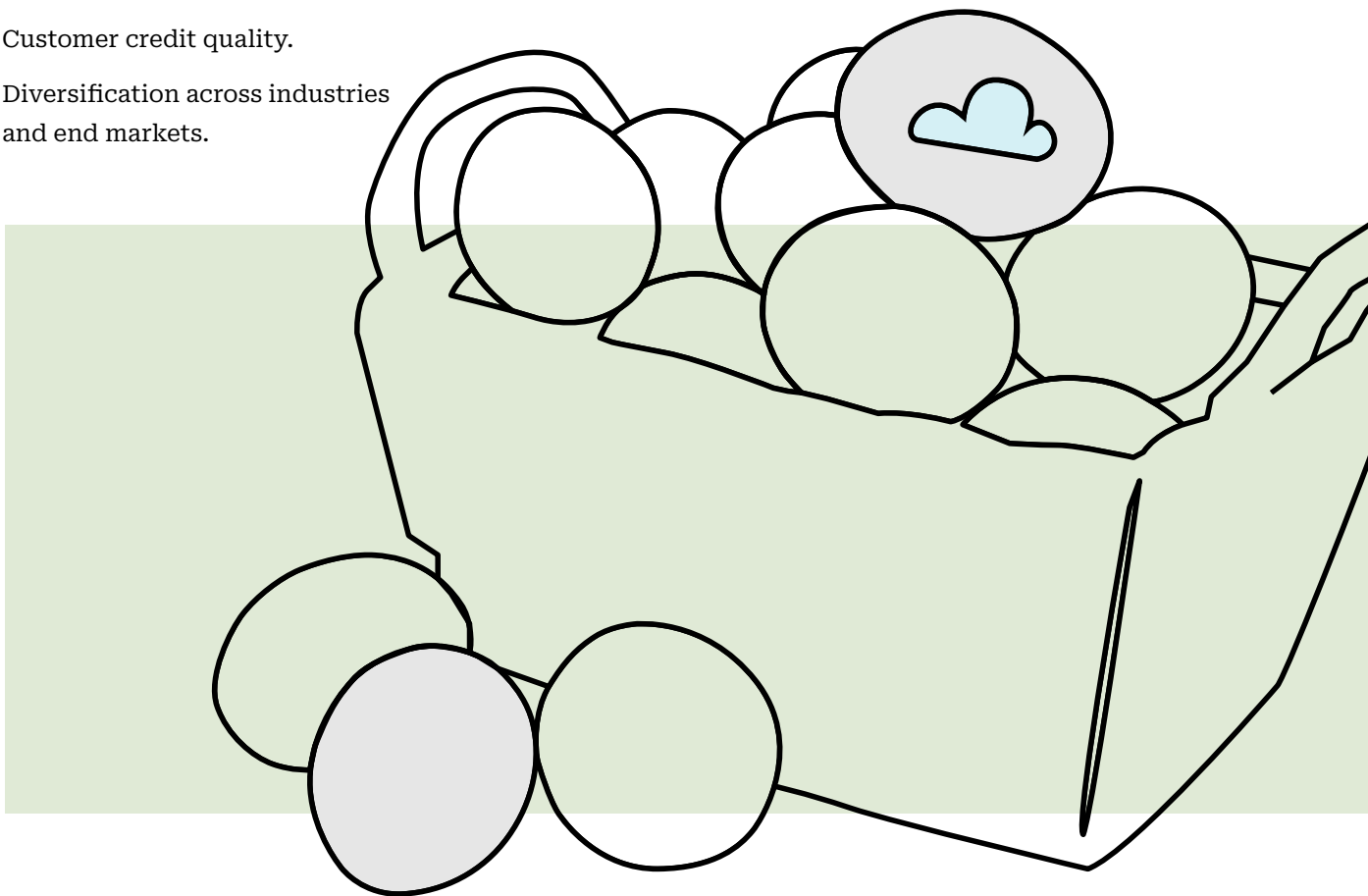
- Revenue concentration among top customers.
- Contract duration and renewal terms.
- Customer credit quality.
- Diversification across industries and end markets.

The strongest borrowers typically demonstrate both customer diversification and long-term contractual visibility.

The Challenge of Vying for Top Talent

Infrastructure alone does not create successful AI operations. Skilled personnel remain critical as the industry faces intense competition for software developers, systems analysts, engineers, and cybersecurity professionals. Competition for qualified employees can increase labor costs and create operational challenges.

As AI adoption expands, the competition for such specialized talent will only intensify. Lenders should consider management's ability to recruit and retain technical staff, particularly for highly specialized AI infrastructure projects.



Lending to AI: The Path Ahead

The growth of artificial intelligence is creating one of the largest infrastructure buildouts in recent memory, creating attractive growth opportunities for lenders. However, AI data center projects come with unique underwriting risks that deserve special scrutiny. Questions include:

- Does the project have long-term access to reliable and affordable power and water?
- How dependent is revenue on a small number of customers?
- What is the sponsor's experience with operating data center infrastructure?
- How frequently will equipment require replacement or upgrades?
- Are projected utilization rates realistic?

- What cybersecurity and data protection measures are in place?
- How exposed is the project to regulatory, environmental, or community opposition?

The answers to these questions may ultimately matter as much as traditional risk measures such as collateral value and debt service coverage. Lenders that pair niche industry knowledge with disciplined underwriting processes will be best positioned to capitalize on this rapidly expanding market.>

Amy Short is the director of research at Vertical IQ, a company that provides industry intelligence for understanding a borrower's risks and opportunities. Vertical IQ equips users with the confidence and credibility to make memorable first impressions and sustain enduring relationships. It also contributes industry reports to eMentor, ProSight's research tool for credit and lending professionals. To learn more about Vertical IQ, you can visit verticaliq.com or email Vertical IQ at info@verticaliq.com.



ProSight eMentor

Smarter credit decisions start with smarter insights. Access peer comparisons, forecasts, trends, and economic metrics from over 20 years of data collection and more than 1000 industry profiles.

20+
Years
of Data

1000+
Industry
Profiles

Learn more at ProSightFA.org

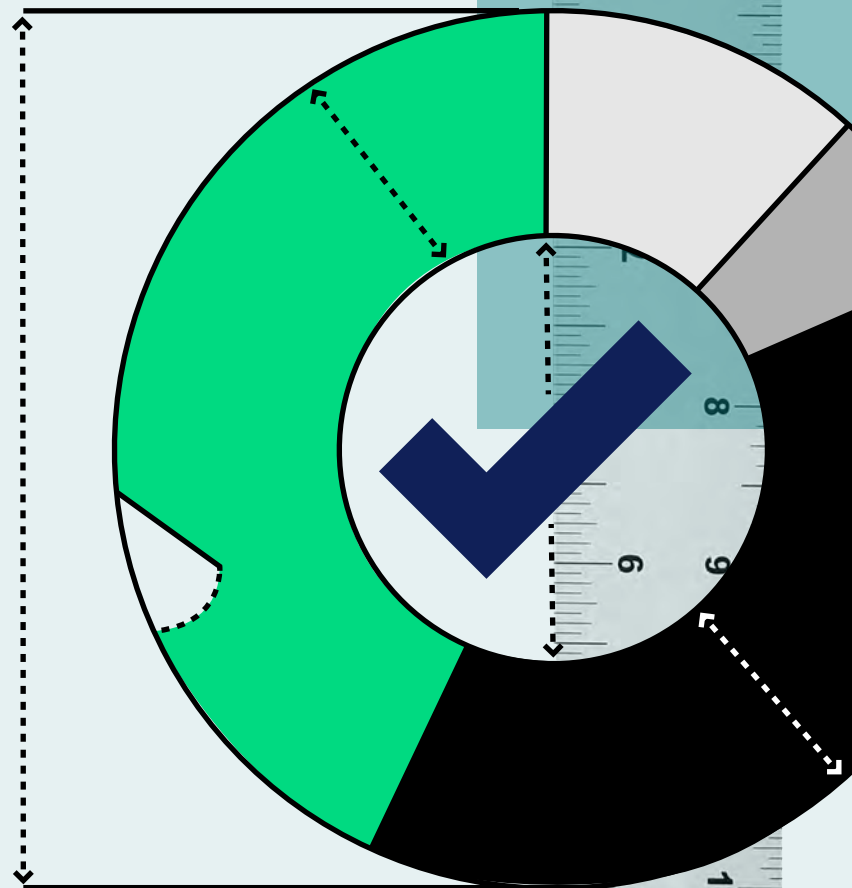


The Issues Management Blueprint

A veteran banker outlines proactive issues management, leadership accountability, prioritization, training, and remediation.

TODAY, AS FINANCIAL institutions contend with everything from geopolitical hazards and AI-driven transformation to regulatory volatility and evolving models for credit risk, it is critical to have a comprehensive and timely plan for resolving issues.

This is where issues management—the process of identifying, tracking, managing, and resolving issues related to operational, compliance, credit, and regulatory risk—comes into play. Indeed, effective enterprise risk management is not feasible without a consistent and sustainable approach to issues management.



Financial institutions with a robust framework can not only navigate increasing operational complexity but also satisfy the transparency and accountability demands of both regulators and internal assurance providers—including auditors. Tol Broome, a principal at JTBroome Advisors and a former chairman of the Risk Management Association, says that rather than treating issues remediation as episodic, firms should address this as a perpetual task. “Some banks make the mistake of focusing on issues only when they are raised by regulators or by assurance providers, such as internal audit and second-line risk partners,” he says. “This can be avoided by developing an issues management framework that has a leader, a formal process for governance and oversight, and an accountability matrix that requires issue owners to resolve their assigned issues by the agreed-upon deadline.”

Broome, who led issues management programs for lending departments across his 41 years in banking, recently shared his perspectives with ProSight on issues management best practices, the need for buy-in from the top, the importance of self-identification and prioritization, and the benefits of implementing a proper framework.

ProSight Financial Association: Can you discuss the role the CEO and other executive leaders play in issues management?

Broome: This is absolutely critical. It [starts] with the CEO and other executive leaders, who should provide the resources to stand up an issues management program and support the efforts of those involved in addressing the issues.

There were three separate times in my career when the line of business or department I was leading had an ongoing, significant number of issues. In every case, our CEO and the executive leader to whom I reported made it clear—both to my issues management teammates and owners and others involved in the process—that the issues management program must be a high priority in our overall risk management framework.

Banks are faced with many competing priorities (e.g., growing revenue, achieving high client service scores, managing expenses,

and minimizing credit/operational losses), and issues management will get lost in the shuffle if executive leadership does not consistently communicate its importance for the enterprise.

ProSight Financial Association: You’re a proponent of the so-called “four-blocker” plan for tracking, managing, and resolving issues. What does this approach entail?

Broome: Also known as a “quad chart,” the four-blocker is a concise tool to identify, track, and resolve issues in a thorough, timely manner. It consists of four sections: (1) summary of scope and stakeholders; (2) key milestones and achievements; (3) risks/dependencies/opportunities; and (4) action steps/upcoming deadlines.

The four-blocker approach, which is also often used in project management, allows you to take a big issue and divide it up into several individual tasks—with deadlines that, if met,

will cumulatively result in the successful resolution of the issue. As progress is tracked, the issue should be labeled green, yellow, or red based on the likelihood of clearing the issue within the specified deadline.

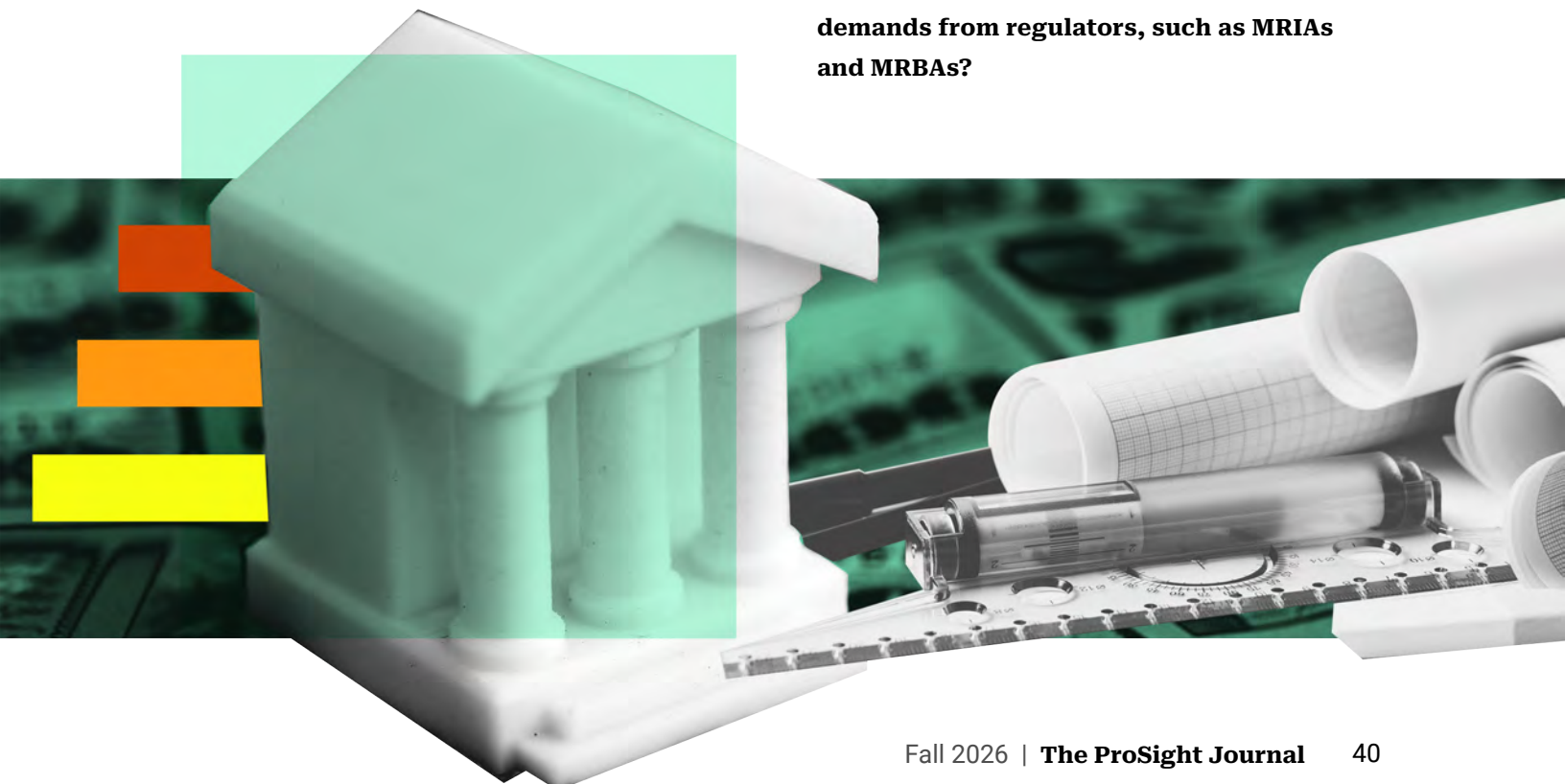
ProSight Financial Association: What system do you recommend for prioritizing issues? Is there a taxonomy that a bank can implement to flag them, so that risks are properly categorized and the most dangerous issues get addressed first?

Broome: Regulators will, of course, prioritize their issues for you, ranging from observations to supervisory recommendations (SRs) to matters requiring immediate attention (MRIAs) to matters requiring board attention (MRBAs). The regulators will require you to develop a remediation plan for the last three, but I also recommend creating an issues plan for observations to avoid having them become SRs or worse during the next visit by the examiners.

The internal taxonomy also should include severity levels. I recommend a three-tiered approach, with level one being significant, level two being moderate, and level three being low. Internal assurance providers, like audit or the compliance department, are tasked with assigning a severity level to each issue. But with matters that are self-identified (MSIs), you will need to assign your own severity rating.

For example, an outdated risk grading model that no longer meets validation standards and is causing inaccurate credit risk assessment is more serious than users making wrong inputs into the model. The outdated model should be rated severity level one and will likely require a major update, or even a model replacement. The input errors, on the other hand, should be rated severity level three, and can be successfully resolved with training and updates to the user guide.

ProSight Financial Association: Does setting severity levels (e.g., high, medium, or low risk) for internal issues help firms remediate issues faster and properly respond to demands from regulators, such as MRIAs and MRBAs?



“As with anything we do in banking, there are three key components to issues management: people, process, and systems.”

—Tol Broome

Broome: It may help with timeliness of remediation, but the more severe issues frequently require more significant internal systems and/or process changes, and can therefore take longer to resolve.

What the severity level does is ensure adequate resources are assigned to the most serious issues and raise the level of awareness for dependency partners that they need to prioritize your issue. The four-blocker will help identify resources needed throughout the bank.

One other point here: it is really important to set realistic deadlines, both for the broad issue and for the iterative tasks that must be done to achieve remediation. I have seen cases in which the deadlines set are unreasonable given the complexity of the resolution plan, causing an unacceptably high level of past-due issues.

ProSight Financial Association: Why is it important for frontline workers (first line of defense) to self-identify and own issues?

Broome: This is important for the second and third lines of defense as well. It is far better for you to identify your own deficiencies proactively, and to set up remediation plans to fix them, than to wait for the regulators or an assurance provider to find them later. Many banks set goals for the percentage of issues that should be MSIs, and that number can be 50% or higher.

It is important to cultivate a culture that encourages MSIs. Teammates should be lauded for identifying and fixing their own issues, but I have seen cases in which there is fear of the stick rather than the reward of the carrot, which causes issues to be ignored.

ProSight Financial Association: How would you describe the roles of risk managers (second line of defense) and auditors (third line) in issues management?

Broome: The primary role of second- and third-line teams in issues management is to provide effective challenge and to identify issues. While many of the issues will be tasked for remediation to the first line, second-line risk partners and other departments—such as loan and deposit operations, IT, HR, and audit—should also have issues management programs.

I'd like to emphasize the importance of balance and reasonableness here. There should be healthy, effective challenge, but assurance providers should focus on issues that create real risk.

During my career, I experienced both sides of this firsthand. I remember one internal audit years ago in which my department received 17 findings, with nearly half of them being tagged severity level one. I thought several of the findings were entirely unwarranted, while others were assigned an overly aggressive severity level. We appealed the audit report with a well-developed response and had the number of findings reduced to about 12, with several changed to a lower severity level.

In other cases, the issues identified by audit, compliance, or credit risk review were deemed to be warranted, and I could not really argue with the number of findings or the severity levels assigned.

ProSight Financial Association: Is employee training for issues management critical, and, if so, are there any best practices you can recommend?

Broome: As with anything we do in banking, there are three key components to issues management: people, process, and systems.

A bank can have an effective and efficient process for, say, loan approval, with strong automation provided by systems. But if the people using the process and the systems are not well trained, then there is bound to be a breakdown in getting loans approved in a timely and effective manner within the bank's credit appetite.

Nearly every remediation plan should include a training component for the changes that will be made to resolve the issue. This can range from a one-hour, self-guided tutorial to a full-day or even multiday training module, if the changes are significant.

Regarding best practices, I will make two points. First, make sure the level of training matches the significance of the changes. Second, the bank should track the training to ensure that 100% of the employees impacted by the change complete the training by the deadline. No exceptions.

ProSight Financial Association: How can you measure ROI on issues management? What types of benefits can an effective issues management framework provide?

Broome: That's a good question. ROI is not always easy to pinpoint in issues management. However, the consequences of not having a robust issues management program are pretty evident.

With a thorough and reasonable approach to issues management, the bank will experience enhanced risk management, which will lead to decreased legal losses and lower credit and operational risks over the long run. Moreover, the bank's relationship with regulators will definitely be enhanced.

A strong issues management program will even improve client service and make the bank more efficient. Well-trained employees who use well-developed processes, supported by strong systems, will allow the bank to better meet the needs of its clients and reduce expenses. So, to answer your question, I suppose that ROI centers on loss avoidance, improved client acquisition and retention, and decreased expenses.>

http://www.



Building a Multigenerational Fraud Strategy

By Cara Wick

Gen Z, it turns out, is the fraudster's new mark.

While the industry grapples with the role of artificial intelligence (AI) in fraud, a fundamental question is whether we understand who fraudsters are actually targeting. Data from the Federal Trade Commission (FTC) indicates we may not.

The FTC's Consumer Sentinel Network shows that 20-to-29-year-olds are more likely than older age groups to report losing money to fraud, [but the industry's focus has been on protecting older fraud victims](#). In 2022, Congress passed the Stop Senior Scams Act, legislation that established a public-private working group to strengthen legal protections for elderly fraud victims. But the act barely mentions younger ones.

Fraudsters are exploiting technology-related behavioral gaps between the generations.

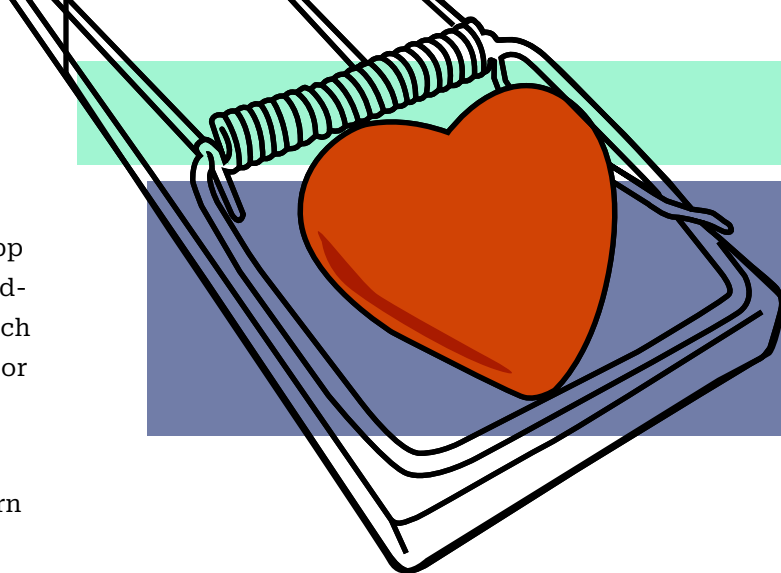
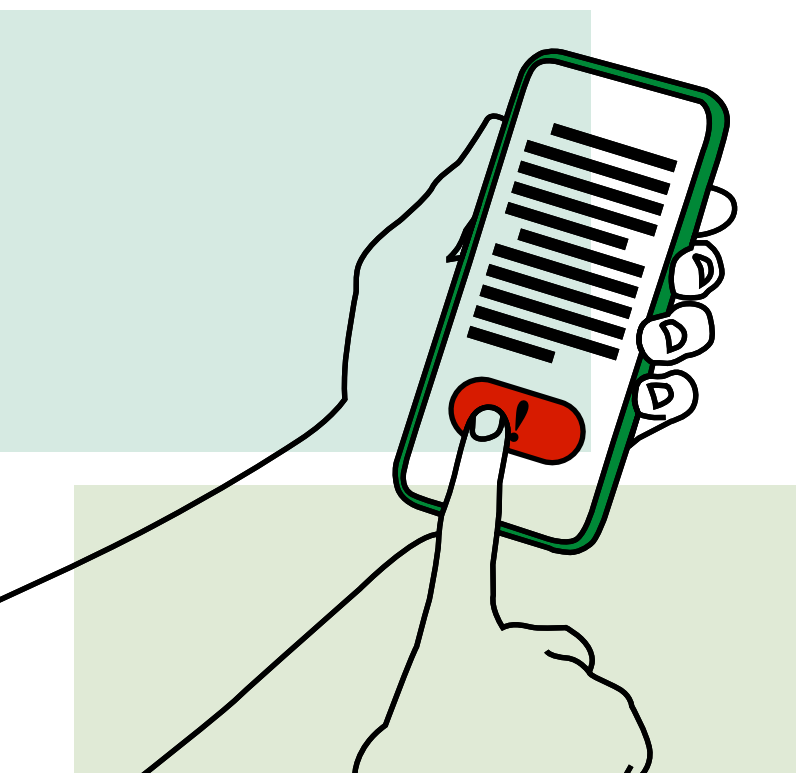
Digital natives, who have never unraveled a phone cord, are so accustomed to clicking links and downloading apps that they miss the red flags of fraud through channels like landlines. Digital immigrants, who grew up before digital technologies were widespread, know how to read a paper map but are less familiar with digital communications and less likely to recognize when to ignore a sincere-sounding direct message.

Once caught in an online scam, a single click can turn a transaction into fraud. Fraudsters can post fake ads for in-demand concert tickets, cars, or electronics on Facebook Marketplace. In an instant, unsuspecting shoppers might send an "upfront payment" via Zelle or Venmo and watch the "seller," along with their money, disappear.

In 2025, Facebook hosted more online fraudsters than any other platform (WhatsApp and Instagram were distant second- and third-place finishers, respectively). People lost much more money to Facebook scams than to text or email scams.

One reason that fraud is rising among young people could be their exposure to it. Folks born after 1996 (Gen Z) spend 7.2 hours per day on their phone watching videos, compared with two to three hours of screen time for other adults, according to [a report by SlickText](#) (as of May 2026).

You'd think that all that digital fluency would make them scam-proof, which leads to the assumption that older people are the main fraud targets. Instead, younger generations' familiarity with online transactions breeds complacency. In a [recent NordVPN survey](#), 28% of 28-to-43-year-olds said they'd clicked on a malicious link more than once—the highest percentage of any age group.



Baby Boomers, meanwhile, fall for online scams of a different color—and lose significantly more money when they do. While younger people report fraud more often, FTC data shows that victims aged 70+ suffer far greater losses per incident, likely because many of them have larger savings and retirement accounts to draw from.

Fraudsters can pull the purse strings by tugging on older folks' heartstrings. Those born between 1946 and 1964 are more vulnerable to scams that manipulate personal connections, NordVPN's study found. In 2023, a 77-year-old New York woman was [swindled out of more than \\$177,000](#) in a romance scam in which the fraudster contacted her via Facebook. In December 2024, checks totaling \$158,000 that she attempted to send were stopped by her bank, preventing her from losing even more.

Effective detection rules, like those that stopped this scam, are based on customer behavior and transaction context, not just demographics. A longtime customer who suddenly starts sending large wire transfers or checks to foreign countries could be involved in a romance scam. A new customer who deposits a check and then immediately makes outbound ACH, Zelle, or wire transfers to an unknown business could be ensnared in employment fraud.

Rules that use account age to compare customer behavior to normal activity are part of standard risk management.

More than just stopping transactions, banks that use a layered approach—behavioral flags, in-app step-up verification for unusual transfers, and real-time alerts—leverage multiple intervention points before, during, and after a transaction to stop fraud before funds are gone.

Messaging also matters. Research on scam-prevention messaging from the Scams Against Older Adults Advisory Group, created by the Stop Senior Scams Act, suggests that one-size-fits-all fraud-prevention campaigns don't work. [Older adults are more likely to retain positive, connection-oriented anti-fraud messages](#). Rather than saying, "Don't fall for fake tech support calls," deploy a positively framed message like, "You don't have to handle tech problems alone. Calling your bank directly using the number on your card means you always have someone trustworthy in your corner." Younger adults, on the other hand, are more urgency-tolerant, especially when the urgency is gamified. "See how fast you can spot the scam" campaigns, for example, create engagement and awareness.

Traditional communication channels, such as in-branch and by mail, still work. Digital immigrants are likely to listen to a banker who tells them the signs of a romance scam. And a

In-the-moment warnings can be effective for all ages, especially if they are action-oriented.

fraud information mailer that would be ignored by Gen Z is not obsolete for older Americans, who [open physical mail at higher rates than younger ones](#).

In-the-moment warnings can be effective for all ages, especially if they are action-oriented. [Studies suggest](#) that for people to take a newly prescribed action, the message must be both memorable and actionable at the time of the required behavior. A pop-up message on a phone during a deposit could prompt necessary reflection: "Is this a job reimbursement check? Learn why [these are often fake](#)."

Threats of urgency and scarcity ("Act now or you will lose") send all of us into fight-or-flight mode, whether we are online or offline, young or old. "The real moment of attack is when someone feels rushed, scared, or pressured into trusting too quickly," [says NordVPN Chief Technology Officer Marijus Briedis](#). That's why a comprehensive fraud strategy is so important. Targeted counter-messaging—this urgency could be a scam—bolsters our judgment before it fails.

Our biggest vulnerability isn't a cleverer algorithm or a more convincing deepfake. It's the belief that scams don't happen to us. This "optimism bias" distorts perceptions of personal risk, according to the aforementioned research on scam messaging. The industry has its own version of this blind spot—assuming fraud is mostly an older adult's problem. Bias brings down our guard and lets scammers into our minds and our accounts. Fraudsters don't discriminate based on age. The industry shouldn't either. >

Cara Wick, as global financial crimes executive at Bank of America, leads the team that monitors the bank's automated detection program. A frequent speaker at industry conferences, her articles have appeared in The ProSight Journal and other publications. Cara is a member of ProSight's Editorial Advisory Council and can be reached at cara.wick@bofa.com.



Fraud moves at machine speed. AI redefines fraud threats and prevention.

Get ahead of AI-accelerated fraud and modernize your fraud prevention strategies with the ProSight Fraud Alert Network community.

AI is compressing the time between attack and impact. Twenty-seven seconds is one of the fastest eCrime breakout times on record in 2026.*

Connecting experts. Sharing knowledge. Mitigating fraud.

Join the ProSight Fraud Alert Network

Complimentary for ProSight members for one year

*2026 CrowdStrike Global Threat Report: AI Accelerated Adversaries

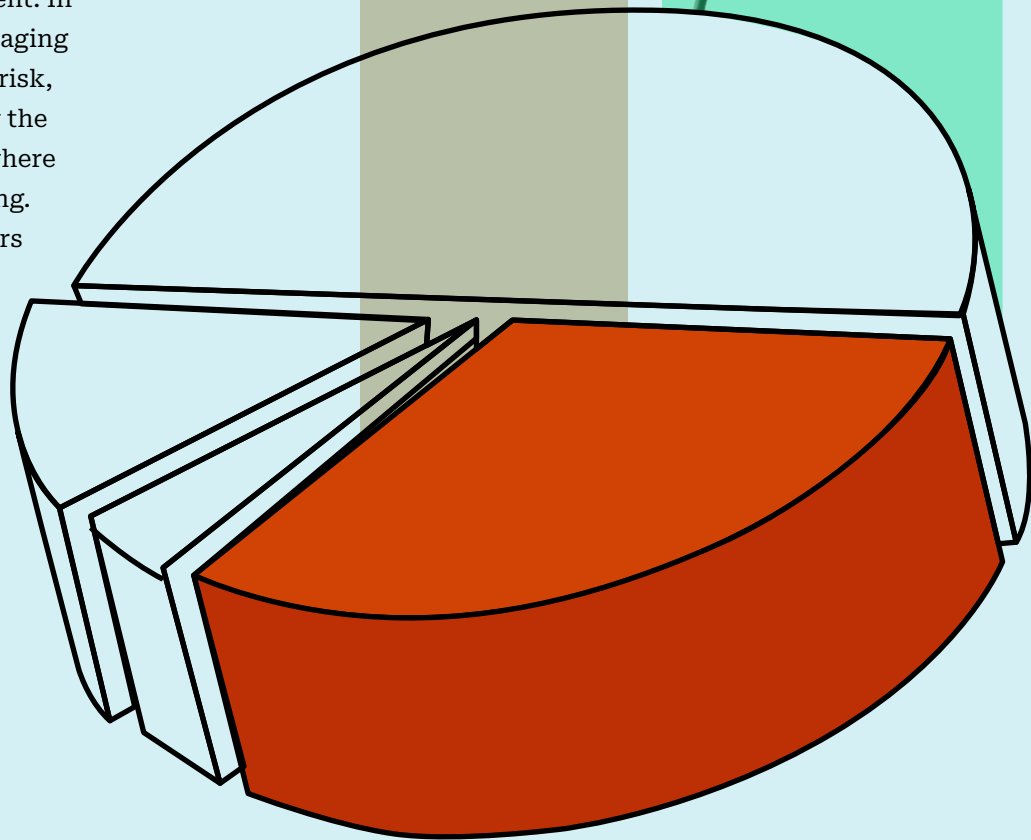


Primer:

A Look at Credit Risk Insurance

A mainstay in trade financing, the product is commonplace in Europe but has yet to catch on broadly in the U.S.

CREDIT INSURANCE PROTECTS lenders and businesses against losses from borrower or customer nonpayment. In this Q&A, Kevin Humphrey, managing director, trade credit & political risk, at Brown & Brown, explains how the product works in practice and where it fits within modern bank lending. He discusses why adoption differs between the U.S. and Europe, and how credit analysis done by insurers can complement the work of banks. The conversation also explores the role of credit insurance in supporting lending growth while managing risk.



ProSight: Define “credit insurance.” Does it mainly relate to trade credit?

Humphrey: Trade credit is a major piece, but not the whole picture. In banking, credit insurance can also cover borrower risk or offtaker risk outside traditional trade contexts. In practice, people use “trade credit insurance” and “credit insurance” interchangeably, even though applications are broader.

ProSight: Who typically buys the insurance—the bank or the borrower?

Humphrey: Both structures are common. Sometimes the borrower buys the policy and names the bank as loss payee. In other cases—especially structured or portfolio-level deals—the bank itself is the insured. The structure depends on the transaction and the bank’s goals.

“In asset-based lending, banks often exclude certain receivables due to concentration or cross-border risk.”

ProSight: How does this work in a typical U.S. lending scenario?

Humphrey: In asset-based lending, banks often exclude certain receivables due to concentration or cross-border risk. When those receivables are insured, banks may allow them back into the borrowing base, improving liquidity while maintaining a secondary source of repayment.

ProSight: Why are foreign receivables usually excluded without insurance?

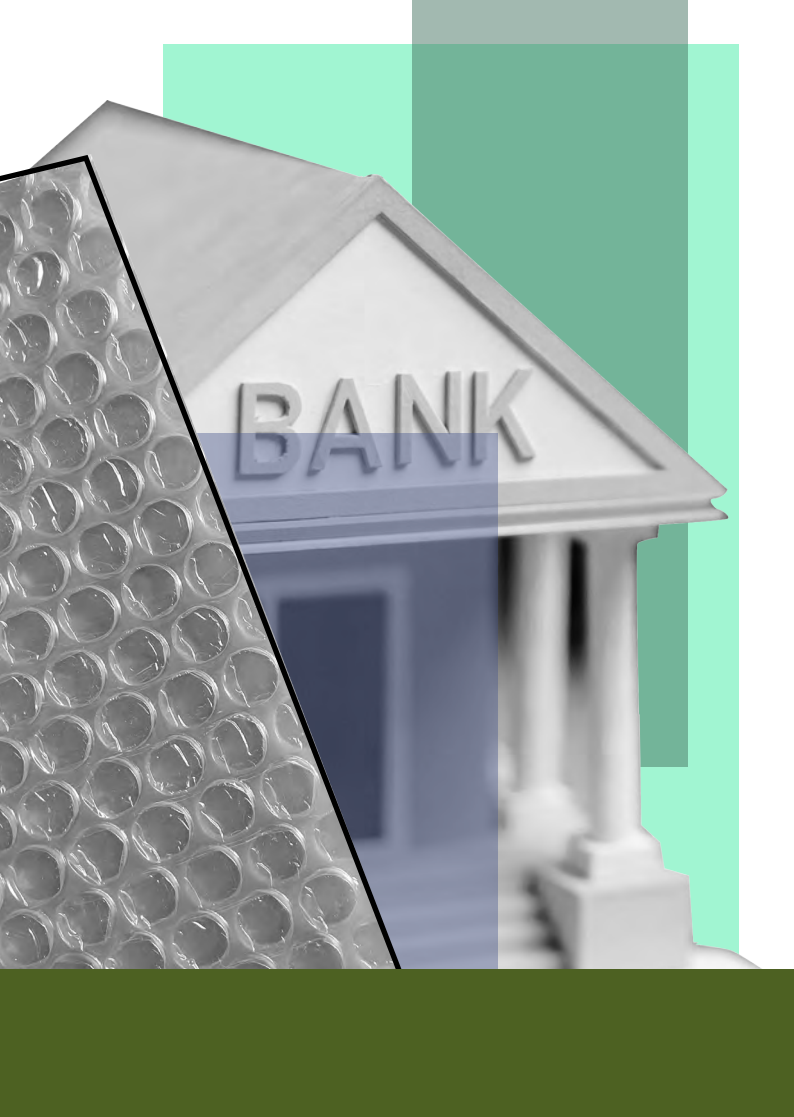
Humphrey: Banks generally can’t perfect or enforce security interests across borders. Even with local counsel, recoveries tend to be minimal in a foreign bankruptcy. Insurance provides protection where legal remedies are weak.

ProSight: Does credit insurance encourage banks to take more risk?

Humphrey: No. Banks still apply the same underwriting standards. Insurance simply adds another layer of protection, allowing banks to support lending growth while staying within their risk appetite.

ProSight: How do insurers underwrite these risks?

Humphrey: Large insurers use robust internal credit-scoring models and portfolio criteria. Banks can rely on insurers’ credit analysts as a complement to their own teams, in some cases effectively outsourcing counterparty risk assessments.



ProSight: Who gets paid if there's a loss?

Humphrey: It depends on who is insured. If the borrower is insured, they file the claim and the bank receives proceeds as loss payee. If the bank is insured, the bank controls the claim. In that case, the borrower's benefit is increased liquidity rather than insurance proceeds.

ProSight: How do you position credit insurance in the U.S. banking market right now?

Humphrey: Credit insurance remains significantly underutilized in U.S. banking. While it's widely used in Europe, most U.S. banks are unfamiliar with it as a credit-risk management tool. There's little institutional muscle memory, which creates an education gap.

ProSight: Why has the product taken hold in Europe but not in the U.S.?

Humphrey: Europe has over a century of experience integrating insurance into banking and trade finance. Banks and insurers often coexist under common holding companies, and cross-border trade exposure is routine. In contrast, U.S. banks historically relied on letters of credit, collateral, and guarantees and were shaped by Glass-Steagall. Those differences produced very different risk cultures and operating habits.

ProSight: Is capital relief the main modern use case in Europe?

Humphrey: Since around 2015, yes. As Basel III took hold and insurance gained recognition in certain structures, European banks increasingly used credit insurance to manage capital while maintaining client relationships.

ProSight: Economically, does it only make sense if banks get capital relief?

Humphrey: No. Banks may use credit insurance purely as a risk mitigant. It can support higher lending limits, improve portfolio stability, and enable more lending to existing clients. Capital relief is a benefit, but not the only rationale.



ProSight: How much of the difference in adoption in the U.S. is about regulatory capital treatment?

Humphrey: Capital treatment matters, especially after the financial crisis and Basel III, but it isn't the full explanation. Credit insurance was widely used in Europe long before regulators allowed it to substitute for capital. Regulatory recognition accelerated adoption, but it built on an already established practice.

ProSight: Is regulatory uncertainty the biggest barrier to adoption in the U.S.?

Humphrey: It's a barrier, but not the biggest one. Even without capital relief, there are solid risk-management reasons to use credit insurance. The larger issue is unfamiliarity—banks don't see peers using it, so they're reluctant to be first movers.

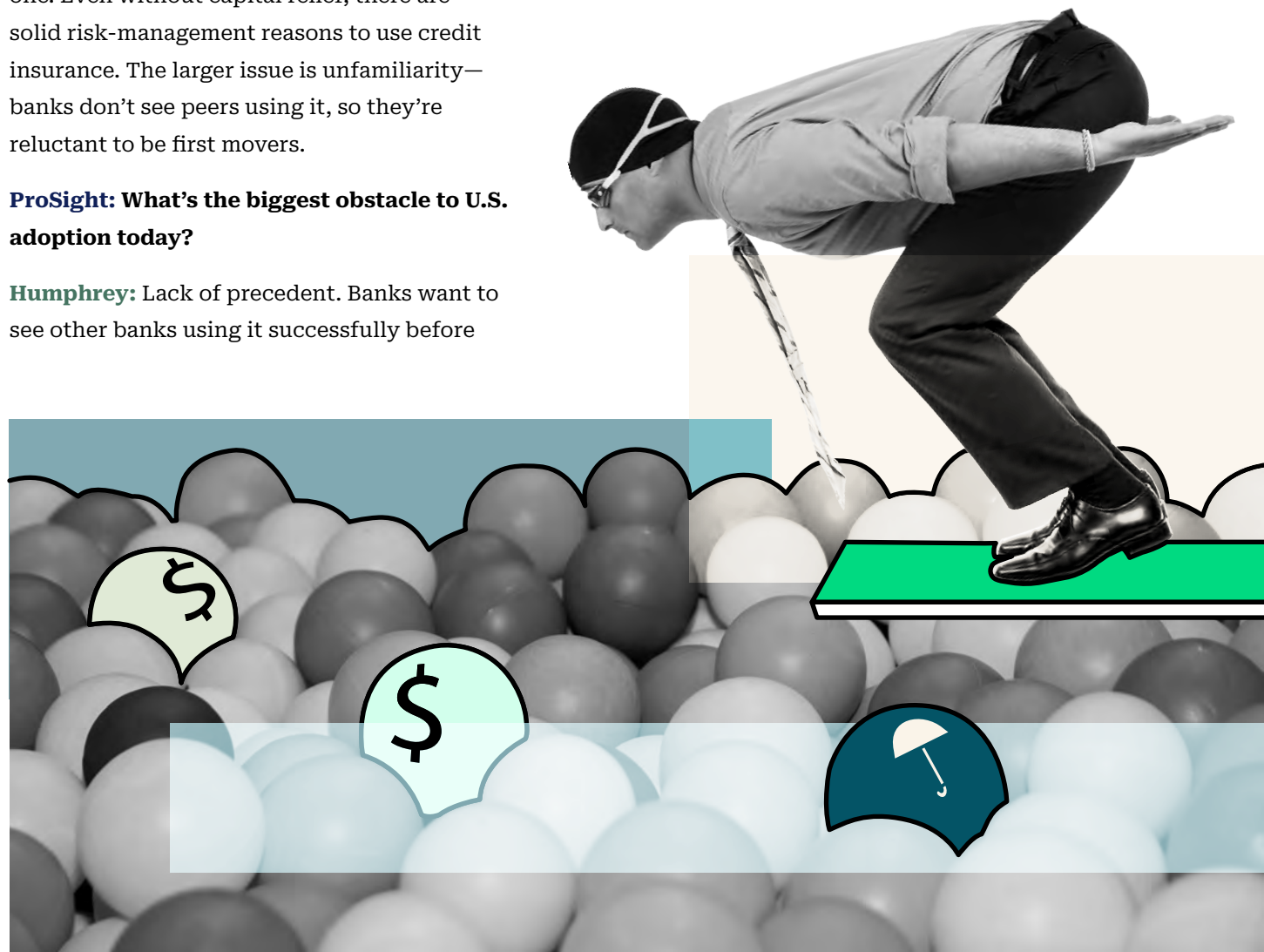
ProSight: What's the biggest obstacle to U.S. adoption today?

Humphrey: Lack of precedent. Banks want to see other banks using it successfully before

adopting it themselves. Even though it isn't prohibited, there's a learning curve and most institutions don't yet have internal experience with the product.

ProSight: Are efforts underway to change regulatory recognition in the U.S.?

Humphrey: Yes. There have been lobbying efforts and policy discussions for several years aimed at educating regulators and improving recognition, but progress has been gradual.>





Newsletters

Stay Current. Bring Better Insight to Your Work.

Banking keeps changing. ProSight newsletters help you follow important developments, understand what they mean, and find ideas you can apply in your role.

ProSight Banking Strategies Daily

Timely weekday coverage to help you stay on top of the issues affecting your institution and your work.

ProSight Insider

Relevant news, research, data, and expert insight selected for practical value across the banking industry.

ProSight Banking Strategies Weekend

A broader Saturday perspective on the trends, challenges, and opportunities shaping banking's next moves.

Subscribe:

info.ProSightFA.org/subscribe

