ProSight

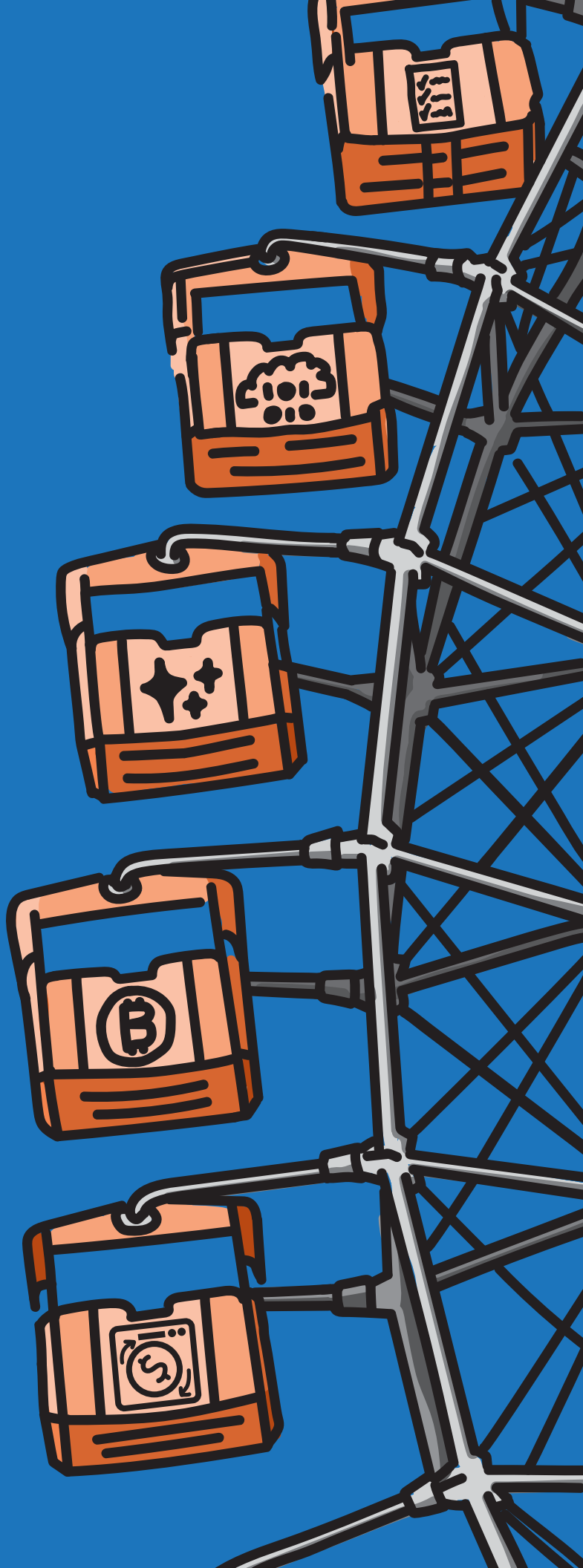
The ProSight Journal®

Summer 2026 | ProSightFA.org

The 2026 ProSight Compliance Outlook Survey: Relaxed Regulation, Steady Vigilance

Plus:

- Redrawing the ERM Map for an Evolving Risk and Competitive Landscape
- Effective Strategies for Managing an Appraiser Shortage



ProSight

PROSIGHT ANNUAL CONFERENCE
NOVEMBER 2-5 | VIRTUAL

Growing Forward: Turning Disruption into Opportunity

At the **ProSight Annual Conference**, experts will explore how institutions are adapting risk management in a rapidly evolving environment.

Advance your professional journey with CPE, CEU, and CERP, CRCM, and CAFP credits.

REGISTER AT PROSIGHTFA.ORG

Members have access to early bird discounts now through September 4.

Summer 2026
volume 1 / number two

Departments

Features

Features (continued)

Index to Advertisers

The ProSight Journal®

Executive Editor: Celina Rogers
Editor-in-Chief: Frank Devlin
Senior Editor: Dan Washburn
Senior Editor: Michael Bender
Art Director: Christopher Santoro

Article submission 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 rmahq.org/TheRMAJournal. No parts of this publication may be reproduced by any technique or process whatsoever without permission.

Advertising: ptaylor@ProSightFA.org

ProSight Proudly Introduces **New Member Institutions**

Palmetto State Bank | Hampton, SC

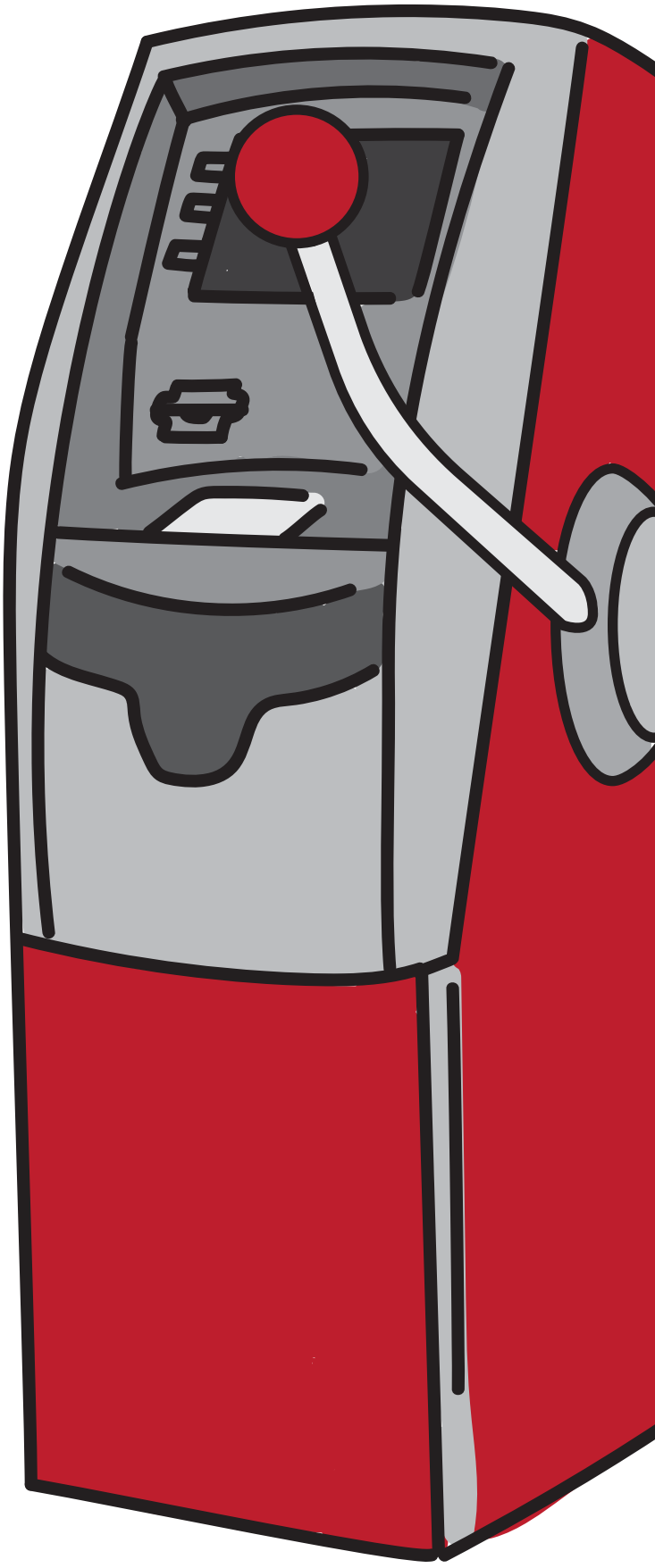
Potomac Bank Inc. | Charles Town, WV

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.

Banks Layering Protections Against Jackpotting Surge



By: Michael Bender

ATM jackpotting crime is surging. The Federal Bureau of Investigations warned banks in a February advisory that of the 1,900 such attacks tracked since 2020, 700 totaling more than $20 million in losses occurred last year.

Data from the ATM Industry Association through November 2025 show that 72% of all reported crime related to ATMs last year was jackpotting/cash-out attacks, with physical attacks on ATMs now representing less than 10% of all attacks. In one recent, high-profile jackpotting case, a federal grand jury returned an indictment charging 93 defendants in an alleged nationwide conspiracy to commit bank and computer fraud and burglary.

While ATM jackpotting is legally considered fraud, banks often distinguish it from other types of fraud that involve exploiting a customer's personal data or stealing their funds,

explained the head of cash & ATM operations at one regional bank. Jackpotting, instead, involves a direct attack on the machines collecting and dispensing money in customer transactions, without using customer data.

Threat actors gain access to an ATM's internal hard drive using generic physical keys. Then, as the FBI explained, they introduce malware, including the Ploutus family of malware, to attack the software layer instructing the ATM what to physically do. If the would-be criminal can issue their own commands to the eXtensions for Financial Services (XFS) layer, they can order the ATM to dispense cash, without using a valid card, customer account, or bank authorization message.

With this rise in software-related criminal tactics, banks have shifted energy in recent years to technical security and safeguarding the machines themselves, while maintaining physical security of ATMs, or protecting the space and customers around the machines.

"The tricky part about it is not setting up the monitoring. It's finding the needle in the haystack that's the bad guy hacking the system," the ATM operations head said. "That's why the industry promotes a layered defense."

Those layers still include physical deterrents such as cameras, alarms, and locks, but banks are stepping up cyber vigilance and basic tech hygiene to improve security. That means updating ATM software regularly and incorporating the latest cybersecurity features from machine makers as they become available. "Don't be the slowest gazelle," he said.

In its advisory, the FBI recommends focusing on removable storage usage, controlled file access, and delivery of high-fidelity jackpotting detection—with minimal system overhead—as part of a focused audit policy. It also outlines more than two dozen steps banks can take to harden their ATM protections. Whitelisting devices and networks, configuring automatic shutdown conditions on the machine, and collaborating with industry groups are among them.

That collaboration, the ATM operations head said, has heightened awareness among banks and law enforcement, including at the federal level. Whether the Justice Department prosecutes ATM jackpotting as a federal crime depends, in part, on the circumstances of the crime and the actors, including whether the theft happens on bank property or international criminal organizations are involved.

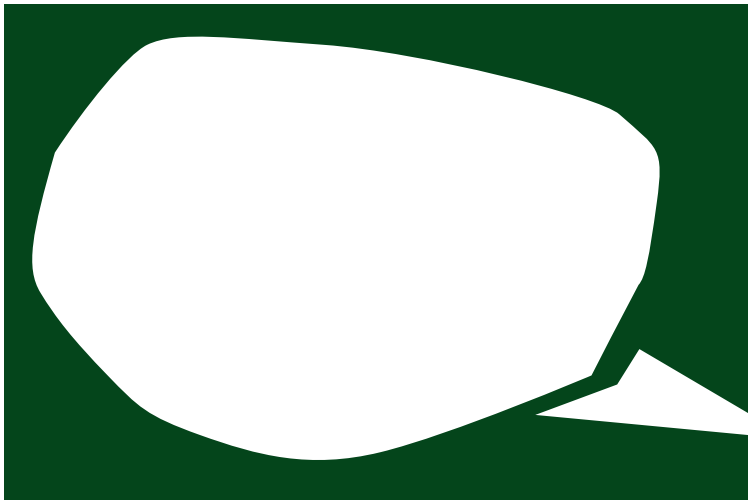
The recent high-profile indictment named members of a gang designated a Foreign Terrorist Organization among those conducting jackpotting attacks across the U.S. Crimes committed against non-bank ATMs and ATMs off bank premises are handled by local law enforcement.

To redress these enforcement inconsistencies and ensure the safety of independent ATMs, a bipartisan group in Congress re-introduced a bill last year that leveled enforcement standards for all ATMs. The Safe Access to Cash Act would afford non-bank ATMs the same federal protections as bank-owned machines.

Co-sponsor John Rose said, "independent ATMs serve as a lifeline to the underbanked and those lacking access to traditional financial services," calling the bill common sense for providing independent ATMs "the same federal legal protections under the Bank Robbery Act as other ATMs."

Community Bank Voices:

AI and the Human Value Proposition



By Michael Bender

Community banks are built on personal connections. While technology is core to service, the human touch remains a top draw at smaller institutions for customers and staff alike.

Preserving this people-centric sensibility is vital, say community bank leaders, as artificial intelligence begins infusing operations and performing tasks people once did. Though usually following their big-bank counterparts in AI uptake and implementation, community banks increasingly are embracing a future with AI and are laying the emotional and practical foundations for its use.

“We are starting with a philosophy about how we’re implementing AI so that our employees and teammates can get comfortable that the goals for AI projects are not job elimination,” said Dawn Mugford, chief risk officer at Norway Savings Bank.

It’s no wonder, these leaders say, that their workforce is worried about a technology often described as deeply human. Generative AI, after all, can replicate human communication with speed, accuracy, and scale. Agentic AI is learning to do what people do, increasingly without prompting. The temptation is to use this powerful capability broadly in the interest of cost savings, and overhaul banks top to bottom.

> "When you're a smaller institution, there's a lot you do manually, but as you start to grow you have to consider more automation. Where it makes sense, you'd much rather have people doing analysis [and other high-value functions]."

But that's not the plan at his bank, says David Stewart, chief credit officer at Kleberg Bank. "One perspective is to create a culture where you're using it to reduce headcount. Another, and this is where we're planning to take it, is to increase the efficiency of existing staff," he said.

A Culture of Usage

"Efficiency" can mean different things to different people. For some, it's synonymous with cost-cutting. For others, it's making it easier and quicker to perform everyday tasks. Given already tight staffing numbers, heightened sensitivity to customer and employee experience, and the strong desire to protect their value proposition, community bank leaders seem to agree that efficiency, in the case of using AI, means empowering instead of replacing people.

Few, meanwhile, see ignoring AI as an option. In ProSight's 2025 Community Bank Survey, for example, 80% of respondents said that using AI effectively would be critical to meeting strategic objectives over the next five years. But they are also playing catch-up. In ProSight's 2026 CRO Outlook Survey, 68% of respondents at banks with less than $50 billion in assets said they'd not developed AI upskilling or training programs for their workforce (vs. 24% for larger banks). Almost half said they'd not built AI technology infrastructure either.

But that's quickly changing, Stewart believes. "There might be some leaders who aren't forward-looking and want to keep doing things the way they always have. But if you're sitting in this [executive] seat, it's hard not to see what's around the corner," he said.

Familiarizing the organization with potential applications of AI, getting executives and employees comfortable with the technology, and painting an energizing picture of how employees can work with AI are all part of the setup work happening at some community banks. "AI is a great tool for generating conversations about how we do things as a bank," Mugford said. "When you're a smaller institution, there's a lot you do manually, but as you start to grow you have to consider more automation. Where it makes sense, you'd much rather have people doing analysis [and other high-value functions]."

In this way, AI has potential as a talent-development tool. "We love it when people stay a long time. AI can create opportunities for folks to train and do different things; to be able to do some projects we maybe haven't had capacity for before," she said.

Companies use "human in the loop" to describe an arrangement in which people oversee AI outputs and apply higher-level judgments to create a final product. The term has also become HR shorthand for "no job losses." Creating a culture where people are users and beneficiaries, and not victims, of AI supports community banks' ambitions to adopt it, Stewart suggested.

Including people is practical and risk-focused, too. Half of CRO Outlook Survey respondents said that using AI without adequate human verification would be a top AI-related risk for their organization.

Vendors and Customers

This vein of concern runs through employee, vendor, and customer approaches. Community banks run on limited technology budgets and depend on vendors for off-the-shelf products and capabilities. In the case of information-intensive AI, marrying internal stores of data with external large language models presents thorny data custody and privacy issues banks must manage.

“We’re really raising our game in vendor due diligence to make sure we’re asking all the right questions about how our data is being shared, stored, and used in model training,” Mugford said. When a vendor’s practices don’t readily align with the bank’s guiding principles on data usage and storage, it’s a sure sign to reconsider that partnership, she added.

The right vendor products are shortcuts for small banks to new AI capabilities. Use in customer service workflows and fraud detection frameworks is already happening at bigger banks, which may have the resources to build their own tools. Community banks depend more heavily on vendors and are extra-selective about their use cases, the bankers suggested. Still, they see areas such as loan origination and monitoring as fruitful targets for the technology—always with human validation embedded in the process.

When it comes to customers’ awareness of and experience with AI in the banking context, the less apparent it is the better. Consumers want seamless services that deliver to their expectations. If AI performs a customer-facing task poorly, it can destroy a bank’s service reputation almost instantly. If it replaces a valued human interaction, it can undermine the personal-touch value proposition.

“A big part of how we differentiate is knowing your customer and having a personal interaction,” Mugford said. Theoretically, AI could support these personal connections: “If you had, for example, detailed informational prompts at your teller lineup such as birthdays or other data…they could help you create or deepen those relationships with your customers,” she said.

Banks big and small are wrestling with similar issues as they reframe growth, operations, and strategy through an AI lens. For their customers, AI is invisible infrastructure; it’s the outcomes in service that matter. AI adoption at community banks must fit around relationship banking, not redefine it.

“When vendors are properly vetted and managed, the customers don’t care if it’s AI that’s helping to protect them from fraud or delivering a better product. They want to be able to pick up the phone and talk to somebody and have intelligent touchpoints like a great mobile experience. That’s how we differentiate,” Stewart said.>

ProSight

PROSIGHT INTERNAL AUDIT CONFERENCE
NOVEMBER 15-18 | OMNI FORT LAUDERDALE

Internal Audit Rewired: Navigating Technology, Risk, and Change

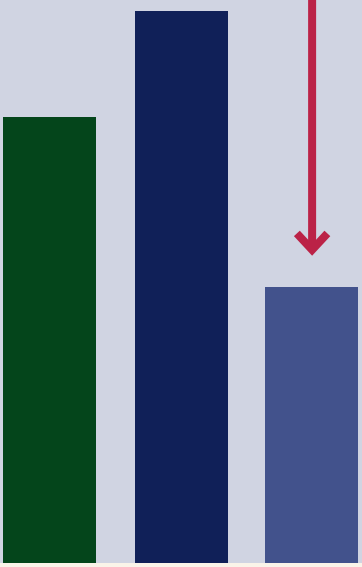
The **ProSight Internal Audit Conference** will focus on the evolving role of internal audit in the changing financial services landscape.

- **Explore** how technology is transforming internal audits
- **Benchmark** emerging practices to enhance audit relevance and agility
- **Network** with hundreds of industry professionals
- **Earn** up to 18 NASBA-approved CPE credits

Early bird discounts through September 18.

Register at
ProSightFA.org

What's Driving the Proposed Changes in MRA Issuance, and What They Mean for Banks



Over a three-decade career at the Office of the Comptroller of the Currency (OCC), Kris McIntire's duties included overseeing community, mid-size, and large banks. He served as the examiner-in-charge at three major financial institutions, had a role on the OCC's National Risk Committee, and was named an international member of the Basel Committee on Bank Supervision's Cross-Border Crisis Management Group.

Currently, as part of his work as a consultant for Ludwig Advisors and Huron—and as a national bank board member for SoFi, where he participates on the audit, risk, and compensation committees—McIntire has taken a keen interest in the proposed changes in how banking supervisors treat Matters Requiring Attention (MRAs). Captured in the Notice of Proposed Rulemaking Regarding Unsafe or Unsound Practices and Matters Requiring Attention, the changes are designed to focus attention on material financial risks, contributing to a stronger financial system, he said.

Examiners will no longer be constrained by a long checklist that led to concerns of "mission creep" as the 2008 financial crisis receded into the distance. The changes leave some banking leaders believing they'll have a clearer idea of what supervisors expect and a freer hand to shore up in-house safeguards. The joint revision from the OCC and FDIC sets a higher bar for issuing MRAs that allows examiners to largely rely on their own judgment to detect and determine if banking activity rises to "unsafe or unsound practices," according to the joint release of proposed supervisory standards.

However, some observers say the proposed rule leaves a lack of clarity in how to define "material financial risk."

The time is right to more precisely define what rises to the level of an MRA, McIntire said. "But I also agree with those who are calling for clarity in defining what is considered to be a material financial risk. That will be an important aspect in the final rule.

"I want to see where the industry tries to go and where the regulators end up with a final rule. There needs to be a more consistent definition of material financial risk for MRAs that is positive not just for the industry but for regulatory agencies as well," he said.

The comment period on the OCC and FDIC proposal closed at the end of last year. Hammering out the finer details continues ahead of an unconfirmed 2026 release date. Separately, the Federal Reserve has shared a memo of operating principle priorities.

In the Q&A below, which has been edited for length and clarity, McIntire gives his perspectives on the proposed changes and what they might mean for financial institutions.

ProSight Financial Association: What is driving the proposed rulemaking on safety and soundness and MRAs?

McIntire: One is an overarching driver that is influencing not just this topic but, frankly, the whole regulatory regime. And that is to "right-size" the supervisory approach. Whether we're talking about the OCC, which I'm most familiar with, or the Fed or FDIC, they're all similar in what they're trying to achieve. At its core, this is a refocus on helping institutions be an integral part of the economic engine that will support growth in the U.S. In doing that, the federal banking agencies are refocusing the examination approach on material financial risks. You hear that in speeches that [Comptroller of the Currency] Jonathan Gould or members of his senior leadership team give.

The second driver is around the industry's call that federal banking regulators had perhaps gone too far in what they consider to be MRAs. When we think back to the financial crisis of 2008 and post-crisis, there were a lot of regulatory requirements put in place through law and regulation, and secondarily, changes

in the way federal banking regulators carried out their jobs. Tolerance for that degree of scrutiny rose because that was human nature in the wake of a big crisis. Now it's time for reflection: "Have we perhaps taken it too far?"

The industry learned great lessons and instilled tremendous discipline on the financial side of the house: capital management, credit risk, liquidity risk, etc., over the past decade. And that gives one pause to ask if that's, in part, why you may have an increase in MRAs or other supervisory findings in non-financial areas such as compliance risk, operational risk, etc. Have financial risks been getting less attention and do they need energy refocused toward them?

ProSight: How would you characterize the way the issuance of MRAs has evolved?

McIntire: Speaking directly from my experience as a private sector board member, the number of MRAs that institutions have faced, whether by the OCC or the other federal banking agencies, greatly increased. In some instances, an institution may be dealing with 100-plus MRAs. The resources associated with that are tremendous. What the OCC is trying to do here is bring more clarity and more consistency in defining what constitutes an MRA so banks can be more critically focused on issues that could or are already impacting their financial condition. For instance, the rulemaking rewrite puts a focus on bank practices or acts that present a material risk of loss to the deposit insurance fund as one proposed criterion for citing an MRA.

I also think that in recent years, as what some would call "mission creep" occurred and a checklist of risks to account for developed, examinations tended to be more process-oriented and less about examiner judgment.

"Speaking directly from my experience as a private sector board member, the number of MRAs that institutions have faced, whether by the OCC or the other federal banking agencies, greatly increased."

–Kris McIntire

We can use the speed of the run on Silicon Valley Bank as an example—although keep in mind I have not consulted in an official capacity on that institution, so any analysis is purely speculative from my point of view. But one could argue that the SVB situation is exactly where this proposed rulemaking may be going, meaning you can argue that its closing was largely a missed liquidity crisis and signs, if noticed,

would have constituted a material financial risk. Did internal or supervisory focus waver too much from looking at core aspects like liquidity, liquidity management, contingency planning around liquidity, or scenario planning? This is a potential thesis that this proposal by the FDIC and OCC may be attempting to address.

I take comfort in the fact that the OCC and the FDIC will still afford their examiners the opportunity to share observations with the institutions that they supervise, either in written form or verbally. There is risk that any bank will or will not act on what is a recommendation or observation. Most bankers that I dealt with [as a regulator] appreciated that aspect of the supervision, the part of the consultation that wasn't always criticism. Similarly, it behooves the industry to instill more discipline around giving appropriate attention to those observations and recommendations. At the end of the day, you don't do something for a regulator or banking agency. You act because it's right for the organization you manage.

ProSight: One proposed adjustment calls for immediately closing an MRA once a bank can verify an underlying issue is corrected. And the section of the memo on operating principles that does away with "overly broad" examinations stresses supervisors should invite feedback from banks on whether an MRA is justified. So banks are helping to determine what remediation might include.

McIntire: It's never a one-sided process. There are any number of discussions that happen between the examiners and the supervised institutions before exam reports or supervisory letters are written. Examiners are reasonable. If they hear something or are provided with new or different information, they will take that into account before reaching a final conclusion. That process will continue to exist after this proposal.

The industry should largely be self-policing. Regulators are there as a safety net. It's really a mandate from Congress that they exist. This proposed MRA regulatory change does not mean that if I'm a bank CEO I now just sit back and relax a lot more. In many ways, that job may have gotten tougher now that they need to make sure in-house processes, systems, and controls are stronger because the regulatory environment has changed and may continue to change.>

Redrawing the ERM Map for an Evolving Risk and Competitive Landscape

By Rachel Koning Beals

Given today's evolving competitive, regulatory, and risk landscapes, the enterprise risk management (ERM) functions at financial services firms are in the midst of a transition. Against this dynamic backdrop, leading ERM models leverage their firmwide perspective to strategically position their organizations to manage downside risk while exploiting upside opportunities.

Toward this goal, ERM functions are sharpening their capabilities by simplifying processes, actively incorporating artificial intelligence (AI)—generative AI (gen AI) in particular—into their programs, and investing heavily in talent.

"Given the world we live in and how the industry is evolving, standing still is not an option," says Kim Persaud, managing director and head of ERM strategy, risk frameworks, and engagement, at Citigroup.

"ERM teams may have built great capabilities that have served them well," she says. "But teams need to evolve those capabilities to be relevant for the risks and opportunities banks are facing today."

That need for evolution is no longer theoretical. In light of this shift, ProSight, Oliver Wyman, key risk leaders such as Citi's Persaud, and a working group with representatives from more

than 25 North American financial institutions examined ERM in practice. The collaboration surveyed Category I to IV banks about their current ERM function and future plans. The results are summarized in a new ProSight research report, "From Serious Cartographer to Strategic Navigator: The Evolution and Future of ERM in Financial Services."

Risk Leaders Share What's Driving Change Now

As uncovered in the survey results, ERM functions historically served as the primary second line oversight for enterprise-wide processes such as risk identification or risk appetite, or as an incubator to establish frameworks for nascent risks such as climate or AI adoption. Today, that remit is expanding. ERM teams are sharpening their focus on business impact, scalability, and risk efficiency. These new objectives call for greater investment in automation and advanced tooling.

"Banks are entering a period where strategy, technology, and risk are increasingly inseparable," says Avani Parekh, senior vice president and executive risk advisor at TD Bank. Parekh was also a leading adviser on the project.

"As decisions around growth, digitization, and operating models accelerate, ERM practices will be tested in their ability to inform those decisions in real time," Parekh says.

Parekh agrees that the ERM function cannot be static.

"The next few years will test not whether ERM frameworks exist, but whether ERM can keep pace with how quickly decisions and risk are evolving," she adds. "What once felt like an extreme or improbable set of risk scenarios is now uncomfortably closer to reality. That realization is part of why ERM needs to evolve—from documenting what we know, to helping leaders prepare for what's hard to predict."

In fact, speed to decision is a key factor underpinning the focus of several survey respondents when addressing refreshing core ERM programs to remove multiple layers of reviews or approvals, extensive documentation requirements, and an over-emphasis on comprehensiveness without risk stratification. These tendencies lengthen cycle times, reduce the relevance of program output, and slow decision-making, all of which can

"The next few years will test not whether ERM frameworks exist, but whether ERM can keep pace with how quickly decisions and risk are evolving."

–Avani Parekh

prove problematic in today's fast-moving and complex environment, respondents say.

The survey and report analysis identified AI, particularly gen AI, as a potential solution, positioning ERM teams to move beyond backward-looking risk assessments to more proactive scenario analysis and issue identification. Used effectively, this technology can empower business leaders and risk managers to anticipate disruptions, identify risk hotspots, and prioritize actions based on probabilistic insights.

The report emphasizes that even as the ERM function relies on technology and gets operationally leaner for "navigation," team leaders can't forget its pedigree. ERM must retain the foundational strengths of a "cartographer past"—discipline, rigor, and consistency.

The difference is one of orientation. Where ERM once focused primarily on mapping risks, its value today is increasingly realized through navigation: helping leaders understand trade-offs, anticipate uncertainty, and make informed decisions in the face of change.

"As the old world order reconstitutes itself, it's more important than ever for ERM teams to help the organization stick to its core risk management principles, mobilize and act with agility, and proactively manage change," says Citi's Persaud.

How To Use the Report

In this concise report, ProSight, Oliver Wyman, and the risk leaders synthesize survey results to bring greater understanding to the shift in the ERM function and how ERM leaders can act. The report is not exclusive to ERM personnel and can be used to inform the entire organization about the valuable role of ERM, offering insight to the board and executives, to MDs and non-managers, and distributed across business lines.

"For years, ERM's success was measured by how well it could map risks across the enterprise. Today, that's no longer enough," says Parekh. "This work reflects the shared recognition that ERM's value is realized when risk insight shapes an organization's real decisions—not just ERM reports."

"In a world defined by faster change, greater interconnectedness, and less certainty, that shift matters more than ever," Parekh adds. "This shareable report captures what that next chapter looks like in practice."

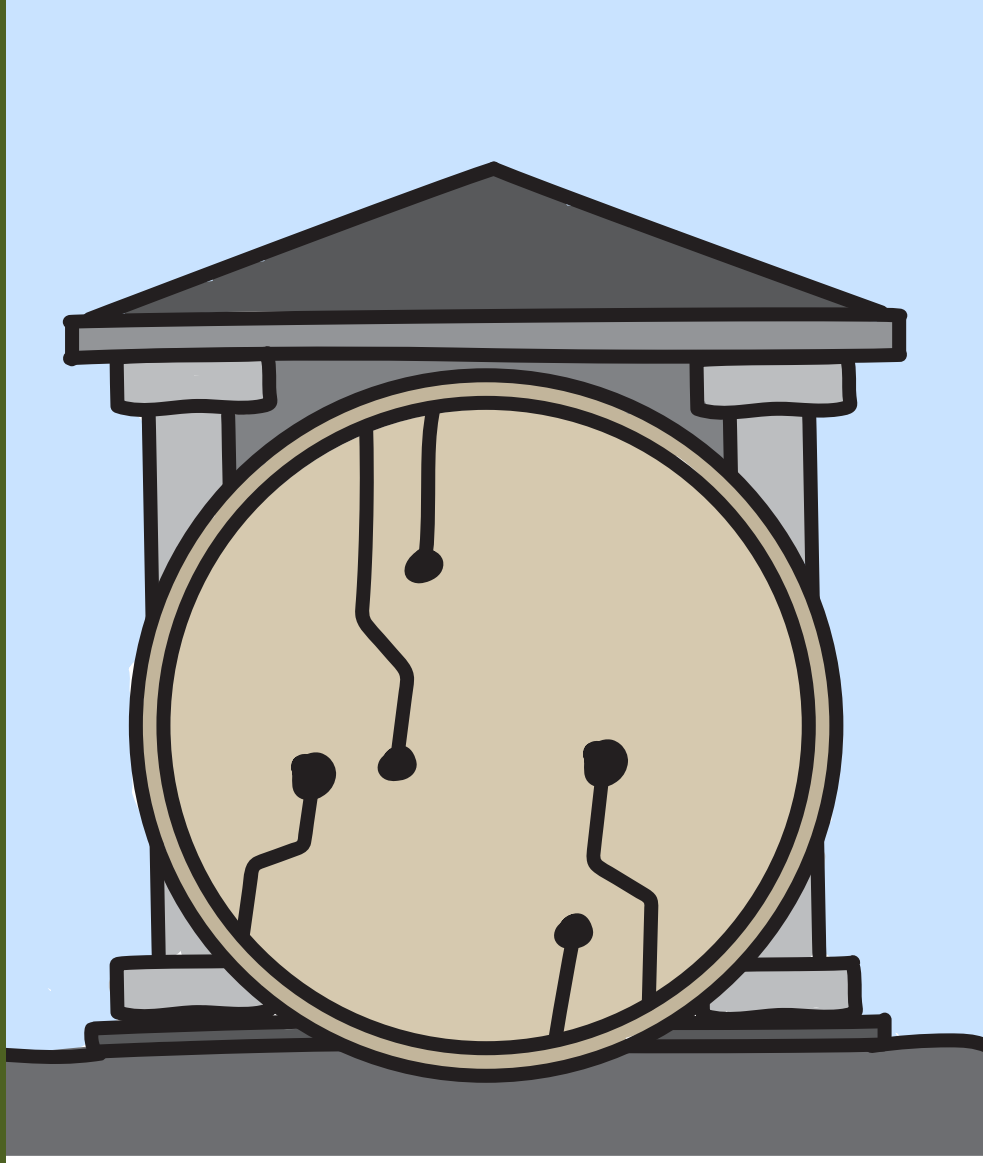
And since ERM practitioners put special emphasis on the need to upskill their teams, the piece could be especially beneficial for human resources departments. As the report stresses, there is a real demand for team members who bring clarity to emerging risks and engage strategically with business and risk leaders on technical risk topics. Leading ERM teams blend these backgrounds, along with an understanding of AI applications, to drive collaboration with data scientists and technology teams.

Ultimately, this is a report intended to ease the path for change. With that in mind, participating risk leaders advise that organizations manage this transition in an authentic and disciplined way.

"It's potentially going to feel overwhelming. What to change; what order to change it, how to get teams on board; how to sell the approach up and across the organization," says Persaud. "While it might be easier to just copy what others are doing, making this pivot will land better if it's grounded in what your organization wants to be. Link the work to the strategic priorities for your firm, not just any firm. That will help teams prioritize where to start evolving first. It will be easier to get engagement and buy-in."

Q&A

Considering the GENIUS Act's Impact on Traditional Banking



The Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act is landmark legislation aimed at creating a comprehensive regulatory framework for payment stablecoins in the U.S. Signed into law in July 2025, this first-of-its kind federal guidance lays policy groundwork for integrating digital assets into mainstream finance.

Estimates of the growth in stablecoin market capitalization range from $2 trillion to $4 trillion by 2028. In its Q1 2025 report, the U.S. Treasury's Treasury Advisory Borrowing Committee cited the lower end of the range—an 8.5x increase from the current $234 billion market cap in 2025. The amount of block-chain enabled payments is projected to reach $7 trillion by 2027.

In interviews with ProSight Financial Association, Roy Ben-Hur, managing director and US digital asset financial services lead at Deloitte & Touche, shared insights on the regulatory climate, product developments, and decisions ahead for the banking industry as it comes to terms with technology and new forms of virtual money that will radically change global finance. Ben-Hur dives deeper on this ProSight webcast, "Digital Assets and the Genius Act: How Banks Can Prepare."

For a decade the U.S. government and regulators cautiously monitored the growth in digital assets, severely restricting their path into everyday finance. Now we're moving rapidly to broad-based normalization and adoption in everyday finance. What changed?

I would call this a "shock and awe" approach from the current administration, legislators, and regulators in terms of driving market adoption. The landscape has shifted, leading to everything from the repeal of standing regulations to the review of the accounting and tax treatments of digital assets. We also see some states progressing now with issuing stablecoins of their own.

Can you touch on some of the use cases we expect to see for stablecoins coming out of the Genius Act?

From a pure payment perspective, the notion of stablecoin being a payment rail, first and foremost, and the ability to move money across borders, cheaper, faster, and in a programmable manner. That programmability is likely to be an appealing feature for a lot of institutions. Another use case is for corporate treasurers who will see this as a way to optimize accounts globally at different entities and a real-time way to send money anywhere day or night.

How will stablecoins affect bank deposits?

Citing the April report from the US Treasury, stablecoins could put $6.6 trillion of bank deposits at risk. It will depend on the functionality that stablecoins provide. If it's just a payment rail, then the impact will be much smaller. But if it's a stablecoin linked to a tokenized deposit or money market account that provides yield, that will create more of a flow away from traditional bank accounts into banks with deposits that are digital asset- or stablecoin-based.

What options do banks have for playing in the digital asset space? Sounds like doing nothing is not an option.

Doing nothing is the worst approach. Start by educating your leadership. Understand what the implications are for the industry and your bank. Even if you're skeptical about digital assets, it helps to build some muscle memory in this space. Engage operations people, get your compliance people on board, and start thinking about risks and controls. It's not that easy to jump in and accelerate this overnight, especially when you need talent onboard who understands it.>

"Citing the April report from the US Treasury, stablecoins could put $6.6 trillion of bank deposits at risk."

–Roy Ben-Hur

Effective Strategies for Managing an Appraiser Shortage

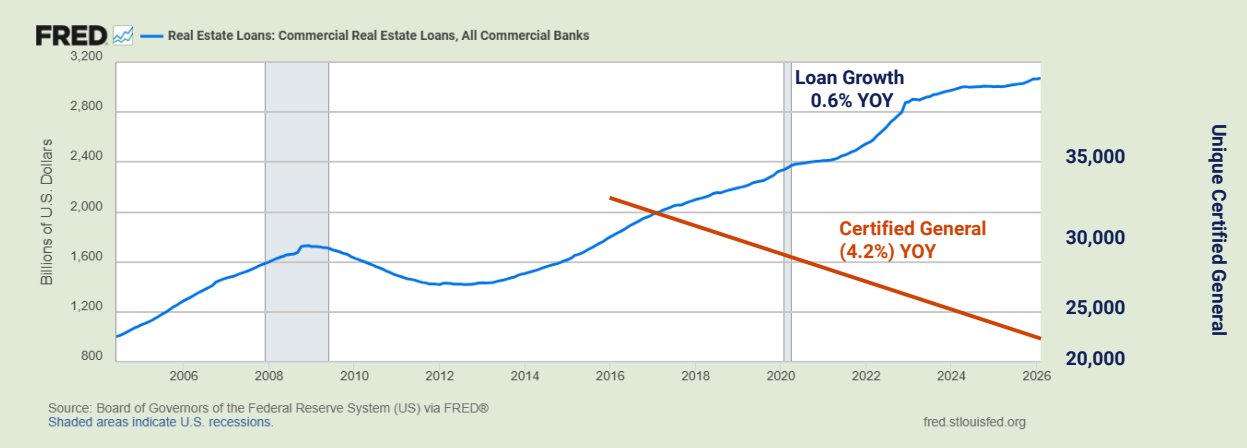
By Beverlea Gardener

Is there an appraiser shortage? While most appraisers say "no", longer turn times and publicly available data suggest otherwise. Since the number of appraisers peaked in 2007, productivity improvements and generally stable loan demand have reduced the overall need. But a continued decline in the number of appraisers per Appraisal Subcommittee (ASC)[1] data suggests the industry is facing a potential shortage.

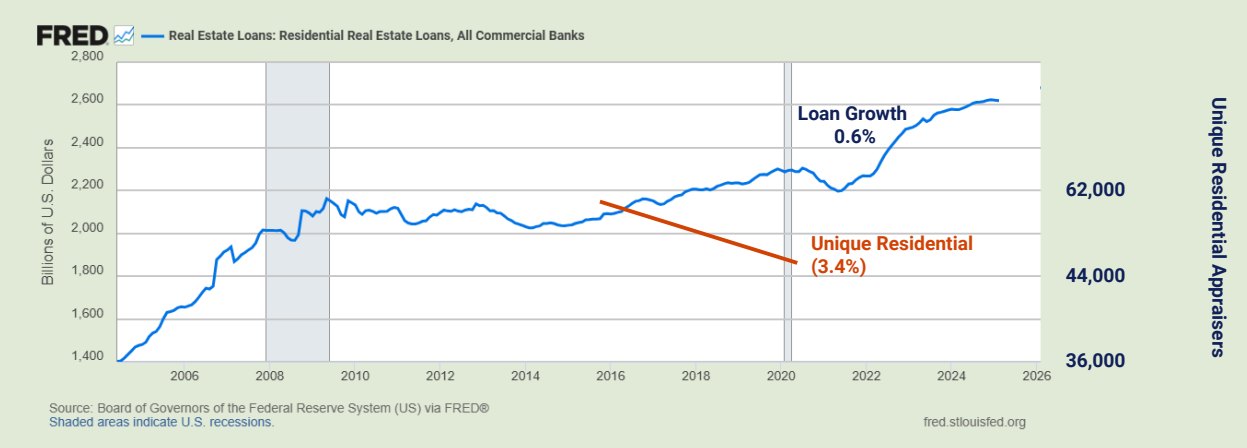
It takes years for new entrants to meet educational and experience requirements before they can independently perform assignments that comply with the Uniform Standards of Professional Appraisal Practice (USPAP). This long developmental period creates a lag in appraiser capacity to meet loan growth, especially when there is a surge in demand from new loans.

Data provided by the Board of Governors of the Federal Reserve System[2] shows commercial real estate loan volume in all commercial banks grew 0.6% year-over-year from 2020 through 2025 thanks to a combination of new construction, appreciation, and other factors. The number of certified general appraisers increased by just 0.1% during the same timeframe, ASC statistics show. However, this count is overstated as many certified general appraisers hold a credential in multiple states.

A more concerning trend emerges in the number of unique certified general appraisers, which has declined by more than 20% over the past five years (see graph).



A similar concern appears when comparing residential loan volume to the number of unique residential appraisers.



A deeper dive into the ASC database as of year-end 2024 finds that 66,715 appraisers hold about 91,000 credentials[3] as compared with U.S. Bureau of Labor Statistics employment data[4] reporting 59,070 as of May 2024. The difference may be due in part to appraisers who are not actively practicing. For example, one industry source[5] estimates that 15% of all residential appraisers currently provide appraisal-related services, such as managing the process or reviewing reports, but don't produce appraisal reports. Overall, the data corroborates that there is a declining trend in the number of real property appraisers.

Effective strategies to ensure that lenders' ability to process real estate-secured transactions in a timely manner is not impacted by a scarcity of appraisers include:

Use more carrots, less stick

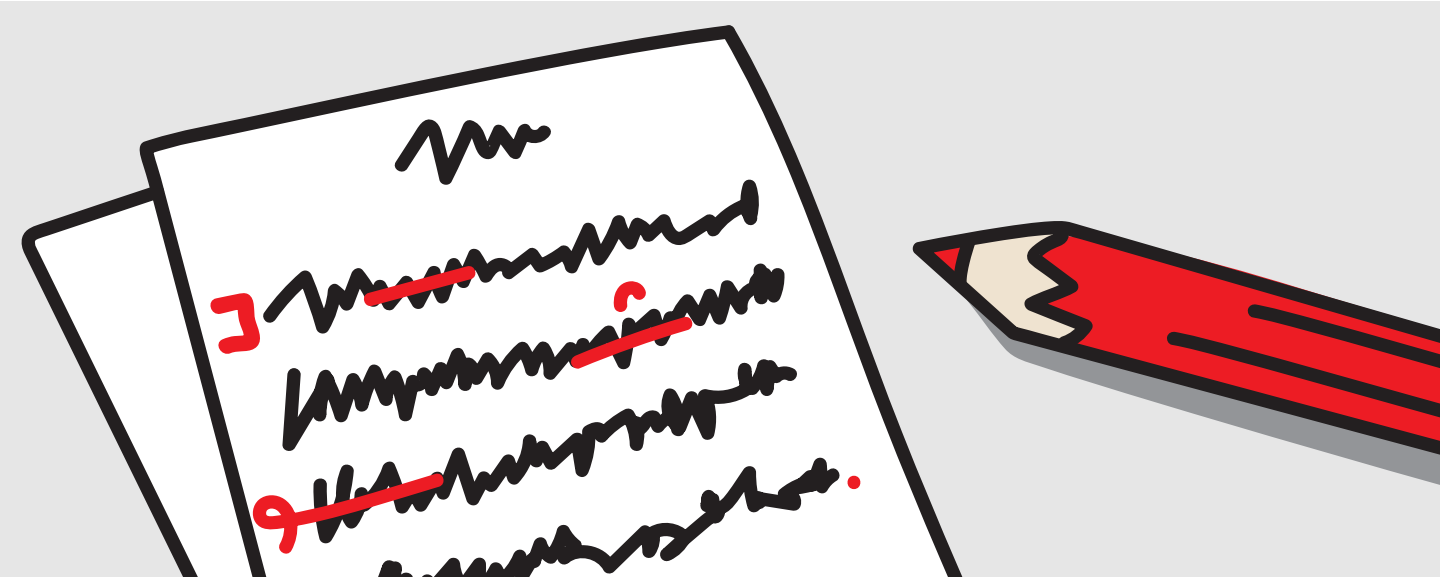
- Pay appraisers well for delivering good quality appraisal reports that support the value conclusion while saving your organization money due to less staff time spent on "fixing" them.
- Engage appraisers for their expertise such as for complex or atypical commercial, residential, or agricultural properties, as the valuation process can be more art than science at times, especially when little supporting information is available.
- Respect reasonable turn times rather than requesting rush appraisal deliveries when they are truly not needed to maintain report quality and reduce appraiser burnout.

Order alternative valuation products

- Use regulatory exceptions from the appraisal requirement and order alternative valuation products, such as evaluations or validations, to originate small-dollar loans and renew credit to existing borrowers, even if new funds push the loan amount over the regulatory dollar thresholds.
- Form strategic partnerships with third-party vendors who leverage technology to deliver compliant alternative valuation products in a cost-effective and efficient manner, instead of vendors who generate "low-cost, low-quality" products that may not comply with the regulations.
- Create mutually beneficial relationships where lenders receive conforming evaluations and validations in shorter turn times while borrowers obtain loans with lower closing costs.

Stop policing typos, start managing risk

- Set clear thresholds (Materiality Tests) within the review process for both residential and commercial transactions which allows reviewers to accept minor mistakes without having to contact the appraiser or vendor. This strategy enables all parties (reviewers, appraisers, and vendors) to focus their time on what really matters—errors that potentially raise legal concerns or materially impact the value conclusion. The Materiality Tests can provide parameters that address three primary types of significant concerns:
  - *Legal errors*. Correct key factual mistakes in legal information, property characteristics, legal description, owner or borrower names, address, county, zoning, regulatory definitions, or appraiser certification.
  - *Bias or discrimination*. Investigate allegations of appraiser bias or discrimination whether internal or external.
  - *Mistakes in value conclusion*. Establish thresholds based on the value conclusion to determine when errors are or are not material. For example, some organizations set a "5% Rule" —errors that impact the market value by 5% or less are accepted without requested revisions.
- Disregard minor issues. Typographical, grammatical, and stylistic preferences that do not meet the Materiality Test are inconsequential. Mention them in the appraisal scorecard if necessary, but they do not warrant further time or pursuit.
- Verify the accuracy of the property description and ensure all essential information is available at the onset of engaging the appraiser or vendor to minimize errors, reduce costs, and improve turnaround times.



Begin building your bench now

- Waiting to build your bench is like waiting for avocados to ripen. Oops! Too late! Start building your bench today so you will have appraisers available tomorrow.
- Seek competent appraisers as well as newer entrants to the industry for your approved vendor panel. Third-party vendor management should focus on quality, not quantity.
- Offer internships to potential new candidates who can train under a qualified supervisory appraiser.

Mind your manners, even when others do not

- Treat appraisers and vendors in a professional manner throughout the process to promote a collaborative rather than an adversarial relationship.
- Provide appraisers and vendors with a "scorecard" that rates both product (technical) and interaction (interpersonal) skills. This process will give them constructive feedback and assist lenders in deciding whether they should be engaged for future assignments.
- Recognize that the development of a value conclusion involves judgment, assumptions, and estimates. A market value that significantly differs from expectations may mean the lender needs to reassess the terms of the loan, not that the appraiser botched the assignment.

In summary, data shows the financial industry is facing a potential shortage of appraisers. Whether there will be enough appraisers to complete residential or commercial real estate assignments in a timely manner in the future remains to be seen. Lenders who implement effective strategies to allocate appraiser resources based on transaction risk, use compliant alternative valuation products when permitted, and apply materiality tests in their review processes can minimize the impact of appraiser shortages and stay competitive during periods of high loan demand.>

Notes:

1. See at FFIEC Appraisal Subcommittee 2024 Annual Report.
2. See at Real Estate Loans: Commercial Real Estate Loans, All Commercial Banks (CREACBM027NBOG) | FRED | St. Louis Fed.
3. See at Analysis of 2025 ASC Appraisal License Data – Appraisal Buzz.
4. See at Occupational Employment and Wage Statistics Profiles, Major Occupational Group is Business and Financial Operations and Detailed Occupations is Property Appraisers and Assessors.
5. See at Residential Appraiser Trends Since 2016; New Projections for 2025-2030 – MtgeFi.

Beverlea S (Suzy) Gardener is an FDIC Appraiser (Retired).

ProSight

Invest in Your Professional Network

ProSight Roundtables and Forums bring together leaders and professionals in financial services for open, small-group discussions on the most pressing issues.

FEATURED UPCOMING EVENTS

8/11/2026 | Chicago, IL
ProSight Contact Centers Executive Roundtable

8/12/2026 | Chicago, IL
ProSight Operations Executive Roundtable

8/14/2026 | Chicago, IL
Operational Risk Management Forum

8/18/2026 | Virtual
ERM for Mid-Tier Banks Roundtable

9/9/2026 | Philadelphia, PA
Commercial Underwriting and Portfolio Management Roundtable

9/9/2026 | Denver, CO
ProSight Chief Credit Officer Executive Roundtable for Community Banks

9/14/2026 | Virtual
Health Care Credit Officers Roundtable

9/15 | Philadelphia, PA
Commercial Real Estate Lending Forum

9/15 | Philadelphia, PA
Credit Department Management Forum

9/15 | Virtual
Environmental Risk Managers Forum

9/15 | San Francisco, CA
Heads of ORM (Mid-Tier Banks) Roundtable

9/15 | Virtual
Northeast Credit Officers Virtual Roundtable

View more events and register at ProSightFA.org

Leverage Branches as Effective Learning Hubs in the Fraud Fight

By Rachel Koning Beals

Branch leadership can think creatively even when it comes to one of the most serious issues facing banking today: minimizing fraud.

ProSight regularly engages with fraud and cybersecurity experts who stress that as routine banking reaches across several channels, branches provide a personalized and conversational atmosphere, focused audience attention, including personnel, plus traction within the community. Targeted fraud education efforts might include well-placed signage, inviting small business leaders for in-person workshops on detecting fakes from a batch of legitimate checks, or hosting breakroom pub-style quizzes and mocktails to test staff knowledge of phishing.

"Given the seriousness of risks and the range of fraud vectors, anti-fraud messaging in statement inserts and emails that may get lost in a mix of all-bank messaging just doesn't cut it anymore," said Bobbie Paul, managing director, fraud, at consultancy Huron, who led a ProSight Banking Trends webinar on prioritizing fraud prevention goals in 2026.

Because fraudsters are regularly upgrading technology and expanding their reach, including with AI, strategists advise addressing fraud-protection steps early and often in banking relationships.

Jason Bartolacci, director of the ProSight Fraud Alert Network (FAN), said messaging should be strategic across email, apps, social media campaigns, and within anti-fraud directives on a bank's website, as well as part of in-branch signage and teller-to-customer engagement. A key access point, he says, is education built into account opening, which is an onboarding process that ProSight research shows remains a popular in-branch function.

"Any kind of fraud education campaign can work like a marketing campaign. You want to make sure that it's sticky," Bartolacci said in an interview on balancing fraud mitigation and limiting customer friction.

Data shows that consumers have heightened awareness of fraud dangers, which means banking customers are increasingly becoming a receptive audience to greater fraud prevention education. Some 60% of Gen Z customers said they are at least "somewhat" and up to "very" worried about fraud, the same percentage as Gen X, while roughly 55% of Millennials feel this way and 58% of Boomers on up expressed this level of concern, according to survey data in the ProSight Banking Outlook: 2026 Trends.

Busy bank branches aiming to function with right-sized staffing may find it challenging to fit in these conversations beyond fleeting messaging, but making time for anti-fraud education, reinforcement, and outreach campaigns can be vital to safeguarding customer confidence in the institution.

For every 10 customers asked, between two and three said they had switched providers after they were impacted by a single fraud event, said Ray Olsen, senior director of enterprise fraud management at Wintrust, who joined Huron's Paul on the fraud trends webinar. Olsen said he based this figure on multiple reports and combined the results for a snapshot of banking behavior.

And it's not only retail customers who will abandon their primary provider if spooked by criminal activity; some 30% of small businesses will leave after a lone fraud exposure, according to at least one survey from Abrigo.

Matt Meis, cyber fraud manager at Summit Credit Union and a fraud trends webinar participant, said his organization has stepped up anti-fraud training and retraining for frontline employees, including customer-facing branch staff. Efforts include updating personnel on shifting fraud vector trends, data vulnerabilities, and local crime incidents.

Plus, security leaders at Summit expose staff to physical fake ID and faulty check examples so that suspicious materials "are brought into the real world," not abstract, Meis said.

Wintrust's Olsen emphasized regularly changing the message on fraud to lower the likelihood an internal and external audience grows desensitized or complacent. Olsen, whose responsibilities include his regional bank's suburban Chicago branch network, said he conducted nearly 50 fraud educational seminars for retail customers and commercial clients at events inside the branch or by pushing into his community to address business groups or assisted living facilities, over the past year.

Here are some strategies to consider.

Steps directed at customers and members

Balanced tone. Data breaches. AI-powered deepfakes. The dark web. For many customers, fraud and cybersecurity language may resemble their Netflix programming pitches and not everyday banking, or so they think. Serious messaging will get the point across, but overt scare tactics may have the opposite effect. Customers and members need reassurance that the institution is acting in their best interest and that sound habits by individuals all work toward keeping their money as secure as possible. The emphasis should be on a consistent fraud-mitigation approach that resonates and is memorable. Keep messages simple, visual, and story-driven, say experts.

Simple, repeat messaging works. When a branch does promote fraud and cyber awareness, anti-fraud campaigns should have intention and employ results tracking like any good marketing effort. While adhering to FDIC compliance requirements for signage, branches can hang posters and banners, plus use digital sign capabilities that promote cybersecurity and fraud awareness keeping pace as new schemes emerge. And don't consider branch awareness efforts in isolation, say experts. Use social media platforms such as Facebook, Instagram, TikTok, YouTube, and LinkedIn, to reinforce branch events and share tips, stories, or resources.

Neither the public nor branch staff can be expected to be experts in all vulnerabilities. Best practices may be conceding branch

Best practices may be conceding branch personnel expertise limitations and turning concerned patrons onto additional anti-fraud, security, and law enforcement resources.

personnel expertise limitations and turning concerned patrons onto additional anti-fraud, security, and law enforcement resources.

"We're talking about an action as simple as a teller taking an extra moment to remind the customer about the risk of scams or emphasizing that the bank will never call or text and ask for an account number — a step that is quick and easy," Olsen said.

Consider programming aids such as from American Bankers Association's Banks Never Ask That and the ABA Foundation's Safe Banking for Seniors campaign.

Steps directed at tellers and other staff

The frontline as anti-fraud ambassadors. Edward Callis, vice president of IT risk management and assurance at Abrigo, said keeping branch employees energized in this fight can be as important as the focus on customers, and that means coaching in innovative ways. He suggests organizing in-branch activities or contests that test cybersecurity and anti-fraud knowledge and skills such as a virtual escape room exercise set up in the branch or team puzzle-solving for prizes or incentives.

Similarly, leaders should ensure that all employees feel invested in the fraud and cybersecurity fight, said Callis. It's no longer exclusively an IT issue to care about cybersecurity, or only a risk team concern to focus on fraud, and branches are a first line of defense. The National Cybersecurity Alliance (NCA) provides educational materials and the federal government's Cybersecurity & Infrastructure Security Agency promotes Cybersecurity Awareness Month, for a focused awareness campaign, typically in October, as well as providing year-round resources, which should be posted and visible for branch staff.

ProSight's Fraud Alert Network (FAN) is designed for institutions to share non-private data and trends for deeper fraud tracking. ProSight's Bartolacci advises that branch employees can also bookmark two sites that top his list of favorites for open-source insights and professional exchange:

IAFCI (International Association of Financial Crimes Investigators): A professional association offering investigative resources, training, and networking for those combatting financial crime worldwide. Bartolacci follows IAFCI's LinkedIn group, where members regularly share case studies, red flags, and emerging fraud schemes.

ACFE (Association of Certified Fraud Examiners): The world's largest anti-fraud organization and training body for fraud examiners. Its publications and LinkedIn community provide timely articles and practical guidance accessible to professionals outside of dedicated fraud teams.

Fraudsters are betting on human vulnerability. Why is it important that fraud education extend to internal targets as well as external? Criminals are looking for the point of least resistance and while that is not specific to an institution's size, community bank branch staff may not be protected by the same security budget as larger banks. That puts extra responsibility on insider diligence to avoid exposing the branch and the community bank network to phishing emails or smishing texts, said Callis. Posting visible branch reminders

and holding regular in-branch education sessions are a must. Messaging should address the risks of access, especially when employees click on unconfirmed links and don't follow proper safeguards. Information retention will be strongest when training is fresh and inspiring, he emphasizes.

"Phishing and smishing remain a significant fraud inroad because email and text [for the fraudster] is basically free, and they can send thousands and thousands at a time," said Callis.

Combined efforts in branches

Manageable assignments. Callis recommended community workshops directed toward a nonprofessional audience. Branch leadership might consider hosting sessions for employees, customers or members, and the community at large (banks and credit unions might also stream the event as a virtual webinar for wider distribution). Programming can cover topics that are teachable in a single session such as password management or how to recognize phishing. In-person workshops allow for trouble-shooting sample texts and Q&A. Callis said the topic mix can smartly blend digital banking topics with a branch setting because many customers use more than one channel.

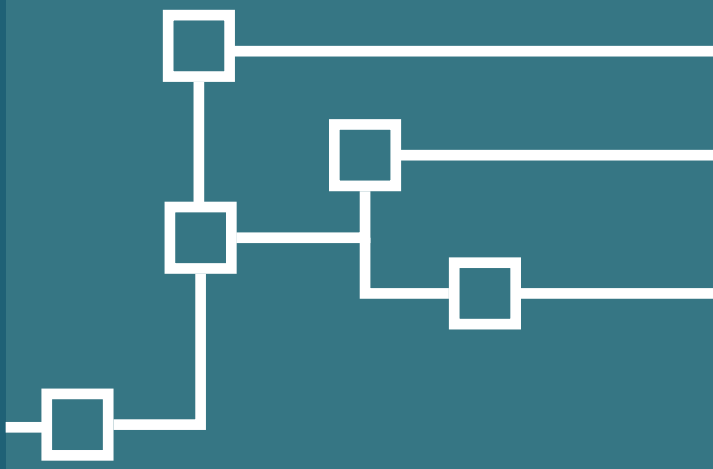
Trusting a hunch and reporting. Wayne Jacobs, special agent in charge of the FBI's Philadelphia division, in a release about financial scams, encouraged banks and credit unions to make reporting suspicious activity simple and judgement-free for customers and staff. Banks can generously post contact information throughout the branch such as the FBI's Internet Crime Complaint Center (IC3) phone number or its online portal at ic3.gov, he said.

An ounce of prevention for check writing. Digital banking popularity isn't turning back but paper checks have their place, often for higher-value amounts. Checks feature in the banking mix especially among older Americans and small business clients—customer categories that also tend to visit branches. Atlanta Fed research reveals a slow realization of the fraud risks associated with checks—such as sophisticated chemicals, forged signatures, and outright mail theft.

It all points to branch engagements as prime opportunities to boost awareness among the most vulnerable victim targets and bank staff most likely to be handling checks. Education on fakes can be found in the Federal Reserve Financial Services Check Fraud Mitigation Toolkit, which was created with industry input. And banking leaders seek more understanding around preemptive check approval clearance known as positive pay, which lowers real-time fraud-detection pressure on customers and branch staff.>

Fraud Model Validation:

A Q&A with Flagstar's Chandrakant Maheshwari



By Robert Sales

Even before the rise of AI, fraud model validation was an incredibly difficult task. But with the explosion of generative AI (gen AI)—and the more recent ascension of agentic AI—testing, evaluating, and verifying fraud models has become a monumental challenge.

Cybercriminals are exploiting technological advancements to execute AI-driven scams, like account takeovers, phishing, and security identity fraud, that look and sound authentic. Meanwhile, modelers are now using gen AI and agentic AI to develop fraud prevention systems. Those AI-based models, however, must be thoroughly vetted to ensure accuracy, reliability, and compliance with regulations.

Chandrakant Maheshwari, the lead model validator at Flagstar Bank and one of the key authors of ACAMS' CAM7 course work on anti-money laundering (AML) compliance, has decades of experience in financial crime prevention and fraud modeling. He is the author of a forthcoming book on financial crime risk modeling, "Validating Financial Crime Risk Models: A Guide to Managing Data Quality, Transaction Monitoring, and Compliance," scheduled to be published by Springer later this year.

Recently, ProSight spoke with Maheshwari about fraud trends, validation best practices, the limitations of traditional back-testing for financial crime, the pros and cons of buying versus building models, and the complexities that AI brings to fraud model validation.

ProSight: What types of fraud are the most difficult for banks to manage today?

Maheshwari: The hardest fraud to manage is the kind that looks like legitimate behavior until it is too late. Account takeover, authorized push payment fraud, and first-party fraud all exploit the same data signals that banks use to approve genuine transactions. Synthetic identity fraud compounds this because the fraudulent customer never existed in any prior data set. The model has no baseline to compare against. What makes these categories especially difficult is not their technical complexity. It is the speed. Fraud risk manifests in minutes to days. By the time a pattern is confirmed, the loss has already occurred.

> "AML monitoring must be holistic, tracking behavioral patterns across a customer's full history over months."
>
> –Chandrakant Maheshwari

ProSight: What are the structural differences between anti-fraud and AML model architectures?

Maheshwari: The most important structural difference is rarely discussed: money launderers are internal customers. They hold accounts, maintain relationships with the institution, and use its products to move illicit funds. The financial system is their laundering mechanism. Fraudsters, on the other hand, are typically external actors targeting the bank or its customers. The financial system is their victim. That distinction drives everything about how models are built and validated.

AML monitoring must be holistic, tracking behavioral patterns across a customer's full history over months. Fraud monitoring, in contrast, is transactional and time-critical, designed to stop a loss within minutes. The validation challenge is also structurally different. Fraud models can be back-tested against confirmed loss events. AML models cannot.

A suspicious activity report is not a confirmed case of money laundering. The AML validator must assess whether the model is well-designed to detect illicit behavior, not whether it actually caught it. That epistemological gap is what makes AML model validation a discipline in its own right.

ProSight: How are financial institutions using AI, including gen AI and agentic AI models, to combat fraud?

Maheshwari: Machine learning has been part of fraud detection for over a decade. What is new is the application of generative AI to the investigative layer. Banks are beginning to deploy large language model-based systems to draft suspicious activity report (SAR) narratives, summarize alert context, and support analyst decision-making. Agentic AI takes this further by orchestrating multiple tasks autonomously—retrieving transaction history, cross-referencing typology libraries, and generating a recommended disposition. The productivity gains are real—but so are the governance risks. These systems must be validated like any other model under SR 11-7. The output is a compliance decision, and the accountability remains with the institution.

ProSight: What specific steps do banks need to take to validate their fraud models? Can you recommend any best practices?

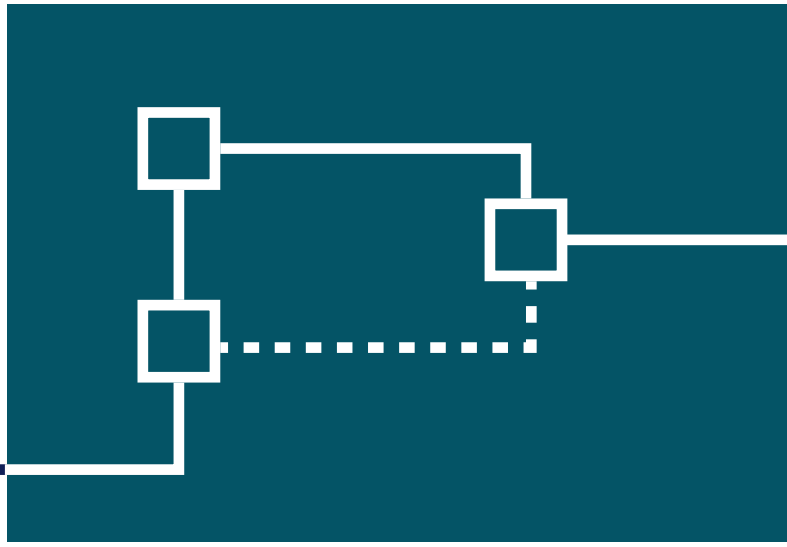
Maheshwari: Validation must begin with the fraud risk assessment. Every model assumption should be traceable back to the institution's documented risk profile. From there, validators should assess conceptual soundness, data quality, and ongoing performance. For fraud models specifically, the labeled data set is critical. Confirmed fraud cases are sparse and may not represent the full range of attack vectors. Validators therefore must challenge whether the training data reflects current typologies or whether it is already outdated.

Threshold validation, segment-level performance analysis, and fairness audits across customer demographics are not optional. They are the baseline. Documentation must support a full audit trail of every tuning decision.

ProSight: How do the standards for validation shift when firms incorporate agentic AI into their fraud models?

Maheshwari: The entire pipeline becomes the model. Under SR 11-7, a model is defined by its inputs, processing logic, and outputs. An agentic system that retrieves documents, applies reasoning, and generates a recommendation meets that definition at every stage.

Validators must assess each component—the retrieval architecture, the prompt design, the inference layer, and the output formatting. The challenge is that agentic systems are not deterministic—i.e., the same input can produce different outputs depending on retrieval results and model version. Validation must therefore establish reproducible testing protocols, define acceptable variance bands, and confirm that human oversight is embedded before any consequential decision is finalized.



ProSight: Are AI models being increasingly adopted because of the limitations of traditional back-testing for financial crime?

Maheshwari: Partly, yes. But the more precise answer is that AI adoption is driven by the limitations of rule-based systems at scale, not by back-testing failures specifically. Rules degrade. Criminals adapt. A threshold set 12 months ago may be systematically exploited today. Machine-learning models can detect patterns that no rule anticipated.

The back-testing problem is a separate issue and a serious one. In AML, there is no ground truth. You cannot back-test against confirmed money laundering the way you back-test a credit model against actual defaults. AI does not solve that problem, but it does change the shape of it.

ProSight: How should banks determine whether to buy or build their fraud models, and what are the pros and cons of employing external models?

Maheshwari: The most defensible answer is that banks should neither buy nor build exclusively. Rather, they should use a hybrid approach. Vendor models bring breadth. They are trained on data from thousands of institutions across geographies and fraud typologies. Emerging attack patterns, synthetic identity networks, and cross-institutional mule activity are things a single bank simply cannot see from its own transaction history alone.

Relying entirely on internally built models means the institution is always one step behind threats it has not yet encountered. At the same time, vendor outputs are a starting point, not a final answer. The vendor model does not know your customer base, your product mix, or your institution-specific risk profile. Banks that layer their own models on top of vendor outputs—refining scores, adjusting thresholds, and adding institution-specific features—get the best of both worlds. The vendor provides coverage, while the internal model provides precision.

The validation obligation applies to both layers equally, and the interaction between internal and external models must itself be validated. A well-tuned internal refinement layer on top of a poorly understood vendor model only compounds the opacity, rather than resolving it.

ProSight: Are there any fraud model validation trends that you will be following closely throughout the remainder of 2026?

Maheshwari: Two areas stand out. First, fairness and bias auditing is becoming a front-line validation requirement, not an afterthought. Segment-level performance disparities are a regulatory and reputational risk. Second, the integration of the fraud risk assessment into model validation and governance is gaining attention.>

**The opinions expressed by Chandrakant Maheshwari in this article are his own and do not reflect those of his employer.*

States Filling Gaps in Federal Consumer Law

As federal banking regulators retreat from some areas of consumer protection oversight, states are moving decisively to fill the gap. The result is not less regulation for banks, but a more fragmented and, in many cases, more challenging compliance landscape.

States have always played a role in consumer financial protection. Attorneys general enforce state consumer laws, state banking regulators supervise local institutions, and state legislatures regularly pass financial statutes. Even national banks have historically faced state actions, often alongside federal enforcement. What has changed is the intensity and coordination of that activity, says Brian Hughes, a senior advisor at consultant BCG.

That incentive has grown as the Consumer Financial Protection Bureau (CFPB) has stepped back from some of its activities, creating space for state officials to act.

State action, Hughes explained, generally falls into three buckets: building regulatory agencies, passing new laws, and enforcing those laws.

Several states have focused first on capacity-building. California and Pennsylvania, in particular, have developed regulatory agencies modeled on the CFPB. California expanded its Department of Financial Protection and Innovation in 2020 with broad consumer oversight authority and has appointed former CFPB director Rohit Chopra to lead a new business and consumer protection "super agency." Pennsylvania has maintained a CFPB-style unit for years.

"These are essentially mini-CFPBs," Hughes said. "They're specifically stepping in and saying, 'The CFPB is stepping back, and we're taking charge.'"

Alongside agency-building, legislatures are strengthening the legal tools available to regulators. Hughes pointed to New York's Fair Act as one of the most consequential examples. The law effectively brings the CFPB's unfair, deceptive, or abusive acts or practices—known as UDAAP—standard into state law.

"That gives the New York attorney general a full-blown UDAAP toolkit," Hughes said. "UDAAP requirements are intentionally vague. It gives regulators a lot of discretion, and that's what makes it such a powerful enforcement tool."

In recent months, New York and Pennsylvania joined more than a dozen other states in a multistate enforcement action against a nonbank lender, even though the company had already settled similar allegations with the CFPB.

That discretion is now being exercised. In recent months, New York and Pennsylvania joined more than a dozen other states in a multistate enforcement action against a nonbank lender, even though the company had already settled similar allegations with the CFPB.

"The response from the states was basically, 'We don't care,'" Hughes said. "We've got our own laws, and federal settlement doesn't preempt state action."

Consumer Focus

Despite the broad reach of this activity, it is concentrated primarily in consumer protection and, to a lesser extent, AML. When it comes to larger financial institutions, states have shown little interest in stepping into areas such as bank safety and soundness, which remain federal priorities.

Prudential regulation, he added, is an area where federal regulators have said they intend to be more assertive, not less.

States are also unlikely to pick up areas like reputational risk that federal regulators have deemphasized. From a risk management perspective, he argued, reputational risk is better understood as a consequence of failures elsewhere. "It's a consequential risk. It usually arises because of poor risk management in another area."

Geographically, the most active states are clear. New York and California "are all over this," Hughes said. Pennsylvania is close behind, with Massachusetts and Colorado also emerging as notable players, particularly around so-called junk fees and consumer disclosures.

Complexity, Not Relief

For many banks, this proliferation of state activity has countered the regulatory relief some may have expected when federal oversight eased. Instead, it has introduced new complexity.

"You now have a fragmentation of regulation," Hughes said. "As soon as a state does something, you have to analyze whether they have jurisdiction, whether preemption applies, and if it doesn't, you have to comply. It makes things harder, not easier."

That complexity is reflected in banks' compliance budgets which, data from ProSight's 2026 Compliance Outlook Survey show, are expected to rise in the year ahead. While some institutions have reduced spending, Hughes said those cuts are often tied to the completion of costly remediation efforts following enforcement actions, not to a belief that compliance is no longer necessary.

"There's no clear trend of banks saying, 'We don't have to worry about this anymore,'" he said.

One reason is uncertainty. Priorities can change quickly with political shifts, and future federal leadership could restore the previous regulatory approach. Even rules that have been deprioritized federally can be revisited retrospectively.

"A lot of banks are saying, 'We're not changing,'" Hughes said. "A new CFPB director can still examine the period we're in right now and put their own interpretation on what is required for compliance."

That caution reflects a broader view of compliance as risk management rather than box-checking. It also reflects institutional values. Some banks, Hughes noted, maintain strong consumer protection practices not only to manage regulatory risk, but because they believe it benefits customers and the institution over the long term.

In that sense, current trends aren't so much about deregulation as they are about redistribution. Federal oversight may ebb and flow, but regulation itself is not disappearing. It is shifting to the states and banks are being forced to adjust.>

How Extreme Weather Is Reshaping Credit Risk—and Opportunities—for Banks

By Debra Cope

Extreme weather is moving from a distant environmental concern to a direct financial risk for banks and other financial institutions, analysts from Jupiter Intelligence said during a recent ProSight webinar. Risk managers increasingly recognize that hurricanes, floods, wildfires and other events can disrupt borrowers' cash flows and affect the value of the assets securing loans.

"Financial institutions, when they talk about adjusting for extreme weather risk, are fundamentally trying to understand the stability of cash flows and asset valuations under this uncertainty paradigm," said Wahib Ghazni, lead financial economist at Jupiter.

Some institutions are beginning to incorporate forward-looking weather and climate data into financial models that traditionally relied on

historical averages. Their goal is to understand how physical risks translate into changes in credit performance, asset valuations and portfolio resilience.

In practical terms, Ghazni said, lenders and investors are asking how climate-related events could affect borrowers' ability to repay debt and companies' financial outlooks.

"If a climate event occurs, whether it's a hurricane, wildfire or flood, what does that mean for their loan payments? What does that mean for their bond servicing? What does that mean for their earnings outlook going forward?" he said.

One persistent misconception, Ghazni added, is the tendency to treat climate risk primarily as a regulatory or disclosure issue.

"A lot of times boardrooms are thinking that this is just a compliance issue," he said. "But climate risk is not static, and it compounds. It accelerates."

That distinction matters because the financial consequences extend well beyond reporting requirements. Rising losses from extreme weather events are already affecting insurance markets, operating costs and asset values.

"This is not a disclosure problem," Ghazni said. "This is a valuation and a solvency problem."

Insurance Markets Signal Growing Exposure

Insurance markets have become one of the clearest ways physical climate risks reach financial institutions. In several parts of the United States, insurers have raised premiums sharply or reduced coverage in areas exposed to hurricanes, wildfires or flooding.

Kevin Cei, head of customer success and solutions at Jupiter Intelligence, said those developments are prompting banks to rethink how they incorporate physical risks into their decision-making.

"A lot of the banks have reprioritized, moving away from the regulatory requirements and focusing on business decision making," Cei said.

Insurance costs can quickly affect borrowers and lenders alike. When premiums rise sharply or coverage becomes unavailable, the economics of property ownership fundamentally changes.

"These insurance rates are increasing at a very high rate in many of the areas across the United States," Cei said. "And we're seeing what those downstream impacts are."

The effects can ripple through credit portfolios. Higher insurance costs can increase operating expenses for property owners, which in turn may affect their ability to service debt.

Cei said financial institutions need to understand how those developments translate into financial risk.

One consequence may be changes in asset values. Higher insurance costs or greater exposure to extreme weather can make properties less attractive to buyers or investors, potentially affecting resale values and loan-to-value ratios.

Cei said the effect often comes down to operating economics. Higher insurance premiums, utility costs or other expenses can increase the cost of owning a home, which can affect what buyers are willing to pay. For commercial properties, similar pressures can reduce net operating income, a key driver of asset valuations.

"If you've got asset values that are changing, that could change the dynamic between the amount the borrower owes and the market value of the asset," Cei said.

Marking Climate Risk Across Loan Portfolios

To address those questions, some institutions are beginning to incorporate climate-adjusted asset values into their credit analysis. Comparing traditional loan-to-value ratios with values that account for future weather risks can help lenders identify loans or regions where exposures may be higher than previously understood.

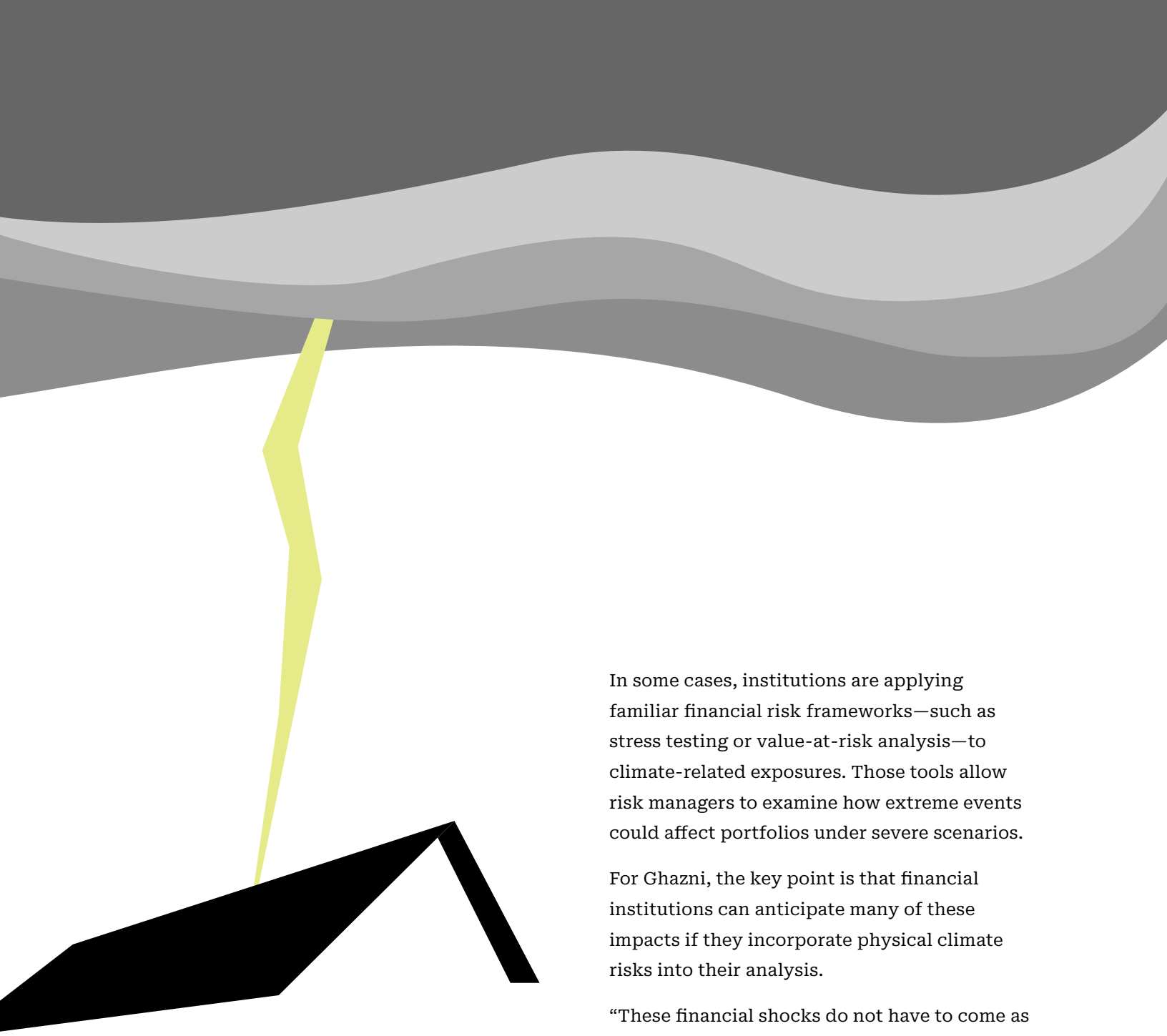
That approach can also reveal concentrations of risk within a portfolio. Geographic exposure to extreme weather, insurance coverage gaps and changes in operating costs can all influence how risk accumulates across a lending book.

Cei said the analysis can also help banks take a more strategic view of their lending portfolios. By mapping climate risks at the asset level, institutions can identify where exposures are increasing and where new opportunities may emerge. Banks can do this on their own portfolios, Cei said. "Banks are creating heat maps that are not just about the general hazards but where the highest exposures of potential loan defaults due to climate are."

Over time, he said, institutions can use that insight to shape their portfolios deliberately rather than reacting after losses occur. "How do you proactively start shaping that portfolio toward where those opportunities are to gain market share?" Cei said.

"Banks are creating heat maps that are not just about the general hazards but where the highest exposures of potential loan defaults due to climate are."

–Kevin Cei



Potential uses for climate-related data extend beyond credit analysis, Cei added. Financial institutions are also exploring how the same information can inform investment portfolios, operational planning and other areas of risk management.

“What we’ve seen with climate data and extreme risk data is that there’s so many different areas within the organization where this can be used,” he said.

In some cases, institutions are applying familiar financial risk frameworks—such as stress testing or value-at-risk analysis—to climate-related exposures. Those tools allow risk managers to examine how extreme events could affect portfolios under severe scenarios.

For Ghazni, the key point is that financial institutions can anticipate many of these impacts if they incorporate physical climate risks into their analysis.

“These financial shocks do not have to come as a surprise. With forward-looking climate risk analysis, institutions can see many of these impacts before they materialize,” he said.

As extreme weather events grow more frequent and costly, the integration of physical climate risk into financial analysis remains a developing discipline. But for many risk managers, the central question is shifting from whether these risks matter to how quickly institutions can incorporate them into everyday financial decisions.>

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-ProSight

ProSight™

The 2026 ProSight Compliance Outlook Survey:

Relaxed Regulation, Steady Vigilance

This report is based on the 2026 ProSight Financial Association Compliance Outlook Survey, which was conducted online in the first quarter of 2026, gathering 150 responses from a range of compliance leaders at financial institutions of all sizes. Find out more about the survey, including the demographic profile of respondents, here. A downloadable version of this report is available here.

In the second year of a presidential administration that made looser financial industry regulation a priority, financial institution compliance leaders are finding that the overall environment they face can be complicated by countervailing state stances and plentiful uncertainty about the future. At the same time, rapid advances in AI—including its implications for fraud—and the uptake of digital assets are prompting compliance teams to develop new muscles in the race to keep up. With that in mind, the 2026 ProSight Compliance Outlook Survey set out to capture insights from leaders with oversight of compliance from global, regional, mid-tier, and community banks as well as credit unions. Its main findings, including the top challenges as compliance leaders see them and their plans to address them, align to two key themes:

A Changed Regulatory Environment—For Now: Survey respondents described a federal regulatory environment that feels streamlined for the near term, but which is part of a larger picture. While 88% of respondents said they have a clear view of federal regulatory priorities for the next three years and more than 90% plan to focus on material financial risks rather than process-heavy compliance, this shift is not reducing workloads. Nearly half (46%) of respondents expect compliance budgets to rise by at least 5% annually, driven largely by inconsistent state-level regulation and heightened scrutiny of emerging risks such as AI-enabled financial crime, digital assets, and geopolitical threats. After the survey was fielded, concern over the release of Anthropic's Mythos tool, including a special meeting with bank CEOs called by top regulators, illustrated the need to manage emerging risks. Many compliance leaders also warned that anticipated re-regulation under a future administration creates ongoing uncertainty and demands sustained compliance vigilance. While the favorable regulatory benefit could be expected to benefit compliance teams, survey respondents are not, in fact, abandoning their compliance framework because the underlying risks have not gone away.

A Changed Technology and Talent Environment—Here to Stay: Survey respondents highlighted technology-driven transformation as a defining compliance challenge over the next three years. The category of data privacy, cybersecurity, and information security ranked as the most resource-intensive area (78%), followed by digital assets (61%) and payment systems (58%), reflecting rising fraud, faster payments, and complex, multi-jurisdictional regulation. Strategically, institutions are prioritizing data analytics, automation, and AI governance. Compliance leaders emphasize pairing technology investment with workforce

upskilling, succession planning, and strong human judgment to sustain effective, scalable compliance programs.

Survey Background

The 2026 ProSight Compliance Outlook Survey casts light on the challenges in managing changing regulations, the complexities of fraud mitigation, the momentum of digital banking, and opportunities and threats presented by rapidly advancing AI. The leaders of financial institutions are always keenly aware of the risks and opportunities of any circumstance. To borrow from a saying from the U.S. national pastime: that's banking. But these days it's particularly hard to consider a positive development without seeing the potential negatives flashing red on the other side—and vice versa. Has looser federal regulation been a positive for financial institutions? Yes, the ProSight survey shows, but it has also prompted state regulators to fill in perceived gaps and created other complexities. And at the same time AI makes for frighteningly effective fraud and cyber exploits, it can be a force multiplier for compliance and risk management efforts to defend against those and other threats.

Christopher J. Boersma, ProSight Product Manager of Compliance with Learning and Development, describes the state of compliance work in 2026 as "operating in a paradox—lower federal oversight but higher, more complex compliance demands. Despite federal deregulation, compliance departments must maintain or boost compliance budgets to tackle emerging technology risks and rising state-level legislation and enforcement, while improving data quality and placing a larger focus on the recruitment and development of compliance talent."

This report is based on 150 responses to an online survey ProSight fielded in the first quarter of 2026. It features the perspectives of a range of compliance leaders—including chief compliance officers, chief risk officers, and other executives—from a group of financial institutions varying in size from small community institutions to global money center banks. Throughout, it highlights the top challenges and priorities of compliance officers and how they are being addressed.

A Changed Regulatory Environment—For Now

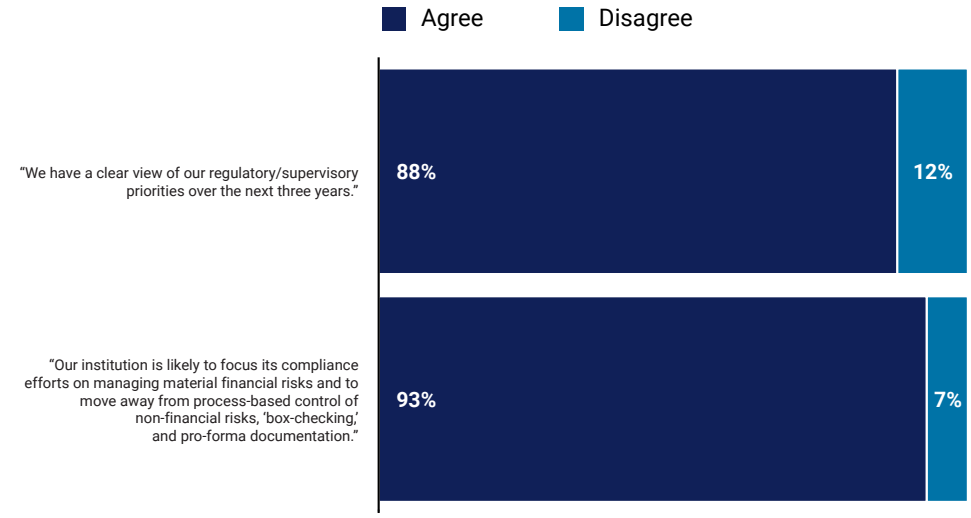
The headlines about a loosening of federal regulation—and the related relief that a reduced focus on check-the-box and non-financial risks brings—do not capture the whole story about the impact on financial institution compliance. Missing is the reality of some states stepping in where they perceive gaps in federal regulation, as well as the expectation of a future swing of the regulatory pendulum.

After a steady flow of pronouncements and rule changes from federal regulators, including an end to examining for reputation risk and a de-emphasis of non-financial risks in general, the vast majority of survey respondents—88%—agreed strongly or somewhat with this statement: "We have a clear view of our regulatory and supervisory priorities over the next three years." (See Figure 1.) Given that clarity, more than 90% said they are likely to focus on managing material financial risks rather than on "process-based controls of nonfinancial risks, 'box-checking,' and pro-forma documentation."

The headlines about a loosening of federal regulation—and the related relief that a reduced focus on check-the-box and non-financial risks brings—do not capture the whole story about the impact on financial institution compliance.

Figure 1. A confident, cautious regulatory outlook

A clear view of regulatory priorities and focus on material financial risks



"The current Administration's approach to U.S. federal bank regulation of financial institutions is likely to prompt..."

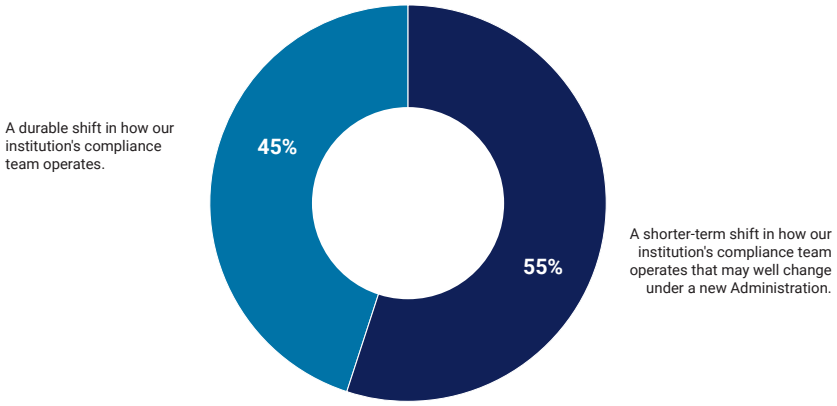
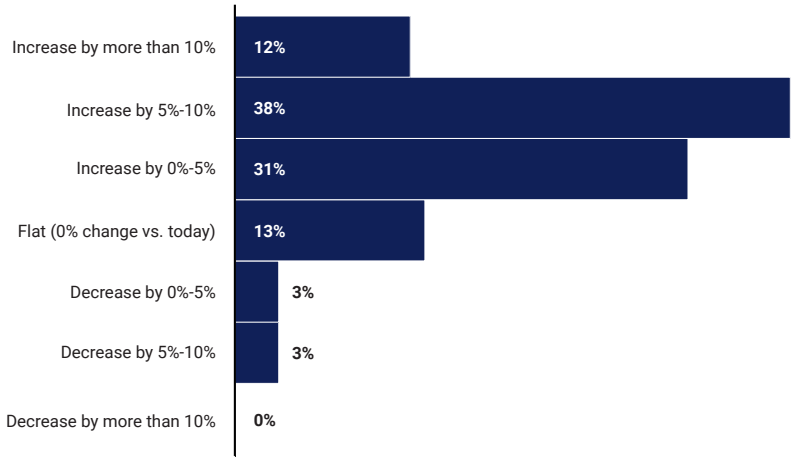
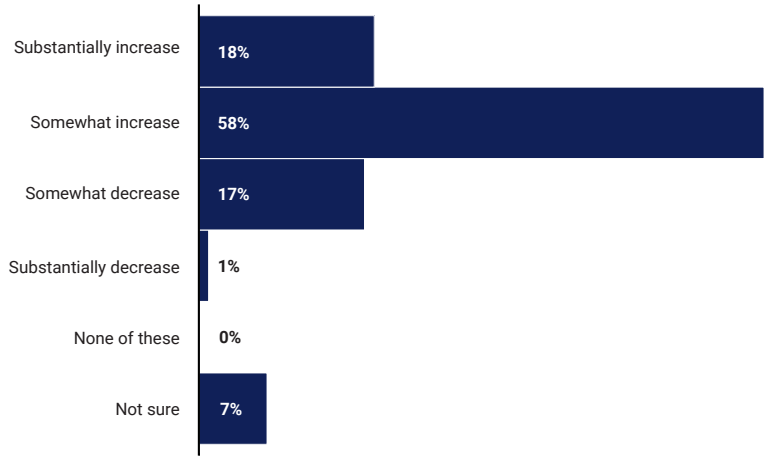


Figure 2. Compliance budgets will rise in the years ahead

What change, if any, do you expect annually in your regulatory compliance budget over the next three years?



The current Administration's approach to banking regulation is likely to _____ our compliance budget over the next three years.

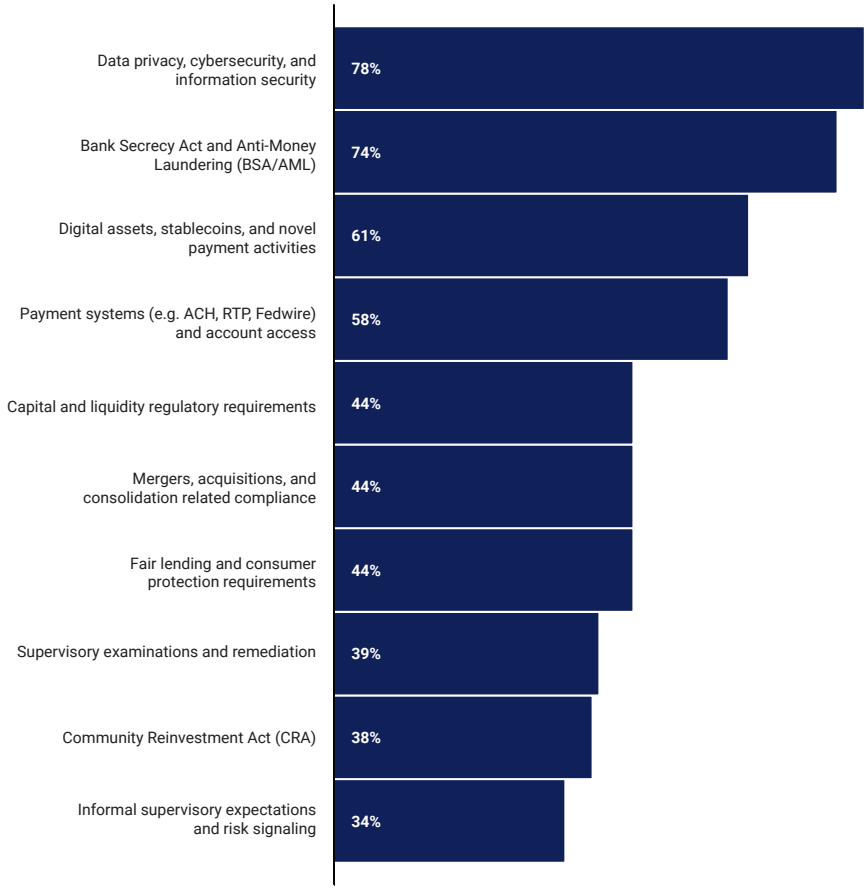


That shift, however, is not translating to a lighter financial institution compliance load, according to respondents. And respondents from smaller institutions were much less likely to express a very high level of clarity on their regulatory/supervisory priorities over the next three years compared with their peers from larger organizations. Only 11% of respondents from institutions with less than $25 billion in assets strongly agreed that they had a clear view on these priorities; 49% from banks over $25 billion said the same. (This ProSight report will be followed by additional articles detailing the differences in perspective among banks of various asset sizes; visit prosightfa.org to find them.)

Overall, half expected compliance budgets to rise by 5% or more annually over the next several years, while less than 10% anticipate lower budgets. (See Figure 2.) Seventy-six percent agreed with the statement, "The current administration's approach to banking regulation is likely to increase our compliance budget over the next three years," consistent with a concern expressed by some research participants that an unintended consequence of federal deregulation could be increased regulatory burden overall in terms of documentation and costs.

Figure 3. Information security and BSA/AML will require more time, attention, and resources from compliance teams

Over the next three years, which of the following regulatory and supervisory compliance areas are likely to require more time, management attention, and resources at your institution?



Boersma said financial institutions "are currently struggling to manage a fragmented regulatory environment, characterized by a conflict between federal deregulation and numerous and inconsistent state-level laws regarding AI, privacy, digital assets, and consumer protection."

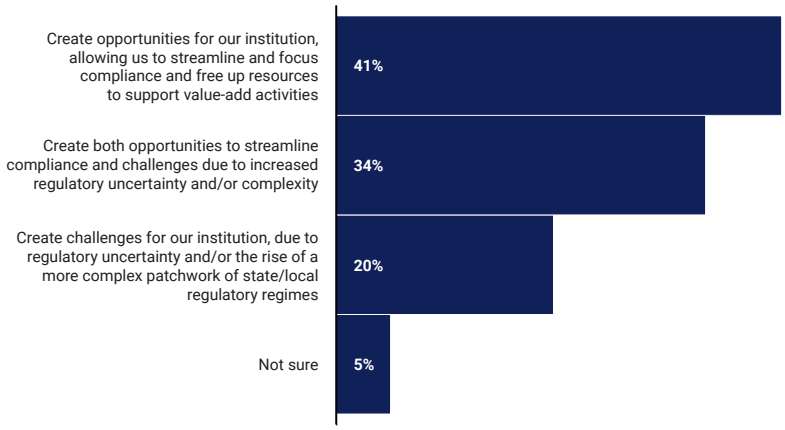
"This patchwork of requirements forces multi-state institutions to navigate conflicting compliance standards, resulting in significant operational challenges," he said. In a written survey response, a respondent from a California-based institution said, "We assume that the state will offset any decreases in federal compliance drag."

Compliance leaders are also grappling with the fact that certain areas of federal regulatory oversight are requiring more compliance activity. "It is crucial to note that while the intensity or breadth of some traditional regulatory expectations may decrease, there is a concurrent, heightened focus from regulators on emerging financial crime risks," a financial crimes executive at a global bank said. "This includes areas like the amplified AML/CFT risks posed by AI and deepfake technologies, the burgeoning digital asset markets, vulnerabilities within the non-bank financial institutions (NBFI) sector, and broader geopolitical risks." Nearly three-quarters (74%) of respondents said they expected compliance with the Bank Secrecy Act and anti-money laundering statutes to demand more time, management attention, and resources over the next three years. (See Figure 3.)

Several respondents, in written comments, noted that managing non-financial risk well remains crucial even if regulators are tipping their focus more toward financial risk. That point was highlighted after the survey was fielded, as alarm greeted the release of Anthropic's Mythos model. In response to concern about the AI tool's ease in finding software security vulnerabilities, Treasury Secretary Scott Bessent and Federal Reserve Chair Jerome Powell gathered large-bank CEOs for an April 7 meeting.

Figure 4. Deregulation offers freedom to manage risk and compliance concerns

On balance, the current Administration's approach to U.S. federal banking regulation is most likely to…



Adding to the complex picture: a potential shift to a different federal regulatory approach under a future presidential administration. More than half of survey participants (55%) see the current state as a short-term shift in priorities which may well change. (See Figure 1.) The chief risk officer of a Midwestern community bank said in a free-text response, "Our bank continues to evaluate systems and solutions that can improve our compliance risk [management]. Even with some easing of regulations, we anticipate the pendulum may swing back if there is a change in administration at the next national elections."

Another respondent, a senior compliance executive at a $500 million bank in the South, said, "With the uncertainty of what the regulatory landscape looks like under the current administration, we are trying to stay nimble and able to pivot easily in either direction (ramp up or down)."

There is also a question of how actions financial institutions are taking now—or not taking—could have consequences under a changed regulatory regime. "Lookbacks are common requests from BSA/AML examiners," a senior line of business leader at a global bank said. "Banks must anticipate re-regulation to mitigate the risk of a lookback—what did we miss during the less stringent regulatory environment?"

Said the CRO of a New England bank holding company: "We are acutely aware that our actions today will be judged by a new administration with a potentially different set of expectations."

In the meantime, though, many respondents believe the current regulatory approach does give them a freer hand to manage risk and compliance concerns in ways that best match their institutions' strategy and profile. On balance, 41% said the approach would create opportunities, 20% said it would create challenges, and 34% said it would do both while the rest of the respondents said they were unsure. (See Figure 4.)

Notably, respondents from banks below $25 billion were less optimistic as a group, compared with their larger peers. They split evenly on the opportunities versus challenges presented by the current regulatory approach at 27% each, while 43% selected both challenges and opportunities (4% were unsure). In contrast, half of respondents from banks above $25 billion said the approach would largely create opportunities, while 16% chose challenges, and 28% chose both challenges and opportunities (5% were unsure).

"My anticipation is that regulatory expectations for our institution will de-crease somewhat in the near term," the global bank financial crimes executive said. "This could translate into a slightly less intense supervisory approach in certain areas. Furthermore, we observe a growing global trend, especially within UK and EU regulatory bodies, towards 'simplification' and 'streamlining supervision,' which aims to reduce unnecessary burdens and foster more risk-based regulatory practices… potentially allowing for greater efficiency and a focus on high-impact areas."

A Changed Technology and Talent Environment—Here to Stay

As financial institution compliance activities and strategy adapt to a fluid regulatory environment, they also reflect profound changes brought about by the shift to electronic transactions, the rise of digital assets, and the growing capabilities and reach of artificial intelligence.

Technology and technology-related concerns figured prominently when survey respondents were asked to name the regulatory and compliance areas that will receive the greatest attention in the next three years, as well as the areas that will get the most strategic focus and resource investment.

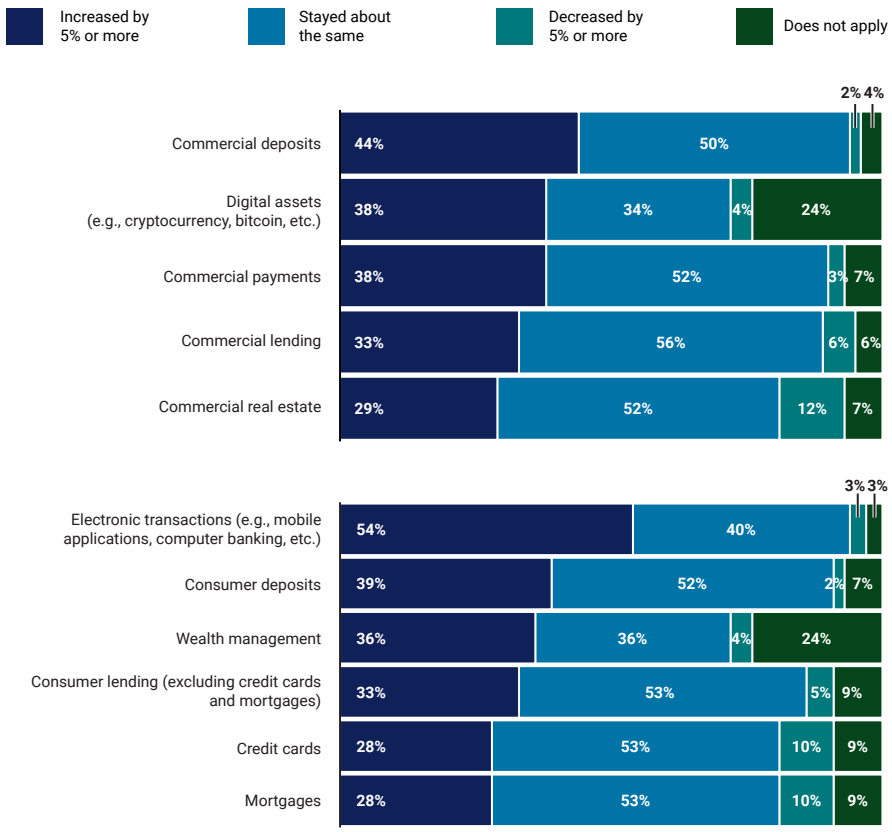
Data privacy, cybersecurity, and information security was the most-selected category (78%) when respondents were asked about the compliance areas that will demand the most time, management attention, and resources over the next three years (See Figure 3). The digital assets category was selected by 61%.

"Digital assets are significantly increasing compliance costs for financial institutions by forcing them to adapt to rapidly evolving and complex federal and state regulatory frameworks," Boersma said. "To mainstream digital assets, firms are investing heavily in specialized technology and upgraded systems to manage elevated financial crime risks, such as money laundering and tax reporting deficiencies, and blockchain transactions across state and federal borders."

Digital assets was another notable area of distinction between banks above and below $25 billion: 49% of respondents from the larger institutions said their compliance budget for digital assets increased by 5% or more this year, while only 22% of respondents from smaller institutions saw a similar increase.

Figure 5. Substantial budget increases for compliance tied to electronic transactions

Across your overall organization, how did your budget change for each of the following compliance areas in fiscal year 2026 compared to fiscal year 2025? (Please choose one in each row.)



The category of payment systems (such as ACH, RTP, and Fedwire) was selected by 58% of respondents, while 54% said compliance spending regarding electronic transactions—prime targets for fraud, especially as faster payments make recovering funds exceedingly difficult—increased more than 5% from 2025 to 2026, as shown in Figure 5.

"Fraudsters shift constantly and crime evolves as quickly as new financial products become available," said a senior line of business executive at a community bank in the Southwest. "It takes focus and investment to stay ahead of financial crimes."

Boersma said that in this increasingly challenging environment, "many banks are enhancing internal cooperation between their cybersecurity and anti-fraud teams and seeking information about the latest exploits from peer institutions and groups like ProSight's Fraud Alert Network."

In a world where deep-fake and other AI-enabled attacks are proliferating, getting cheaper for bad actors to launch, and supercharging cyber exploits "we need to enhance fraud detection and prevention at all phases and end-points of the client lifecycle," said the chief risk officer at the New England bank holding company.

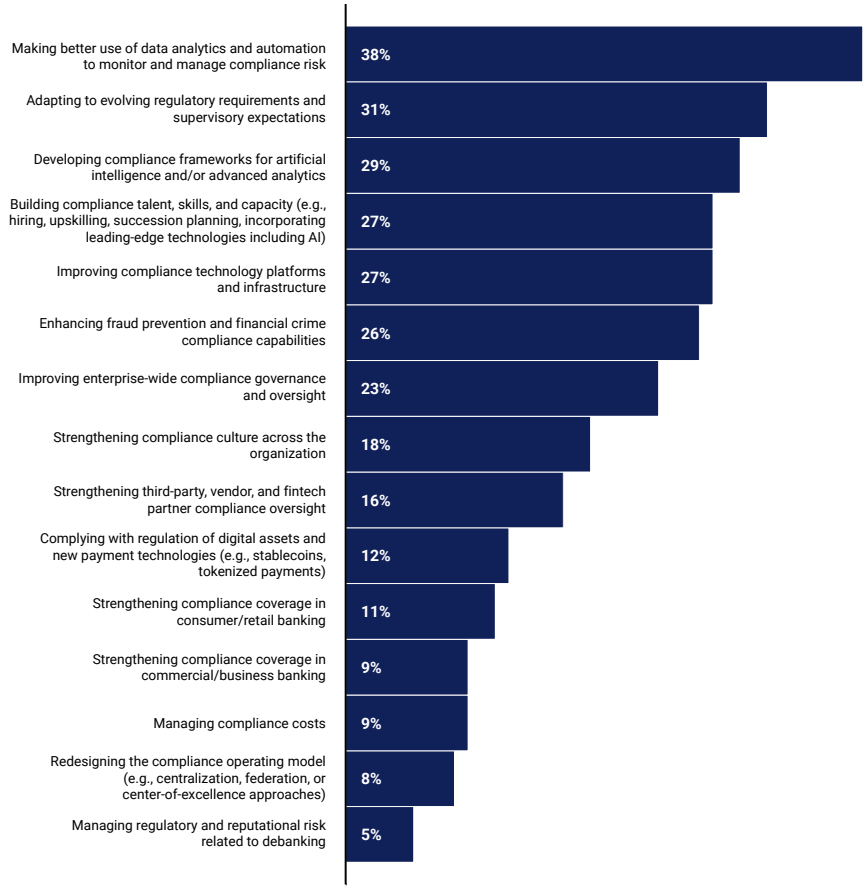
A senior compliance officer at a small credit union said, "We will continue to work with our third-party fraud monitoring vendor to utilize their capabilities to the fullest extent. All staff will continue to receive extensive training in the areas of fraud and financial crimes."

Regarding areas of greatest strategic focus and investment for compliance activities over the next three years, 38% of respondents—the top response—selected "making better use of data analytics and automation to monitor and manage compliance risk" as a top priority (see Figure 6). Twenty-nine percent cited "developing compliance frameworks for AI and advanced analytics."

"We will continue to work with our third-party fraud monitoring vendor to utilize their capabilities to the fullest extent. All staff will continue to receive extensive training in the areas of fraud and financial crimes."

Figure 6. Compliance teams focus on technology and talent development

Over the next three years, which areas will receive the greatest strategic focus and resource investment within your compliance organization?



"Making better use of data analytics and automation is a core strategic initiative for how our organization monitors and manages compliance risk," a senior global bank executive said. "Our focus and investment in this area are designed to enhance the precision, efficiency, and scalability of our risk management processes, moving beyond traditional manual methods."

A senior compliance executive at a regional bank said, "We are investing in advanced data analytics and automation to continuously monitor compliance risks, identify anomalies, and surface emerging issues earlier. By automating controls, reporting, and testing, we aim to improve accuracy, reduce manual effort, and enable more timely, data-driven decision-making across the compliance lifecycle."

New technology is essential, said a respondent from a global bank, due to the massive amounts of data generated by auditors and other functions: "This is key to any improvement to current audits and audit functions. As the technology scales up and information increases, we must use data analytics to keep up with the scale of information now being produced."

Respondents expect to ramp up AI use to help them meet their compliance goals. Importantly, that includes training employees to use AI effectively—understanding how inputs influence AI outputs, and how to assess the quality of those outputs. The global bank executive noted a "firm-wide effort to integrate AI, as demonstrated by initiatives like mandatory AI prompt training and the deployment of AI agents to improve productivity, ensuring our teams have the necessary institutional and technological understanding to address new risks."

The aforementioned global bank senior line of business officer said that amid all that AI, "We need talented humans to tell our compliance story—what we do well, what are our weaknesses, what we do to mitigate risk."

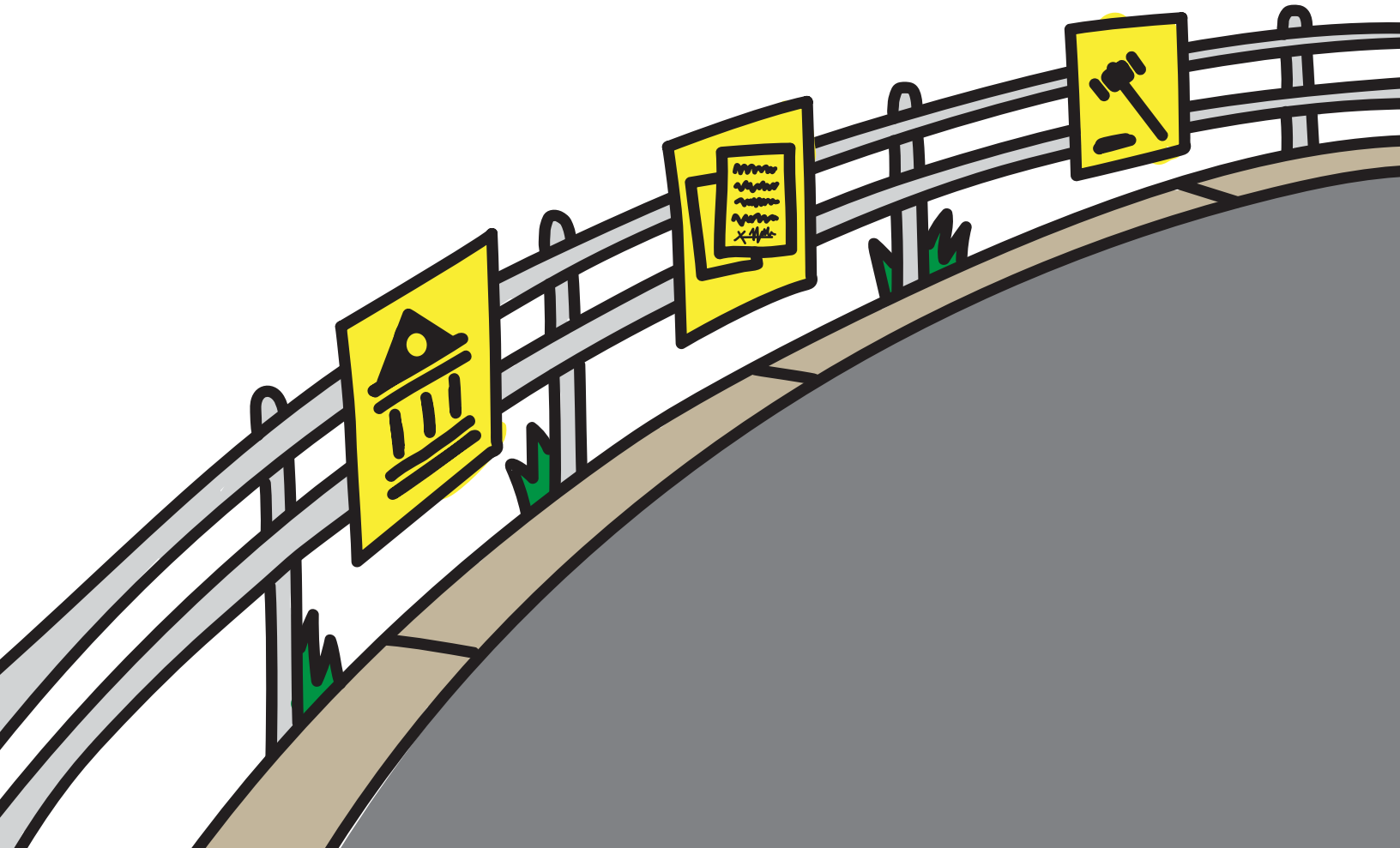
Respondents cited a need to develop expertise and "bench strength" to support growth and backfill retiring experts. The regional bank senior compliance executive said, "We are investing in compliance capability through targeted hiring, focused upskilling, and clear succession planning. This includes building regulatory and leadership depth while leveraging AI and advanced analytics to increase efficiency, scalability, and proactive risk management."

Similarly, the chief compliance officer at a mid-tier bank in the East said, "Strengthening compliance talent and capacity will be a priority in 2026. By investing in skill development, role clarity, and scalable resourcing, we aim to enhance program effectiveness, reduce key-person risk, and better support sustainable growth."

Closing Thoughts

Taken together, the 2026 ProSight Compliance Outlook Survey findings underscore a compliance environment defined by regulatory relief but also sustained complexity and enduring transformation. While many institutions welcome near-term clarity and a more risk based federal regulatory posture, state-level activity, heightened enforcement in areas such as AML, and the strong possibility of regulatory reversal demand continued vigilance.

At the same time, technology change is not cyclical—it is permanent. The rapid growth of digital assets, faster payments, AI, and AI-enabled fraud are forcing institutions to invest simultaneously in advanced analytics, cybersecurity, and human expertise. As one respondent warned, adversaries evolve as fast—or faster—than financial innovation, requiring constant attention at every point in the client lifecycle. The institutions best positioned for the future will be those that remain nimble, anticipate re-regulation, and pair technology investment with strong governance, skilled talent, and disciplined judgment—ensuring compliance remains resilient, credible, and strategically aligned regardless of how the regulatory pendulum swings.



About This Report

In the first quarter of 2026,* ProSight surveyed 150 leaders with responsibility for compliance at financial institutions varying from small community institutions to global money center banks in the United States and Canada. The inaugural annual ProSight Compliance Outlook Survey sought perspectives on the top challenges and priorities of practitioners including chief compliance officers, chief risk officers, and other executives.

Represented institutions by asset size

- Less than $25 billion: 44%
- $25 billion-$50 billion: 12%
- $50 billion-$100 billion: 11%
- $100 billion-$250 billion: 10%
- $250 billion-$500 billion: 6%
- $500 billion-$1 trillion: 9%
- More than $1 trillion: 8%

Positions held by respondents

- Chief compliance officer or equivalent: 24%
- Senior compliance executive (e.g., EVP, SVP): 18%
- Compliance executive (e.g., VP, Director): 16%
- Head of a line of business (e.g., divisional CEO, EVP, SVP): 16%
- Senior risk management executive (e.g., VP, Director): 10%
- Chief risk officer or equivalent: 5%
- Senior line of business executive (e.g., VP, Director): 4%
- Information technology executive: 2%
- Senior corporate finance executive (e.g., EVP, SVP): 1%

**This survey was fielded prior to Treasury Secretary Scott Bessent and Fed Chairman Jerome Powell's April 7 meeting with large-bank CEOs about Anthropic's Mythos release. The new AI tool caused alarm over its unprecedented ability to find security vulnerabilities in software.*

ProSight™

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