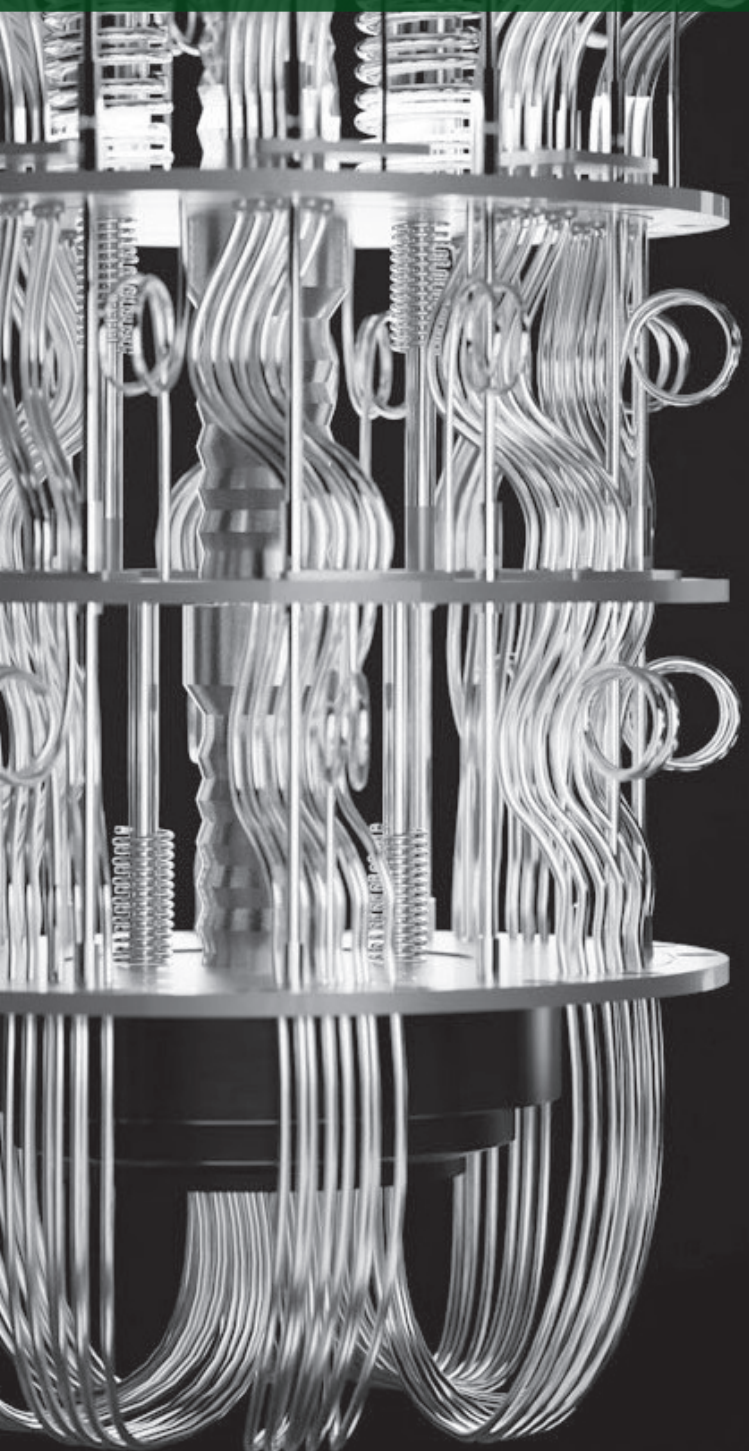
ProSight | ProSightFA.org

January 2026

The ProSight

Executive Report

A ProSight Financial Association Publication



Technology Transformation in Banking

Including:

Tech transformation with an eye on remediation

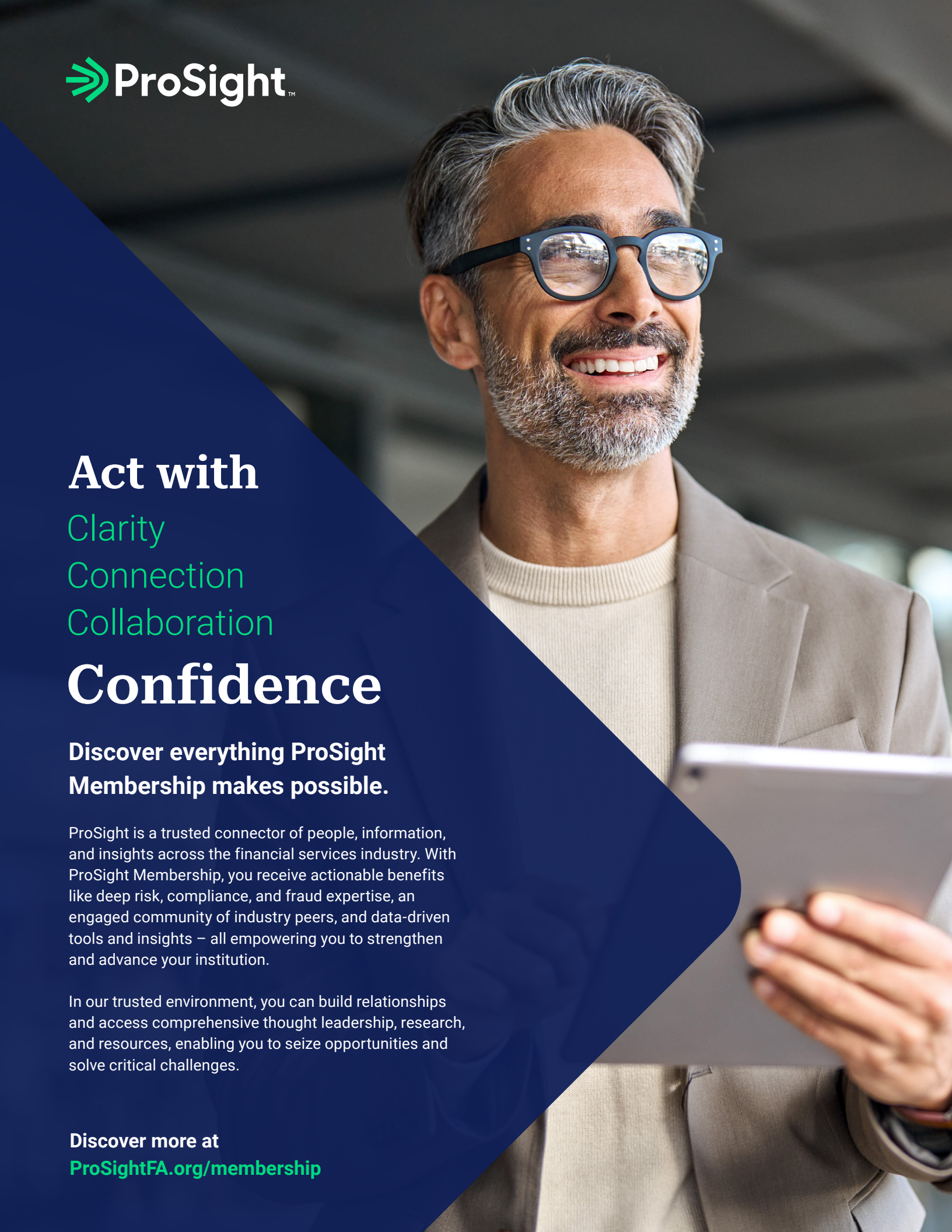
Business-as-usual tech can be an albatross for the industry when promising new solutions are coming to market. Outdated infrastructure drains resources, sloppy architecture yields silos, and neglected data hobbles efforts to create value. Technologies such as agentic AI, blockchain and quantum computing are forcing institutions to examine old habits borne of urgency to fix how they approach transformation.

Sure, cleaning up legacy tech and processes doesn't make headlines. But as we learn in this month's Executive Report, to "keep up with the Joneses" on innovation, banks need to have one eye on the horizon and another on the road behind them to prepare for the possibilities and perils new technology presents.

Michael Bender
Senior Editor,
ProSight Financial Association
mbender@ProSightFA.org

In this issue

ProSight™



Act with

Clarity

Connection

Collaboration

Confidence

Discover everything ProSight Membership makes possible.

ProSight is a trusted connector of people, information, and insights across the financial services industry. With ProSight Membership, you receive actionable benefits like deep risk, compliance, and fraud expertise, an engaged community of industry peers, and data-driven tools and insights – all empowering you to strengthen and advance your institution.

In our trusted environment, you can build relationships and access comprehensive thought leadership, research, and resources, enabling you to seize opportunities and solve critical challenges.

Discover more at
ProSightFA.org/membership

Snapshots

CROs' top concerns; an updated Tech Risk Framework; and AI creators and doers.

CROs see risks converge in cyber-security, fraud, and AI

Technology and cyber risk now sit at the center of numerous banking challenges—and they're increasingly fueling fraud. In ProSight's 2026 CRO Outlook Survey, 74% of respondents ranked technology and cyber among their top five risks. CROs said the ongoing push toward digitalization and AI gives bad actors more ways in, while connecting new systems to old infrastructure creates integration weak spots. Geopolitical risk—named a top risk by 22% of respondents—adds another layer, as nation-states target critical infrastructure like financial services.

Fraud is increasingly AI-enabled. Fraud and financial crime ranked No. 2 on the list of top risks, named by 55% of respondents, and survey comments stressed the interplay with cyber, AI, and geopolitics. A large bank CRO warned: "If you combine cyber, AI, and what will happen in the coin space, you will see a faster proliferation of fraud. The threat actors are going to be able to move more nimbly than the governance." Real-world attempts are getting harder to spot. The same CRO said a fraudster emailed a client while impersonating him—the message "read like an email I would send. It was near flawless." Nearly a third of respondents (32%) said the possibility that AI could be used to perpetrate fraud was a top AI-related risk.

Third-party risk is the fault line. Given the expanding attack surface, about a quarter of respondents identified operational resiliency as a top risk. One large-bank CRO called out third-party exposure specifically—both as a gateway for exploits and as a reason banks may need to sever connections quickly during an incident to contain spread. The through-line for leaders: shore up resiliency where your digital business is most exposed.

Verification is the countermeasure. Banks are moving AI from pilots to production—54% have adopted AI in production—but governance is still catching up. Only 12% of respondents said their AI governance and approvals framework is "highly developed." Nearly a third (32%) named the possibility that AI could be used to perpetrate fraud as a top AI-related risk. As one large-bank CRO put it: "We want to make sure everyone in the company understands the risks that may be present in using AI and not doing it blindly, ensuring there is a human in the loop."

Executive takeaway: Cyber, AI, and fraud are converging—treat them as interconnected risks. Prioritize third-party exposure, identity/verification, and human-in-the-loop AI.

Read more on what CROs told ProSight in its annual survey

-Frank Devlin

A framework for managing the risks of new technology

Adding new technology without a plan for evaluating and managing associated risks can expose an institution to unwanted vulnerabilities and undesirable outcomes.

ProSight's revised Technology Risk Framework reflects five years of member feedback and hard-won lessons. The update builds on the original 2020 tool by refining terms, adding flexibility for different risk taxonomies, and stressing a point many banks are still learning: technology risk isn't just IT's problem. The revision also offers practical guidance institutions can use to strengthen oversight and prepare for what's next.

Rethink who owns tech risk. "Technology [teams] and technology risk are not one and the same," said Erika Crandall, chief risk officer at Xpansiv Limited. The revised framework makes clear that every business line takes on risk when it relies on technology. By leaving organizational charts out of the picture, the document reinforces that responsibility is shared across the enterprise.

Use the taxonomy as a roadmap. The framework provides an exhaustive list of risk categories to help institutions identify and classify exposures—from operational disruptions to third-party service provider risks. For mature institutions, the revision serves as a sense-check on coverage. For those just getting started, it's a roadmap with definitions and examples to help build a foundation.

Start small but measure consistently. Measurement is where many banks struggle. "Knowing what to measure is hard. Knowing what information to bring to leadership is hard," said Joshua Henrich, SVP and head of information security governance and risk management at U.S. Bank. Companion guidance suggests focusing on metrics that connect directly to enterprise risks. Smaller banks should narrow in on a handful of key risk indicators that can be tracked reliably. "You start with a handful that are the most meaningful to your organization, that you can measure with a high degree of confidence," Crandall said.

Connect technology and enterprise risk. While the framework distinguishes technology risk from other categories, it links directly to ProSight's Enterprise Risk Management Framework. Used together, they encourage banks to think holistically about risk appetite and interdependencies across the organization.

Keep evolving. Technology risk won't sit still, and neither should risk management. "This is ever-changing, and we'll adapt to the changing needs of the industry," Henrich said. The framework is meant to evolve with member input, giving banks a tool that can mature with them.

Read more about ProSight's Technology Risk Framework.

-Michael Bender/Dan Washburn

Creators and doers: AI's digital helpers

Generative artificial intelligence (gen AI) is *sooo* 2025. While financial institutions continue to mine value from significant investments in the technology, agentic AI is increasingly where it's at. A study from Google Cloud conducted in the second quarter of 2025 found that more than half of financial institutions (53%) are already using AI agents in production. Just under half (49%) said their institutions will allocate 50% or more of their future AI budget to developing agentic AI.

Attracted by agentic's ability to initiate and complete tasks on its own, banks are building agents to run processes throughout the enterprise to improve efficiency and address strategic priorities.

What's emerging are "digital employees" and "multi-agent teams (or squads)" responsible for everything from data management to fraud detection.

Agentic AI and gen AI offer fundamentally different capabilities, but both rely on large language models (LLMs) for their outputs. Agentic AI plans, performs and decides how to execute tasks using reasoning and understanding derived from LLMs. It can act autonomously or with minimal human oversight—a doer—breaking down goals into steps and self-correcting with user and system input.

Gen AI, meanwhile, triggers only when prompted. It creates text, video, pictures, code, etc., using patterns identified from large samples of external content. It works only when asked to and depends more heavily on human inputs and/or oversight—a passive creator. Agentic AI might incorporate gen AI prompting into its task sequences, using the outputs to take its next action.

Given agentic AI's versatility, banks are using it for hyper-personalized financial guidance, just-in-time service marketing and tailored advice. In contact centers, virtual assistants and chatbots are handling complex customer interactions and routing challenging calls. Increasingly, institutions are using it to monitor customer behavior, identify sophisticated fraud and flag potential threats. More research from Google Cloud shows that AI has already demonstrated the ability to detect two to four times more confirmed suspicious activities.

-Michael Bender

Putting Quantum in Context After FS-ISAC's Cryptography Warning

Views might differ on when quantum will be ready for primetime, but financial institutions need to prepare for it now.

By Frank Devlin

In September, the Financial Services and Information Sharing and Analysis Center (FS-ISAC) released "The Timeline for Post Quantum Cryptographic Migration." The white paper warns of "crypto-procrastination," and urges the industry to appropriately develop and implement the post-quantum cryptography (PQC) that will be needed to protect systems and data in a quantum world. "The time to prepare for quantum computing is arguably growing shorter, and the risks to security and resilience are clear," the paper says, calling for global coordination and a common timeline for PQC.

We recently interviewed Dean Yoost, author of the RMA book "Exponential Technologies Require Critical Thinking in the Boardroom," for his perspectives on quantum's risks and opportunities for banks, and how financial industry leaders are addressing it. Among other roles, Yoost is a past board member for Pacific Life Insurance Company and MUFG Union Bank and

currently serves as an advisory board member of the American Honda Finance Corporation.

Q: Is there a danger that, with so much technology focus on AI, quantum computing could be overlooked? Are you seeing any evidence of this now?

A: Generative AI is dominating boardroom agendas today. There is a growing risk that the near-term focus on AI could crowd out attention to quantum computing. That would be a mistake. Quantum brings two simultaneous realities: (1) a strategic opportunity for advantage in industries including financial services and (2) a systemic risk to today's public key cryptography and long migration timelines. Multiple regulators and standards bodies are publishing quantum-safe road maps and deadlines. Boards that only address AI will be late to the quantum opportunities and unprepared for the risks.

Almost all board and CEO surveys rank generative AI at or near the top of strategic priorities, signaling potential crowd-out for quantum readiness. In contrast, according to a 2025 survey by the quantum computing firm QuEra Computing, over 65% of businesses report being prepared or very prepared to adopt quantum computing within the next 2-3 years. Directors and management should consider benchmarking against peers to avoid being late to the quantum computing opportunities or unprepared for the emerging risks.

Q: What is the level of concern and attention in C-suites and boardrooms regarding quantum right now?

A: C-suites and boardrooms are showing rising but uneven attention toward quantum, balancing growing opportunities about its transformative potential with concern over the emergent risks. Most organizations remain in early awareness or pilot phases. The greatest area of boardroom concern is quantum-related cryptographic risk, especially the threat of "harvest now, decrypt later" attacks that could expose sensitive data once quantum computers achieve cryptographically relevant capability. Global regulators and industry bodies are urging businesses to begin quantum readiness planning, including migration to post-quantum cryptography and scenario analysis. Meanwhile, directors and management recognize potential competitive advantages in optimization and risk modeling. The boardroom discourse is shifting from speculative curiosity to strategic vigilance, as those in the boardroom increasingly demand risk mapping, vendor diligence, and quantum-safe transition roadmaps to ensure resilience and future readiness.

Q: The FS-ISAC paper talks about the need for cooperation among financial institutions and the regulators. What can individual banks do to prepare?

A: Banks need to begin developing a quantum readiness plan that aligns with their longer-term digital and cybersecurity goals. This includes establishing an internal task force to monitor advances in quantum technologies and their implications for encryption, data protection, and financial modeling. Banks should inventory which parts of their infrastructure rely on cryptographic protocols that could be rendered vulnerable by quantum attacks and start transitioning toward quantum-resistant algorithms. Investing in relationships and partnerships with quantum research institutes and technology providers can help banks recognize the emerging opportunities in quantum-enhanced risk modeling, portfolio optimization, and fraud detection.

> "Few, if any, financial services companies develop their own cryptographic tools."
>
> Dean Yoost, author, *Exponential Technologies Require Critical Thinking in the Boardroom*

Education and training programs for directors, management, and IT and risk management staff are essential to build organizational awareness and capability. Banks could also engage with the regulators to ensure compliance and contribute to the development of industry-wide standards for quantum.

Q: Can you discuss, to the extent possible in layman's terms, how quantum might enable fraud and financial crime?

A: Quantum computing could make it easier for bad actors to commit financial fraud by breaking the encryptions that currently protect sensitive banking data and online transactions. Most of today's security systems rely on mathematical puzzles that even powerful legacy computers could take centuries to solve. A quantum computer, however, could solve these puzzles in seconds or minutes, allowing hackers to access confidential customer information, manipulate digital records, or impersonate authorized users. This means that without quantum-safe encryptions, banks could see their defenses suddenly become obsolete, opening the door to large-scale theft, fraud, and financial crimes.

Q: What can banks do now regarding their cryptography processes to start preparing for quantum?

A: Few, if any, financial services companies develop their own cryptographic tools. The vast majority are dependent on third parties. As such, emphasizing third-party risk management with the appropriate inventory of cryptographic use across the business and vendor due diligence is essential.

Banks can begin preparing their cryptography processes for quantum by conducting a comprehensive inventory of all cryptographic systems

currently in use, including data-in-transit and data-at-rest. They can identify which systems rely on public-key algorithms that are most vulnerable to quantum attacks, and prioritize these for transition planning. Banks should start testing and piloting post-quantum cryptography algorithms recommended by the National Institute of Standards and Technology (NIST), ensuring interoperability and performance under real operational conditions. Banks can also develop governance frameworks, staff training, and vendor requirements that embed quantum readiness into their longer-term cybersecurity strategies. The readiness of vendor requirements should begin immediately as current contracts are renegotiated. The guidelines in preparing for post-quantum cryptography created by the Department of Homeland Security and NIST in 2021 provide useful steps to start preparing for quantum.

Q: Who are likely to be the bad actors? Will quantum computing require infrastructure and hardware that would only be available to big companies and nation-states? Would exploits in the early days of quantum likely be by terrorist groups/nation-states?

A: In the early days of quantum computing, the most likely bad actors will be state-sponsored groups, cybercriminal organizations, and advanced hacking collectives seeking to exploit the transitional period before quantum-resistant encryptions are widely implemented. Nation-states with significant resources are likely to target banks, government systems, and critical infrastructure to gain advantages through data decryption and espionage. Sophisticated cybercriminal networks could focus on harvesting encrypted data today to be exploited once quantum machines become capable of breaking the current cryptographic defenses. The combination of geopolitical ambition and criminal profit incentives seems to make these bad actors the most dangerous in the transition to quantum.

Q: What kind of timeline are we looking at in terms of when quantum will be developed enough to be put into use?

A: Most experts agree that broadly useful quantum systems remain some years away. They generally place practical quantum advantage—the point when quantum computers exceed the capabilities of supercomputers—in the 2030s, while Google's leadership recently claimed that commercial quantum applications may surface within five years. But the future could arrive sooner than expected, so board members and management need to evaluate the potential impact of quantum on the industry and their business—and prepare for it.

This interview has been edited for length and clarity.

Frank Devlin is editor-in-chief of the ProSight Journal and a ProSight senior editor.

Building Banking's Future While Carrying Technology's Past

With promising technologies here and on the horizon, institutions see legacy software and infrastructure cluttering paths to innovation.

By Michael Bender

Banks named technology their top 2026 investment priority, voting with their wallets as advanced digital and data strategies drive change in the industry. Institutions are cleaning up obsolete code, consolidating and enhancing current capabilities and anticipating investments in game-changing technologies as part of ongoing digital transformation efforts.

All the while, they're carrying burdening technical debt, a de facto tax on innovation and growth. By some estimates, technology maintenance consumes 50% to 70% of Tier 1 banks' technology budget—dollars spent running the bank instead of growing it.

"Technical debt is anything that hinders a company from prosecuting its markets more

aggressively or anything that shackles the engineering footprint," said Ryan Lockard, principal in Deloitte's engineering practice and head of engineering for the banking and capital markets segment.

Tech maintenance costs represent one clear measure of technical debt and broadly they are rising year over year at most banks, Lockard noted.

While not strictly betting the bank (h-hmm) on technology, institutions increasingly view tech transformation, agility and modernity as the path to differentiation and growth—and a journey of constant reinvention. It's crucial for creating sustainable business value and satisfying a demanding customer.

With consequential technologies such as blockchain emerging and last year's must-haves like Zero Trust cybersecurity still in implementation, deciding which capabilities deserve attention—and which to update—will be essential to charting a course for business, competition and customer satisfaction, industry professionals say.

"There's an opportunity cost," said one head of information security governance and risk management. "What features would you have to give up the time and cost for in order to upgrade" out-of-date systems and infrastructure? Importantly, he added, are the older systems so brittle that they present a security risk or prevent the company from building advanced technologies on top of them?

As technology rapidly advances, keeping up with the state of the art partly depends on banks' ability to move on from the primitive parts of their tech footprint and redesign operations. And it means moving fast, before the newest technology replaces the newer technologies that banks are still studying.

Among 1,000 senior banking leaders surveyed in the ProSight Banking Outlook: 2026 Trends study, a majority (57%) named technology integration and platforms as a top-three investment priority this year. Half (50%) picked customer digital experience (50%), and about a third (35%) chose fraud mitigation—both heavily technology dependent.

But transformation can be tricky without fixing the fundamentals first.

Cleaning up: Data disarray and technical debt

"Banks often aren't spending their technology budgets on the hard problems," Lockard said of the challenges banks face when balancing the obligations of retiring technical debt with building the next big thing. Competitive pressures force banks to "keep up with the Joneses" when developing new market-facing features and functionality, he said. This adds to maintenance burdens and kicks technical debt clean-up further down the road.

For an if-it's-not-broken-don't-fix-it industry still running critical processes on mainframe computers, removing technical debt can be a heavy lift, especially when these systems' designers moved on long ago. Still, banks keep these monoliths, Lockard said, "because their biggest flaw is that they just keep working."

Reverse engineering code is the easy part; understanding and recreating the systems' intent and building stability and resiliency into their replacements are the primary goals when re-architecting for future development and operating needs.

Another critical issue financial institutions face can be a messy data house. A product of siloed systems, weak data governance and technology-led data management, the sometimes-chaotic state of banks' data has made it harder to optimize AI and personalization capabilities—key ingredients in improving efficiency and creating fine-tuned services for consumers.

> "More than half of the ProSight survey's bank respondents described their digital customer experience as average or worse."

With the data dependencies of generative AI models, and the opportunities emerging to customize and personalize just-in-time customer services, banks are getting more serious about putting their data houses in order, experts say. In ProSight's survey, banks said that the top way they could improve their customers' experience is by making better use of data for product and service recommendations.

Consolidating: Customer experience, cybersecurity

For most, a better digital experience is the key to pleasing customers. In ProSight's Consumer study, for instance, 58% of Generation Z respondents said they would switch financial services organizations for better mobile banking app/digital capabilities.

It's an area where banks admit they're falling short. More than half of the ProSight survey's bank respondents described their digital customer experience as average or worse. And they cited digital as their biggest gap overall in customer experience, far underperforming in-person interactions.

Protecting customers' information and accounts is a continued priority. Fraud fighting and new tools and tactics are on banks' roadmaps, and new technology, again, can help. Among the top uses for gen AI at banks is fraud detection and prevention, a white-hat application of the

technology to combat the rise in its black-hat uses by cybercriminals.

Cybersecurity was a leading risk in ProSight's 2026 Chief Risk Officer Outlook Survey, with 74% of respondents citing it as a top-five risk, edging out second-place fraud. As threat actors change tactics, the industry must continually adapt and upgrade defenses, leading respondents to name cyber risk the second-most important emerging risk (areas most likely to be or remain top risks over the next two years) in the study. Implementing approaches such as Zero Trust security—based on the principle of "never trust, always verify" every user and device—is among the steps banks are taking to keep pace with ever-changing security threats.

Even then, visibility and control can be challenging as technology estates extend beyond internal systems. While vendors increasingly are a pathway to technical progress, they're also a backdoor to risk. "We can spend a lot of time cyber protecting ourselves, but you need only one weak link and things can go really wrong," said one big-bank CRO.

In areas such as model risk, improving contract language with vendors upfront can lead to better visibility into inputs and work practices and help banks better manage these third-party risks, bankers say.

Enhancing: Path to productive AI

More banks are using AI in their operations. The percentage of CRO survey respondents whose banks don't use it or who didn't know whether they used it declined to 24% in 2025 from 38% a year earlier. In every area of the institution the survey identified, bank use of AI increased year to year, with its application in internal modeling more than doubling to 47%. Its second-widest use is in identifying and reducing fraud (44%).

Coordinating efforts at the enterprise level, though, remains challenging, creating whack-a-mole conditions for governance teams as siloed groups test run their own applications. Banks are investing a lot of energy, CROs on a recent RMA NYC Chapter event panel said, in categorizing AI use-case risk to manage the "avalanche" of innovation and clear the lowest-risk applications to go live.

Whether great expectations of efficiency and profitability for gen AI pan out remains unclear. Volatile market prices for AI-related providers' stock recently illustrate a wavering belief that returns will match frenzied spending—a "bubble" is what most now fear.

CROs on the RMA Chapter panel said they model the likelihood and bursting of a potential AI

> “Traditional banks are partnering with third parties to accelerate business strategies, drive growth, manage costs and enhance offerings.”

“bubble” in their scenarios as the industry plows ahead with trillions of dollars of estimated AI capital spending over the next few years. The presumption among banks is that AI will make them a lot of money, “but what happens if the AI bubble really is a bubble, and we find out it won’t make us any money?” said one CRO.

Meanwhile, if last year’s adoption imperative in AI was generative, the industry is rapidly advancing this year to agentic AI, lured by its workflow orchestration and decision-making abilities. While gen AI is passive, relying on human prompts, agentic AI is proactive, taking initiative on its own to help move work forward faster. Software and platform company Splunk calls agentic “a fundamental shift from prompt-driven intelligence to a focus on proactive outcomes.”

For banks, agentic AI can create capable “digital employees” that aren’t just workflow companions to humans, but are autonomous doers, capable of performing tasks independently.

And these agents can be allies in efforts to clear technical debt. Lockard described applying a digital agent to remediating old code. What took seven people two weeks took one agent three days, “getting more juice from the squeeze,” he said, while explaining the prescriptive nature of the task and the importance of having tightly managed guardrails to review the agent’s outputs.

Almost 80% of respondents in the ProSight banking survey said their institutions work with vendors that use AI. More than a third of those said working with those third parties made it harder to do business, echoing concerns about the opacity of third-party technology and the risks associated with the technology relationships of those vendors.

Traditional banks are partnering with third parties to accelerate business strategies, drive growth, manage costs and enhance offerings. That includes acquiring fintechs to bring niche services in-house and consolidating platforms to scale and compete more efficiently. In ProSight’s 2026 Trends Survey, 61% of respondents said they plan either to collaborate with or acquire fintechs in the year ahead. More than half said they would apply lessons learned from fintechs to develop similar in-house capabilities.

Innovations such as cash-flow-based underwriting and better credit scoring are helping to shape the industry under open-banking mandates,

while embedded finance is creating new business models for banks by integrating financial services into nonfinancial platforms.

Anticipating: Digital assets, blockchain, quantum

While payment services are banks' bread and butter, changing standards, upstart competitors and new payment rails are upending what for decades had been an essential and plain-vanilla bank offering. Institutions spent 2025 upgrading systems to meet the mandated ISO 20022 standard and hope to offer new services based on its enhanced transactions and customer data reporting requirements. Meanwhile, fintechs and challenger banks continue to gain ground in payments with a disciplined approach to customer experience, data analysis and personalization.

But the potentially earthshaking change in payments is regulatory approval of stablecoin issuance through the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act and growing policy and market support for blockchain-based financial networks. Deciding strategy for digital assets generally is a near-term imperative. On stablecoins, banks have choices to make: become an issuer, join a consortium, support the stablecoin ecosystem and/or pursue tokenized deposits.

In the meantime, global payments provider SWIFT is piloting a blockchain-based payments platform for digital assets to enable real-time, 24/7 cross-border payments, which experts say could work well alongside existing bank payment rails.

As with AI, developments in quantum computing present both opportunities for and threats to the industry. Quantum computers can perform complex computations at speeds unimaginable with current computing technology. Financial institutions could run millions of calculations and trading scenarios in seconds; unfortunately, would-be criminals could use the same technology to crack previously "unbreakable" encryptions, exposing systems to data breaches and cybercrime.

While predictions about timelines for quantum's real-world viability vary, banks should start evaluating its potential impacts and prepare, before they creep up on the industry.

Closing thoughts

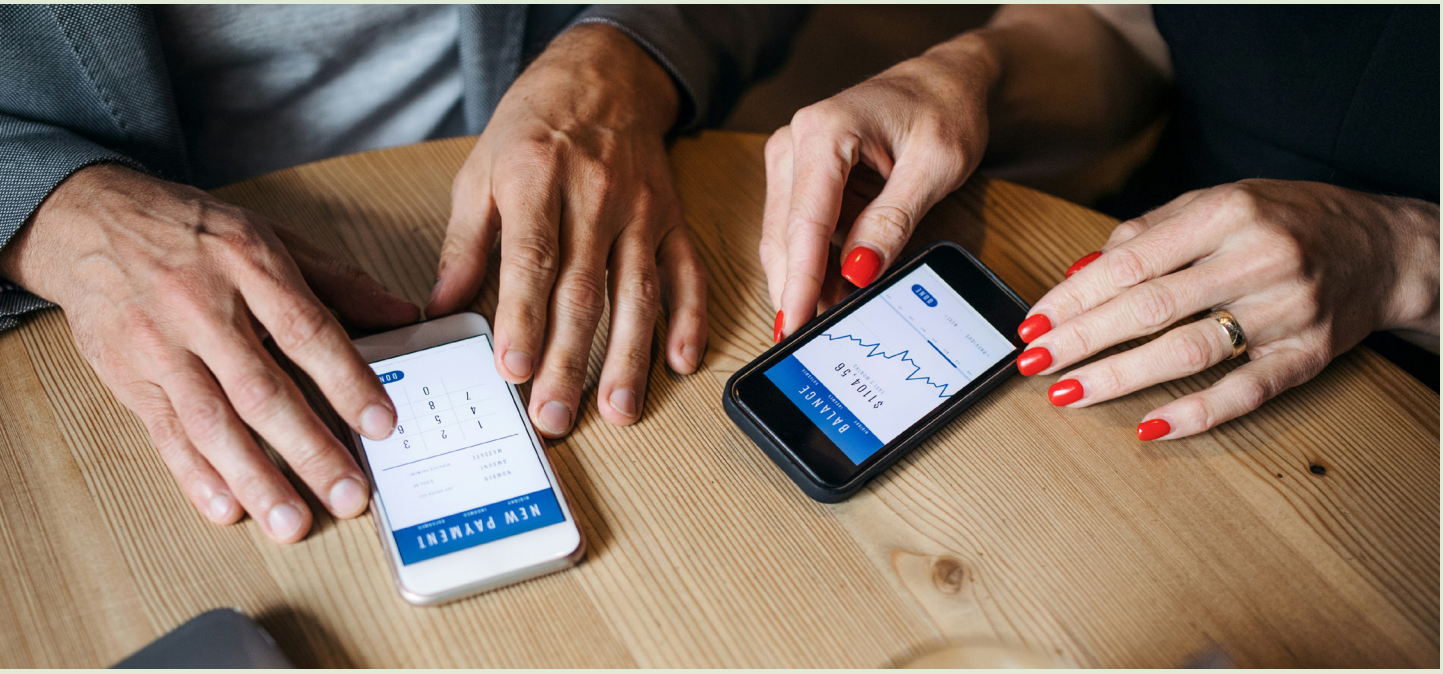
As banks navigate the complexities of digital transformation, their future depends on striking a balance between innovation and remediation. Technical debt, data disorganization and legacy systems consume valuable resources while technologies such as AI, blockchain and quantum computing offer significant potential for growth and differentiation.

Institutions that can modernize, harness data effectively and adopt emerging tools with discipline will not only reduce risk but also unlock new avenues for customer satisfaction and competitive advantage. As Deloitte's Lockard said: "Banks can't shut down innovation to retire old technologies. They need to find ways to build resilience and harden their systems to more reliably and seamlessly onboard new technologies."

Breaking The Bank (Technology Stack): Why Connection Beats Collection In Digital Transformation

A unified digital sales and service platform helps banks break free from the limitations of legacy technology and drive growth, engagement and operational efficiency.

By Taylor Adkins



Financial institutions sometimes mistake layering in solutions with digital transformation. While new platforms might seem necessary, the separate technology stacks that run them can compound issues of siloed infrastructure, disconnected data and piecemeal workflows already turning function into friction in customer management. Users experience inconsistencies; staff sees inefficiency;

and leadership wonders why growth has stalled despite heavy technology investments.

To move beyond this legacy, financial institutions must shift from using digital banking solely as a service channel to adopting a unified sales and service platform that delivers smarter engagement, stronger relationships and measurable business outcomes. How well they connect and synchronize their technologies, teams and data will define this next stage of digital transformation.

From personalization to anticipation

Most digital strategies still focus on basic personalization, using someone's name in a message or suggesting a credit card based on age. That's a start, but with rising expectations from today's consumers and businesses, it's not enough.

What account holders really want is anticipation.

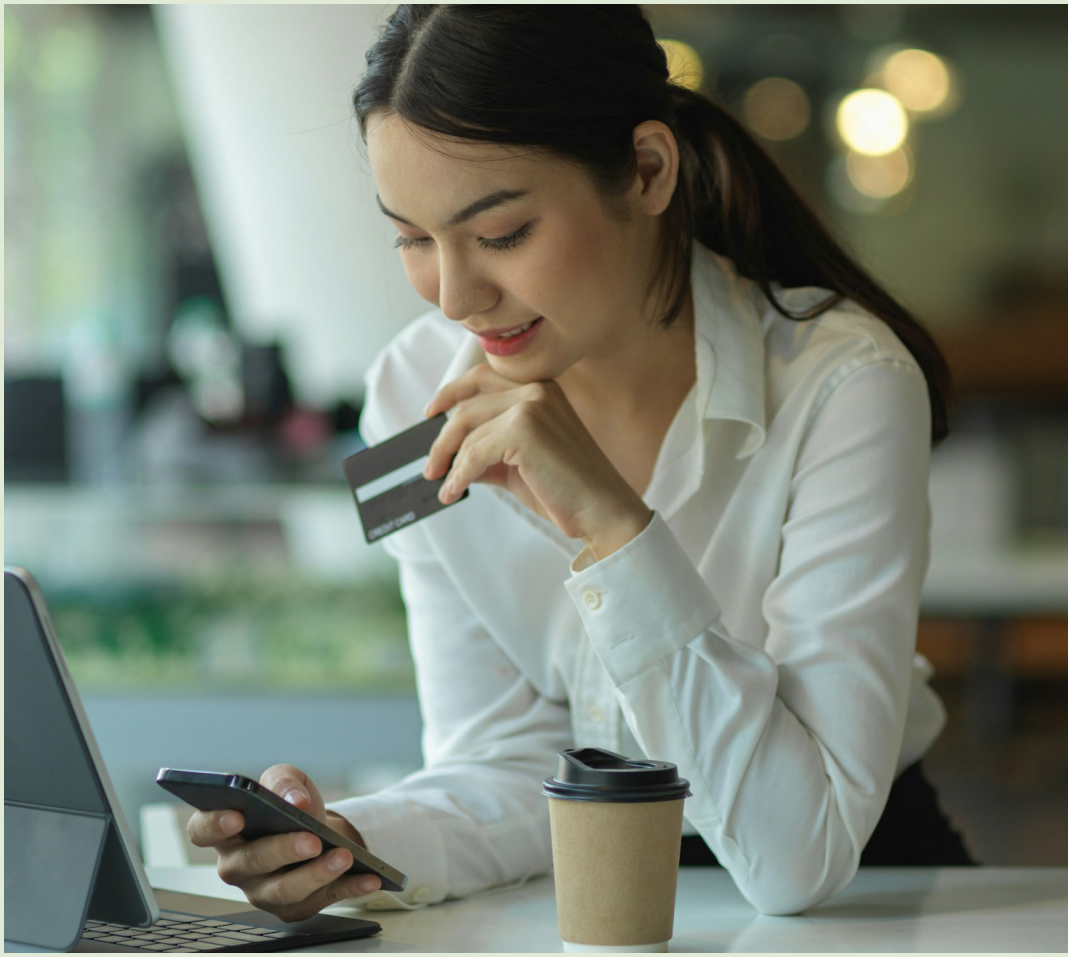
They expect their financial institution to recognize patterns in their behavior and respond proactively. They want guidance, not just transactions, and they expect their digital experience to reflect the same level of understanding they'd receive in person. Recent research commissioned by Alkami shows that nearly half of digital banking customers in the U.S. want their primary financial provider to do a better job of anticipating their financial needs and goals.

Using real-time data and intelligent automation to anticipate needs helps institutions meet account holders exactly where they are and, more importantly, where they're going to be. Financial institutions solve customer problems in real time with tailored support instead of generic offers, deepening relationships in the process.

Examples include:

- Offering short-term liquidity options when an account balance is low to prevent overdraft penalties
- Launching customer retention campaigns when deposits seem unstable
- Promoting tools to support a side hustle that appears to be turning into a small business
- Predicting potential cash-flow shortfalls and offering a line of credit to bridge the gap

These aren't far-off ideas. They're on the horizon, supported by the shift from disconnected systems to a unified-platform approach. In those moments when customers need them most, institutions can prevent financial disruption and strengthen their role as a trusted partner, delivering value that goes beyond the transaction.



Unstacking: One platform, three outcomes, endless impact

The challenge isn't that banks and credit unions lack technology. It's that too much of their technology operates in isolation. One system manages account opening. Another handles digital banking. A third powers marketing. Insights are trapped in separate tools, and the experience for both users and staff suffers.

As a result, many institutions are rethinking their approach and looking to unify these workflows. Forward-looking institutions are beginning to pursue a more integrated digital foundation that brings together three essential capabilities:

1. Onboarding & account opening

Fast, secure and omnichannel account opening supports both retail and business users. Applicants can start the process in one channel, such as online, and seamlessly complete it in another, like a branch or contact center, without starting over. Staff have visibility throughout the entire journey, making it easy to pick up where the user left off and provide informed, personalized support. When automation powers steps like Know Your Customer (KYC), risk scoring and funding, employees spend less time on manual tasks and more time building relationships.

2. Digital banking

A modern, extensible platform serves as the daily digital hub for consumers and businesses alike, offering a seamless, intuitive experience backed by real-time insights and flexibility to evolve with user needs. Seventy percent* of digital banking customers in the U.S. think a bank or credit union's digital experience reflects how much they care about their customers or members.

3. Data & marketing

Institutions are turning passive data into proactive engagement. With behavioral triggers, intelligent segmentation and in-channel messaging, campaigns can respond in real time and drive deeper product adoption.

Each capability delivers value on its own, but integrated capabilities enable institutions to work more intelligently across the entire account-holder journey.

Outcomes that go beyond legacy

Technology alone doesn't move the needle—outcomes do. The value of a unified digital sales and service platform isn't just in its features, but in how it helps financial institutions grow, retain and deepen relationships, at scale. It's about turning digital investment into measurable impact. Here's how that comes to life:

- ### Faster acquisition

  With instant account funding, pre-filled forms and seamless handoffs between channels, digital account opening becomes a top-performing "branch." Institutions adopting these capabilities are seeing increases in both application volume and conversion rates. More importantly, omnichannel account opening, supported by real-time data and intelligent workflows, helps attract higher-quality relationships, reducing dormancy and early account closures.

- ### Smarter engagement

  With data flowing across onboarding, digital banking and marketing, institutions can offer relevant products at precisely the right moment. Instead of one-size-fits-all campaigns, you get hyper-targeted journeys that drive adoption and foster deeper, more meaningful relationships from day one.

- ### Higher retention

  Disengagement doesn't happen overnight. The platform identifies early warning signs like outbound transfers or drop-offs in usage and launches retention efforts in real time. No manual intervention required.

- **Operational efficiency**

  Breaking the stack reduces swivel-chair workflows, eliminates redundant systems and empowers staff with tools that are easier to manage and scale.

Build what's next without breaking everything

Every financial institution is on its own path toward digital transformation. Some are replacing outdated legacy systems; others are looking to make their existing technology work smarter. Regardless of where they start, the priority is clear: flexibility, integration and measurable impact.

A unified, modular digital sales and service platform approach makes it possible to begin where the need is greatest—whether that's onboarding, digital banking or data-driven marketing—and expand over time.

Most importantly, this platform gives institutions the ability to bring their greatest differentiator, relationship banking, into the digital channel. By connecting systems and data, financial institutions can deliver proactive, personalized experiences that reflect how well they know and serve their account holders.

As the industry moves beyond legacy systems, those who unify their digital strategy will be best positioned to drive growth, deepen relationships and adapt in real time. This is how the next era of relationship banking takes shape—one that's always on, always connected and built around the user, not the system.

That's how institutions stop stacking tools and start building what's next.

Taylor Adkins is Vice President, Product Management, at Alkami.

---

* The Center for Generational Kinetics research, commissioned by Alkami. One thousand five hundred U.S. participants (ages 22–65). Survey was conducted online from February 24, 2025, to March 14, 2025.

Alkami

Good Enough Isn’t Growth Enough.

It’s time to demand more from your digital banking provider.

The gap between digital leaders and laggards is widening fast. Banks that cling to legacy providers risk being outpaced by competitors who can launch faster, personalize smarter, and scale securely.

Switching providers is now NOT as scary as you think

90% Would Make the Switch Again

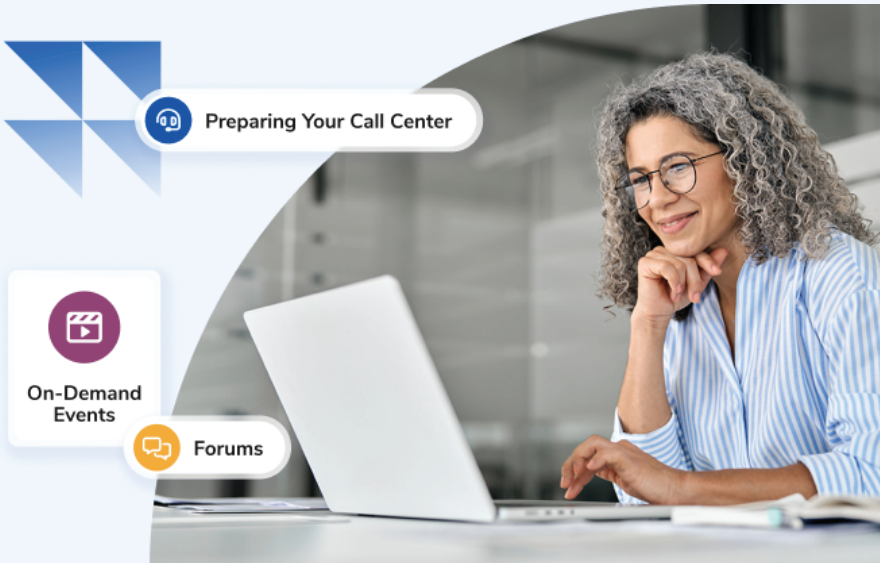
In a recent survey, nine out of ten financial institutions that switched digital banking providers in the past three years said they’d make the same move again.

Be the Next Success Story

The Digital Banking Conversion Toolkit transforms that 90% success rate into a clear, repeatable path for your institution.

Yes — it took effort, but the payoff was worth it.

Access the toolkit



The ProSight Executive Report

ProSight Financial Association empowers financial services leaders to strengthen and advance our industry. Formed through the merger of BAI and RMA—trusted organizations with rich histories and deep expertise in risk, fraud, compliance, and retail and commercial banking—we provide connections, training, insights, tools, and analytics to help you act with confidence. Our work creates positive ripple effects throughout financial services organizations and the industry, generating new opportunities for growth and ultimately helping consumers, businesses, and communities thrive. Learn more at ProSightFA.org.

The ProSight Executive Report is published by ProSight Financial Association.

Please direct inquiries to Kim Collins at info@ProSightFA.org.

At ProSight, Michael Bender edited the January 2026 edition of the Executive Report, with contributions from Frank Devlin and Meredith Boe. Design by Christopher Santoro.

January 2026

ProSight™

ProSightFA.org

BAI & RMA:
Together we're ProSight