Regulatory Dispatch

Timely news and resources community bankers can use to better stay on top of a rapidly changing world.

October 21, 2026

The latest issue of Consumer Compliance Outlook is now available

The Second Issue 2026 of *Consumer Compliance Outlook* (*CCO*) is now available on the *CCO* website. This issue includes the following articles and features:

- Alternative Data: Expanding Access to Credit
- Consumer Protection Considerations in Bank Merger and Acquisition Applications
- 2025 Aggregate Consumer Violations Data for Federal Reserve–Supervised Institutions
- Common Community Reinvestment Act (Regulation BB) Data-Related Violations in the Federal Reserve System in 2025
- Regulatory Calendar of Current and Proposed Regulations
- Regulatory Calendar of Regulations Under Review
- Download the complete issue (PDF)

We welcome your suggestions for topics for *CCO* articles and Outlook Live webinars, or any other feedback you wish to provide, at outlook@phil.frb.org.

Bank Management

	CSBS Adversarial AI: Meeting Emerging Risks and Threats in Financial Institutions (10/15/2026) – Recent developments in the field of artificial intelligence (AI) are generating a considerable amount of excitement. In a time where news of exciting advances in AI is a near-daily occurrence, there is reason for optimism when thinking of how AI might improve internal administrative and operations processes, drive meaningful change in how customers interact with our financial institutions, and make our organizations more secure. However, there is also reason for concern. The power and capabilities that could benefit the financial sector also introduce significant risks and threats. There is a sense of urgency in the frequency and tone of bulletins and alerts coming from government cybersecurity agencies and industry organizations, and financial institutions are, in many ways, now entering a time when they must enhance their focus on cybersecurity to address the growing threat of adversarial AI use. CSBS has identified three primary areas of concern for financial institutions. First, AI is enabling increased vulnerability discovery capabilities, which will change the volume and nature of patching. Powerful frontier AI models can identify large volumes of vulnerabilities, including zero-days, and are reportedly capable of generating proof-of-

concept exploits and even vulnerability chaining for identified vulnerabilities. While these capabilities will greatly benefit security teams, they will also drive a necessary change in how institutions approach patching and vulnerability management. There are concerns over increasing patch volume, vulnerability severity and prioritization, and the capabilities of smaller institutions and the service providers that often support their efforts.

To respond to increasing vulnerability volume, institutions should reexamine existing patch and vulnerability management processes, as well as strengthen fundamental supporting cybersecurity controls. Faster patching alone will not be sufficient to address risks from the vulnerability discovery capabilities of AI.

The use of AI to create sophisticated social engineering, phishing, vishing, and deepfakes is yet another concern for financial institutions. Quite simply, AI makes social engineering more efficient and effective. Today's AI is powering the automation of victim reconnaissance by parsing social media and open-source information to profile and target victims - all at a speed and scale that no human can match.

Phishing emails, vishing, and deepfakes are becoming increasingly effective, all due to the injection of AI into the development and execution of campaigns. Today's attempts are dangerous, sophisticated, and targeted, and the wide availability and growing utilization of AI by threat actors will only serve to make these attack vectors more exploitable at scale in the future.

Finally, AI is automating the design, development, and deployment of malware. There is evidence that AI is being utilized in all phases of the attack lifecycle. Threat actors use AI to streamline reconnaissance and victim targeting. There is also growing concern over the emergence of new malware families that leverage AI to more dynamically adapt to individual environments in which they are introduced. Threat actor groups are developing AI-generated or AI-assisted malware, and there is reason to believe that by many Ransomware-as-a-Service platforms are using AI, making these services an even more attractive option for less sophisticated actors. A key point of risk for financial institutions is the prospect of AI-driven or AI-enhanced malware creating new, significant challenges for existing cyber defense mechanisms, increasing the overall volume and complexity of attacks and opening doors further for new threat actors.

Currently, there are a number of recommendations from government cybersecurity agencies and industry groups to address these emerging threats. CSBS has outlined nine fundamental recommendations for financial institutions that closely mirror many of these recommendations. These actions, which are an amalgamation of recommendations from FS-ISAC, the European Central Bank, and other sources, address:

- Strengthening the institution's security perimeter
- Reevaluating vulnerability prioritization and shortening patching timelines
- Validating and updating critical asset inventories
- Replacing end-of-life (EOL) technology and strengthening EOL management processes
- Enforcing strong user access controls and privilege management
- Governing the use of open-source software
- Using available AI models for defense
- Verifying that third-party risk management practices are fit for purpose
- Building and testing robust incident response and resilience capabilities

	In December 2025, CSBS released Cyber Hygiene Fundamentals for FInancial Institutions, which provides additional foundational detail on many of the concepts contained in the recommended actions noted above. In addition, the CSBS Ransomware Self-Assessment Tool is an excellent resource for bank and nonbank institutions of all sizes to use to identify areas requiring attention to address readiness for confronting ransomware and other cyber threats. We recommend that all institutions review these documents now to support preparations for addressing today's rapidly evolving threat environment.
	FRB Beige Book (10/14/2026) – National Summary **Labor Markets** Most Districts described little or no net change in overall employment levels. While three Districts described modest increases, five reported slight increases, and four reported no significant change. Overall, labor market conditions were little changed. Labor supply was generally adequate to meet demand; however, shortages persisted for specialized, technical, and skilled trade workers. Five Districts reported that some firms had either reduced staffing levels (through attrition), delayed hiring, or anticipated less job creation after increasing productivity by investing in AI. Five Districts described moderate growth in overall wages, four reported modest growth, and two reported slight growth. Several Districts noted that inflation has spawned additional wage pressure in the form of higher cost-of-living demands from individuals as well as challenges from rising benefit costs. Staffing contacts in the Boston District noted that workers were motivated to seek new jobs as wage increases lagged inflation. **Prices** Three Districts characterized overall price growth as robust, while eight noted that growth was moderate—and three of the eight noted that input price pressures were intensifying, if not already growing robustly. One District reported modest price growth. Moreover, four Districts reported that the pace of price increases picked up since the prior period. Higher oil prices permeated all District reports. Firms reported elevated diesel prices and noted that fuel surcharges were passing on increased costs throughout the supply chain. Contacts in multiple Districts also noted continued price pressure from other commodities, tariffs, and insurance. Consumer-facing firms noted tighter profit margins as price-sensitive customers continue to resist price hikes. Contacts are managing their margins with selective price hikes, targeted incentives, and menu changes that reduce their costs. Firms in several Districts cited persistent uncertainty around energy and tariffs and expect that prices will increase further in the coming months, as existing contracts expire, and firms must renegotiate hedge contracts for their own inputs and/or delivery contracts to their customers.
	OCC Comptroller Gould Discusses Findings of Debanking Report (10/14/2026) – WASHINGTON—Comptroller of the Currency Jonathan V. Gould today discussed finding of the Office of the Comptroller of the Currency's newly-released report on large banks' debanking activities during a press conference held in Lexington, Kentucky, with U.S. Congressman Andy Barr. During the event, representatives of local Kentucky coal and firearms industries provided insights about the specific impacts of the debanking practices to their businesses. Excerpts from Comptroller Gould's remarks are below. His full statement can be found here.

	On Ensuring Fair Access to Financial Services for All Americans The President directed federal banking regulators to examine whether financial institutions had denied Americans access to banking services because of their political or religious beliefs or lawful business activities. Thanks to his leadership as well as that of U.S. Treasury Secretary Bessent, we are continuing to take steps to ensure that all Americans have fair access to the financial services they need to finance mortgages, fund small businesses, and support their families. On Report Findings We found that all of these banks had adopted reputation risk policies at various levels which allowed political considerations, public opinion, and social pressures to influence who banks deemed not worthy to access financial services. Americans were denied banking services because of their political or religious affiliations and entire industries faced scrutiny due to the fact that their lawful business activities were considered "controversial" by some banks or their employees. What began as decisions made by executives to debank disfavored industries became institutionalized and opaque bureaucracies that empowered bank employees to cut off industries and persons from financial services or created procedural frictions that achieved the same result as a practical matter. On Specific Impacts to Coal and Firearms Industries Our review found that many of the banks maintained policies restricting financing for new or expanded coal mining operations and coal-fired power plants. Some went even further, restricting financial services to companies based on how much of their revenue is derived from coal. These decisions were not based on financial risk; instead, banks cited concerns about negative headlines, public protests, and the perceived reputational consequences of supporting the industry. We found similar practices affecting the firearms industry. Several banks restricted financing for firearms manufacturers and retailers. In one instance, a bank denied a firearms business assistance with an initial public offering because the company's policies governing lawful firearms sales did not align with the bank's own standards. Banks should not be denying customers for activities protected by the constitution of the United States. We are not forcing these banks to serve every customer. Instead, banks should evaluate every customer on objective, risk-based criteria. On OCC Continuing Efforts to Eliminate Debanking At the OCC, we have eliminated reputation risk from our supervisory framework. As our report makes clear, there is more work to do to ensure that Americans are not denied financial services simply because of their beliefs or that their businesses have fallen out of favor.
	CSBS Community Bankers Signal Economic Warning (10/13/2026) – Despite continued optimism about their own institutions, community bankers are increasingly concerned about monetary policy and future business conditions.

	Community bankers have long served as a valuable barometer of economic conditions on Main Street. Their daily interactions with households, small businesses, and local employers provide a unique perspective on the health of the U.S. economy—often revealing emerging challenges before they become apparent in national economic statistics. The latest Community Bank Sentiment Index (CBSI) from the Conference of State Bank Supervisors (CSBS) offers a particularly interesting message: Community bankers remain confident in their own institutions, but their confidence in the broader economic outlook is deteriorating. As shown in Chart 1, the third-quarter 2026 CBSI fell nine points to 120, marking its fourth consecutive quarterly decline. The index has now fallen 13 points from its reading of 133 one year ago. Although the latest reading remains comfortably above the neutral level of 100, the direction and composition of the decline warrant attention. ***Comment: Acco9rding to the survey results, emerging tools like artificial intelligence and stablecoins are introducing sharp competitive pressures. Community banks report that the primary barriers to adoption are persistent cybersecurity threats, talent constraints, and unclear returns on investment. Also noteworthy is the drop in 'Future Business Conditions' index to 83.***

BSA / AML

	FinCEN Alert to Counter Iranian Abuse of Religious Charity Networks (10/15/2026) – The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Alert to assist financial institutions in identifying and reporting potential Iranian abuse of religious charity networks, including diversion of religious tithes or khums. This Alert supports Treasury's efforts as part of Operation Economic Outcast targeting the Iran and its financial enablers, including the Islamic Revolutionary Guard Corps (IRGC). The information contained in this Alert is derived from analysis of Bank Secrecy Act data, as well as open-source reporting and law enforcement information. ***Comment: Banks are instructed to flag related Suspicious Activity Reports (SARs) using the designated key term FIN-2026-IRANCHARITYABUSE. FinCEN noted that no single red flag automatically proves illicit behavior, and banks must review the totality of circumstances.***

Technology / Security

	CISA Chinese Government-linked Cyber Threat Actors Combine Automated and Hands-on Hacking Tools to Steal Sensitive Data (10/08/2026) – Chinese government-linked cyber threat actors, enabled by the Integrity Technology Group, are combining automated scanning tools, large-scale botnets, and hands-on exploitation techniques to target and steal sensitive data from organizations worldwide, including US critical infrastructure sectors. These actors exploit vulnerabilities by using scanning tools, cross-site scripting attacks, and password spraying on Microsoft Exchange servers, while establishing persistence through VPN software and exfiltrating emails and credentials using scripts. To help mitigate against this activity, organizations should prioritize disabling unused services and ports, sanitizing web application inputs to prevent injection attacks, implementing

	multifactor authentication for all services, and applying timely patches to reduce risks of compromise.

Open for Comment

Included only when specific to or relevant for community banks to comment on. Date posted may not be the same as the Federal Register Date.

09.24.2026 **FRB** Application Procedures for Board-Supervised Insured Depository Institutions Seeking Approval for a Subsidiary to Issue Payment Stablecoins SUMMARY: The Board of Governors of the Federal Reserve System (Board) proposes to issue regulations that would establish procedures to be followed by an insured State member bank that seeks to obtain Board approval for a subsidiary to issue payment stablecoins pursuant to the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act). **DATES: Comments must be received by the Board on or before November 16, 2026.**

09.11.2026 **Joint** Proposed Third-Party Risk Management Guidance SUMMARY: The OCC, Board, FDIC, and NCUA (collectively, the agencies) invite comments on this proposed third-party risk management guidance. The proposed guidance would reflect the agencies' supervisory experience and lessons learned through examining banking organizations' third-party risk management practices. In particular, the proposed guidance would discuss the potential benefits that may accrue when a banking organization aligns its third-party risk management practices in relation to the reasonably assessed risk levels specific to each of its third-party relationships. This approach may assist banking organizations in the prioritization of third-party risk management based on material financial risks, compliance with laws and regulations, and resource allocation. The proposed guidance also would help banking organizations consider potential strategies for tailoring their third-party risk management practices according to the banking organization's size, complexity, and risk profile, as well as the nature of its third-party relationships. The agencies plan to rescind and replace existing guidance on third-party risk management to promote consistency and innovation in the banking industry. **DATES: Comments must be received on or before November 16, 2026.**

07.31.2026 **FDIC** Extensions of Credit to Insiders SUMMARY: The Federal Deposit Insurance Corporation (FDIC) is proposing to increase quantitative thresholds for certain extensions of credit to insiders of FDIC supervised institutions, as restricted by the Federal Reserve Act and regulations promulgated thereunder. Specifically, the proposal would increase the thresholds for certain (1) extensions of credit to executive officers not otherwise specifically authorized by statute from $100,000 to $400,000; and (2) extensions of credit to insiders requiring prior approval by the board of directors from $500,000 to $2,000,000. The proposal would also establish an indexing methodology to periodically update such thresholds over time. **DATES: Comments must be received on or before November 4, 2026. (Extended from October 5, 2026)**