

Spring 2026

# COMMUNITY BANKING ADVISOR



FDIC REDUCES COMPLIANCE BURDEN FOR MANY COMMUNITY BANKS

DETERMINING THE "RIGHT" LEVEL OF INTEREST RATE RISK

DO YOUR HOMEWORK WHEN  
PARTNERING WITH A FINTECH PROVIDER

BANK WIRE



ANDREWS HOOPER PAVLIK PLC



COMMUNITY BANKING  
ADVISORY NETWORK

# FDIC REDUCES COMPLIANCE BURDEN FOR MANY COMMUNITY BANKS

In November 2025, the Federal Deposit Insurance Corporation (FDIC) approved a final rule easing the regulatory burden on community banks under the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA). The rule, effective at the beginning of 2026, increases the FDICIA asset thresholds and provides for them to be indexed for inflation in the future. Here's a look at the changes.

## UPDATED COMPLIANCE THRESHOLDS

Once a bank's assets reach specified thresholds, the FDICIA imposes significantly more stringent independent audit, internal control and reporting requirements. These heightened regulatory obligations were intended to apply to larger, more complex institutions. However, because many of the original asset thresholds had remained unchanged since 2005 or earlier, inflation and economic growth have brought many community banks within FDICIA's purview.

Under previous rules, certain reporting requirements kicked in once a bank's total assets reached \$500 million. Now, this amount has doubled to \$1 billion. (Note that for FDICIA purposes, a bank's total assets are measured as of the beginning of its fiscal year, as reported on its most recent call report.)



Additional requirements may apply for larger banks. Previously, internal control over financial reporting (ICFR) and independent audit committee requirements applied once a bank's total assets reached \$1 billion. The new rule increased the threshold to \$5 billion. Finally, the new rule increases the threshold for certain restrictions on audit committees under the FDICIA from \$3 billion to \$5 billion, starting in 2026.

## ANNUAL INDEPENDENT AUDIT AND REPORTING REQUIREMENTS

When a bank crosses the total asset threshold (\$1 billion for 2026), it becomes subject to the following requirements:

**Annual reports.** The bank must prepare annual reports and file them with the appropriate federal and/or state banking agencies within 120 days after the end of its fiscal year (90 days for publicly traded banks). These must include:

- ▶ Audited financial statements,
- ▶ Independent auditors' reports, and
- ▶ Management reports acknowledging management responsibility for preparing financial statements, establishing and maintaining adequate ICFR, and complying with certain safety and soundness laws and regulations.

**Auditor independence.** The bank and its auditors must comply with the strictest auditor independence standards applicable to public companies, which means auditors must avoid conflicts of interest and prohibited financial relationships with the bank, rotate audit partners at least every five years, and refrain from providing prohibited non-audit services to the

bank (including bookkeeping, financial statement preparation, valuation, internal audits and tax services for specific bank insiders).

The new rule also increases the asset thresholds at which more stringent requirements take effect for audit committees. For instance, when a bank's total assets reach \$1 billion, its board of directors must have an audit committee made up of outside directors, the majority of whom are independent of management.

### ENHANCED REQUIREMENTS

When a bank's total assets exceed \$5 billion for 2026 (up from \$1 billion), it must submit:

**Expanded management reports.** In addition to the reports mentioned above, these must include an evaluation of the effectiveness of ICFR as of the end of the fiscal year, based on a recognized framework.

**External opinion on ICFR.** The annual report also must include an independent auditor's attestation report on the effectiveness of ICFR as of the end of the fiscal year.

In addition, when a bank's total assets reach \$5 billion, *all* (rather than merely a majority) of its audit committee members must be outside directors independent of management.

Finally, when a bank's total assets reach \$5 billion for 2026 (up from \$3 billion), its audit committee must also 1) include members with banking or related financial management expertise, 2) have access to its own outside counsel, and 3) not include any large bank customers.

### OTHER FACTORS

Keep in mind that the FDICIA isn't the only law that governs your audit and reporting requirements. You

### FUTURE ADJUSTMENTS TO FDICIA THRESHOLDS

In addition to boosting the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) asset thresholds, the new Federal Deposit Insurance Corporation (FDIC) rule provides for the thresholds to be indexed for inflation going forward. As community banks prepare for ongoing FDICIA compliance, it's important to monitor projected asset growth and consider estimated future adjustments to the threshold amounts.

Under the new rule, the FDIC will adjust the threshold dollar amounts every other year based on the cumulative percentage change in the nonseasonally adjusted Consumer Price Index for Urban Wage Earners and Clerical Workers (CPI-W). The thresholds may be adjusted more frequently if the CPI-W exceeds 8% in an intervening calendar year.

may be subject to more stringent requirements under state law or regulations, or under the rules of other federal agencies, such as the Federal Reserve Bank, the U.S. Department of Housing and Urban Development, Fannie Mae or Ginnie Mae.

Of course, regulatory compliance isn't the only reason to implement strong internal controls and governance practices. Depending on your bank's risk profile, it may derive significant benefits from audited financial statements and audit committee independence, regardless of its asset size.

### MONITOR YOUR BANK'S ASSET GROWTH

The higher asset thresholds ease regulatory burdens on community banks that had become subject to FDICIA requirements under the old thresholds or were approaching those thresholds. As your bank grows, continue to keep tabs on total assets, particularly as you approach the \$1 billion and \$5 billion marks. It's critical to start planning well in advance to ensure a smooth transition to your new regulatory regime. ■

## DETERMINING THE “RIGHT” LEVEL OF INTEREST RATE RISK

What’s the right level of interest rate risk for a community bank — and what’s the right way for your bank to manage that risk? To answer these questions, it’s necessary to analyze your bank’s comparative size, its operational complexity and whether it has sufficient capital on hand to maintain profitability despite interest rate fluctuations. Based on your circumstances, management also needs to develop sound asset and liability risk management practices that hold up over time.

### WHAT’S INTEREST RATE RISK?

Interest rate risk means risk to a bank’s financial condition or resilience (that is, its ability to withstand periods of stress) caused by movements in interest rates. There are several types of interest rate risk, including:

**Repricing risk.** Banks experience this risk when their assets and liabilities reprice or mature at different times. Suppose, for example, that a bank makes a five-year, fixed-rate loan at 7% that’s funded by a six-month certificate of deposit (CD) at 3%. Every six months, when the CD renews, the bank is exposed to repricing risk. If the CD rate increases to 4% after six months, then the bank’s net interest income drops from 4% to 3%. Conversely, if the CD rate declines, the bank’s net interest income increases.

To gauge repricing risk, banks can compare their volume of assets and liabilities that mature or reprice over a given time period. The potential impact of fluctuating interest rates will depend in part on whether a bank is asset- or liability-sensitive. If it’s asset-sensitive — meaning assets reprice more quickly than liabilities — then its earnings generally increase when interest rates rise and decrease when they fall. If it’s liability-sensitive — meaning liabilities reprice more quickly than assets — then its earnings generally increase



when interest rates fall and decrease when they rise. Some banks are neutral — that is, their assets and liabilities reprice at the same time.

**Basis risk.** This arises when there’s a shift in the relationship between rates across markets or financial instruments. Suppose, for example, that an asset and a related liability are tied to the prime rate and the one-year U.S. Treasury rate, respectively. If the spread between those two rates widens or narrows, it will affect the bank’s net interest margins.

**Yield curve risk.** This risk arises from changes in the relationships among yields from similar instruments with different maturities. Let’s say that a bank funds long-term loans with short-term deposits. A typical yield curve reflects rates that rise as maturities increase. However, if market conditions cause the yield curve to flatten or even slope downward, the bank’s net interest margins can shrink or even turn negative.

**Options risk.** Bank assets and liabilities often contain embedded options, such as the right to pay off a loan or withdraw deposits early with little or no penalty. The bank is compensated for offering customers this flexibility (typically with higher interest rates on loans or lower interest rates on deposits). But granting these options creates interest rate risk. For example, if

interest rates rise, deposit holders will have an incentive to move their funds into investments that enjoy higher returns. If rates go down, many borrowers will pay off their loans to refinance at a lower rate.

### HOW CAN YOU MANAGE YOUR RISK?

Banks can apply financial modeling techniques to measure and monitor their interest rate risk. If your interest rate risk is unacceptably high, consider strategies for mitigating it, such as:

- ▶ Adjusting your bank's mix of assets and liabilities to reduce interest rate risk,
- ▶ Increasing capital to help absorb the impact of fluctuating interest rates,

- ▶ Reducing options risk by controlling the terms of loans and deposits, or
- ▶ Using interest rate swaps or other techniques to hedge against interest rate risk.

Keep in mind that a key component of interest rate risk management is stress testing.

### BE RISK-AVERSE

Community banks face many interrelated and evolving issues, including risk management. Whether that risk involves interest rates, rapidly changing AI and technology, or issues related to liquidity vs. capital, an ongoing, integrated risk management system can support your bank's profitability and long-term success. ■

## DO YOUR HOMEWORK WHEN PARTNERING WITH A FINTECH PROVIDER

To remain competitive with larger banks in the current market, community banks must deliver the innovative, technology-driven tools customers have come to expect. For many community banks, the most effective strategy is to partner with financial technology ("fintech") providers. These partnerships give banks access to cutting-edge technologies, specialized expertise and cost efficiencies that would be difficult to achieve independently. But thorough due diligence is essential to achieve optimal results.

### COMMON FINTECH COLLABORATIONS

Banks are collaborating with fintech providers to develop a variety of customer offerings, including:

- ▶ Digital account opening,
- ▶ Digital loan origination,

- ▶ Person-to-person payments,
- ▶ Mobile wallets for contactless payments,
- ▶ Remote deposits,
- ▶ Personal financial management tools, and
- ▶ Security, identity and fraud prevention technology.

Embracing digital tools not only helps community banks retain existing customers who seek convenience, it also expands their geographic footprints, allowing them to attract new customers.

### DUE DILIGENCE CONSIDERATIONS

When conducting due diligence on prospective fintech partners, the specific steps you take depend on the type of technology provided, the nature of the relationship and the level of risk to the bank. When

developing your due diligence strategy, consult the federal banking agencies' *Interagency Guidance on Third-Party Relationships: Risk Management*. This 2023 publication outlines sound risk-management principles for banks when contemplating relationships with fintech companies and other providers.

MAKE SURE THE FINTECH PROVIDER HAS THE FINANCIAL CAPACITY TO PROVIDE THE CONTRACTED ACTIVITIES, REMAIN A GOING CONCERN AND FULFILL ITS OBLIGATIONS TO THE BANK.

Another valuable tool is the agencies' publication, *Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks*. It outlines the topics banks should consider when conducting due diligence on a fintech provider. Examples include:

**Business experience and qualifications.** Does the fintech provider have the ability to conduct the contracted activities "in a manner that enables a community bank to comply with regulatory requirements and meet customer needs"? Among other things, consider client references and complaints as well as any legal or regulatory actions against the fintech company.

**Business strategies and plans.** Will the fintech company's strategies or planned initiatives affect or impede their implementation of the activities?

**Qualifications and backgrounds of directors and company principals.**

Does the company have the requisite staff and expertise to handle the activities?

**Financial condition.** Does the fintech have the financial capacity to provide the contracted activities, remain a going

concern and fulfill its obligations to the bank? You should understand the company's funding sources, including cash flow from the business, loans, capital injections, venture capital or planned public offerings.

**Market information.** Consider the fintech company's competitive environment, its reliance on a few key clients and its susceptibility to geopolitical events or other external risks.

**Legal and regulatory compliance.** Review the company's organizational documents, licenses, charters or registrations, as well as its risk and compliance processes. In particular, evaluate the fintech company's ability to support the bank's privacy, consumer protection, fair lending, anti-money-laundering, and any other legal or regulatory obligations.

Other considerations include the fintech company's risk management and control processes, information security program and business continuity plans. Also scrutinize proposed service-level agreements to ensure they meet expectations.

### A WIN-WIN SITUATION

Federal banking regulators have high expectations for banks when it comes to third-party risk management. To ensure the best possible results as your bank explores potential fintech solutions, it's critical to have robust due diligence in place to manage the risks associated with third-party relationships. ■



# BANK WIRE

## FAQs ON SAR REQUIREMENTS

The federal banking agencies recently published answers to FAQs regarding banks' suspicious activity report (SAR) obligations. The FAQs are intended to "assist financial institutions with their compliance obligations while enabling institutions to focus resources on activities that produce the greatest value to law enforcement." Key issues addressed include:

**Potential structuring-related activity.** Banks aren't required to file an SAR merely because a transaction or a series of transactions is near the \$10,000 currency transaction reporting (CTR) threshold. A filing is required only if the bank knows, suspects or has reason to suspect that a transaction is designed to evade CTR requirements.

**Continuing activity reviews.** Banks aren't required to review a customer or account following an SAR filing to determine whether suspicious activity has continued. Rather, they may rely on risk-based internal policies, procedures and controls to monitor and report suspicious activity as appropriate. The Financial Crimes Enforcement Network had previously suggested that banks report continuing suspicious activity every 90 days, but the FAQs clarify that this timeline isn't mandatory. Banks have the flexibility to file SARs as appropriate in line with applicable deadlines.

**Documentation of decisions not to file an SAR.** The FAQs confirm that banks aren't required to document decisions not to file an SAR, though such documentation is encouraged as a best practice. If a bank chooses to document SAR decisions, the level of detail depends on the complexity of the activity being reviewed. The documentation should be concise and tailored to the bank's internal policies, procedures and controls. ■

## BSA/AML: RECENT DEVELOPMENTS

The Office of the Comptroller of the Currency (OCC) made several recent announcements of interest to community banks regarding Bank Secrecy Act (BSA)/anti-money laundering (AML) compliance. These include Bulletin 2025-37, which establishes tailored, less burdensome BSA examination procedures for community banks. These are intended to reflect community banks' generally low levels of money laundering and terrorist financing risk.

In addition, Bulletin 2025-38 discontinues annual mandatory data collection from community banks under the Money Laundering Risk (MLR) System. The OCC found that there are alternative, less burdensome means of assessing community banks' money laundering and terrorist financing risks and, therefore, the MLR System is no longer necessary.

Finally, Bulletin 2025-39 contains a request for information (RFI) about community banks' engagement with their core service providers and other essential third-party service providers. The RFI "focuses on ensuring that community banks can remain competitive in a rapidly evolving marketplace, and includes questions on the challenges community banks face related to contract negotiations and terms, fees, billing practices, oversight, due diligence, innovation, core conversions, data access and modernization, and interoperability issues." ■



*This publication is distributed with the understanding that the author, publisher and distributor are not rendering legal, accounting or other professional advice or opinions on specific facts or matters, and, accordingly, assume no liability whatsoever in connection with its use. ©2026*



ANDREWS HOOPER PAVLIK PLC  
5300 Gratiot Road, Saginaw, MI 48638

## Community Banks

Andrews Hooper Pavlik PLC provides a broad range of accounting, audit, tax, and consulting services to the community banking industry. Our services are customized to meet your needs and include collaboration with your management teams.

With extensive industry experience, Certified Bank Auditors and Certified Regulatory Compliance Managers on staff, and the ability to staff highly-trained service professionals on every engagement, you can count on us to meet your needs and exceed your expectations.

### Audit & Accounting

- Accounting and Compliance Consulting
- ACH Self-Audit
- Asset Liability Management Review
- Customized Training
- Director Exams and Supervisory Committee Audit
- Financial Statement Audit
- HUD Audit
- Independent Loan Review
- Internal Audit
- Model Validation
- Quality Control Review
- Regulatory Compliance Audit
- Risk Assessment Assistance
- Sarbanes-Oxley (SOX) Assistance and Testing
- System and Organization Control (SOC) Examination
- Trust Administration Internal Audit

### IT Consulting

- Cybersecurity and IT Consulting
- General IT Controls Audit
- GLBA Compliance Audit
- Penetration Testing
- Social Engineering
- Vulnerability Assessments

### Mergers & Acquisitions

- Due Diligence Loan Review
- Due Diligence Review of Deposits and Human Resources
- Interim Period Financial Statement Audit
- Pro-Forma Financial Statement Assistance
- Regulatory Compliance Consulting
- Tax and Accounting Assistance

### Tax

- Accounting for Income Taxes
- IRS Examinations
- Tax Planning
- Tax Research
- Tax Return Preparation

