

AUGUST 31, 2026 | PUBLICATION

Client Alert: When Your Bank Fails: A Practical Guide for Financial Services Businesses

Introduction

On August 21, 2026, Pennsylvania state regulators shuttered Tioga-Franklin Savings Bank, a community institution in Philadelphia that held roughly \$68 million in assets and \$67 million in deposits as of mid-year. The Federal Deposit Insurance Corporation (FDIC) stepped in as receiver and facilitated the transfer of all deposit accounts and substantially all assets to Second Federal Savings and Loan Association of Philadelphia. The FDIC has preliminarily estimated the cost to the Deposit Insurance Fund at approximately \$5.5 million.

Tioga-Franklin marks the fifth FDIC-insured institution to close in 2026, which is more than double the two failures recorded in each of the prior two years. At the current pace, 2026 is poised to surpass 2017 as the most active year for bank failures in nearly a decade. The four earlier closures this year—Metropolitan Capital Bank & Trust (Chicago), Community Bank and Trust—West Georgia (Georgia), Kentland Federal Savings and Loan Association (Indiana), and Small Business Bank (Kansas)—underscore the breadth of the trend.

For fintechs, small to mid-sized businesses (SMBs), regional chartered banks, and other financial services entities these closures carry tangible consequences for daily operations, contractual relationships, capital adequacy, and regulatory compliance. Notably, the median adjusted Texas Ratio across U.S. banks climbed to 3.9 percent in the second quarter of 2026, its highest level in five years, which although not independently alarming, suggests that further stress within the banking sector may lie ahead.

This article provides a practical framework for understanding how a bank failure could affect your business,

INDUSTRY SECTOR

Financial Services
Technology

SERVICE LINE

Data Privacy
Technology

RELATED PROFESSIONALS

Elizabeth R. Brusa

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

what you should be doing now to prepare, and what immediate steps to take if a failure impacts your operations.

How a Bank Failure Would Impact Your Business

A bank failure ripples outward in ways that depend on your business model, your relationship with the failed institution, and the speed of regulatory resolution. Below, we address impacts specific to financial services entities.

Fintechs and Banking-as-a-Service (BaaS) Programs

For fintechs that depend on sponsor bank partnerships, a bank failure, or even a bank's voluntary withdrawal from BaaS, can threaten the viability of the entire business. The April 2024 bankruptcy of Synapse Financial Technologies remains the most instructive cautionary example. According to court filings and Consumer Financial Protection Bureau (CFPB) enforcement records, approximately \$265 million in customer funds was rendered inaccessible, affecting more than 100,000 end users whose balances were held at FDIC-insured banks. The root cause was a fundamental recordkeeping breakdown. Synapse's middleware platform could not reliably match individual customers to their proportionate share of pooled For Benefit Of (FBO) custodial accounts.

A sponsor bank's failure can abruptly sever a fintech's ability to process payments, originate Automated Clearing House (ACH) transactions, and issue debit or prepaid cards. While FDIC coverage insures depositors against bank insolvency, it offers *no* protection when the breakdown occurs at a technology intermediary positioned between the customer and the insured institution. The regulatory environment has intensified. Between 2022 and 2025, the FDIC, Office of the Comptroller of the Currency (OCC), and Federal Reserve collectively brought consent orders against seven banks serving as BaaS sponsors. Industry data indicates that by mid-2025, banks subject to active enforcement action supported close to half of all BaaS-connected companies. A growing number of chartered institutions are choosing to exit BaaS altogether, leaving fintech partners to find new banking relationships under compressed timelines.

Small to Mid-Sized Businesses

For SMBs, a bank closure generates immediate operational friction. Although deposits generally transfer to an acquiring institution and remain FDIC-insured, the integration window, which can stretch from several days to several weeks, may interrupt payroll runs, delay vendor disbursements, and disrupt ACH settlement. Outstanding credit facilities are particularly vulnerable. An acquirer may curtail or restructure loan commitments as it evaluates the purchased portfolio. Additional counterparty risk surfaces when the failed institution served as a correspondent bank or payment processor for a client's vendors or customers.

Regional Chartered Banks and Credit Unions

Regional banks confront significant contagion risk when peer institutions fail. The 2023 crisis surrounding Silicon Valley Bank (SVB) provided a stark illustration. On March 9, 2023, SVB's depositors withdrew approximately \$42 billion in a single day—roughly one-quarter of the bank's total deposits. Correspondent banking exposures, loan participations, and interbank credit lines can transmit losses from a failed institution to otherwise stable banks. On the credit union side, closures reached their highest annual level in seven years during 2025, and the National Credit Union Administration's (NCUA) April 2026 proposed rulemaking

on credit union-to-bank mergers signals a tightening regulatory posture across the sector.

Key Takeaways

- Fintechs face existential risk from sponsor bank failures or exits, particularly where For Benefit Of Account (FBO) account reconciliation is inadequate.
- FDIC insurance does not protect against non-bank intermediary failures, only against the insolvency of the insured institution itself.
- SMBs should expect operational disruption during the transition period following a bank failure, even where deposits are fully assumed.
- Regional banks and credit unions face deposit flight risk, counterparty exposure, and heightened regulatory scrutiny in the wake of peer failures.
- The Tioga-Franklin consent order (dating to April 2024, citing Bank Secrecy Act / Anti-Money Laundering (BSA/AML) violations) demonstrates that regulatory red flags often precede failure by years.

Action Items Checklist

- ☑ Identify all banking relationships and map which functions depend on each institution.
- ☑ Quantify uninsured deposit exposure across all accounts.
- ☑ Assess whether any current banking partners are subject to consent orders or enforcement actions.
- ☑ For fintechs: audit FBO account reconciliation processes and confirm the ability to identify beneficial ownership at all times.
- ☑ For SMBs: confirm backup payment capabilities for payroll, vendor payments, and ACH.
- ☑ For regional banks: quantify correspondent banking and loan participation exposure.

What You Should Be Doing Now to Prepare

Preparation is the most cost-effective risk mitigation strategy. The following steps apply broadly, with specific considerations for each financial services entity segment.

Diversify Banking Relationships

Businesses should spread critical banking functions, including operating accounts, payroll, and payment processing, across no fewer than two FDIC-insured institutions, ensuring that no single bank represents a single point of failure for essential operations. For deposit balances that exceed the standard FDIC insurance limit of \$250,000 per depositor per institution, insured deposit networks and automated sweep programs offer practical mechanisms to extend coverage across multiple banks.

Monitor Bank Health Indicators

Regularly review publicly available indicators of financial distress affecting your banking partners. The Texas Ratio, which compares a bank's non-performing assets to the sum of its tangible equity and loan-loss reserves, is among the most widely tracked early-warning metrics in the industry. Institutions whose ratio exceeds 100 percent have historically faced materially higher failure rates. The median adjusted Texas Ratio across all U.S. banks rose to 3.9 percent in the second quarter of 2026, a five-year peak. Clients should also monitor capital adequacy ratios, published regulatory enforcement actions, and any consent orders or formal

agreements entered into by their banking counterparties.

Strengthen Your Contracts

Contract drafting is a critical preparedness tool. We recommend:

MAC/MAE Definitions: Ensure that Material Adverse Change (MAC) or Material Adverse Effect (MAE) clauses expressly cover regulatory enforcement actions, capital adequacy deterioration, and appointment of a receiver.

Termination Triggers: Include termination rights tied to regulatory actions (consent orders, cease-and-desist orders), with 60-90 day cure periods.

Wind-Down Protocols: Build contractual wind-down provisions that address data transition, customer notice, interim servicing obligations, and fund recovery procedures.

Audit Rights and Data Access: Secure contractual rights to audit compliance programs, access ledger data, and obtain customer records on demand. This is particularly critical for fintechs operating through FBO accounts.

Liability Caps: Rather than relying on a single aggregate cap, structure tiered liability limits that reflect the distinct risk profile of each compliance function. At minimum, carve out from any cap the following categories of loss: failures to implement agreed-upon BSA/AML or fair lending controls, regulatory penalties directly traceable to the counterparty's conduct, and breaches of specific data-provision or recordkeeping representations.

Fintech-Specific Preparedness

Fintechs should negotiate relationships with multiple sponsor banks in advance of any disruption, eliminating the risk inherent in single-bank dependency. FBO ledger access should be both contractually guaranteed and periodically tested to confirm operational readiness. All customer-facing representations regarding deposit insurance should be audited for accuracy and compliance with FDIC requirements. Compliance programs should be built to withstand direct regulatory examination. Federal banking agencies have consistently held that outsourcing activities to a third party does not relieve a bank of its supervisory obligations, and enforcement actions increasingly extend scrutiny to fintech partners themselves.

Develop Contingency Plans

Every business should maintain a written contingency plan for the loss of its primary banking relationship. This plan should identify backup institutions, document migration procedures, establish communication protocols for customers and vendors, and designate responsible personnel.

Key Takeaways

- Diversification across multiple FDIC-insured institutions is the single most effective mitigation strategy.
- Texas Ratios, regulatory actions, and capital adequacy ratios are publicly available early-warning indicators.
- Contract provisions, including MAC clauses, termination triggers, wind-down protocols, and audit rights, should be drafted with bank failure scenarios expressly in mind.
- Fintechs should secure multi-bank arrangements and verify FBO ledger access before a crisis arises.
- Written contingency plans should be maintained, tested, and updated at least annually.

Action Items Checklist

- ☒ Establish relationships with at least two FDIC-insured banks for all critical functions.
- ☒ Implement sweep programs or insured deposit networks for deposits exceeding \$250,000.
- ☒ Run quarterly Texas Ratio and capital adequacy checks on all banking partners.
- ☒ Review all bank-related contracts for MAC/MAE definitions, termination triggers, and wind-down provisions.
- ☒ Negotiate audit rights and data-access provisions in all banking and BaaS agreements.
- ☒ Calibrate liability caps with specific carve-outs for BSA/AML failures and regulatory fines.
- ☒ Fintechs: pre-negotiate backup sponsor bank arrangements and test FBO ledger access procedures.
- ☒ Draft and maintain a written contingency plan for loss of primary banking relationship.
- ☒ Assign a responsible officer to monitor regulatory actions affecting banking partners.

What to Do If a Bank Failure Occurs

If a bank failure affects your institution or business relationships, speed and precision matter. Below is a framework for immediate and near-term action.

Immediate Steps (First 24–72 Hours)

Confirm the basics: Identify the receiver (typically the FDIC), the acquiring institution (if any), the scope of the assumption transaction, and the status of your accounts. In the Tioga-Franklin Savings Bank closure, Second Federal Savings and Loan Association assumed all deposits and substantially all assets, but this is not always the case.

Verify access to funds: Confirm that you can access operating accounts, process payroll, make vendor payments, and execute ACH transactions. During the transition, some services may be temporarily unavailable.

Continue obligations: Continue making loan payments, escrow contributions, and other contractual obligations unless formally instructed otherwise by the receiver or acquiring institution. Failure to pay during a transition period can trigger default provisions.

Claims and Legal Rights

File proofs of claim promptly: The FDIC as receiver establishes a formal claims process governed by strict filing deadlines. Under federal law, allowed claims are satisfied after administrative expenses in the following order of priority: depositors first, then general unsecured creditors and senior debt holders, followed by subordinated debt holders, and finally equity holders (12 U.S.C. § 1821(d)(11)). A missed filing deadline can permanently extinguish the right to any recovery.

Review your contracts: Examine all agreements connected to the failed bank for MAC/MAE clauses, force majeure provisions, termination rights, assignment restrictions, cross-default provisions, and notice requirements. A bank failure may trigger rights or obligations under contracts you may not immediately associate with the failed institution.

Notifications and Communications

Notify counterparties, customers, employees, vendors, and regulators as required by contract or law. Timely communication preserves relationships and protects legal rights. For regulated entities, consult compliance counsel regarding disclosure obligations.

Fintech-Specific Response

Fintechs should immediately secure FBO ledger access and confirm the status of all customer funds. Activate backup sponsor bank arrangements. Preserve all customer data and transaction records. Communicate transparently with end users regarding the status of their funds and the timeline for resolution.

Key Takeaways

- Confirm the receiver, acquirer, transaction scope, and account status immediately.
- Do not stop making payments unless formally instructed as default provisions remain enforceable during transition.
- File proofs of claim promptly. FDIC priority rules determine recovery order.
- Review all contracts for triggered rights and obligations, including less obvious cross-default and assignment provisions.
- Transparent, timely communication with stakeholders preserves both relationships and legal rights.

Action Items Checklist

- ☒ Identify the receiver, acquiring institution, and scope of the assumption transaction.
- ☒ Verify access to operating funds, payroll systems, vendor payment capabilities, and online banking.
- ☒ Continue all loan, escrow, and contractual payments unless formally instructed otherwise.
- ☒ File proofs of claim before the FDIC deadline.
- ☒ Conduct a full contract review for MAC/MAE, force majeure, termination, assignment, and cross-default provisions.
- ☒ Issue required notifications to counterparties, customers, employees, vendors, and regulators.
- ☒ Fintechs: secure FBO ledger access, activate backup sponsor banks, and preserve all customer data.
- ☒ Document all communications with the receiver and acquiring institution.
- ☒ Engage legal counsel to assess litigation risk and preservation of claims.

Conclusion

The closure of Tioga-Franklin Savings Bank reinforces that bank failures, though far less frequent than during the 2008-2013 crisis, remain a present and material risk for financial services entities of all types. In this case, the warning signs were publicly available well in advance: the FDIC's April 2024 consent order identified unsafe and unsound banking practices, violations of BSA/AML requirements, and weaknesses in board oversight, management performance, and strategic planning. The subsequent June 2025 civil money penalty for flood insurance violations added a further indication of institutional distress.

For fintechs, SMBs, regional banks, and other financial services entities, the time to prepare is before a

failure occurs, not after. Diversified banking relationships, robust contractual protections, active monitoring, and tested contingency plans are the foundations of resilience.