Shumaker

AUGUST 14, 2026 | PUBLICATION

Who Owns the Compliance Failure? Bank-Fintech Liability Allocation in Banking-as-a-Service (BaaS) Programs

After Years of Enforcement Actions and the Synapse Collapse, the Contract is the Last Line of Defense

INDUSTRY SECTOR

Financial Institutions & Insurance
Financial Services
Technology

SERVICE LINE

Data Privacy
Technology
Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Elizabeth R. Brusa

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

I. The Enforcement Pattern: Regulators Are Holding Banks Accountable

Between 2022 and 2025, the Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), and Federal Reserve issued consent orders against seven sponsor banks operating Banking-as-a-Service (BaaS) programs. The pattern is unambiguous: regardless of what the partnership agreement says about compliance responsibilities, it is the chartered bank—not its fintech partner—that bears the regulatory consequences of fair lending and Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) failures. The FDIC, OCC, and Board of Governors of the Federal Reserve System's June 2023 Interagency Guidance on Third-Party Relationships: Risk Management codified this principle, stating that third-party use does not diminish or remove a banking organization's responsibility to perform all activities in a safe and sound manner, in compliance with applicable laws and regulations. The following table summarizes, at a high level, regulator enforcement actions taken in the past few years:

Bank	Regulator / Date	Conduct at Issue	Remedial Obligations
Cross River Bank	FDIC; March 2023	Unsafe/unsound fair lending practices; weak oversight of fintech partners' credit models (Reg. B/ECOA)	Independent third-party assessment of monitoring capability; risk assessment of all credit products/third parties; fair lending resources study; enhanced Compliance Management System

Bank	Regulator / Date	Conduct at Issue	Remedial Obligations
Blue Ridge Bank, N.A.	OCC; August 2022 (agreement); January 2024 (formal consent order)	Systemic BSA/AML internal controls breakdowns; weak independent testing; failure to remediate 2022 deficiencies; "troubled condition" designation	Board-level oversight of fintech accounts/subaccounts; risk-based suspicious activity report (SAR) compliance program; enhanced independent BSA/AML testing; order terminated only after risk control overhaul and exit from BaaS sector
Discover Bank	FDIC; September 2023 (consent order); April 2025 (amended and restated consent order)	Failure to maintain adequate compliance management system for consumer financial protection regulations	Prior FDIC approval required before any new fintech relationship (effectively froze BaaS expansion); increased board oversight and audits of third-party vendor management
Piermont Bank	FDIC; February 2024	Inadequate internal controls and information systems relative to scope of third-party relationships, risk management, and compliance with AML/BSA controls, training, and testing	Look-back review of all transactions since September 2022; Electronic Fund Transfer Act (EFTA) dispute review since August 2020; BSA training; improved third-party risk management and board supervision
Sutton Bank	FDIC and Ohio Dept. of Commerce; February 2024	Unsafe/unsound banking practices and BSA violations	Full inventory of third-party relationships; designated program managers per partnership for card identification data (CID) /monitoring/SAR filing; BSA officer reporting to board; dedicated board compliance committee
Lineage Bank / Thread Bank	FDIC; January 2024 and May 2024	Fast, multimillion dollar growth via approximately35 fintech programs through partnerships with middleware firm, Unit; post-Synapse exposure and compliance gaps; insufficient due diligence, AML/countering the financing of terrorism (CFT) compliance, and third-party oversight	Contingency plan for termination with third-, fourth-, and fifth-party providers upon service interruptions; contingency plan to orderly terminate significant third-party fintech partner relationships; improved oversight and capital standards, including independent risk analysis and audit

Bank	Regulator / Date	Conduct at Issue	Remedial Obligations
Evolve Bancorp, Inc., and Evolve Bank & Trust	Federal Reserve; June 2024 (cease-and-desist)	Deficiencies in fintech risk management, AML/BSA compliance, and consumer compliance programs; failures reconciling For Benefit Of (FBO) pooled deposit ledgers for middleware provider, Synapse-affiliated end users	Cease and desist requiring remediation of risk management, BSA/AML compliance programs, and third-party oversight deficiencies

KEY TAKEAWAY & NEXT STEP

Regulators have consistently held the sponsor bank—not the fintech—responsible for compliance failures and now treat the absence of a wind-down contingency plan as an independent violation.

Action items:

- Banks: Benchmark your current fintech oversight program against the remedial obligations in the table above (board-level reporting, per partnership compliance officers, look-back reviews) before a regulator does it for you.
- Fintechs: Ask your sponsor bank what independent testing and reporting it is already subject to as your business continuity depends on the bank's compliance posture.
- Both parties: Confirm your current agreement includes a wind-down contingency plan; regulators now treat its absence as a standalone deficiency.

II. Why This Pattern Is Doctrinally Compelled, Not Incidental

This enforcement pattern is not a policy choice that could shift with the next administration, as it is a structural feature of bank regulatory law. The Bank Secrecy Act (31 U.S.C. § 5311 *et seq.*) and its implementing regulations impose BSA/AML obligations directly on "banks" as defined at 31 CFR 1010.100(d). Each federal banking agency's regulations—including 12 CFR 21.21 (OCC), 12 CFR 208.63 (Federal Reserve), and 12 CFR 326.8 (FDIC)—require the bank itself to maintain a multi-part BSA program: internal controls, independent testing, a designated BSA officer, ongoing training, and appropriate risk-based procedures for ongoing customer due diligence.

Critically, most fintech partners are technology providers with no independent BSA obligations. Even those that qualify as money services businesses carry materially less comprehensive AML requirements than banks. A contract provision purporting to shift responsibility for BSA/AML compliance to the fintech does not and cannot alter the bank's statutory exposure. It may reallocate cost through indemnification, but it does not relieve the bank of its regulatory duty. Regulators look through contractual delegation clauses to the bank's actual governance, monitoring, and audit practices. Banks cannot delegate their BSA/AML obligations to their fintech partners and hope for the best.

KEY TAKEAWAY & NEXT STEP

BSA/AML compliance obligations attach to the bank by statute and cannot be shifted to a fintech by contract. A delegation clause may reallocate cost but does not reduce the bank's regulatory exposure.

Action items:

- Banks: Review BaaS contracts to confirm compliance delegation language does not overstate what the contract can accomplish; maintain independent audit/testing rights rather than relying on fintech self-certification.
- Fintechs: Recognize that your BSA/AML representations will be tested against the bank's actual regulatory exposure, not just contract language; be prepared to submit to bank-directed audits.
- Both parties: Confirm the contract distinguishes between compliance ownership (non-delegable, stays with the bank) and cost allocation (contractually negotiable).

III. Synapse and the Litigation Frontier: Testing Economic Risk Allocation

If regulators will always hold the bank responsible for compliance failures, the next question becomes whether contract provisions can at least shift the economic consequences. The Synapse Financial Technologies (Synapse) bankruptcy, filed April 22, 2024 in the Central District of California, Case No. 1:24-bk-10646, has become the paradigmatic test case.

Synapse operated as middleware connecting approximately 100 fintechs to partner banks, serving roughly 10 million end users. When a planned asset sale to TabaPay collapsed in May 2024 after Evolve Bank & Trust and other stakeholders disputed accountability for a multimillion-dollar shortfall in FBO pooled customer accounts and refused to cover the shortfall, Synapse cut off partner banks' access to its technology platform, freezing consumer access to funds.

The fallout has been extraordinary. The Consumer Financial Protection Bureau (CFPB) commenced an adversary proceeding in August 2025 and entered a stipulated judgment in September 2025, allocating approximately $46 million to victims from the CFPB's Civil Penalty Fund, the first distribution of its kind in a BaaS failure. A class action targets both Evolve Bank & Trust and Lineage Bank, alleging mismanagement of customer funds following Synapse's collapse. The FDIC issued a proposed "Synapse rule" in September 2024 requiring banks to maintain accurate beneficial-owner records in custodial accounts, but the FDIC subsequently withdrew the proposed rule. Courts are scrutinizing broad-form "no-fault" indemnities—particularly where there is bargaining power imbalance—and reading indemnification clauses narrowly against a party seeking to escape a nondelegable statutory duty.

KEY TAKEAWAY & NEXT STEP

The Synapse bankruptcy shows that indemnification and risk-allocation clauses are now being tested in real litigation, and courts are skeptical of vague, capped, or misaligned indemnities when regulators and consumers pursue every party simultaneously.

Action items:

- Both parties: Stress test your indemnification language against a "what if all parties get sued at once" scenario rather than assuming contractual allocation will hold.
- Fintechs and banks: Confirm that reconciliation and beneficial ownership recordkeeping for pooled/FBO accounts is real time and auditable, as Synapse's core failure was a ledger gap, not just a compliance gap.
- Legal teams: Monitor for anticipated renewed proposal of the FDIC's "Synapse rule" on beneficial owner recordkeeping and begin conforming practices now rather than waiting for a final rule.

IV. Drafting for the New Regulatory Reality: A Practical Checklist

Sophisticated market participants should not respond to this landscape by abandoning BaaS, as it remains a commercially valuable model. Rather, they should respond by drafting contracts that anticipate regulatory expectations instead of merely allocating blame after the fact. The following framework separates nondelegable regulatory compliance ownership from legitimately allocable economic risk.

A. Representations and Covenants

The contract should explicitly acknowledge that BSA/AML, fair lending, and safety-and-soundness compliance ownership is nondelegable and remains with the bank. Within that framework, the fintech should provide the following representations and ongoing covenants:

- **BSA/AML and Office of Foreign Assets Control (OFAC) program maintenance.** The fintech represents

and covenants that it maintains a BSA/AML and OFAC screening program commensurate with the risks posed by the end customers or bank products, paired with a covenant granting the bank the right to require independent third-party testing or audit of that program at specified intervals.
- **Fair lending data provision.** The fintech covenants to provide promptly upon request the customer, transaction, and product information necessary for the bank to independently determine and monitor fair lending compliance across credit products, third parties, and credit models.
- **Beneficial ownership and ledger reconciliation recordkeeping.** For pooled or FBO account structures, the fintech covenants to maintain real time, auditable records of beneficial ownership and ledger reconciliation—directly responsive to the FDIC's proposed "Synapse rule" and designed to prevent the reconciliation failures that left millions of dollars in consumer funds unattributable after Synapse's collapse.
- **Subcontracting disclosure and liability.** Where the fintech relies on subcontractors or middleware, the agreement should require disclosure of all subcontracting arrangements, specify which party is liable for a subcontractor's conduct, and grant the bank approval rights over material subcontracting changes, consistent with the interagency guidance recommending that contracts specify the third party's liability for activities or actions by its subcontractors.

B. Liability Caps and Indemnification

Generic dollar caps or fee multiples are ill suited to BaaS partnerships because regulatory penalties, consumer class-action exposure, and remediation costs can dwarf program fees. Instead:

- **Calibrate caps to specific compliance functions.** Rather than a single aggregate cap, consider tiered caps that reflect the actual risk of each compliance obligation—a higher or uncapped exposure for BSA/AML control failures and a standard cap for routine operational service levels.
- **Carve out from any cap:** (i) losses from the fintech's failure to implement an agreed BSA/AML or fair lending control; (ii) regulatory fines or consent order remediation costs directly attributable to fintech conduct; (iii) losses from breach of specific representations and covenants (particularly the data provision and recordkeeping covenants above).
- **Define "losses" expressly.** State whether recoverable losses include attorneys' fees, consequential damages, regulatory penalties, and remediation costs (e.g., independent consultant fees, look-back review expenses). Ambiguity here is a frequent source of post-dispute litigation.
- **Avoid broad "no-fault" indemnities.** Courts have scrutinized and may decline to enforce indemnities making one party responsible for "any and all regulatory action" regardless of which party's conduct caused the violation, especially where there is bargaining power imbalance. Tie indemnification to identified conduct, not to regulatory outcome alone.

C. Termination and Wind-Down Provisions

Contracts should address:

- **Regulatory risk termination triggers.** Include termination rights triggered by a partner's receipt of a regulatory enforcement action, examination finding, or failure to remediate identified deficiencies within a specified period (e.g., 60–90 days)—rather than relying solely on generic "material breach" language that may require extended cure periods.
- **Orderly wind-down planning.** Build data transition protocols, customer notice obligations, and interim servicing continuity arrangements directly into the contract. Specify timelines for data migration, formats for customer record transfer, and responsibility for customer communications during the transition. The Synapse collapse demonstrates that abrupt terminations are what convert ordinary compliance risk into consumer harm and creditor recovery uncertainty.

- **Monitoring, reporting, and escalation.** Specify reporting frequency, escalation triggers, and named compliance contacts on both sides. Include rights to increase oversight frequency upon triggering events.
- **Fee and cost allocation on exit.** Specify which party bears audit, examination, and wind-down costs. Avoid burdensome termination fees or reimbursement obligations that create perverse incentives to remain in a deteriorating relationship rather than exit promptly when compliance conditions demand it.

D. Subcontractor Oversight

Where BaaS arrangements involve middleware or program management layers, additional protections are essential:

- The bank should reserve the right to terminate without penalty if a fintech's subcontracting arrangements fail to comply with contractual compliance obligations or receive an adverse regulatory finding.
- Require effective pre-established protocols enabling rapid recovery of customer funds in the event of a middleware or BaaS platform failure, designed to eliminate protracted bankruptcy proceedings and ensure consumer access to funds within days, not months.
- Include flow-down requirements ensuring that the fintech's subcontracts contain materially equivalent compliance, audit, termination, and data access provisions, so the bank's contractual protections are not rendered hollow at the subcontracting layer.

KEY TAKEAWAY & NEXT STEP

Treat compliance ownership representations, calibrated liability caps, and proactive termination/wind-down mechanics as core deal terms—not boilerplate—because generic caps and vague indemnities may prove inadequate once a compliance failure or platform collapse actually occurs.

Action items:

• Audit existing liability caps against the carveout list above (BSA/AML control failures, attributable regulatory fines, breach of specific reps) and replace flat dollar caps or fee multiples with risk-calibrated structures.

• Add termination triggers tied to a partner's receipt of a regulatory enforcement action or exam finding, not just generic "material breach" language.

• Build a specific wind-down protocol into the contract now (data transition steps, customer notice, interim servicing continuity) rather than improvising one during an actual termination.

V. The Ultimate Stakes: Proprietary Risk, Not Just Regulatory Risk

The consequences of poorly structured BaaS agreements extend well beyond consent orders. Abrupt BaaS terminations can strand consumer receivables in true sale/true lender ownership limbo, disrupt servicing, and create genuine bankruptcy priority contests over both deposit-type custodial funds and loan receivable portfolios.

The true lender doctrine asks whether the named lender is the "true lender" or whether another entity—typically the fintech—holds the predominant economic interest or acts as the true lender under the specific facts and circumstances.

The Synapse proceeding demonstrates these stakes in real time. The core failure was a reconciliation mismatch between fintech app ledgers and sponsor bank records, meaning individual consumers could not

be reliably matched to their share of pooled custodial accounts. Evolve retained approximately $8 million through self-help setoff to cover potential losses in winding down its relationship with Synapse—itself contested in the bankruptcy. And because Synapse did not hold customer deposits directly, the dispute became an unusual insolvency priority contest over funds at non-debtor banks, turning on unreliable ledger data rather than clean legal characterization.

KEY TAKEAWAY & NEXT STEP

The ultimate risk of getting compliance and contract structure wrong is proprietary and financial—not just regulatory. Abrupt BaaS terminations can strand receivables and custodial funds in ownership limbo, triggering genuine bankruptcy priority contests.

Action items:

- Confirm which entity holds economic ownership of receivables under a true lender/predominant economic interest analysis and consider participation-based structures to reduce true lender challenge risk.
- Establish real time beneficial ownership ledger reconciliation for pooled or FBO custodial accounts before a platform failure occurs.
- Negotiate preestablished rapid fund recovery and wind-down protocols into the BaaS agreement itself to avoid protracted bankruptcy or court resolution.

Conclusion. The lesson of the past few years is straightforward: in a BaaS relationship, regulatory liability stays with the bank by operation of law, and no contract can change that. What the contract can do is allocate economic risk intelligently, create governance structures that satisfy regulators in the first instance, and provide orderly exit mechanisms that protect consumers and preserve asset value when—not if—a partnership deteriorates. The cost of getting this wrong is no longer theoretical. It is measured in frozen consumer accounts, contested receivables, multiyear look-back reviews, and lengthy bankruptcy and insolvency proceedings. For both fintechs and sponsor banks, the time to negotiate these protections is before the consent order, not after.

For more information about bank-fintech liability allocation in BaaS programs, please contact Elizabeth Brusa.

© 2026 Shumaker, Loop & Kendrick, LLP. All Rights Reserved. Privacy Policy/Disclaimer

Shumaker