Infinicept

GET PAYMENTS GOING YOUR WAY™

The New Standard for Sponsor Bank Oversight: Meeting Regulator Expectations in 2026

Table of Contents

In May 2024, more than 100,000 consumers lost access to accounts where they had deposited funds totaling more than $265 million.

The financial nightmare for these consumers began when Synapse, a company that served as a middleman between banks and consumer-facing financial apps, filed for bankruptcy in late 2023.

During the bankruptcy proceedings, Evolve Bank, which held funds for users of these apps in pooled custodial accounts, said that it could not reconcile balances in Synapse's systems to the funds in the accounts and shut down access to those accounts.

Ultimately, banks and regulators discovered a shortfall in the tens of millions between the funds that customers had in accounts associated with Synapse partners and the amount of money that was actually in the bank.

While money has been returned to many consumers, many are still waiting. Lawsuits have been filed and new rules have been proposed to address the underlying issue: poor recordkeeping that the bank did not see until it was too late.

While it was ugly, the Synapse failure wasn't an isolated one. One law firm analysis found that regulatory agencies had entered into more than 45 cease and desist orders from June 2023 to June 2024 citing risk management failures between banks and their third-party partners.

The Synapse meltdown simply put a public face on what many observers had been warning of: systemic weaknesses in bank oversight of the fintech companies that made banking and access to money more convenient.

What message can we take away from all this? The old approach isn't enough anymore.

Where in the past a bank might have been able to look at things linearly, today's environment requires a much more holistic approach. The entire ecosystem must be understood.

That understanding begins with the regulatory environment. Banks have to go beyond complying with the letter of their regulators' requirements, to understanding the context around those requirements and how they relate to other entities that govern banks' oversight activities.

The FDIC's Proposed "Synapse Rule"

When things go south within the financial system, regulators respond with new rulemaking intended to address the structural issues that enabled the problems.

In response to the Synapse situation, the FDIC proposed a new rule in 2024. Part of the issue with the Synapse case is that consumers who deposit money in these accounts don't have individual accounts at the banks where the money is kept. Instead, the money is pooled in larger custodial FBO (for benefit of) accounts.

The FDIC's new rule sought to increase consumer confidence by outlining more explicit requirements about the records companies that pool money in FBO accounts must maintain. This new rule is similar to what the card networks require of payment facilitators.

In the press release announcing the proposed rule, FDIC Chairman Martin J. Gruenberg mentions Synapse as he explains the reasoning behind the agency's action:

"The Notice of Proposed Rulemaking approved by the FDIC Board today is an important step to ensure that banks know the actual owner of deposits placed in a bank by a third party such as Synapse, whether the deposit has actually been placed in the banks, and that the banks are able to provide the depositor their funds even if the third party fails," Gruenberg said.

The proposed rule includes:

- New recordkeeping requirements for custodial accounts, so banks or their third parties maintain accurate records of the owners of funds within those accounts and the balance for each owner.
- A requirement that banks have "direct, continuous, unrestricted access" to records
- Daily reconciliation requirements

The Divergence Problem: Federal vs. Card Network

That's what happens when a serious gap in the financial system is identified. But while federal regulators respond to financial crises, they also respond to the prevailing political winds, which sometimes rein in that regulatory response.

The growing role of fintechs in public life raises issues that are often on the minds of legislators. For example, a House bill introduced in December 2025 directs regulators to study partnerships between banks and fintechs to gain more data about how these partnerships affect the entire ecosystem.

Within lawmakers' efforts, there is a continual push and pull between the ideas of consumer protection and enabling innovation. Recently federal regulators also announced that they were eliminating the consideration of reputational risk during underwriting. This might allow companies more space to conduct business, but it is a step away from consumer protection and robust risk management.

While federal agencies bend to the current political will, card networks are evolving their own rules in favor of more robust protections. In 2025, Visa tightened controls with its new Visa Acquirer Monitoring Program (VAMP) and in 2024 its Visa Acceptance Risk Standards (VARS) replaced an older framework for risk controls.

For this reason, banks always need to stay vigilant and make sure they are designing programs and implementing protections that keep a holistic view of the ecosystem in mind.

States are also making their own moves. After a junk fee rule at the federal level was significantly weakened, several states enacted pricing transparency laws to ensure that all mandatory fees are included in pricing upfront.

The takeaway here for banks is that they are governed by a multilayered system. Some banks maintain a narrow view and think if they pass an audit from the office of the Comptroller of the currency (OCC), for instance, they've done what they need to do.

In reality, this leaves them at risk for enforcement actions from the card networks whose requirements may not necessarily be met. When the federal winds blow toward deregulation, states and card networks tend to step in to fill in consumer protection gaps.

For this reason, banks always need to stay vigilant and make sure they are designing programs and implementing protections that keep a holistic view of the ecosystem in mind. Rather than reacting to political winds blowing at the federal level, the more prudent approach for banks is to build robust programs that position them well regardless of regulatory direction.

The Consent Order Pattern

When regulators identify deficiencies within a bank's practices they might issue consent orders. These orders are public and they lay out what the bank must do to correct violations or unsafe practices.

The orders are called consent orders because the bank agrees to comply with them without admitting any wrongdoing, rather than go through legal proceedings.

Over the last few years, banks with significant fintech partnerships such as Thread Bank, Blue Ridge Bank, Sutton Bank and Lineage Bank, have agreed to consent orders related to their relationships with fintechs, the infrastructure they have in place to oversee them, and the risk management procedures associated with them.

A look at these consent orders reveals some common themes.

These include lapses in verification, where banks may have requirements but they're not verifying that those requirements are being followed with solid documentation and a regular oversight cadence. This is the "trust but not verify" trap.

The orders are also identifying scaling failures, where a bank's processes and staffing levels aren't growing as their fintech portfolio grows, insufficient processes for addressing Bank Secrecy Act (BSA) requirements and other anti-money laundering rules, weak board oversight, and inconsistent risk calibration across partner types.

Finally, regulators are watching for gaps in banks' access to data because of an overreliance on ledgers that the fintechs themselves maintain. The Synapse debacle brings the dangers of this to the public consciousness in a very painful way.

As noted earlier, bank oversight of third parties today requires a holistic approach that looks not only at individual transactions but the entirety of the ecosystem surrounding a bank's portfolio.

For consumer fraud, we need to think about before the transaction is authorized. For merchant fraud or other merchant issues, we need to focus on the period after the transaction is authorized but before paying the merchant.

Banks need to not only monitor merchant transactions but also understand where their goods are coming from. If they have any future delivery products in their portfolio, for example, they have to stay on top of the geopolitical landscape, as tariffs or bickering countries may cause delivery issues with the potential to result in chargebacks.

They also have to understand scams, where the payment is the last leg in the scheme, to be able to help stop harmful transactions.

With that backdrop in mind, here are some of the critical components that make up a bank's third-party oversight system.

Verification Metrics

To verify the activities of their third-party partners properly, the bank must establish certain metrics, as well as thresholds and escalation triggers for these metrics, and require their third parties to comply with them.

These metrics cover the entirety of a fintech partner's relationship with its merchants or customers. They begin during the underwriting process. The bank needs to know the percentage of merchants that are auto-approved, pended, and manually approved. They should also know how many are approved with KYC / KYB or other regulatory or policy overrides.

Further metrics are related to the processing itself. These include loss percentages and chargeback ratios by type, including but not limited to fraud, not as described, did not receive, or refund not received.

Banks should also go beyond evaluating single metrics in isolation. For example, it's important to consider how losses relate back to how the merchants were approved in the first place. Are there larger or more frequent losses coming from those who were approved with policy overrides? And banks can glean useful oversight information from further combinations of metrics such as, of the auto-approved merchants, how many were closed for fraudulent transactions.

Finally, banks also need to know the percentage of the partner's processing in high-risk categories, so they have a true picture of their partners' risk exposure. These high-risk categories include card network-defined merchants that pose credit, fraud, or regulatory risk as well as other types of merchants.

As noted, "high risk" refers to more than those which must be registered with the card networks. It also includes, among other things, high-chargeback merchants or financially weak merchants with future service products.

Verification Cadence

It's important for banks to carefully consider how often they must review different aspects of a third party's programs.

For example, the Visa Integrity Risk Program (VIRP) is a program to ensure businesses do not sell illegal, harmful, or unethical products online. These might be things like prescription drugs without the prescription, counterfeit goods, promises about what a product can do that it cannot, as well as even illegal drug sales and human trafficking.

A lot can happen in a year. If the bank reviews its partners only annually, as has been seen in banks who have received consent orders or card network violations, they might be fine when they're reviewed. But maybe their personnel changes, or they become overwhelmed. They may begin to slide and not do all of the required or promised diligence.

Changes in a partner's behavior will be hard for a bank to catch if they are only coming back for verification once a year. The bank could be blindsided by violation notices from the network mid-year.

However, if they review some items monthly and others no less often than quarterly, they are more likely to be able to correct the issue before a violation is received or a consumer is harmed.

Data Ownership and Access

The Synapse failure highlighted another critical piece of the puzzle for banks. Relying on partner systems and data leaves both banks and consumers vulnerable if the third party fails.

The FDIC's proposed Synapse rule requires banks to have "direct continuous access" to records and data to provide a fallback to make sure the appropriate records are being kept. In some cases, banks may even need to bring this data in house rather than relying on their partner systems.

The third party doesn't have to fail, however, for this access to data to be important.

When banks allow third parties to settle elsewhere, or they don't make sure beneficial accounts are properly maintained, it is easier for client funds to be misrepresented on the partner's financials. Banks must make sure funds are properly classified so they have a clear and accurate picture of the third party's own financial strength. Proper maintenance of beneficial accounts makes any improper mingling of funds easy to spot.

Banks also need data access so they can monitor their partners' settlement practices. They need to make sure funds are balancing properly on a daily, weekly and monthly basis, and ensure that KYC, and KYB when appropriate, is conducted on those receiving payment.

They also need strong oversight over reserves, the practice of holding back a certain percentage of funds from a merchant to guard against losses, to verify that the fintech is using this tool properly, especially with its riskier merchants.

The bank does not have to perform these duties for the partner, but they must have access to the information so they can review and verify that the third party is performing them with banking levels of care.

Board-Level Accountability

The consent orders issued by federal regulators don't tend to point the finger at lower-level employees. The Thread Bank order, for example, places responsibility for compliance squarely with the bank's Board of Directors.

The order directs the bank's Board to monitor and verify compliance with the order, and it assigns specific items within the bank's strategic planning and policies and procedures to the Board to address. It even goes so far as to stipulate that the bank's Board must review risk tolerance thresholds for each individual fintech partner.

Laying out the responsibility to the Board in this way ensures that the bank's directors truly understand its portfolio, not just a high-level aggregation of its partners.

Business Continuity for Third-Party Failures

Finally, the Synapse failure highlighted a critical point that many banks neglect: what happens when an intermediary goes down?

Many of these fintech companies have great ideas and obtain enthusiastic funding that legitimizes their operations. We've all seen firsthand how the best intentions are simply not enough.

To protect themselves and to protect their consumers, banks must ensure that their relationships with third party partners include contractual provisions that protect their access to data and funds so consumers can more easily be made whole if a fintech becomes unable to fulfill its obligations.

Making Oversight Strengthen Relationships

Some banks are reluctant to implement the verification needed to provide true oversight to their third-party partners. And this isn't without reason. Perhaps they have solid relationships with their partners and feel that high-level conversations about compliance are enough. Perhaps the third party has enough market power to push back against the banking regulations and receive dispensation.

Fintechs, for their part, speak innovation rather than compliance. They don't always fully understand the nuances of what's needed as well as a bank, which has compliance in its DNA, and they tend to be resistant to what feels like oversight overreach.

But it remains a bank's responsibility to do what must be done. Setting expectations early at the outset of the relationship and framing the need for verification as protection of everyone in the ecosystem (the consumer, yes, but also the bank and the fintech) can help blunt the feeling of not being trusted.

The Synapse meltdown and other consent orders can help the bank make its case early by serving as cautionary tales about what happens when even the best of intentions come up against the reality of market forces.

Scaling Without Adding Headcount

Oversight staffing levels are of course an important consideration for banks, which need to manage their limited resources wisely. There are ways for banks to scale their capabilities while keeping their personnel costs from soaring.

One prudent approach is focusing resources by assigning partners to tiers of risk. Banks that truly understand their portfolios can use their resources wisely by applying more focus on the partners that present the most risk.

This doesn't mean ignoring their other partners, of course. But a robust understanding of the risk inherent in your portfolio enables you to apply more rigor and depth where it is warranted, and to adjust that as your portfolio and the merchants within it evolve.

This is where technology can also come to our aid. Automated underwriting and transaction monitoring systems use machine learning to identify anomalies in patterns across large sets of data. These systems can take care of the simpler cases and flag concerns for human review and judgement, again helping to apply more expensive resources where they're most needed.

As more resources are applied within the technology industry to developing AI tools, these systems are likely to continue to improve as well, speeding the rate at which decisions can be made and helping humans to focus on what matters most.

KEY TAKEAWAYS

- Be sure you've established appropriate metrics for your third-party partners and verify that they're complying with them.
- Increase the cadence of your oversight. There are daily oversight items as well as weekly, monthly and even quarterly items. Understand the risk presented by the third parties' portfolios and conduct your reviews of tasks like underwriting, KYB and KYC activities, transaction monitoring, and sales agent vetting and activities accordingly.
- Have strong settlement oversight. Ensure the proper settlement vehicles are used and that the third party has daily settlement balancing along with their monthly duties.
- Remember to review the financial strength of third-party partners. Ensure that client funds are not being touted as part of their strength.
- Ensure that contracts contain appropriate provisions to protect your access to data and funds in the event of a partner failure.
- Educate your third parties on the "why" of oversight, not just the "how." Make them a partner in the oversight process.
- Understand how technology and prudent practices like risk tiering can help you scale as your portfolio grows.
- Have an outside partner review your oversight to ensure it meets not only regulatory and card network requirements, but industry best practices. An outside partner should also review your third parties to ensure there are no trust but verify gaps and that their processes meet not only your requirements, but regulatory and card network requirements and industry best practices. Companies such as Infinicept can advise you and help you navigate this complex and continually shifting landscape.

THE PATH FORWARD

A look back at decades of history in the payments space tells us that the oversight environment will continue evolving. The only true constant is change, as they say.

But it's critical for banks to keep in mind that effective oversight isn't just about avoiding consent orders and staying current with the regulatory flavor of the day.

It's about creating sustainable partnerships where open communication replaces misunderstandings and missed opportunities. And it's about catching issues early and rectifying them long before poor practices are baked into a fintech's processes or a regulatory entity, whether that's the federal or state government or a card network, finds reason to complain.

As a bank, you have fiduciary responsibility to protect those whose funds are in your institution first, your income and shareholders second. Banks that build robust programs will be well positioned regardless of regulatory direction. They'll avoid attention for oversight failures and instead attract the best partners interested in creating solutions that serve consumers in safe, secure environments.

ABOUT INFINICEPT

Infinicept brings decades of hands-on payments expertise to help banks, payment companies, and their fintech partners build the robust oversight programs today's environment demands. Our Paysolve advisory team, whose experts literally wrote the ETA's guidelines on Payment Facilitator best practices, offers Fitness Reviews to assess your current third-party oversight against regulatory and card network standards, Card Network Review services to ensure VARS and Mastercard compliance before issues arise, and comprehensive Policy and Procedure development tailored to your specific portfolio and risk profile. Whether you need a gap analysis of your existing program or a ground-up build of your oversight framework, our consultants work alongside your team to create sustainable, scalable solutions.

Beyond advisory services, Infinicept's Payops platform gives registered PayFacs a comprehensive solution to manage their payment facilitator program, from automated underwriting and transaction monitoring to merchant management and ongoing oversight. And for software companies ready to monetize payments, Launchpay delivers flexible PayFac-as-a-Service infrastructure backed by the same deep expertise that guides our advisory practice.

To learn how Infinicept can strengthen your oversight capabilities, visit infinicept.com or connect with our team at ETA TRANSACT.