The questions sponsor banks actually ask.

2026 edition. First edition. Two parts: thirty-six questions your sponsor bank will ask, and the document pack it will ask you to produce. Ordered by what most often goes wrong. Free, ungated, no form.

CONTENTS

What changed

If your compliance program was built before 2024, it was built to satisfy a regulator. That is no longer where the pressure comes from.

Federal enforcement has measurably slowed. Federal Reserve enforcement actions are down roughly half since the pandemic (Brookings, July 2026). The Fed folded its dedicated crypto and fintech supervision program back into normal supervision in August 2025 (Federal Reserve press release). In April 2026 the OCC and FDIC finalized a rule barring examiners from citing reputation risk or pressuring banks to end third-party relationships over lawful but disfavored business (OCC Bulletin 2026-12; 91 FR, 10 April 2026). An Executive Order signed in May 2026 directs every federal financial regulator to identify what "unduly impede[s] fintech firms from entering into partnerships with federally regulated institutions" (EO 14405, signed 19 May 2026).

None of that made your life easier, because the demand did not disappear. It moved. It now arrives through your sponsor bank's diligence questionnaire and your partnership agreement rather than through the Federal Register.

The clearest illustration is a rule that never passed. The FDIC proposed a custodial account recordkeeping rule in October 2024: beneficial-owner-level records in a standardized electronic format, direct continuous bank access, independent validation, and an annual certification signed by an executive officer (89 FR 80135, 2 October 2024). Comments closed in January 2025. It now sits in the Unified Agenda's long-term actions with a final date of "to be determined" (RIN 3064-AG07). It was not withdrawn. It was not finalized.

And banks wrote its substance into their contracts anyway.

The rule never passed. Your bank adopted it anyway. That is the environment this list describes.

One more thing did not loosen. Consumer-compliance supervision softened considerably; BSA and sanctions did not. The single bank-level fintech-partnership enforcement action in the first three quarters of 2026 was a BSA/AML order, and you will meet it in question 8.

How to use this

Answer every question one of three ways.

Yes. You can answer from your systems today, with a record, without asking anyone. **Only by hand.** You could answer, but you would have to assemble it yourself. **No.** You could not produce it.

A flat no is visible in a first review and gets fixed. **"Only by hand" is the bigger problem**, because it survives the first review and fails the second, when the reviewer asks for the same thing again and notices it took two weeks both times.

PART ONE: WHAT THEY WILL ASK YOU

Thirty-six questions. These test whether you can answer.

---

1. The question that predicts the rest

1. Can you produce every enhanced due diligence decision your team made in the last ninety days, with the reasoning, by tomorrow?

Start here. If the answer is a two-week project, you can stop marking up the rest of this list, because you already know what it will say.

A defensible answer is produced from the system, not reconstructed from it. Most teams can describe what they would do in a given case. Far fewer can produce what they actually did. That distinction is the thing every other question below is circling, and it is where diligence cycles most often go sideways.

---

2. The sponsor-bank relationship itself

This section did not exist in a 2023 version of this list. It is now where diligence concentrates.

2. Can your bank independently reconstruct end-user balances at any moment, to the penny, without depending on you and without delay?

A defensible answer addresses the bank's independent capability, not yours. Note the shape of the question: it is not "do you reconcile." Post-Synapse, the expectation is that the bank can reconstruct the position without your cooperation, because the failure mode being guarded against is precisely a fintech that cannot or will not cooperate. "Our system reconciles nightly" answers the question as it was asked three years ago.

3. Where does data replication or escrow sit, and what are your bank's step-in rights?

A defensible answer points at an executed arrangement, not an intention. FBO and omnibus structures were not banned after Synapse. What changed is that they now come with hard controls attached: replication or escrow, independent reconciliation, and enforceable step-in rights. If your agreement is silent on step-in, your bank's next counsel review will not leave it silent.

4. Where do customer funds sit at each point in the flow, in whose name, and under what account structure?

A defensible answer is a diagram, not a sentence. Every entity, every account, and the legal character of the holding at each step. This is the question the entire post-Synapse environment exists because of, and it is the one most often answered at a level of generality that would not survive a follow-up.

5. What reserve does your bank hold against your program, how was it sized, and what changes it?

A defensible answer explains the sizing logic rather than just the number, and knows what would trigger a change: volume growth, a shift in product mix, a chargeback or return-rate threshold, a new geography. A program that does not know why its reserve is what it is cannot forecast its own working capital.

6. What is your settlement timing, and what happens to funds in transit if you or a processor fails mid-cycle?

A defensible answer covers the failure case specifically. Settlement timing under normal conditions is easy. The question behind the question is whether anyone has thought through a mid-cycle failure, and whether the answer is written down anywhere a third party could follow.

7. Do you understand your own indemnity and liability position under the partnership agreement?

A defensible answer can state, without looking it up, whether BSA/AML exposure sits inside or outside the liability cap, whether regulatory fines are carved out, and what triggers termination on regulatory grounds as distinct from material breach.

The reason a bank asks a version of this is not curiosity about your contract. It is testing whether the people running your compliance program know what the company is exposed to, because a team that does not know tends to be a team that has not read the agreement against its own operations. The underlying principle is worth stating plainly: BSA/AML obligations attach to the bank by statute and cannot be shifted to a fintech by contract. That is precisely why the bank pushes the cost of failure onto you, and why it wants to see that you understand what you signed.

Also appearing, though more often in agreements than in questionnaires

These two show up in partnership agreements and in counsel's redlines more reliably than they show up in a diligence call. Treat them as things to have ready rather than things you will definitely be asked.

Your wind-down plan. In 2024 this was a clause in the termination section. It is increasingly a document, with data transition mechanics and customer notice timelines, that a bank wants to see before signing.

Subcontractor disclosure and approval rights over material changes. This reaches your vendors' vendors. Changing your screening provider may now be a notifiable event.

---

3. Monitoring, thresholds, and who governs them

8. How were your monitoring thresholds calibrated to your risk profile, who approved them, and what happened to the alerts that closed without human review?

A defensible answer produces the calibration record and the disposition of auto-closed alerts.

This is the most consequential question on the list right now, and it is not hypothetical. In April 2026 the OCC issued a consent order against Community Federal Savings Bank, docket AA-ENF-2025-21, made public in May (OCC enforcement release). CFSB is the sponsor bank behind Wise's USD accounts and Crypto.com's prepaid card issuance. The central finding was that the automated suspicious-activity monitoring system's filtering criteria and thresholds were not calibrated to the bank's risk profile, with the result that alerts requiring human review were auto-closed. The order also cited inadequate customer due diligence and failure to identify foreign correspondent accounts, and observed that the bank had grown its payment processing line without building controls commensurate with that growth.

Your bank read that order. Assume the question is coming.

Two questions travel with this one, and they are usually asked as follow-ups rather than on their own. **Can engineering change a monitoring threshold without compliance approval?** The answer should be no, demonstrated with a control rather than asserted as a norm; this is one of the fastest ways for a reviewer to conclude that compliance does not actually govern the system. And **when did you last tune your scenarios, and what changed?** The tuning documentation should include thresholds you deliberately left alone, with the reason. A tuning exercise that changed everything reads as panic. One that changed nothing reads as theatre.

9. What scenarios or rules do you run, what risk does each address, and who approved them?

A defensible answer maps rules to the risks in your own risk assessment. Rules that exist because they shipped with the vendor, addressing risks your business does not have, signal a program that was bought rather than designed.

10. What are your alert volumes, your alert-to-case conversion rate, and your backlog?

A defensible answer gives the numbers and explains them. A very low conversion rate suggests rules that do not work; a very high one suggests rules that are not tuned. A backlog is not automatically a finding. An untracked backlog is.

4. Customer onboarding

11. Walk us through what happens between a customer submitting an application and being able to move money.

A defensible answer is a flow the reviewer can follow, matched against what the platform actually does. The common failure is not a bad process. It is that the described flow and the implemented flow diverged at some point and nobody updated the description.

12. Show us the last fifty accounts you approved. How many had exceptions, and who approved them?

A defensible answer comes out of the system in minutes. Exceptions are where policy meets commercial pressure, and an exception process that lives in a chat thread is not an exception process.

13. What identity elements do you collect, and how do you verify them?

A defensible answer distinguishes collection from verification and names the sources and match logic. "We use [vendor]" does not describe how verification works.

Worth knowing: since June 2025, an exemptive order from FinCEN and the banking agencies permits banks to collect a customer's taxpayer identification number from a third party rather than from the customer before account opening (FinCEN, 27 June 2025; the Federal Reserve joined on 31 July 2025, SR 25-2). It is optional, and the bank still needs written risk-based procedures and a reasonable belief it knows the customer's true identity. If your model depends on this flexibility, know that it is an exemption rather than a right.

14. For business customers, how do you identify and verify beneficial owners, and at what threshold?

A defensible answer covers both the ownership and control prongs, explains layered structures, and says what happens when the structure cannot be resolved.

15. What is your process when a customer fails verification, and can they reapply?

A defensible answer addresses the reapplication loop specifically. A program with no controls there can be defeated by persistence.

5. Risk rating and enhanced due diligence

16. How do you risk-rate customers, what drives the rating, and how often is it refreshed?

A defensible answer shows the factors, the weighting, and evidence that ratings actually move. A model where 96% of customers land in low risk is read as a model that does not discriminate.

17. What triggers enhanced due diligence?

A defensible answer connects the trigger logic to question 1. If the triggers are documented but the decisions are not retrievable, you have a policy rather than a control.

18. How do you identify politically exposed persons, and what do you do differently for them?

A defensible answer covers identification at onboarding and on an ongoing basis, and specifies what "differently" concretely means: approval level, review frequency, documentation.

19. What customer types or activities do you prohibit, and how is that enforced in the product?

A defensible answer points at a control in the system, not a line in a policy. Reviewers test this by naming a prohibited category and asking what would happen if such a customer applied.

6. Sanctions

20. What lists do you screen against, at what points in the customer lifecycle, and how quickly after a list update?

A defensible answer treats onboarding, ongoing rescreening, and transaction-level screening separately, and states the refresh interval as a number.

21. What are your matching thresholds, who set them, and when were they last tuned?

A defensible answer names the person or committee that owns the threshold and produces the tuning record. Thresholds set by a vendor at implementation and never revisited are a standard finding, and after the CFSB order in question 8 they are a conspicuous one.

22. Show us your last twenty potential matches and how each was dispositioned.

A defensible answer carries a written rationale on each disposition, not just a cleared flag. A disposition with no reasoning cannot be defended later by anyone who was not in the room.

23. What happens operationally when you get a true match?

A defensible answer covers blocking, reporting, and notification, with the timeline stated in hours. The regulatory clock here is short.

---

7. Investigations, cases, and filings

24. Walk us through a case from alert to closure.

A defensible answer is walked through in the live system, with a real case on screen. Programs that present this as a slide instead usually have a gap between the slide and the system.

25. What are your SAR volumes and your average time from alert to filing?

A defensible answer states both and can break the timeline into stages. The question behind the question is whether the thirty-day clock is managed or discovered.

26. Show us a SAR narrative you filed.

A defensible answer is a narrative someone unfamiliar with the case could follow. Narrative quality is a common weak point and one of the cheapest to fix.

27. How do you handle continuing activity, and what is your process for deciding not to file?

A defensible answer documents no-file decisions with the same rigor as filings. Undocumented decisions not to file are among the harder findings to remediate after the fact.

---

8. What you tell your customers

New in this edition, and the most commonly overlooked category on the list.

28. Does any customer-facing language describe funds as insured, protected, or safe, and can you support every word of it?

A defensible answer traces each claim to the actual structure: which entity holds the funds, at which institution, under what insurance category, and whether pass-through coverage genuinely applies.

Why this now sits alongside the AML questions: the regulator that actually collected money from a fintech over the Synapse collapse was not a prudential regulator. It was the California Department of Financial Protection and Innovation, which announced a $1 million settlement with Yotta Technologies in May 2026 over representing accounts as FDIC insured when they were not (DFPI press release). The CFPB's own action against Synapse, entered September 2025, carried a $1 civil money penalty, the mechanism that unlocked roughly $46 million in Civil Penalty Fund redress for end users (CFPB enforcement page). A state consumer-protection theory, not a safety-and-soundness one. Add the FTC's March 2026 warning letters to major payment processors over deplatforming, and a CFPB running at reduced capacity after withdrawing more than sixty guidance documents in 2025, and the pattern is clear enough.

Deposit-insurance language in your marketing is now a more probable enforcement vector than a prudential exam finding. Your compliance team has probably never read your landing page.

---

9. What you owe your customers

Section 8 is about what you claim. This is about what happens when a customer has a problem. It is the fastest-growing area of exposure for fintechs and the one compliance teams are least likely to own.

29. Who handles customer complaints, how are they tracked, and does your bank see them?

A defensible answer produces a complaint log with categories, timelines, and resolutions, and can say what the bank receives and how often. Complaints are a leading indicator: a bank watching a rising complaint rate in a category it did not expect will ask about it long before a regulator does. "Support handles that" is not an answer, because support is not tracking it the way a reviewer needs.

30. What is your error resolution process, and can you evidence that you meet the timelines?

A defensible answer covers the process and the proof. Timelines here are regulatory rather than aspirational, and the question is not whether you have a procedure but whether you can show the dates on real cases. This is one of the more common gaps between a written policy and what the system records.

31. Which disclosures does the customer see, who wrote them, and who approved them?

A defensible answer traces the disclosure a customer actually sees in the product back to the person who approved it, and confirms that what is in the app matches what is in the agreement. Disclosures written once at launch and never reviewed against a changed product are a standard finding, and unlike most findings, this one is visible to anyone who downloads your app.

10. Governance, testing, and third parties

32. Who is your BSA Officer, what is their reporting line, and what authority do they hold to stop a product launch?

A defensible answer names a person, produces the appointing resolution, shows the reporting line does not run through revenue, and can point to a time the authority was used. A BSA Officer who cannot delay a launch is a title.

33. When did your board last review the AML program, and what were they actually shown?

A defensible answer produces dated minutes and the materials presented. Reviewers read the materials more closely than the minutes. A board pack showing volume but no risk metrics describes a board that cannot oversee the program.

34. When was your last independent AML audit, what did it find, and what is the status of every open finding?

A defensible answer produces the report including the findings, plus a tracked issues log with owners and dates. A clean report from a reviewer with no independence is worth less than a report with findings from one who has it. Overdue findings are less damaging than untracked ones.

35. Which third parties touch your compliance stack, and what happens if one of them fails?

A defensible answer covers your identity, screening, and monitoring vendors, anyone processing customer data, and the contingency if a vendor goes down or is acquired.

---

11. The production test

36. Produce the following, now: every customer onboarded last month with their risk rating, every alert generated in the last thirty days with its disposition, and every SAR filed in the last twelve months.

A defensible answer takes minutes.

Everything above tests whether you have a program. This tests whether the program produces a record. They are not the same thing, and the difference is the entire subject of this document.

PART TWO: WHAT THEY WILL ASK YOU TO PRODUCE

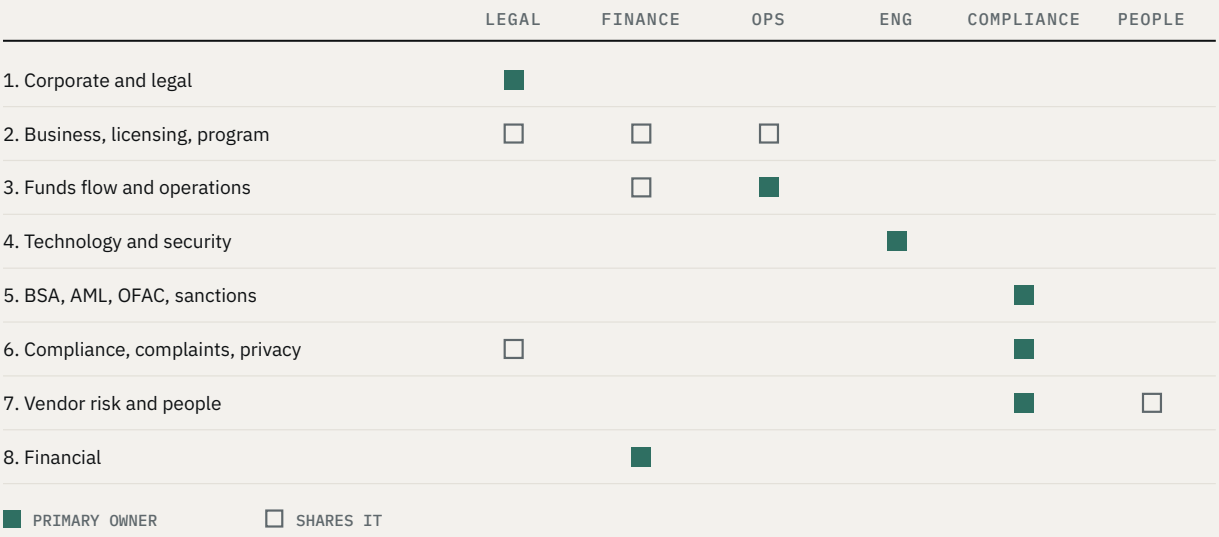
Part One tests whether you can answer. This tests whether you can produce.

They are different failures. A program can have good answers to every question above and still take six weeks to assemble the pack, because **most of the diligence pack is not owned by compliance.** Finance owns the financials. Engineering owns the penetration test. HR owns the training records. Legal owns the entity documents. Nobody has ever collected them in one place, and the request arrives with a deadline.

This is a composite, drawn from sponsor-bank onboarding request lists and from engagements we have run. It is not a rule, and no single bank asks for all of it. Everything below appeared in more than one request.

It is ordered the way banks order it rather than by risk, so you can hold it against a pack you have actually been sent. For each category: what gets requested, why the bank asks, who in your company owns it, and where it usually goes wrong. If you only pressure-test three, test categories 3, 4, and 8.

The most useful thing you can do with this list is not to gather everything. It is to find out today how long each category would take, and who you would have to ask.



Compliance is the primary owner of three categories out of eight. The other five sit with people who do not report to it and have their own quarter.

1. Corporate and legal

What they want. Formation documents and operating agreements. Active DBAs and state and local business licenses. Tax identification confirmation. An organizational chart showing ownership percentages. A full list of directors, officers, and control persons with short biographies. Full identifying detail for every beneficial owner at 25 percent or more, and entity details where an owner is a company. Certificates of insurance covering cyber, directors and officers, and errors and omissions or crime. Disclosure of pending or threatened litigation, administrative proceedings, and government inquiries. Copies of any historical consent orders.

Why they ask. The beneficial ownership detail is not curiosity. Under 31 CFR 1010.230, a final rule, the bank must itself identify and verify every individual owning 25 percent or more of a legal entity customer, and it cannot discharge that with your summary. The litigation and consent order disclosures feed its third-party risk assessment under the Interagency Guidance on Third-Party Relationships, 88 FR 37920, which is guidance in force, not a regulation. See question 14.

Who owns it. Legal, and often outside counsel or a corporate secretary who is not in your building.

Where it goes wrong. Ownership charts that are out of date after a financing round. Beneficial ownership detail that nobody wants to chase from an investor. Insurance certificates that lapsed. And the litigation disclosure, which people answer too narrowly: "threatened" and "inquiry" are broader than "lawsuit."

2. Business, licensing, and program

What they want. A strategic business plan with projected transaction flows and financial models. Money services business registration and its acknowledgment. Current state money transmitter licenses, a matrix of licenses in progress, or legal memoranda supporting any exemption relied on. Any subagents carrying meaningful volume. Non-US licenses and the international jurisdictions you support. Your existing programs with fee schedules, velocity limits, and product terms. Profiles of your largest merchants including legal names, business activities, locations, and processing volumes. Payment network memberships. Three years of loss and fraud experience, including

chargebacks and recoveries. Every prior and current sponsor bank, processor, and program manager relationship, why each one ended, and whether you have ever been offboarded or given notice.

Why they ask. A bank cannot knowingly serve an unregistered money services business, and registration under 31 CFR 1022.380, a final rule, is among the first things checked. Where you rely on an exemption, or on someone else's license, the bank is buying your legal reasoning and needs it written down.

Who owns it. Split between legal, finance, and the commercial team. This is the category most likely to have no single owner at all.

Where it goes wrong. Exemption memos that were never written down, only reasoned. Three years of loss and fraud data that exists in a processor's reporting rather than in yours. Merchant profiles, where the honest version of "business activities" is more specific than the marketing version. And the banking history, where the temptation is to describe a termination as a strategic decision. Say plainly what happened. The gap between your account of it and what the bank finds on its own is worse than the fact.

3. Funds flow and operations

What they want. End-to-end funds flow diagrams and a written narrative covering account architecture, FBO balances, transit accounts, payout rails, and settlement timing across every party. An operations organizational chart with management biographies. Written operational policies covering dispute resolution, dormant and unclaimed property, and legal process such as garnishments and reclamations. An anti-fraud program description. Your quality assurance framework, key risk and performance indicators, and samples of the reporting your executives actually see. Operational audit reports, including payment network and clearing house audits.

Why they ask. Two reasons, one settled and one pending. The bank's deposit insurance treatment depends on ownership being ascertainable from records under 12 CFR 330.5, a final rule. And the FDIC's custodial account recordkeeping rule, 89 FR 80135, still proposed and not finalized, would require the bank to reconstruct end-user balances daily. Banks are asking for the evidence now regardless of where that rule lands. See questions 2, 5, and 6.

Who owns it. Operations, with finance on the settlement mechanics.

Where it goes wrong. This is the category that decides the outcome. Very few companies have the funds flow drawn. Fewer have it drawn accurately enough to survive a follow-up question about a specific dollar at a specific moment. See question 4.

4. Technology, IT governance, and security

What they want. IT strategy, budget overview, and the control framework you have adopted. IT and information security organizational charts with biographies and a first-line responsibility matrix. Your software development lifecycle policy and outsourced development vendors. Information security policies covering encryption, access control, patching, and authentication. SOC 1 and SOC 2 reports with certification timelines. Payment card security attestation. Cybersecurity risk assessments and gap analyses. Your most recent external penetration test and vulnerability assessment, **with remediation plans**. Business continuity and disaster recovery plans and recent test results. Cloud strategy and infrastructure vendors.

Why they ask. The Interagency Guidance on Third-Party Relationships, 88 FR 37920 puts the bank on the hook for the security and resilience of anything you run that touches its customers or its data, and it cannot delegate that assessment to your assurance that you are fine. The remediation plan matters more than the test, because a test on its own shows nothing about whether you act on findings. See questions 3 and 35.

Who owns it. Engineering and information security. In a small fintech, one person, who is busy.

Where it goes wrong. The penetration test is usually available; the remediation plan usually is not, and the gap between them is the finding. Business continuity plans that have never been tested. And SOC 2 reports whose exceptions nobody has read closely enough to explain.

5. BSA, AML, OFAC, and sanctions

What they want. Formal designation of your BSA officer with role description and biography. An AML and sanctions organizational chart, including where compliance staff physically sit. Your policy manual covering identification, due diligence, enhanced due diligence, and politically exposed persons. Onboarding and verification flowcharts. Customer risk rating methodology. Enterprise risk assessment with a narrative summary. Country risk matrix. Your compliance technology stack and your transaction monitoring detection scenarios. Most recent independent audit with the issue log and management responses. Model validation report and its issue log. Quality assurance policy and process documentation.

Why they ask. The bank's own AML program obligation under 31 CFR 1020.210, a final rule, includes independent testing, and it does not stop at the bank's perimeter when you are performing customer-facing functions in its name. Model validation is a separate thread, and the standard behind it moved in April 2026. The agencies replaced the 2011 model risk guidance with SR 26-2 and OCC Bulletin 2026-13, rescinding with it the 2021 interagency statement on model risk for BSA and AML systems. The revised guidance sets no enforceable standard, is aimed principally at banks above $30 billion in assets, and excludes "deterministic rule-based processes and software where there are no statistical, economic, or financial theories underpinning their design or use" from the definition of a model. It also puts generative and agentic AI outside its scope altogether, on the stated ground that both are "novel and rapidly evolving." That does not retire the question. It changes the answer you need: find out whether your bank still treats your monitoring stack as a model, and if it does not, what it wants in place of a validation report. If your monitoring or your alert triage leans on AI, note that there is now no supervisory standard to point at, which means your bank's own expectation is the only standard and it will be improvised. See questions 32 through 34.

Who owns it. Compliance. The only category you fully control.

Where it goes wrong. Rarely the policies. Usually the issue logs, the model validation, and the physical locations question, which is really a question about offshore staffing you may not have expected.

Part One covers this category in depth. If the rest of the pack is thin, this one being strong will not save it.

6. Regulatory compliance, complaints, and privacy

What they want. Your compliance management system description and risk assessment methodology. Committee charters and executive reporting schedules. A centralized issue management log. Every customer-facing disclosure, electronic signature policy, and your advertising and marketing standards. Complaints management policy and procedures, the logging workflow, category classifications, and sample escalation reports. A log of complaints that arrived through a regulator, a state attorney general, or the Better Business Bureau. Privacy program documentation and notices covering the federal financial privacy regime and applicable state and international regimes. Cross-border data transfer mechanisms. Identity theft red flags policy, risk assessment, and program description.

Why they ask. Two of these are freestanding obligations of yours rather than the bank's: a written identity theft prevention program under 16 CFR 681.1, and privacy notices under Regulation P, 12 CFR part 1016. Both are final rules. The complaints material is asked for because complaints are the earliest signal a supervisor has, and a bank that cannot see yours is blind to its own risk.

Who owns it. Split across compliance, legal, marketing, and support. Nobody owns the whole thing.

Where it goes wrong. Marketing standards, because most fintechs do not have written ones. The regulator and attorney general complaint log, because most companies do not maintain it separately and cannot produce it on request. And the identity theft program, which is frequently missing entirely at companies that assume it does not apply to them.

See questions 28 through 31.

7. Vendor risk and people

What they want. Your vendor risk management program and policy, and who owns it. Vendor selection, scorecard, and risk rating methodology. Your standard risk-based contract requirements covering service levels, data protection, audit rights, and continuity obligations. An inventory of every third party that hosts, accesses, or interfaces with bank or customer data. Pre-hire screening and background check policies for employees and contractors. Onboarding and

training programs covering financial crime, security, and privacy. Your learning system and annual training completion reporting. Contractor confidentiality templates and non-employee workforce policies.

Why they ask. The Interagency Guidance on Third-Party Relationships, 88 FR 37920 is explicit that a bank's third-party risk runs through to your subcontractors. That is why the question is not "who are your vendors" but "who hosts, accesses, or interfaces with bank or customer data," and why an inventory that stops at direct vendors fails it. See question 35.

Who owns it. Compliance and HR, jointly, which in practice often means neither.

Where it goes wrong. The vendor inventory, which is almost always incomplete on first attempt because it stops at direct vendors. Training completion reporting, which needs to be by name and role rather than a percentage. And contractor policies at companies with a large contingent workforce they had not thought of as in scope.

8. Financial

What they want. Most recent balance sheet and income statement. Audited or accountant-prepared financials for the last two years, including footnotes. Three years of program profit and loss covering volume, revenue, and program expenses. Three-year pro forma financials and program volume projections. **Twenty-four months of average FBO and pooled customer account balance history.** Internal audit program description and your external audit providers.

Why they ask. The balance history is evidence, not accounting. Pass-through deposit insurance depends on ownership being ascertainable from records under 12 CFR 330.5, a final rule, and the proposed custodial recordkeeping rule (89 FR 80135, not finalized) would place a daily reconciliation obligation on the bank. See question 2.

Who owns it. Finance.

Where it goes wrong. The FBO balance history, which surprises people. It is asked for because it is the clearest available evidence of whether your customer funds behaved the way you said they would, and because a balance history that

does not reconcile to your own reporting is a serious finding. Two years is a long look back for a company that has changed banking arrangements in that time.

What to do with this

Time each category, do not gather it. Ask the owner of each one how long they would need. The categories where the answer is "I would have to find out" are your real exposure, and you can learn that this week.

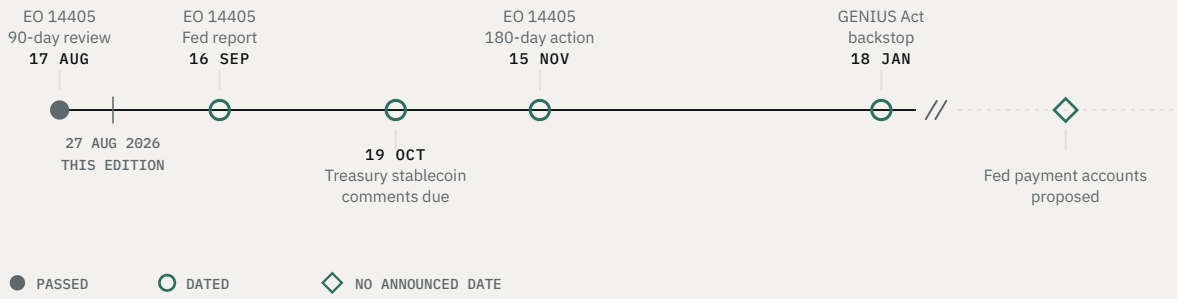
Notice how little of it is compliance's. Five of the eight categories are owned primarily by someone other than your compliance team. This is why diligence takes months. Not because the documents do not exist, but because assembling them requires six people to prioritize something none of them own.

Name a single owner for the pack. Not for the documents, for the pack. Someone whose job is knowing where all of it lives and what state it is in. Most companies appoint this person the week the request arrives, which is the week it is least useful.

Keep it current between cycles. The pack is not a project, it is a standing asset. The companies that handle diligence well are not faster at assembling. They are never fully disassembled.

What is coming

A short calendar, because several of these will reshape the questions above.



Three of the five dated items are Executive Order deadlines. The first has already passed.

17 August 2026, now passed. The 90-day deadline under EO 14405, signed 19 May 2026 for every federal financial regulator to review existing regulations, guidance, supervisory practices and application processes and identify what could be updated to facilitate innovation. Nothing has been published against it that we have seen. Absence of a public output is not evidence that no review happened, but it is worth asking your bank what its regulator said.

16 September 2026. The same Executive Order asks the Federal Reserve to report to the President on options for nonbank access to Federal Reserve accounts and services, within 120 days. This is the deadline most likely to move something you can feel, because it bears directly on the "skinny" payment accounts below.

19 October 2026. Comments due on Treasury's proposed rule on payment stablecoin issuance, offer, and sale (91 FR, 18 August 2026, RIN 1505-AC95).

15 November 2026. The Executive Order's 180-day deadline for each regulator to take steps to encourage innovation, in consultation with the Assistant to the President for Economic Policy.

No announced date. The Federal Reserve has proposed "skinny" payment accounts, which would give qualifying nonbanks limited direct access to Fedwire, FedNow, and the National Settlement Service. The Board published the proposal on 20 May 2026 and set no timetable for finalizing it. It asked Reserve Banks to pause pending access decisions while comment is taken. Comments closed 27 July 2026. Governor Barr dissented on AML grounds and community banks have objected. A year-end target has been reported in the trade press; we have found no Board statement setting one. If finalized, it changes the strategic calculus of every sponsor-bank relationship.

Worth watching, not yet real. The FDIC has reportedly been working with an industry coalition on a standards-development organization for third-party service providers to banks, covering third-party risk, cybersecurity, consumer compliance, BSA/AML, and governance. This is sourced to a draft term sheet reported in early August 2026. There is no formal announcement, no timeline, and no docket, and compliance with any such standards would not be a safe harbor. Treat it as a signal about direction rather than a requirement.

18 January 2027. The GENIUS Act's backstop effective date. The agencies missed the statutory one-year rulemaking deadline in July 2026; every stablecoin rule remains proposed, none final.

Two things you may have read that are no longer true. The CFPB's Section 1033 open banking rule is enjoined, its April 2026 compliance date suspended, and a new proposal went to review in August 2026. And the Tenth Circuit's November 2025 decision on Colorado's DIDMCA opt-out was vacated when rehearing en banc was granted in April 2026, so the question is undecided. Published commentary still gets both of these wrong.

What did we miss?

This is a first edition. It is drawn from what we see asked, which means it will be incomplete in places and out of date in others.

If a sponsor bank has asked you something that is not on this list, or has asked one of these in sharper wording than ours, send it to us and it goes into the next edition. Corrections to the regulatory statuses are equally welcome. They are as at 22 August 2026 and reviewed quarterly.

If you answered no

A no is a question you could not answer at all. "Only by hand" is one you could answer, but not from anything that already exists.

If this produced a list, that list is what a readiness engagement is for.

Bright Sea Advisors · kevin@brightseaadvisors.com · brightseaadvisors.com

Sources

Every regulatory claim in this document is linked to a primary source where one exists. Statuses below are as at 22 August 2026 and are reviewed quarterly.

CLAIM	SOURCE	STATUS
FDIC custodial account recordkeeping requirements	89 FR 80135 · RIN 3064-AG07	**Proposed, not finalized.** Long-term actions, final date to be determined
Monitoring thresholds and auto-closed alerts	OCC enforcement release, May 2026, consent order AA-ENF-2025-21	Final consent order
Reputation risk prohibited as a supervisory basis	OCC Bulletin 2026-12 · 91 FR, 10 April 2026	**Final rule.** OCC and FDIC only; the Federal Reserve is not a party
Novel Activities Supervision Program discontinued	Federal Reserve, 15 August 2025	Effective
Federal enforcement volumes declining	Brookings, 8 July 2026	Research, not regulatory
Bank responsibility for third-party oversight	Interagency Guidance on Third-Party Relationships, 88 FR 37920 · OCC Bulletin 2023-17	**Guidance, in force.** Not a regulation
Synapse: recordkeeping failures and redress	CFPB enforcement action	Judgment entered September 2025
Deposit insurance misrepresentation	California DFPI, May 2026	Settled
Treasury stablecoin issuance rulemaking	91 FR, 18 August 2026, RIN 1505-AC95	**Proposed.** Comments due 19 October 2026
Federal Reserve limited payment accounts	Board proposal, 20 May 2026 · Barr dissent; comments closed 27 July 2026	**Proposed.** No Board timetable. A year-end target has been reported without a primary source
CFPB Section 1033 open banking rule	Enjoined, E.D. Ky.; new proposal at OIRA August 2026	**Enjoined.** April 2026 compliance date suspended
Colorado DIDMCA opt-out, Tenth Circuit	*National Association of Industrial Bankers v. Weiser*	**Vacated.** Rehearing en banc granted April 2026; undecided
Beneficial ownership identification at 25 percent	31 CFR 1010.230	**Final rule**
Money services business registration	31 CFR 1022.380	**Final rule**
Bank AML program, including independent testing	31 CFR 1020.210	**Final rule**
Deposit ownership ascertainable from records	12 CFR 330.5	**Final rule**

CLAIM	SOURCE	STATUS
Written identity theft prevention program	16 CFR 681.1	**Final rule**
Consumer financial privacy notices	Regulation P, 12 CFR part 1016	**Final rule**
Model risk management, revised guidance	SR 26-2, 17 April 2026 · OCC Bulletin 2026-13	**Guidance, in force.** Supersedes SR 11-7 and SR 21-8; expressly not an enforceable standard
Third-party collection of a customer's TIN	FinCEN, 27 June 2025 · SR 25-2, 31 July 2025	**Exemptive order, in force.** Permissive, not mandatory; identity verification obligations are unchanged

Where this document describes what banks require in practice rather than what a rule requires, that is drawn from sponsor-bank onboarding request lists and from engagements we have run, and is identified as such in the text. Part Two is that kind of material: the regulatory reason given for each category is sourced, the request lists themselves are experience.