The 2026 Sponsor Bank Due Diligence Checklist

What Banks Actually Look For. A Practitioner's Guide for Fintech Founders Preparing for Bank Partnership Review.

Castleigh Johnson

Former Federal Reserve Bank Examiner · Goldman Sachs · EY · AIG · BMO Financial Group · NYU Stern MBA
CEO and Founder, Dreamfund (formerly My Home Pathway)

CJ ADVISORY | CASTLEIGHJOHNSON.COM/ADVISORY | 2026

12 PAGES. NO FILLER. WRITTEN BY SOMEONE WHO HAS SAT ON BOTH SIDES OF THE TABLE.

The 2026 Sponsor Bank Due Diligence Checklist

What Banks Actually Look For

A Practitioner's Guide for Fintech Founders Preparing for Bank Partnership Review

Castleigh Johnson Former Federal Reserve Bank Examiner | Goldman Sachs | EY | NYU Stern MBA

CJ Advisory | castleighjohnson.com/advisory | 2026

12 pages. No filler. Written by someone who has sat on both sides of the table.

This document is for educational and informational purposes only. It is not legal advice. For legal guidance, consult a qualified fintech attorney. © 2026 CJ Advisory. All rights reserved.

Section 1: Why This Exists

Most fintech founders underestimate what "bank-ready" means. Not by a little. By about six months and $80,000.

Here is what typically happens. A fintech company reaches out to a sponsor bank. The initial conversations go well. The bank expresses interest. Then the BSA officer sends over the due diligence questionnaire. It has 40 to 60 line items. Some of them are documents that take weeks to produce. Others reference processes the fintech has never formalized. A few require board approvals that have never happened.

The deal stalls. Sometimes it dies.

The founders are surprised. They shouldn't be. The bank's compliance team is not evaluating the product. They are evaluating whether the fintech company will survive an OCC or FDIC examination. Those are different questions. A strong product with a weak compliance program is a liability, not an asset, to a sponsor bank.

I have been on both sides of this table. At the Federal Reserve Bank of New York, I supervised and examined international banks during the 2008 to 2011 financial crisis. I analyzed compliance programs the way a bank examiner does: looking for gaps between what a policy says and what actually happens, looking for board oversight that exists on paper but not in practice, looking for risk frameworks built for yesterday's business model rather than today's. At Goldman Sachs, I settled $42 billion in loan transactions, which required me to understand what institutional counterparties actually need from fintech and financial services partners. As the CEO of a fintech company, I went through the sponsor bank due diligence process myself, closed eight enterprise partnerships, and earned OCC regulatory collaboration on a responsible innovation initiative.

The gap between what fintechs think banks want and what banks actually require is not a knowledge gap. The information is publicly available. It is an experience gap. Most fintech founders have never read an OCC examination manual. They have never sat across the table from a BSA officer who is deciding whether a fintech program passes muster. They have never had to explain to a bank's board why their third-party risk management program is adequate.

This checklist is built to close that gap. It reflects what banks are actually reviewing, organized in the order a compliance officer thinks about it, with examiner callouts that tell you what a BSA officer is thinking when they see each item.

Use it as a self-assessment. Use it as a gap analysis. Use it to prioritize your remediation work before the bank sends over their questionnaire.

Do not wait for the bank to ask. Prepare before the first conversation.

Section 2: How to Use This Checklist

Three tiers of readiness:

- **Tier 1:** You can produce this document or demonstrate this practice in 24 hours. You are prepared.
- **Tier 2:** You can produce this in 1 to 2 weeks. The item exists in some form but needs completion or updating.
- **Tier 3:** This does not exist yet. This is your highest-priority remediation item.

Self-assessment method:

Go through each item and mark your current tier. Count how many items you have in each tier. The scoring guide is in Section 6.

One rule: Do not approach a sponsor bank with more than 20% of your items in Tier 3. Banks can work with fintechs that have gaps. They cannot work with fintechs that have not thought about what a gap means.

Time horizon: Most fintech companies need 60 to 90 days to move from a typical pre-assessment state to bank-ready. Plan accordingly. If you have a bank conversation scheduled in the next 30 days and more than 25% of these items are in Tier 3, delay the conversation or engage outside support immediately.

Section 3: The Checklist

Category 1: Corporate Governance

Banks begin compliance reviews here. Before a BSA officer looks at your AML program, they want to know that your board knows what compliance is and has demonstrated oversight. A compliance program without board backing is not a program. It is a document.

[ ] 1.1 Board-Approved BSA/AML Policy The written BSA/AML policy has been formally approved by the board of directors and the approval is documented in board minutes.

Examiner note: "Board-approved" means a resolution in the minutes, not a signature on the policy document. If the board has not reviewed and voted on this policy, it is not board-approved, regardless of what the cover page says. Banks that have been through OCC enforcement actions over fintech programs learned this the hard way.

[ ] 1.2 Compliance Committee Charter A formal compliance committee exists, with a written charter defining scope, membership, meeting frequency, and reporting obligations.

Examiner note: Small fintechs often do not have a compliance committee. That is acceptable at very early stages. What is not acceptable is pretending to have one. If you don't have a committee, say so, and describe how compliance oversight is handled at the executive level.

[ ] 1.3 Board Meeting Minutes Reflecting Compliance Oversight At least the last four quarters of board minutes document compliance topics, including BSA/AML, risk assessments, or examination results.

Examiner note: This is one of the most reliable signals of program maturity. Genuine compliance programs generate paper trails. If compliance appears in board minutes only as a line item with no discussion, that tells me the board is not actually engaged.

[ ] 1.4 Designated BSA Officer with Documented Authority A named individual holds the BSA Officer role with a written designation, documented responsibilities, and sufficient authority and budget to perform the function.

Examiner note: I have reviewed compliance programs where the "BSA Officer" was the founder, the CFO, and the General Counsel simultaneously, none of whom had time to perform any of the three roles. A BSA Officer with no budget and no authority is a compliance gap with a name on it.

[ ] 1.5 Organizational Chart Showing Compliance Reporting Lines Current org chart shows the BSA Officer's position and reporting relationship, with clear lines to the board or a board committee.

Examiner note: BSA Officer independence matters. An officer who reports exclusively to the same executive who drives revenue decisions has a structural conflict. Banks look for this.

[ ] 1.6 Annual Board Compliance Training Records Documentation that board members have completed compliance training, including BSA/AML awareness, within the past 12 months.

Examiner note: Board training records are frequently missing. They are also very easy to produce with minimal cost. A missing record here signals that compliance governance is informal, and informal governance rarely survives bank examination scrutiny.

Category 2: BSA/AML Program

This is the core of what a sponsor bank's BSA officer evaluates. Every item here has a specific regulatory basis. Every gap here is a potential examination finding that the bank has to answer for.

[ ] 2.1 Written BSA/AML Policy and Procedures A comprehensive, current BSA/AML policy exists, covering program requirements, roles and responsibilities, training obligations, and program review cadence.

Examiner note: "Current" means reviewed and updated within the past 12 months, or following any material change to the business model. A policy from the company's founding that has not been touched since the product evolved is not a functioning policy.

[ ] 2.2 Risk-Based AML Program Documentation The AML program is documented as risk-based, with the risk rationale explained and the program design tied specifically to the company's customer base, products, and geographies.

Examiner note: Generic AML programs are easy to spot. They use the same language regardless of the business model. A risk-based program for a peer-to-peer payment application looks different from one for a DPA savings product. Banks want to see that you understand your own risk profile.

[ ] 2.3 Customer Risk Rating Methodology A written, documented methodology exists for assigning AML risk ratings to customers, with defined triggers for low, medium, and high-risk classifications.

Examiner note: This is often the first item that exposes a gap between what a policy says and what actually happens operationally. Walk me through how a specific customer type gets rated. If you cannot do that, the methodology exists on paper only.

[ ] 2.4 Annual AML Risk Assessment A formal AML risk assessment has been completed within the past 12 months, covering products, customers, geographies, and distribution channels.

Examiner note: The annual risk assessment is not a checkbox. It should show that you identified your highest-risk exposures and made program design decisions in response. If the risk assessment has not changed the program in any way, it was not a real assessment.

[ ] 2.5 SAR Filing Policies and Procedures Written procedures govern how suspicious activity is identified, escalated, investigated, and reported, including documentation retention and law enforcement contact protocols.

Examiner note: Banks take SAR programs seriously because they are directly supervised on SAR quality and timeliness. If your fintech generates transactions, you need a SAR program, even if you have never filed a SAR.

[ ] 2.6 CTR Filing Policies and Procedures If applicable: written procedures cover currency transaction reporting obligations, aggregation rules, and exemption processes.

Examiner note: Not all fintechs handle cash. If you don't, document why CTR obligations do not apply. If you do, the procedures need to be specific and current with FinCEN guidance.

[ ] 2.7 AML Training Records for All Staff Records show that all employees with customer or transaction-facing responsibilities have completed AML training within the past 12 months, with role-specific content for higher-risk functions.

Examiner note: Training records are the most common documentation gap in fintech compliance programs. An all-hands email with a link to a compliance video is not a training program. It is evidence that you tried.

[ ] 2.8 Independent AML Audit (Annual) An independent review or audit of the BSA/AML program has been completed within the past 12 months by a party with no operational responsibility for the program.

Examiner note: "Independent" does not require an external firm. It requires independence from the compliance function being reviewed. A BSA Officer auditing their own program is not an independent audit. A founder who built the compliance program reviewing it is not independent.

Category 3: KYC / CIP / CDD

Know Your Customer is not just a phrase. It is a set of specific regulatory obligations under the Bank Secrecy Act and FDIC/OCC rules for bank programs. Banks evaluate whether your KYC program is specific, documented, and operational.

[ ] 3.1 Written KYC Policy Covering Individual and Business Customers A comprehensive KYC policy addresses both individual (consumer) and business (commercial) customers, with distinct procedures for each.

[ ] 3.2 Customer Identification Program (CIP) Procedures Specific, written CIP procedures detail minimum identification requirements, identity verification methods, discrepancy handling, and recordkeeping requirements, per 31 CFR 1020.220.

Examiner note: CIP is a regulatory requirement, not a best practice. If you onboard customers without documented CIP procedures, you have a BSA violation, not a gap.

[ ] 3.3 Customer Due Diligence (CDD) Procedures Written CDD procedures address the four core elements: customer identification, customer risk rating, understanding the nature and purpose of the relationship, and ongoing monitoring.

Examiner note: FinCEN's 2016 CDD Rule (31 CFR 1010.230) codified these four elements. Banks were required to comply by May 2018. Any fintech operating under a bank partner program is expected to meet the same standard.

[ ] 3.4 Enhanced Due Diligence (EDD) Triggers and Procedures Written EDD procedures define what triggers enhanced review, what additional information is collected, who approves EDD decisions, and how EDD is documented.

Examiner note: The most common EDD failure I see is having a policy that names high-risk customer types but no actual procedure for what to do when one applies. "Conduct enhanced due diligence" is not a procedure.

[ ] 3.5 Beneficial Ownership Collection Procedures Written procedures cover how beneficial ownership is collected and verified for legal entity customers, per FinCEN's CDD Rule requirements.

Examiner note: Legal entity customers with complex ownership structures are where beneficial ownership failures concentrate. The procedure needs to specify how you handle situations where ownership information is refused or incomplete.

[ ] 3.6 PEP Screening Policy A written policy addresses politically exposed persons: definition, screening method, escalation, and documentation.

[ ] 3.7 Adverse Media Screening Policy Written procedures address adverse media screening for new customers and ongoing monitoring, including source coverage, escalation, and documentation.

[ ] 3.8 Ongoing Monitoring Procedures for Existing Customers Written procedures govern how customer activity is monitored after onboarding, including transaction monitoring thresholds, risk rating updates, and periodic review triggers.

Examiner note: Onboarding-only KYC programs are not compliant. Customer risk evolves. A customer who was low-risk at onboarding can become high-risk as their transaction patterns develop. Ongoing monitoring is what catches that.

Category 4: OFAC Compliance

OFAC violations are among the most serious a bank can face. Banks treat OFAC compliance in their fintech partners the same way they treat it internally.

[ ] 4.1 OFAC Screening Policy and Procedures A written OFAC policy covers screening obligations, applicable sanctions programs, screening frequency, and documentation requirements.

[ ] 4.2 Screening System Documentation Documentation identifies the screening system or vendor used, the sanctions lists screened against, and the update frequency for those lists.

Examiner note: OFAC list updates can occur multiple times per week. A screening system that updates monthly is not OFAC-compliant for a real-time transaction business.

[ ] 4.3 OFAC Match Escalation Procedures Written procedures address what happens when a potential OFAC match is identified: who reviews it, what the decision criteria are, how it is documented, and how blocked or rejected transactions are handled.

[ ] 4.4 Blocked and Rejected Transaction Documentation Records of any blocked or rejected transactions, including the basis for the block, are maintained and accessible.

[ ] 4.5 Annual OFAC Risk Assessment An annual assessment of OFAC risk has been completed, covering customer base, transaction types, geographies, and sanctions exposure.

[ ] 4.6 Screening Update Frequency Documentation Documentation confirms how frequently sanctions list updates are incorporated into the screening system, with a defined SLA for updates following emergency OFAC designations.

Category 5: Consumer Compliance

Consumer compliance is where CFPB and state regulatory exposure concentrates. Banks are increasingly held responsible for their fintech partners' consumer compliance practices under UDAAP and fair lending frameworks.

[ ] 5.1 UDAAP Policy and Procedures A written UDAAP policy defines unfair, deceptive, and abusive acts and practices, covers how consumer-facing materials are reviewed, and addresses complaint handling obligations.

Examiner note: UDAAP is not limited to disclosures. It covers the entire consumer experience, including how customer service handles complaints, how fee structures are disclosed, and whether marketing materials are accurate. If your policy only covers disclosures, your UDAAP program is incomplete.

[ ] 5.2 Consumer Complaint Management System A formal complaint management system captures all consumer complaints, tracks resolution, identifies patterns, and reports aggregate complaint data to compliance leadership.

Examiner note: CFPB complaint data is public. If your customers are filing CFPB complaints and your internal complaint log shows no corresponding records, that tells me your complaint program is not working.

[ ] 5.3 Complaint Log (Last 12 Months) A current complaint log exists and is available for review, with complaint category, date received, resolution, and time to resolution.

[ ] 5.4 Reg E Error Resolution Procedures Written procedures cover the full Regulation E error resolution process: how errors are reported, the investigation process, provisional credits, resolution notices, and recordkeeping.

Examiner note: Regulation E rights attach the moment you issue a prepaid card or facilitate electronic fund transfers. There is no grace period for fintech companies.

[ ] 5.5 ECOA / Fair Lending Policy A written ECOA and fair lending policy covers prohibited bases, adverse action notice requirements, and the process for reviewing credit or program decisions for potential fair lending violations.

[ ] 5.6 Adverse Action Notice Procedures Written procedures address when an adverse action notice is required, what reasons are provided, timing requirements under ECOA (30 days) and FCRA (immediately if a consumer report was used), and documentation.

Examiner note: CFPB Circular 2022-03 clarified that generic reason codes are not compliant. Adverse action notices must identify specific, principal reasons. If your program uses AI-assisted decisioning and you cannot explain the specific reason for a denial, you have a regulatory exposure.

[ ] 5.7 Privacy Policy (GLBA Notice) A current GLBA privacy notice is available to consumers, covers information sharing practices, and reflects the company's actual data practices.

[ ] 5.8 State-Specific Consumer Disclosures Applicable state disclosures are identified, current, and in use for states where the fintech operates or serves customers.

Examiner note: GLBA federal privacy requirements are the floor, not the ceiling. California (CCPA), New York, and other states have requirements that exceed GLBA. If you operate nationally and only have a GLBA notice, check your state exposure.

Category 6: Third-Party / Vendor Risk Management

Sponsor banks are required by OCC and FDIC guidance to oversee their fintech partners as third parties. When a bank partners with a fintech, the fintech's vendors become the bank's fourth parties. Banks require fintechs to manage their vendor relationships with rigor.

[ ] 6.1 Vendor Management Policy A written vendor management policy exists, covering vendor classification, due diligence requirements by risk tier, ongoing monitoring, and termination procedures.

Examiner note: OCC's 2023 Third-Party Risk Management guidance (OCC 2023-17) and the joint FDIC/OCC/FRB guidance from the same year set the standard. Your vendor management policy should reflect this framework. If it was written before 2023, review it against these standards.

[ ] 6.2 Approved Vendor Inventory A current inventory of all vendors is maintained, including vendor name, service provided, risk classification, and contract renewal dates.

[ ] 6.3 Vendor Due Diligence Procedures Written procedures specify what due diligence is conducted before onboarding a vendor, including minimum requirements by risk tier and documentation standards.

[ ] 6.4 Critical Vendor Monitoring Reports For vendors classified as critical or high-risk, ongoing monitoring reports exist and are reviewed at defined intervals.

[ ] 6.5 Bank Partner Oversight Procedures If the fintech has existing bank relationships or sub-servicer relationships, written procedures govern how those relationships are overseen from a compliance perspective.

[ ] 6.6 Concentration Risk Analysis A documented analysis of vendor concentration risk exists, identifying single points of failure in the vendor ecosystem and documented mitigation strategies.

[ ] 6.7 Vendor Contract Templates with Compliance Requirements Standard vendor contract templates include compliance requirements: audit rights, data security standards, regulatory change management obligations, and termination rights for compliance failures.

Examiner note: Vendor contracts that do not include audit rights are a common finding. Banks require the ability to audit their fourth parties. If your contracts do not preserve that right for the bank, renegotiation will be required.

[ ] 6.8 Annual Vendor Reviews Documented annual reviews of all active vendors are completed, with refreshed due diligence for high-risk vendors.

Category 7: Technology and Cybersecurity

Banks face increasing regulatory scrutiny on technology risk in fintech partnership programs. FFIEC IT examination standards apply to the bank's fintech partners as well as to the bank itself.

[ ] 7.1 Information Security Policy A written information security policy exists, covering data classification, access controls, encryption standards, incident response, and security training.

[ ] 7.2 SOC 2 Type II Report (or In-Progress Timeline) A current SOC 2 Type II report is available for review, or a documented timeline and auditor engagement exists for completion.

Examiner note: SOC 2 Type II is now table stakes for most sponsor bank relationships. A SOC 2 Type I report or a SOC 2 readiness assessment is not a substitute. If you do not have Type II, document your timeline and your auditor. Banks can work with a fintech that is 90 days from completion. They generally cannot partner with one that has not started.

[ ] 7.3 Incident Response Plan A written incident response plan covers detection, containment, notification obligations (including bank partner notification timelines), regulatory reporting, and post-incident review.

Examiner note: Bank partner notification timelines are typically contractually required and may be as short as 24-72 hours for material incidents. If your incident response plan does not specify when you notify your bank partner, it is incomplete.

[ ] 7.4 Business Continuity / Disaster Recovery Plan A written BCP/DR plan covers critical system recovery, RPO/RTO targets, communication protocols, and annual testing documentation.

[ ] 7.5 Penetration Test Results (Last 12 Months) Results of an independent penetration test conducted within the past 12 months are available, including scope, findings, and remediation status.

[ ] 7.6 Data Retention and Deletion Schedule A documented data retention and deletion schedule exists, covering customer data, transaction records, and compliance records, with defined retention periods tied to regulatory requirements.

[ ] 7.7 Employee Access Control Documentation Documentation of user access controls exists, including onboarding and offboarding procedures, privilege management, and periodic access reviews.

[ ] 7.8 Encryption Documentation Documentation confirms encryption standards for data at rest and in transit, including the specific protocols and key management practices in use.

Category 8: Financial Health and Operational Capacity

Banks need to know that their fintech partners are financially viable. An undercapitalized fintech that fails midway through a partnership creates regulatory, reputational, and operational risk for the bank.

[ ] 8.1 Two Years of Financial Statements (Audited or Reviewed) Audited or reviewed financial statements for the past two years are available. If the company is pre-revenue, reviewed statements with detailed commentary are acceptable.

Examiner note: "We're a startup and don't have audited financials" is an explanation, not an answer. Get reviewed financials at minimum. The cost is $5,000 to $15,000. The cost of a failed bank partnership is much higher.

[ ] 8.2 Current Balance Sheet A current balance sheet is available within 30 days of the due diligence request.

[ ] 8.3 Burn Rate and Runway Documentation A documented analysis of current monthly burn rate and cash runway exists, with assumptions documented.

Examiner note: Banks want to see that you have at least 12 months of runway. If you have less, have a documented capital plan. A fintech that runs out of capital 6 months into a bank partnership is an operational and reputational problem for the bank.

[ ] 8.4 D&O Insurance Certificate A current directors and officers insurance certificate is available, showing coverage limits and policy period.

[ ] 8.5 Transaction Volume Projections (12-24 Months) Documented transaction volume projections, with supporting assumptions, are available for the next 12 to 24 months.

Examiner note: Banks use transaction volume projections to assess whether their program exposure is within acceptable risk tolerance. Be conservative. Overpromising on volume and underdelivering damages the relationship.

[ ] 8.6 Capital Adequacy Statement A statement of capital adequacy exists, addressing whether the company has sufficient capital to meet its regulatory and operational obligations.

Section 4: Common Mistakes

These five patterns cause fintech companies to fail bank due diligence. They are specific, recurring, and avoidable.

Mistake 1: Policies That Exist But Show No Evidence of Implementation

This is the most common failure pattern. A fintech has a well-written BSA/AML policy. The bank reviews it. Then the bank asks for the last 12 months of AML risk assessment results, the training records, the complaint log, and the SAR investigation documentation. None of it exists.

The policy was written for the due diligence process, not to govern an actual program. Banks can tell the difference. They do it by asking for operational evidence, not just documents.

The fix: For every policy your compliance program has, you should be able to produce evidence that the policy is actually being followed. Training records. Committee minutes. Vendor reviews. If the policy says you do something monthly, show me 12 months of documentation that it happened.

Mistake 2: An AML Program Designed for a Different Business Model

A fintech pivoted six months ago. The AML risk assessment was written for the original product. The customer risk rating methodology was calibrated to the original customer base. The transaction monitoring thresholds were set based on the original average transaction size.

None of it reflects the current business.

Banks are sophisticated enough to spot this. When the risk assessment describes customers and transaction patterns that don't match what the fintech actually does, it tells the BSA officer that the compliance function is not integrated into the business.

The fix: Your AML risk assessment should be updated every time your business model, customer base, or product offering makes a material change. If it hasn't changed since founding, review it now.

Mistake 3: Missing Board-Level Oversight Documentation

The compliance policy says the board oversees the BSA/AML program. The board minutes for the last four quarters contain no reference to compliance at all.

This is a governance failure that the bank's examination team will flag immediately. A compliance program without genuine board oversight is not a compliant program under OCC and FDIC standards.

The fix: Put compliance on the board meeting agenda. Regularly. Document the discussion in the minutes. Even at the seed stage, a 10-minute compliance update in board minutes is a credibility signal that costs nothing to produce.

Mistake 4: A Vendor List With No Due Diligence Documentation

The fintech has 12 vendors. The vendor management policy describes a rigorous due diligence process. When the bank asks for the due diligence files, the fintech provides contracts, but no SOC 2 reports, no security questionnaires, no financial review for critical vendors, and no annual review documentation.

The vendor list existed. The due diligence program existed on paper. The evidence that the program was actually executed did not exist.

The fix: For every vendor on your approved vendor list, there should be a due diligence file. For critical vendors, that file should include: the initial due diligence, the most recent SOC 2 report (or equivalent), and evidence of annual review.

Mistake 5: A Compliance Officer With No Real Authority or Budget

The org chart shows a Chief Compliance Officer. The BSA Officer is named in the policy. In practice, the compliance function has no budget, no staff, no access to the executive committee, and no ability to escalate issues without going through the same person who is responsible for revenue growth.

Banks evaluate compliance authority structurally. A compliance officer who cannot stop a product launch, who has no budget for independent audit or outside counsel, and who does not attend board meetings is a compliance officer in title only.

The fix: Compliance authority must be real, not nominal. If you cannot afford a full-time CCO with genuine authority, the Fractional Compliance Retainer model exists precisely for this stage. What you cannot do is name a compliance officer and give them no resources to do the job.

Section 5: Readiness Tiers

Use this to assess your overall readiness for a sponsor bank conversation.

Tier 1: Bank-Ready (85% or more of checklist items in Tier 1 readiness) Your documentation is substantially complete and your program is operational. Proceed with bank conversations. Have your BSA Officer or compliance advisor review your materials before the first bank submission.

Tier 2: 60 to 90 Days Out (60 to 84% of items in Tier 1 readiness) Your program has meaningful gaps. A bank conversation is premature. Conduct a Regulatory Health Check to get a prioritized remediation roadmap. You can close this gap in 60 to 90 days with focused effort.

Tier 3: 90 or More Days Out (Under 60% of items in Tier 1 readiness) Your compliance program needs foundational work before you are ready to approach a sponsor bank. Engage a compliance advisor to build the program correctly rather than trying to backfill documentation under deadline pressure.

Section 6: What Comes Next

Based on where you are after completing this checklist, three paths forward.

“I want to know exactly where I stand.”

Regulatory Health Check | $7,500 | 10 business days

A comprehensive compliance assessment across BSA/AML, consumer protection, third-party risk, and policy infrastructure. You receive a written findings report and a prioritized remediation roadmap. You also get a 60-minute debrief where we go through the findings and I tell you what the bank is going to ask about first.

This is the fastest way to convert a Tier 2 or Tier 3 assessment into a clear action plan.

“I need to prepare for a bank DD review.”

Bank Partner DD Package | $25,000 | 4 weeks

A turnkey preparation engagement. I build or review every document on this checklist that is in Tier 2 or Tier 3, organize the complete due diligence package the way the bank's BSA officer expects to receive it, and run a mock DD walkthrough with you before the bank submission.

Fintechs in active sponsor bank conversations or preparing to enter them use this package.

"I need ongoing compliance leadership."

Fractional Compliance Retainer | $12,000/month | Minimum 3-month engagement

Fractional CCO-level oversight embedded in your team. 10 dedicated hours per month, ongoing program management, direct BSA Officer availability for bank conversations, monthly compliance committee reporting, and examination support. All the compliance leadership of a senior hire at a fraction of the cost.

Health Check clients can credit their $7,500 engagement toward the first month of the retainer.

If you want to talk through your specific situation before deciding, book a 20-minute call.

No pitch. Just a straight assessment of where you are and what the bank is going to ask for.

castleighjohnson.com/advisory

Section 7: About Castleigh Johnson

Federal Reserve Bank of New York (2008-2011) Bank Examiner and Foreign Financial Institutions Analyst. Supervised and analyzed 30+ international banks across Ireland, Japan, the Netherlands, France, and the United Kingdom during the 2008 to 2011 financial crisis. Ranked the largest 10 US lenders by asset quality and underwriting compliance.

Goldman Sachs (2011-2012) Senior Associate, Bank Debt Operations. Settled $42 billion in loan transactions within one year. Provided technical advisory to investment banking deal teams on loan structuring and compliance.

Ernst and Young (2013-2014) Manager, Financial Services Advisory. Enabled GE Capital's $75 billion bank spin-off. Conducted risk governance assessments for top-20 US financial institutions.

AIG (2014-2015) Team Leader, Enterprise Risk Management. Built the global model governance and board reporting framework from the ground up.

BMO Financial Group (2015-2016) Director, U.S. Model Governance. Led SR 11-7 / SR 15-19 regulatory remediation for a $600 billion asset institution. Directed the annual CCAR compliance process.

My Home Pathway / Dreamfund (2020-Present) CEO and Founder. Closed 8 strategic partnerships including ICE Mortgage Technology, TransUnion, and Chime Bank. Led the company through SOC 2 Type II certification. Secured OCC regulatory collaboration on a responsible innovation initiative.

Education MBA, Finance and Accounting, NYU Leonard N. Stern School of Business | JP Morgan Investment Banking Fellow | Consortium for Graduate Study in Management Fellow | BS, Management and International Business, Pennsylvania State University | Bunton Waller Academic Fellowship | Division 1 Collegiate Soccer

Contact: castleigh.johnson@gmail.com | castleighjohnson.com/advisory

---

This document is for educational and informational purposes only. It is not legal advice. For legal guidance, consult a qualified fintech attorney. © 2026 CJ Advisory. All rights reserved.

Ready to Close the Gap?

If your sponsor bank conversation is within 90 days and more than 25% of these items are in Tier 3, do not wait. Book a 20-minute discovery call. No pitch. Direct assessment of where you stand and what the bank is going to ask for next.

castleighjohnson.com/advisory · **Book a Discovery Call**

> *This document is for educational and informational purposes only. It is not legal advice. For legal guidance, consult a qualified fintech attorney. © 2026 Castleigh Johnson Advisory. All rights reserved.*