BRODY | GAPP LLP

Clarity in Compliance. Confidence in Litigation.

AI Vendor Due Diligence

What to Ask, What to Demand, and What to Watch Out For

Prepared by James W. Brody, Esq. | Founding & Managing Partner

James@BrodyGapp.com | 415.246.3995

> ***Your vendor's representation that their AI is 'compliant' is a starting point — not a safe harbor.***
>
> Under Freddie Mac Guide § 1302.8, every Seller/Servicer — IMB, depository, credit union, mortgage broker, or fintech — is responsible for the AI governance of every tool it uses in connection with Freddie Mac loans. That responsibility does not transfer to your vendor. It stays with you. Vendor representations are a beginning. Contractual rights, audit access, and documentation on file are what matter at examination.

5 NON-NEGOTIABLE QUESTIONS TO ASK EVERY AI VENDOR

1. Provide your Model Card.
This must include training data source and vintage, all model features (inputs), feature importance rankings, known performance limitations, validation results, and fair lending test results disaggregated by race/ethnicity. A model card is the baseline document of a governed AI tool. If your vendor does not have one, that is your answer.

2. What were the results of your fair lending testing?
Ask for specific statistical outcomes — not assertions. Approval rate disparities, pricing disparities, and false positive rates disaggregated by protected class. Ask specifically how they estimated protected class for testing (BISG or similar). Vendor statements like 'our model is fair' without underlying data are not defensible.

3. How do you generate adverse action reasons?
Adverse action reasons must reflect the actual logic of the model — not post-hoc approximations or generic FICO-style codes that were written before AI was in the picture. If the vendor cannot explain the specific mechanism by which model feature importance translates to borrower-readable reason codes, you cannot produce ECOA-compliant notices. That is a pre-deployment disqualifier.

4. How do you notify us of model changes?
Every material model change — retraining, new features, threshold adjustments, architecture updates — must trigger notification to you before deployment. Unnotified changes mean you are running an unvalidated model against which your prior fair lending analysis is no longer accurate. This must be a contractual obligation, not a courtesy.

5. What are our audit rights?
You must have the contractual right to inspect validation reports, training data lineage documentation, and bias testing results. A vendor who refuses on 'intellectual property' grounds is creating a compliance violation for you. Freddie Mac's own framework expects you to be able to demonstrate governance — which requires access to the underlying documentation.

6 RED-FLAG VENDOR STATEMENTS — AND WHAT TO SAY BACK

VENDOR SAYS: *"Our model is a black box — we cannot share features or weights."*

WHY IT'S A RED FLAG: ECOA requires specific, actual adverse action reasons. If you cannot see what variables drive the model's decisions, you cannot produce compliant notices. This is a go/no-go disqualifier — not a negotiation.

WHAT TO SAY INSTEAD: Say: "Provide the top 10 features by importance and their contribution to model output. We require a model card before any deployment discussion proceeds."

VENDOR SAYS: *"Our model is CFPB-compliant."*

WHY IT'S A RED FLAG: The CFPB does not certify or approve AI models. This statement is either factually false or meaningless. Note also that CFPB Circular 2022-03 was withdrawn in May 2025 — any claim of CFPB guidance compliance is doubly hollow.

WHAT TO SAY INSTEAD: Say: "Provide your independent validation report and fair lending test results — specific statistical outcomes by protected class, not assertions."

VENDOR SAYS: *"Our training data is proprietary — we cannot share details."*

WHY IT'S A RED FLAG: If you do not know what data trained the model, you cannot assess data bias, proxy risk, or the accuracy of their fair lending testing. The vendor does not need to share raw data to disclose training data vintage, source, coverage, and known limitations.

WHAT TO SAY INSTEAD: Say: "Provide training data vintage, source, coverage, and any known exclusions. We do not require raw data access — but we require this disclosure before deployment."

VENDOR SAYS: *"We update the model regularly for better performance."*

WHY IT'S A RED FLAG: Every material model update changes the model's risk profile. Without pre-notification and re-validation, you are deploying a model whose fair lending implications you have not assessed.

WHAT TO SAY INSTEAD: Say: "Your contract must include advance notification of all material model changes before they are deployed, with our right to re-validate before implementation."

VENDOR SAYS: *"We have run this for hundreds of lenders — it has been tested."*

WHY IT'S A RED FLAG: Market adoption is not a fair lending test. Systematic bias at scale is worse than individual bias — it creates a class of affected borrowers across every lender who deployed without testing.

WHAT TO SAY INSTEAD: Say: "Provide aggregated fair lending test results across your lender base, disaggregated by approval rate and pricing outcomes by protected class."

VENDOR SAYS: *"Fair lending compliance is your responsibility, not ours."*

WHY IT'S A RED FLAG: This is technically accurate — which is precisely why you need contractual protections to enforce the vendor's obligations. The statement signals the vendor has not performed adequate fair lending due diligence on their own product.

WHAT TO SAY INSTEAD: Say: "Include in the contract: vendor representations that the model has been tested for fair lending compliance, the specific outcomes of that testing, and an ongoing obligation to notify us of any identified fair lending concerns."

AI VENDOR CONTRACT CHECKLIST

☐	Model card delivery required before deployment: training data vintage/source, all model features, feature importance, performance metrics, validation results, and fair lending test results
☐	Vendor representations that the model has been tested for fair lending compliance — with specific statistical outcomes documented, not assertions
☐	Audit rights clause: lender's contractual right to review validation reports, training data lineage documentation, and bias testing results
☐	Advance notification requirement: vendor must notify lender of all material model changes BEFORE deployment — including retraining, new features, and threshold changes
☐	Re-validation right: lender's right to re-validate the model before any material change takes effect
☐	Fair lending incident notification: vendor must promptly notify lender if any fair lending concern is identified in the model at any time
☐	Data sourcing disclosure: vendor discloses training data source, vintage, coverage, and any known limitations, exclusions, or gaps
☐	Version control disclosures: vendor maintains and discloses version history of all deployed model versions with change logs
☐	No unauthorized data use: vendor contractually prohibited from using lender's borrower data to train models for other clients without express written consent
☐	Termination rights: lender may terminate if model is found to violate fair lending requirements or if vendor materially breaches documentation obligations

James W. Brody, Esq.
Founding & Managing Partner
BRODY | GAPP LLP
415.246.3995 · James@BrodyGapp.com · BrodyGapp.com