NELSON MULLINS Themis

Themis Banking School:

Finding Your Perfect Match 💘

The Bank–Fintech Edition

Framing Bank–FinTech partnerships as long-term relationships

Learning Objectives

We want you to take away a full understanding of a Bank Fintech relationship lifecycle. Both the good and the bad.

- Dating Phase (What to look for)
- Asking the Hard Questions (Due Diligence)
- Life After the Honeymoon (Ongoing Maintenance)
- Breakups Happen (Winddowns)

NELSON MULLINS Themis

Section 1:

The Dating Phase: First Impressions 💘

Section 1: The Dating Phase: First Impressions

What are you even looking for in a partner; both as a Bank and as FinTech? What do you want to see? First Impressions matter.

- Product demos, vision, and growth narratives
  - Be honest
- Don't overlook any Red flags hidden by excitement and speed
  - Don't assume everything will be caught in Due Diligence
- Why “cool tech” isn’t the same as a good partner
- Pressure to move fast vs. pressure to get it right
- How are relationships sourced and managed - the importance of a program

Section 1: The Dating Phase: First Impressions

- Ideal Use Cases - Ideal Banks
- What are YOU good at? - focus on that
- What are you looking for and what are your non negotiables?
- Prohibited vs. allowed vs. high risk categories
- What is your organization's perspective?
  - Bank side
  - Fintech side

Strategic Alignment Check

Letter of Intent (“LOI”) or some type of formality prior to moving towards Due Diligence

- Who is involved at this point, why your Bank’s “program” matters
- Revenue models and unit economics
- Growth expectations and scalability assumptions
- Exit strategies and lifecycle planning
- NDAs and initial information

Question for the Audience: What are you looking for in your next partnership?

Section 2:

Due Diligence: Asking the Hard Questions 💘

Business Experience and Qualifications

Evaluating a FinTech company's business experience, strategic goals, and overall qualifications allows a community bank to consider a FinTech company's experience in conducting the activity and its ability to meet the bank's needs

- Business Experience
- Business Strategies and Plan
- Qualifications and Backgrounds of Leaders

Business Experience and Qualifications

- Company overview
- MIssion statement
- Geographic footprint
- Strategic Plans
- Org chart
- Client references
- Complaints
- Legal, regulatory actions
- Media reports

- Past ops failures
- Patents and licenses
- Bios of key personnel
- Employment policies
- Background check process
- Company website, social
- Ownership information
- Bios of board
- Resource plans

Financial Condition

Evaluating a FinTech company's financial condition helps a community bank to assess the company's ability to remain in business and fulfill any obligations created by the relationship.

- Financial Analysis and Funding
- Market Information

- Financial statements
- Annual reports
- SEC filings
- Financial projections
- Funding sources
- Market info on competitors
- Client base

Legal and Regulatory Compliance

Evaluating a FinTech company's legal standing, its knowledge about legal and regulatory requirements applicable to the proposed activity, and its experience working within the legal and regulatory framework enables a community bank to verify a FinTech company's ability to comply with applicable laws and regulations.

- Charter, articles of incorp
- Licenses
- Patents, IP
- Lawsuites, enforcement
- 10K or 10Q
- Policies, procedures
- Risk assessments
- Complaint process
- Issue management

Risk Management and Controls

Evaluating the effectiveness of a FinTech company's risk management policies, processes, and controls helps a community bank to assess the company's ability to conduct the activity in a safe and sound manner, consistent with the community bank's risk appetite and in compliance with relevant legal and regulatory requirements.

- Policies, procedures
- Risk, compliance staffing
- Audit plan and results
- Issue management
- Training materials, schedule
- KRIs, KPIs
- Governance and board reporting

Information Security

Evaluating a FinTech company's information security measures allows a community bank to assess the adequacy and integrity of a FinTech company's processes for handling and protecting sensitive information, including community bank customer information, depending on the third-party relationship and activity proposed.

- Information Security Program, assessments
- Incident management and response policies
- Security training
- Privacy program
- IT policies, procedures
- Overview of tech stack
- Audit, testing results
- Data mapping

Operational Resilience

A community bank may evaluate a FinTech company's ability to continue operations through a disruption. Depending on the activity, a community bank may look to the FinTech company's processes to identify, respond to, and protect itself and customers from threats and potential failures, as well as recover and learn from disruptive events. It is important that third-party continuity and resilience planning be commensurate with the nature and criticality of activities performed for the bank.

- Business continuity plan
- Disaster recovery plan
- Incident response plan
- BCP, DR, Incident testing
- Reports and audits
- Insurance
- Proposed service level agreements
- Historical SLA performance
- Subcontractors

Operational Resilience

A community bank may evaluate a FinTech company's ability to continue operations through a disruption. Depending on the activity, a community bank may look to the FinTech company's processes to identify, respond to, and protect itself and customers from threats and potential failures, as well as recover and learn from disruptive events. It is important that third-party continuity and resilience planning be commensurate with the nature and criticality of activities performed for the bank.

- Business continuity plan
- Disaster recovery plan
- Incident response plan
- BCP, DR, Incident testing
- Reports and audits
- Insurance
- Proposed service level agreements
- Historical SLA performance
- Subcontractors

Due Diligence Takeaways

What happens if a prospect can't provide everything? Can we move forward safely?

- Approve with conditions
  - Add X, Y, Z within 90 days of approval, but before go-live
  - Adjust pricing if there is an ongoing risk acceptance or monitoring burden
- Decline with clear feedback

Be timely and transparent with decision making process!

NELSON MULLINS Themis

Section 3:

Ongoing Monitoring: Life After the Honeymoon 💘

Section 3: Ongoing Relationship: Governance: The Relationship Framework

What does ongoing monitoring look like?

- It is ***not*** catch everything 100% of the time
- It will involve your committees, escalation paths, and decision rights
- Frequency and quality of communication - Risk Based
- Board and executive engagement - Stay informed
- Not all relationships are the same you will need to align your governance to the risk profile on the Bank side and the FinTech side.
- Establish who is monitoring compliance with the MSA and associated SLAs

Third-Party Risk Management in Practice

What is TPRMs role in this stage of the relationship?

- Integrating FinTechs into TPRM programs
- Ongoing monitoring and periodic reviews
  - Determine what that looks like for you, document the conversations
  - What was flagged in due diligence - info sec? liquidity? high risk merchants?
- Issue Management tracking and remediation discipline
  - Where, how and by who?

- Regulator-ready documentation

Examiners are part of the Relationship

- How regulators view bank–FinTech partnerships - Changing views starting in 2025
- Common examination themes and expectations
  - Know the consent orders and guidance
- Exams involve collaboration between parties
- Know your weaknesses: what are your pain points as a Bank/as a FinTech
  - complaints
  - litigation

Scaling the Relationship Safely

- Consider product and geography expansion controls
- Reassessing risk as volumes grow
  - Document risk vs. reward
- Governance evolution over time as risks change
- Avoiding “set it and forget it” partnerships
- Considerations around expansion, diversification of partnerships, licensure and/or obtaininga bank charter

Early Warning Signs of Trouble

- For the FinTech: Missed commitments and shifting narratives - lack of funding of reserve accounts, lack of reporting and/or lack of communication are all red flags
- For the Bank: No problems is a problem
- Resistance to oversight or audits
- Resistance to requests for scaling and/or change management
- Leadership turnover or financial stress
- Lack of compliance with data sharing, reports, and transparency

NELSON MULLINS Themis

Section 4:

Winddown: Breakups Happen

Section 4: Breakups Happen: Ending the Relationship

- Knowing when a partnership no longer fits
  - failure, mutual termination, does not scale, does not meet compliance
- Outlined in the MSA or “will reasonably work together”
- Customer protection during exits
- Data, funds, and operational unwind
- Lessons learned for future matches
- Regulators will have questions around it

NELSON MULLINS Themis

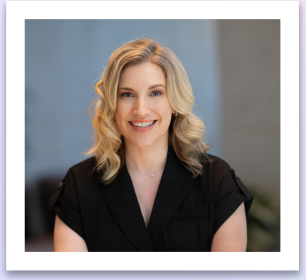
Section 5:

Practical Takeaways 💘

Practical Takeaways

- Slow down early to move faster later
  - Invest in governance upfront
  - Build compliance as infrastructure
- Understand bank obligations and regulatory landscape
- Identify risk appetite and build controls appropriately
- There's no one size fits all - what might work for a competitor may not work for you

Thank you!



Dana Lawrence, CIA, CRMA, CFSA, CAMS, CRVPM

Themis

VP GTM Strategy and Relationships

dana@themis.com

Craig Nazzaro

Nelson Mullins

Partner

craig.nazzaro@nelsonmullins.com

Marianna McDevitt

Nelson Mullins

Associate

marianna.mcdevitt@nelsonmullins.com