NELSON MULLINS Themis

## Themis Banking School:

# Bank Fintech Fundamentals

themis.com

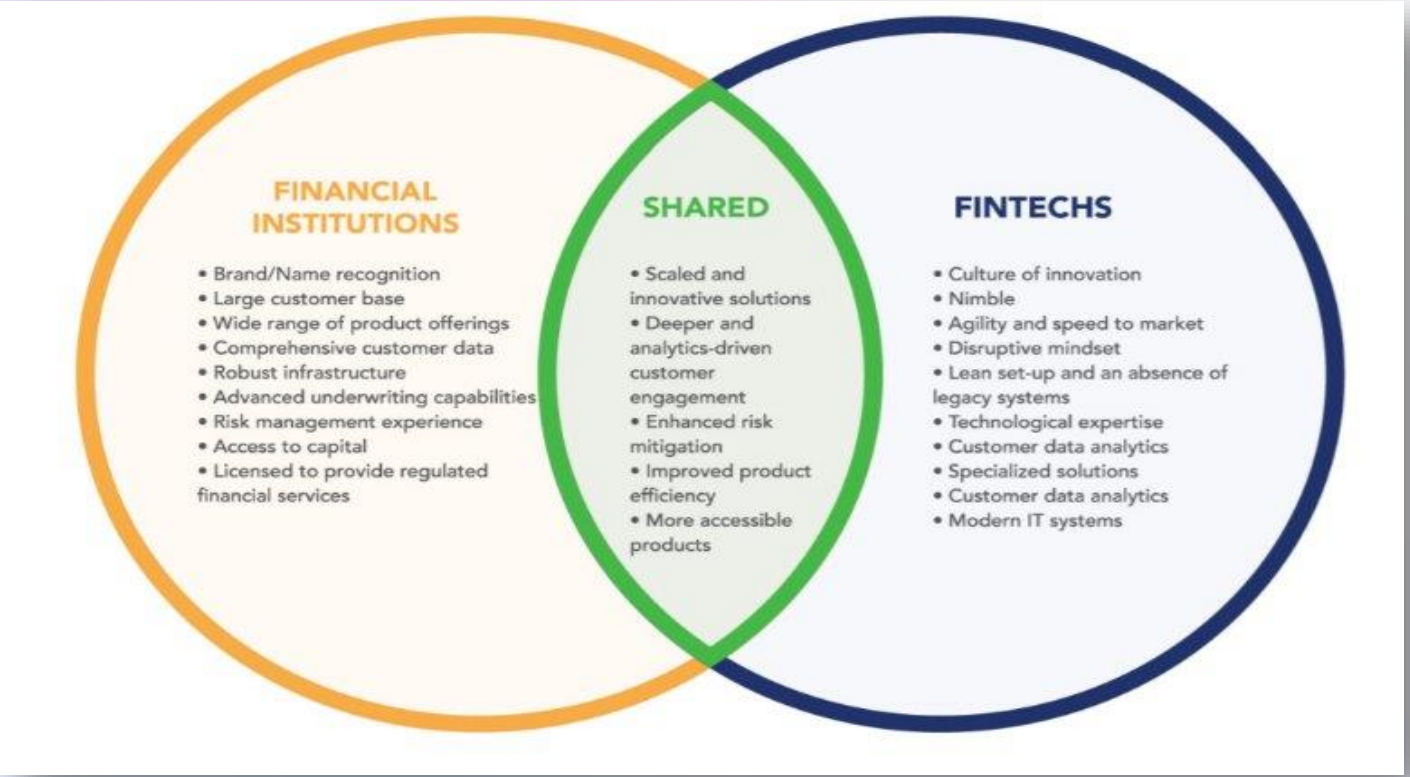
# Learning Objectives

1. What are you offering – What can you offer ?
2. What are the risks – how do you anticipate the risks?
3. How do you control the risks?
4. What are the regulators saying – Innovation vs. Risk?
5. Where are we going?

# Bank-Fintech Models

| | |
|---|---|
| Bank Referrals | • Bank earns revenue by sending customers to FinTech<br>• Can be used where the bank has “gaps” in service offerings |
| Fintech Referrals | • Bank purchases customer leads from FinTech<br>• Bank purchases account or loan assets originated inside FinTech platform |
| Fintech Investment or Acquisition | • Bank invests in FinTech that is mission aligned to bank<br>• Bank buys key technology for private use or sale to other Financial Institutions |
| Private Label Solution/SaaS | • Bank purchases the financial technology to deploy to its customers<br>• Opens new product offerings for the bank |
| Bank to Bank | • Banks partner with each other to fill respective services gaps<br>• Also includes relationships between technology and low-tech banks to offer services |
| Partial Outsourcing | • FinTech assumes limited roles in process—underwriting, data collections, etc.<br>• Allows the bank to “buy” technology or expertise missing in the institution |
| True "Bank Model Partnership" | • Bank serves as the lender/account issuer in FinTech themed ecosystem<br>• Full integration in services with FinTech front-end and bank back-end |

# Mutual Benefits to the Bank and Fintech




*Source: Center for Financial Inclusion at Accion and the Institute of International Finance, July 2017

# Fintech Solutions

- Digital Account Opening (DAO)
- Digital/Mobile Banking
- Full Service ATMs
- Marketplace Lending
- Electronic Payments
- Alternative Underwriting
- Instant Underwriting/Instant Funding
- Deposit Gathering
- Banking as a Service (BaaS)
- Artificial Intelligence/Machine Learning
- “RegTech”
- Stacked Financial Products (Banking + Brokerage + Payments + Investment Advice + Loans)

# Four Pillars of Fintech Regulatory Risk

**Regulatory Risk:** Exposure to substantial fines and sanctions from non-compliance with rapidly evolving financial laws and regulatory expectations

**Reputational Risk:** Compliance failures damage brand equity and erode customer loyalty in competitive markets

**Cybersecurity Risk:** Data breaches and weak security controls threaten customer trust and invite severe regulatory penalties.

**Financial & Operational Risk:** Fraud vulnerabilities, operational errors, and unclear responsibility lines in multi-party partnerships

# Turning Compliance Challenges into Competitive Advantage

**Proactive Collaboration**
Proactive, collaborative compliance is the key to unlocking true fintech partnership value and innovation potential

**Responsible Innovation**
Embrace innovation responsibly to build lasting customer trust and maintain regulatory readiness

**Compliance DNA**
The future belongs to banks and Fintechs that integrate compliance deeply into their organizational DNA

**Build Together**
Let's build the next generation of secure, inclusive, and innovative financial services together

# Regulatory Enforcement Surge: 45+ Cease-and-Desist Orders in 18 Months

**Intensified Oversight**

Regulators are dramatically intensifying their focus on third-party risk management and comprehensive fintech oversight across all partnership models.

**Key Enforcement Areas**

- Bank Secrecy Act (BSA) compliance
- Anti-Money Laundering (AML) protocols
- Unfair, Deceptive, or Abusive Acts or Practices (UDAAP) violations

**Growing Challenge**

Banks face significant challenges in staffing and developing expertise to properly oversee increasingly complex fintech partnerships

# Regulators Pushing Forward:

**Federal Reserve's Novel Activities Supervision Program** – a strategic initiative to monitor and supervise evolving risks from new activities undertaken by banking organizations. It aims to foster responsible innovation while safeguarding financial stability, consumer protection, and a fair marketplace.

- Identification of Novel Activities
- Risk Assessment Framework
- Supervisory Engagement
- Regulatory Evolution

In July 2024, the FDIC, Federal Reserve, and OCC issued a Joint Statement on Managing Risks in Bank-Fintech Relationships. This action signaled regulators' concerns over operational resilience, consumer protection, data security, and AML/BSA compliance risks arising from increasing bank reliance on fintech partners for core services, emphasizing the need for robust risk management. Joint Statement on Banks' Arrangements with Third Parties to Deliver Bank Deposit Products and Services found here.

# BSA/AML Oversight

Robust anti-money laundering controls and comprehensive suspicious activity reporting requirements are needed on both sides of a partnership.

- Bank should mandate standards – can outsource though.

Integrate Know Your Customer, Anti-Money Laundering, data privacy, and payment security into fintech platforms from inception; don’t wait until the Bank's regulator questions it.

Fintech and Bank do not need to grow at the same pace. A Fintech can scale and build controls independently and can outgrow the sophistication of bank partner.

# Alternative Underwriting Data

- Alternative data is anything beyond traditional credit reports that helps a lender predict the likelihood of a consumer's default on a given loan.
- Almost anything can be considered alternative data. Each vendor promises that their alternative data has value at predicting consumer behaviors.

| | | | | | |
|---|---|---|---|---|---|
| Educational Obtainment | Current Job and Income Data | Utility Payment History | Telecom Payment History | Rent Payment History | Insurance Payment History |
| Check Cashing History | Online Banking Data | Payday Loan Payment History | Prepaid Card Spending and Loading | International Remittance History | Cable TV Payment History |

# Alternative Data: Fair Lending Risks

The fair lending risk will vary with the type of alternative data considered.

However, as data becomes more general, looking for corollaries between the data and the performance of the consumer, the fair lending risk increases.

Traditional, credit and credit-like data has been shown to increase protected groups' access to affordable credit.

Some alternative data looks at biographical and personal information about the consumer. This presents significant fair lending risks because of the "consideration" of data relating to a consumer's status in a protected class.

# Fair Lending Abuses in Alternative Data

Alternative Data as a Proxy for Protected Classes:

- **School Attended** (*Sallie Mae* case)
- **Targeted Marketing** (*Facebook* cases): Facebook allegedly offered lenders "hundreds of thousands of attributes" by which they could filter who would see ads, among them categories like "women in the workforce," "moms of grade school kids," "foreigners," "Puerto Rico Islanders," or people interested in "parenting," "accessibility," "service animal," "hijab fashion," or "Hispanic culture"
- **Social Media/Friends and Family**: Some lenders experiment with whether your "friends" have defaulted on loan obligations.
- **Geographic Location**: Has a strong correlation to race and ethnicity.
- **Length of Residence**: Noted by the NCLC as a proxy for a number of protected classes including age and race.
- **High Mileage Vehicles**: Zest Finance, which offers AI and machine learning for credit underwriting, recently noted that AI for used car loans could have a disparate impact on African Americans given the interaction of a car's higher mileage and the consumer's state of residence

# Fair Lending Risks in Alternative Data

## Non-Traditional Credit

- Payday and title loan payment history
- Consumer installment loans payments history
- Rent-to-own payment history

## Credit-Like Information

- Telecommunications payment history
- Utility payment history
- Rent payment history
- Judgments
- Liens
- Bankruptcies

## Employment Information

- Regularity of payments
- Time at workplace
- Overall income
- Amount of overtime and bonuses

## Financial Transaction History

- Prepaid card usage
- Money transfers and remittances
- Account transactions: debits and credit
- Direct deposit usage
- Bank account opening data

## Non-Private Data

- Educational level
- Address and geographical data
- Occupational and employer data
- Assets and real property

## Social Media

- Affiliations with existing customers
- Data provided in online profiles
- Information on usage and friend networks

# Focus on Third Party Risk Management

If you're a Fintech you want a partner that has robust third party oversight program, it may create more work at the beginning but will lay the groundwork for a lasting program.

If you're a bank you can partner with Fintechs to consolidate operational functions, offer new products, improve customer experience through new technology, create stronger compliance controls but no partnership absolves you over required oversight.

You must:

- Review all associated compliance controls
- Documents applicable controls and oversight within an MSA
- Determine the regulatory, reputational and litigation risks associated with partner's operation
- Monitor partner on a schedule applicable to presented risks

Keep in mind the following life stages while building your program:

- Onboarding and initial due diligence
- Due Diligence
- Risk Assessment
- Reporting and Monitoring
- Winddown and Termination

# TPRM – MSA and Associated Agreements

Make sure the MSA and/or SOW provides the Bank with:

- Proper oversight including monitoring and audit rights.
- The proper level of reporting (for example are you seeing complaints?)
- Data privacy controls (are you sharing just enough to obtain the level of services needed)
- Notice from the partner for any and all material changes to scope and or execution.
- Compliance with all laws provision. (Please Note: a lot of tech solutions will shift this to Bank, you need to be aware and have a control in place if this is the case)

Bank will need controls in place to avoid project and/or service creep. Look to confirm that your LOB/Ops teams cannot expand or alter the MSA and/or SOW without controls in place to gain legal and or compliance sign off.

# TPRM - Initial Due Diligence

**Prior to Onboarding**

- Determine the regulatory, reputational and litigation risks associated with partner's operation.
- Diligence partner according to level of risk presented. Prepare a diligence overview and retain internally to showcase to regulator that you not only understand the risks but have an informed and justified level of comfort with the partners controls and overall CMS.
- Discuss findings within all appropriate committees, senior management and share with Board, again always thinking that you will have to defend your position in the event there is a process break within the partners operations.

Who are the SME's within the Bank – You can outsource almost anything - but you cannot outsource the responsibility/liability. Your regulator will look to see if you can handle and understand the increased risks brought with the partnership that was deployed.

# TPRM – Due Diligence Ongoing

**Ensure your TPRM program is robust enough to cover:**

- Ongoing monitoring sufficient to manage the level of risk presented by the partner.
- Defines critical vendors (don't just think of this as critical to ongoing ops/safety and soundness).
- The leveraging of any ongoing reporting that was provided for within the MSA. The data is useless if it is sitting in the Bank untouched. MSA vs Operational Oversight and Controls.

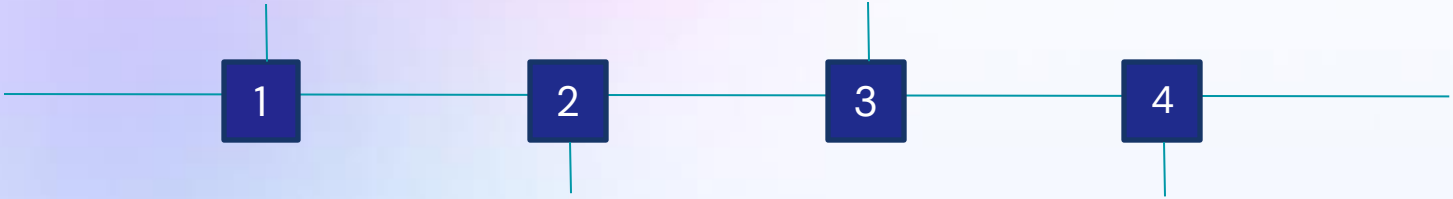
**Termination – Winddown**

# 2025 and Beyond: Trends to Watch

NELSON MULLINS Themis

**AI Explainability**
Increasing regulatory focus on AI explainability and ethical use in financial services operations

**Continuous Monitoring**
Shift from periodic audits to continuous, AI-driven compliance monitoring




**Consumer Protection**
Growing importance of consumer protection amid open banking and data sharing initiatives

**Strategic M&A**
Strategic mergers and partnerships to build compliance resilience and sustainable growth

# 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