NELSON MULLINS Themis

Themis Banking School:

2026 Preview for Banks and FinTechs

themis.com

2025 In Review Summary

CFPB Dismantling	OCC – Emphasis on TPRM	Fintech Charter Push	Federal Reserve Direct Access for Payments
• Pending litigation • State vs federal enforcement changes and how states are handling • Future state	• RFI in for TPRM • Continued focus on innovation	• Who is this best for, who is applying? • Emphasis on safety and soundness	• Who is this best for, who is applying? • Requests for input on payment account eligible with the Fed

CFPB – Dead man walking ?

CFPB dismantling - what they are doing now

- In January acting CFPB Director Russ Vought formally requested funds from the federal Reserve to maintain operations at the CFPB through the second quarter of this year.
- What can they really do with the remaining staff?
- How should you approach?

State vs Federal enforcement

- What are the states prioritizing?
- How are they enforcing?
- How to manage expectations of each and every state?

FDIC

Under Chair Travis Hill, the FDIC has undergone a broad deregulatory and institutional reset. Now that he has been confirmed it pays to read though his statement when he was made acting Chairman. He said he was focusing on:

- Adopt a more open-minded approach to innovation and technology adoption, including (1) a more transparent approach to fintech partnerships and to digital assets and tokenization, and (2) engagement to address growing technology costs for community banks
- Improve the supervisory process to focus more on core financial risks and less on process and reevaluate the supervisory appeals process.
- Encourage more de novo activity so there is a healthy pipeline of new entrants in the banking sector.
- Study deposit behavior to develop a more sophisticated understanding of the relative stability of different types of deposits and depositors.
- Reevaluate our disclosure practices and expand transparency in areas that do not impact safety and soundness or financial stability.
- Ensure the FDIC remains within our statutory mandates and stops coloring outside the lines.

OCC – RFI – Continued Focus on TPRM

The OCC issued and RFI seeking public comment on community banks' engagement with their core service providers and other essential third-party service providers, especially as it relates to community banks' ability to remain competitive in a rapidly evolving marketplace

- Contract negotiations;
- The scope and burden of applicable fees;
- Billing practices and concerns;
- Oversight of core service providers and other third-party service providers;
- The ability to terminate relationships with core service providers in breach of contracts, including service-level agreements;
- Any burdens limiting banks' ability to undertake core conversions that are beyond those inherent in such a process;
- The extent to which interoperability between core service providers and other third-party service providers may facilitate or inhibit innovations necessary for community banks to remain competitive in a rapidly evolving marketplace;
- Supervisory expectations and guidance, including the Third Party Risk Management (TPRM) guidance, or regulatory requirements

Payment FinTechs – Direct FRB Access?

FRB requested public input a "payment account," which Fintech's could use for the limited purpose of clearing and settling their payments.

- The Board is exploring additional risk controls and conditions for Payment Accounts. These controls could take the form of: account agreement conditions, attestation requirements, or periodic reporting requirements. These controls could cover areas of risks to the Reserve Banks and payment system (such as operational or cyber risks) or risks associated with illicit financing.

- The Payment Account would be a separate and distinct type of account from a Reserve Bank master account (a Master Account).

- Consistent with a Payment Account's lower risk profile, staff believes that a request for a Payment Account could generally receive a more streamlined review than a request for a Master Account from a comparable institution.

- Is this the Goldilocks solution?

Bank Charters and Alternatives

FinTech finding a path to Charters – The OCC "Fintech Charter" gone but the movement still there. Applicants now have a more friendly path to obtain a full charter.

Pros:
Greater autonomy
Easier to innovate

Cons:
Direct supervision
Greater capital required

As of December 2026, the OCC listed six pending applications for limited purpose trust companies seeking to engage in cryptocurrency and digital asset activities. This is close to the same number of trust company applications the OCC received over the entire previous four years.

BSA/AML Expectations

Continuous Oversight:

- Ongoing due diligence and dynamic risk assessment remain critical in fintech partnerships to prevent financial crime and maintain regulatory compliance.
- Periodic partner risk reviews
- Regular control effectiveness testing
- Updates emphasize efficiency, fairness, and transparency in AML enforcement, shifting from volume-based to risk-based reporting approaches.

Need clear roles and both contractually and operationally.

Regulatory Supervision

So where are we? What will be showing up in exams? What will regulators be looking at?

- General Competence
  How can you showcase?
- Controls – fraud, credit risk, general compliance
- Operational resilience – liquidity, cyber, prudential risk
- TPRM
- Legal – contracts, winddown, reporting

AI Use Cases in Financial Institutions

Risk and Compliance

- Complaints
- Marketing Compliance
- Policies
- Fraud and Anti-Money Laundering
- Third Party Risk Management

Operations

- Underwriting
- Trading and Portfolio Management
- Customer Experience
- Contract Management
- Procedures Assistant

Cyber Security and Resilience Risks

- **AI is accelerating the arms race**: Attackers use AI for hyper-targeted phishing, deepfakes, synthetic identities, and automated vulnerability discovery, while defenders rely on AI for anomaly detection, behavioral monitoring, and faster incident response, often faster than governance can keep up.

- **Preparedness is overestimated as threats grow more complex**: Geopolitically motivated cyberattacks are now a top risk driver, with infrastructure disruption, espionage, and cloud-based data takedowns increasingly targeting financial institutions and shared technology stacks.

- **Trust boundaries are breaking down**: third- and fourth-party ecosystems are the primary attack surface, and realistic deepfake audio/video scams mean banks can no longer assume transactions are legitimate just because a customer “approved” them. Advanced analytics and continuous monitoring are now essential.

Cyber Security and Resilience Themes

- **Assume AI enabled fraud and deception are the new baseline**: customer approval, voice recognition, and familiar processes are no longer sufficient. Banks must rely on behavioral analytics, anomaly detection, and layered controls to validate intent and legitimacy.

- **Treat third- and fourth-party cyber risk as enterprise risk, not vendor risk**: Shared infrastructure, cloud providers, fintech partners, and data platforms are now the primary attack surface and require continuous monitoring, resilience planning, and clear exit strategies.

- **Prepare for cyber events as liquidity, trust, and stability events**: Cyber incidents will move faster than incident response playbooks, so banks must test decisionmaking, communications, and continuity under hostile, AI driven and geopolitically motivated attack scenarios.

Digital Assets and Stablecoin

Traditional Remittance Challenges

Conventional cross-border transfers face:

- High fees (often 5–10% of transfer value)
- Slow settlement times (2–5 business days)
- Multiple intermediaries, each adding cost and FX spread
- Limited transparency on where funds are during transfer
- These costs can make remittances, especially small-dollar remittances (think migrants sending money to their home countries), expensive

Stablecoins can Improve the Process

Clear regulatory focus/shift to on the benefits of innovation in the space. Internally at bank of fintech - Need to balance Consumer Risk vs Consumer Experience/Benefit.

NELSON MULLINS Themis

Questions for the Audience:

- Top concerns as you enter 2026?
- What technology do you plan to adopt in 2026 to help with compliance?

How to keep up with Change Management

Move from periodic reviews to continuous regulatory monitoring
Track rulemaking, guidance, enforcement actions, and supervisory speeches in near-real time, with clear ownership for intake, interpretation, and impact assessment across lines of business.

- Sign up for regulatory feeds, now with AI digests
- Subscribe to regulators' press updates
- Industry bloggers, newsletters, conferences

Operationalize change, don't just document it
Translate regulatory updates into updated policies, procedures, controls, training, and testing. Evidence execution, not just awareness, to satisfy examiners.

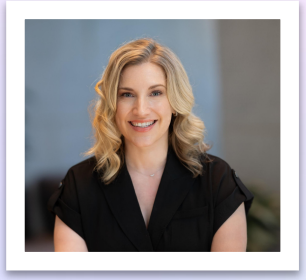
Create strong cross-functional governance and accountability
Establish a formal change management framework that connects compliance, legal, risk, IT, product, and the business, with escalation paths and board visibility for high-impact changes.

Steps You Can be Taking Now for 2026

NELSON MULLINS Themis

Lookbacks and reviews of policies and procedures	What technology are you adopting? How are you applying compliance controls?	If creating efficiencies with technology, are you using the capacity elsewhere?
If you're a bank, be wary of the swing back to scrutiny with change in administration.	Revisit functionality and product offerings through your partnerships.	Revisit MSAs to ensure they are capturing your activity and all controls.

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

Giovana Grupenmacher

Nelson Mullins

Policy Advisor

giovana.grupenmacher@nelsonmullins.com