Future of Fintech: Maintaining a Solid Compliance Foundation Amid Evolving Expectations

By Emily D'Angelo and Mike Scarpa

As fintechs continue to grow and expand their scope of activities, regulatory requirements generally increase along with risks to the organization, its customers, and its partners. Fintechs need to maintain an independent, strong, and adaptable compliance foundation to respond and manage evolving standards with appropriate resources, processes, internal controls, and monitoring techniques. Regulators are expanding requirements for bank partners to impose stricter oversight of their fintech partners. At the same time, however, agencies are making it clear that fintechs cannot rely only on banks to ensure compliance for them and that bank-fintech partnerships will be shut down at the first hint of non-compliance.

Increasing requirements have resulted in more bank partners de-risking and re-evaluating their engagement in fintech relationships. Additionally, the industry has seen banks and their regulators terminate fintech partnerships they deem unsafe and unsound. Fintechs are already under significant strategic, financial, and reputational strain and such terminations create an existential threat for many of them. Bank partners choosing to partner with fintechs have become considerably more selective, by prioritizing those with less burdensome compliance requirements or by working with firms that maintain autonomous and robust compliance and operational risk management programs.

Even amid realignment and refinements for compliance oversight, though, fintech and bank partnership models are here to stay. This reinforces the importance of the partnerships' focus on sustainable compliance and operationally robust foundations.

Increasing Scrutiny and Severity of Penalties

The rise in regulatory requirements for bank and fintech partners has been demonstrated publicly through recent consent orders. Increased scrutiny comes in two primary areas: the business model itself and associated requirements for third-party risk management due to the inherent risks of these relationships. Some examples of increased supervision and targeted examinations are highlighted below:

- A regional bank consented to the issuance of a consent order charging the bank with unsafe or unsound banking practices relating to its third-party risk management program and other aspects of its fintech partnerships. The consent order requires the lender to increase capital levels, terminate some of its fintech partnerships, and enhance its risk management program. Furthermore, the bank must hire a third party to assess its management structure and how staff oversee the risk management of certain lines of business.

- A fintech-focused regional bank received a cease-and-desist order for unsafe and unsound practices, including those related to anti-money laundering, capital ratios, capital and strategic planning, liquidity risk management, and information technology controls. This enforcement action was the second for the bank in less than 18 months. The second enforcement action was unanticipated since it appeared that the bank was taking steps in the right direction to address concerns such as bringing in new leadership and working to raise capital.
- A bank and fintech received a consent order tied to non-compliance with anti-money laundering regulations and risk management matters that could cost millions of dollars. The company continues to invest in people, process, and product improvement to improve capabilities associated with regulatory compliance.

These orders are the latest examples of crackdowns on sponsor banks by regulators due to the compliance failures of their fintech partners. Banks and fintechs should pay close attention to these public enforcement actions, since they can help provide a foundational roadmap of issues that should be scrutinized within their compliance programs.

Also, interagency guidance on third-party relationships has detailed obligations and new considerations for banking organizations to understand and incorporate when monitoring and maintaining their third-party relationships. Accountability is clearer than it has ever been for banks, fintechs, and their regulators. Compliance costs and staffing shortfalls will not be acceptable excuses for the lack of solid compliance infrastructure and execution.

Regulatory focus reaffirms that banks and fintechs are accountable for responsible innovation and that fintechs should adhere to the same standards of operational compliance, anti-money laundering, and safety and soundness that are required of their bank partners. The days of reliance on bank compliance support for fintechs are gone. Fintechs will need to match their programs to the requirements and risks that their products and activities involve.

Implications for Fintechs

The increasingly intricate regulatory environment has made compliance a resource-intensive and costly effort for fintechs—one that was not fully considered when fintechs were developing their strategy and offerings. Often fintechs have limited resources and/or skillsets available to support compliance programs and related operational activities. Additionally, building and maintaining compliance management systems from the ground up can be time consuming and costly.

Bank partners aren't the only ones facing supervisory findings, fines, and other penalties (including cease-and-desist orders) for the non-compliance of their partners. Fintechs have also had to pay the price for violations; for many, these penalties can threaten viability. Recent regulatory actions have showcased these penalties, with fintechs paying heavily for marketing and disclosure violations, among other violations.

Banks and fintechs need to integrate compliance and operational risk efforts before business starts. Launching a relationship requires sufficient time and comprehensive assessment at the outset. Third-party professionals can and should be utilized to reduce risk, lower costs, increase speed to market, and build the foundation for a compliant and operationally effective program.

Critical Operational Principles

Effective fintech compliance requires strong risk and compliance frameworks to ensure business models can operate efficiently with minimal scrutiny from regulatory agencies. Fintechs should take note of the following key areas from the interagency guidance:

- Planning
- Due diligence (by the bank)
  - Aligning with the level of risk and complexity of the relationship. Fintechs should be prepared to undergo more comprehensive due diligence if they perform higher-risk and/or more complicated activities.
- Ongoing monitoring (by the bank with regular input from the fintech)
  - Review of performance and effectiveness of controls
  - Regular testing of controls that manage risks from fintech relationships
- Contract negotiation (by the bank)
  - Fintechs should expect greater attention to:
    - Performance measures or benchmarks
    - The right to audit
    - Responsibility for compliance with laws and regulations
    - Business continuity
    - Subcontracting
    - Indemnification and limits on liability
    - Insurance
    - Default and termination
- Termination of the relationship
  - Awareness of various reasons for termination of the relationship, such as breach of the contract, non-compliance with applicable laws and regulations, or discontinuation of the activity is necessary to ensure continuity.
  - An operational plan should nevertheless be in place in the event of termination.

Conclusion

With fintechs profoundly reshaping aspects of financial services these innovative business models may struggle to conform to current regulatory structures. Recent consent orders, increased regulatory requirements, and growing penalties for non-compliance highlight the need for a proactive and forward-thinking approach to compliance that both fintech and bank partners should prioritize. Consequently, independent third-party opinions should be sought for industry-leading perspectives.

How Treliant Can Help

Treliant understands first-hand the regulatory challenges fintechs face and can provide cost- effective support for these innovative companies. Fintechs are required to have Compliance Management Systems (CMS) and Bank Secrecy Act /Anti-Money Laundering (BSA/AML) compliance programs built into their business models that fit both partner bank and regulatory requirements. To evaluate the adequacy, partner banks supporting fintech activities may need to supplement or complement with experienced and qualified third-party professionals to perform annual independent assessments of fintech programs or to support their build or remediation efforts.

PARTNERSHIP EXPERTISE

We have extensive experience advising fintechs on the build and maintenance of compliance and operational risk management programs. We offer both assurance to the partner bank on internal control reliance and tailored recommendations that assist the fintech in meeting regulatory requirements across its operational activities and product set.

REGULATORY KNOWLEDGE

Our professionals bring a distinctive blend of experience as former regulators, regulatory attorneys, auditors, and Chief Compliance Officers within banks and fintech organizations. We have extensive regulatory compliance and operational risk expertise in assisting fintechs through the challenging regulatory environment.

METHODOLOGY AND APPROACH

Our broad expertise allows us to provide an approach that combines insights with practical advice. We guide clients through the process of building and/or enhancing their compliance programs in a way that not only meets regulatory expectations, but also shows consideration for the size and complexity of the operations and offerings.

Emily D'Angelo
Emily D'Angelo is a Senior Consultant with Treliant. Her professional experience includes process optimization, continuous improvement, target operating model design, strategic transformation, and project management. **edangelo@treliant.com**

Mike Scarpa
Mike Scarpa is a Managing Director in Treliant's Regulatory Compliance, Mortgage, and Operations Solutions practice. He helps set Treliant's regulatory compliance/operations agenda, including key trends, solution offerings, and client pursuits. He also executes on regulatory compliance projects and serves as a subject matter expert. **mscarpa@treliant.com**