March 28, 2023

Navigating the Regulatory Landscape: How Fintechs Can Turn Compliance Into a Competitive Edge

1307 New York Ave NW
6th Floor
Washington D.C., 20005
fsvector.com

FS VECTOR

I. Introduction

Failure to adequately invest in compliance and risk management have led to enforcement actions involving fintechs, increased focus on consumer protection lapses, and pressures on partner banks to strengthen onboarding and oversight within their Banking-as-a-Service partnerships. A lesson is clear: an effective compliance function is vital to the success of any fintech, regardless of maturity. In parallel, an uncertain economic environment has required fintechs to explore ways to optimize expenditures and compliance costs. The recent bank failures and pressures on credit and liquidity are also likely to heighten how institutions evaluate risk, including third-party compliance risk.

For fintechs seeking to allocate finite resources while embedding a culture and practice of compliance, where does this leave them? Fintechs that invest purposefully in compliance stand to benefit in two key ways:

- They set the foundation for long term success and management of compliance and operational risk, evidencing prudent stewards of investor funds, strong partners to banks, and responsible participants in the financial system; and
- They can balance compliance and engineering spend commensurate with their risk profiles, minimizing fraud losses and optimizing opportunity costs associated with over- or under-building compliance infrastructure.

While there is no one-size-fits-all approach to designing and operating compliance programs, firms that get the fundamentals right early will see smoother partner bank onboarding, less chance of de-risking, reduced operating expenditure as a proportion of scale, and an efficient path to long-term success. Though generally viewed as a cost center, compliance can be used by fintechs as a competitive advantage to show value to partners and prevent the much greater costs of noncompliance. For fintechs launching or scaling in the current environment, now is the time to optimize compliance spend in line with their strategic objectives. This article provides practical guidance in five key areas: compliance governance and oversight, fraud, transaction monitoring, complaints management, and staffing options.

II. Solutions

COMPLIANCE GOVERNANCE AND OWNERSHIP

A common mistake of early stage startups is to not actively plan for scaled governance and oversight of the compliance function. Each fintech's maturity will drive the compliance team's composition - ranging from a shared, whole-of-firm approach involving all personnel during the pre-launch build phase, to a specialized and layered function reporting to a Chief Compliance Officer at a matured fintech.

For how long might an early-stage company adopt the all-hands approach? Should they make a CCO one of their first hires?

A pre-launch fintech might reasonably operate with little-to-no dedicated compliance staff, the function instead fulfilled by dual-hatted leadership, e.g., the founders leading both product and compliance. These leaders may also look externally to counsel or advisers for compliance expertise. Were that same firm to invest in a CCO, they could find itself spending too much too soon, while not taking advantage of the CCO's expertise. A full three lines of defense model for example is generally not needed until the fintech is live and scaling.

The approach to hiring must not only be timely, but also strategic and deliberate. By carefully planning and considering when to hire a CCO, it signals to bank partners, regulators, and customers the fintech's commitment to responsible and compliant business practices. Firms should factor in lead time to fill a position, including identifying candidates, conducting interviews, and negotiating compensation. The table below provides guidance on how a fintech should consider investing in compliance leadership based on its maturity.

Exhibit 1: Compliance Governance and Leadership

Fintech Maturity	Compliance Leadership Composition			
	Double Hatted Leadership (e.g., CEO/CCO)	**Part-Time / Fractional CCO**	**Full-Time CCO**	**Considerations**
Pre-Alpha, Alpha, or Proof of Concept	Minimum expectation	Premature	Premature	Someone should be responsible for compliance. It's sufficient to rely on existing resources.
Beta Testing or Pilot Programs	Sufficient	Likely premature	Premature	Someone should be responsible for compliance. It's sufficient to rely on existing resources. The firm should plan for dedicated compliance leadership.
Planning Go-Live	Sufficient	May be premature	Likely premature	Someone should be responsible for compliance. It's sufficient to rely on existing resources. The firm should plan for dedicated compliance leadership.
Live 0-6 Months	Likely insufficient	Sufficient	May be premature	The firm should have dedicated compliance leadership. A part-time/fractional CCO would likely suffice at this stage.
Live 6-12 Months	Insufficient	Sufficient	Sufficient	The firm should have dedicated compliance leadership. A part-time/fractional CCO could suffice at this stage depending on size, growth, and complexity.
Live 12+ Months	Insufficient	Insufficient	Sufficient	Not having a full-time CCO by this stage puts the fintech at risk. Part-time/fractional CCO could be sufficient only in limited circumstances.

FRAUD

Startup fintechs appeal to fraudsters for several reasons: First, the products are almost always digital first. The lack of face-to-face contact at onboarding and on an ongoing basis enables fraudsters to impersonate and appropriate identities. Second, fraudsters actively target startups seeking to identify vulnerabilities in the fintech's fraud risk management. Even those fintechs that implement fraud controls across the business have likely not refined them enough to combat fraud as effectively as those at a matured institution. Third, because they are largely unregulated compared to their traditional bank counterparts, fintechs often don't have their internal fraud controls reviewed or scrutinized in a way that would identify gaps or shortcomings.

Although vulnerable, fintechs can implement anti-fraud practices that will not only reduce fraud related losses/costs, but will help address concerns from regulators that these mostly unregulated financial entities are a hotbed for fraudulent activity.[1]

CUSTOMER ONBOARDING/TRANSACTION FRAUD

Combating sophisticated fraud attempts involves tools that go beyond simple identity verification at onboarding. Today's fraud tools use innovative methods to detect fraudulent customer applications, including document and biometrics verification, email/phone risk analysis, device analytics, IP/VPN monitoring, liveness, and more. Effectively implementing anti-fraud tools at onboarding prevents bad actors from accessing the platform, instilling confidence in the fintech's risk management practices and overall program efficacy.

Even with the most advanced fraud controls at onboarding, bad actors may yet be able to open an account and start transacting. While retroactive transaction monitoring is useful in identifying unusual or fraudulent transactions after they have been conducted, fraud losses remain a burden on fintechs where these are the only controls. Integrating real-time fraud prevention tools into a fintech's transaction flow can stop fraudulent activity at the source - preventing the transaction from being completed and mitigating potential losses. Some third-party tools offer to absorb the fraud loss risk of the firm that integrates their solution. These tools may be particularly appealing for fintechs whose products are exposed to heightened risk of ACH and chargeback fraud.

By efficiently implementing fraud controls during onboarding and thereafter, a compliance program can be optimized to reduce fraud losses, minimize the need for fraud staffing, lower costs, and improve the product's long-term viability.

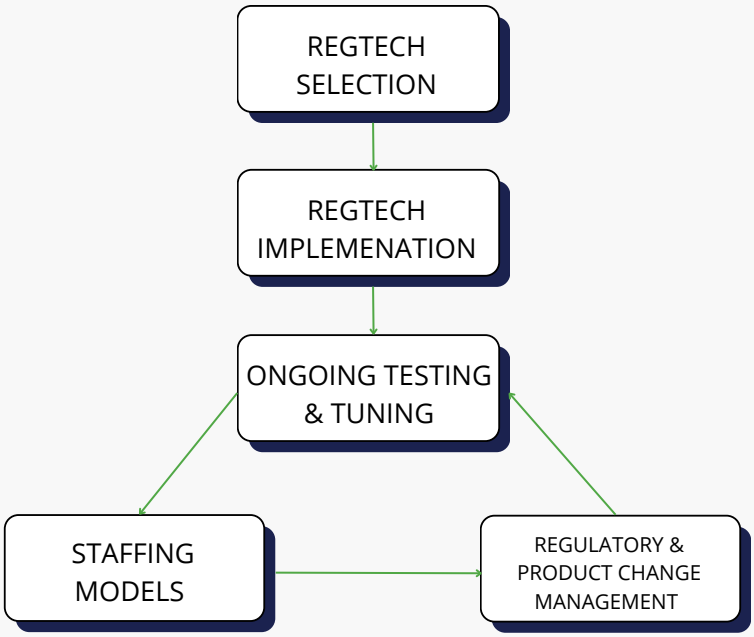
[1] *In a report issued in December 2022, Congress called out fintechs for systematic control failures that largely contributed to the tens of billions in fraudulent Covid-19 related Payment Protection Program loans. https://coronavirus.house.gov/sites/democrats.coronavirus.house.gov/files/2022.12.01%20How%20Fintechs%20Facilitated%20Fraud%20in%20the%20Paycheck%20Protection%20Program_0.pdf*

TRANSACTION MONITORING

Transaction monitoring is a crucial aspect of every compliance program, providing a layer of protection for both the fintech and its customers against illegal activities such as fraud, money laundering, and terrorism financing. In its early stages, fintechs may be able to effectively monitor transactions using internally built processes, such as manually reviewing all transactions during beta testing or generating transaction reports to comb through for unusual activity. Eventually these internal/manual controls will need to be supplemented by more sophisticated tools, generally in the form of a third-party regulatory technology (regtech) tool.

An all too common mistake when implementing a regtech's TM tool is utilizing the vendor's out-of-the-box solution without considering the fintech's specific risk profile. Using cookie cutter rules can put a fintech at risk of having unruly amounts of false positives for its compliance team to manage - an extremely costly endeavor. A bit more concerning from a regulatory perspective, is the risk of large amounts of false negatives, where unusual activity that should have been flagged was missed by the out-of-the box rules. Managing the transaction monitoring program lifecycle efficiently starts with effectively implementing a regtech's tool.

Exhibit 2: Transaction Monitoring Program Lifecycle



What should a fintech do with a regtech's out of the box solution to ensure its use doesn't lead to absorbent compliance costs and/or operational failures?

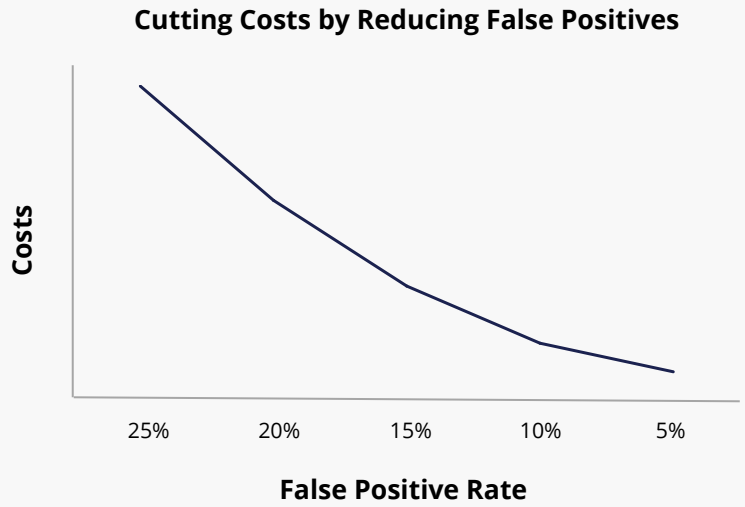
DEVELOP A RISK-BASED RULESET

First, conduct an initial coverage assessment to determine what specific product/service, customer, and geographic risks are relevant to the fintech and rule types can be implemented to cover those risks. Next, conduct an initial rule calibration to identify the ideal thresholds/parameters for the rule types selected during the initial coverage assessment exercise. This should be tailored to the fintech's expectations for its customers, transaction types, amounts, velocity, etc. For instance, a rule monitoring deviations from expected customer activity will vary greatly depending on whether the fintech is a consumer neobank whose average customer spends $500/month versus a commercial neobank whose average customer spends $500/day.

TESTING, TUNING, IMPROVING

Ongoing testing and tuning of rules/thresholds is a key step in the life cycle of every TM program. A benefit of this process is to identify and reduce the number of false positive alerts, which in turn, reduces the amount of staffing costs associated with reviewing TM alerts. As the graph below demonstrates, small reductions in overall false positive rates lead to a direct reduction in compliance staffing costs.

Exhibit 3: False Positive Reduction Graph



COMPLAINT MANAGEMENT

Complaint management is a mechanism for fintechs to ensure they are aware of potential issues with their product, service, or business. It also serves a vital purpose in ensuring overall customer satisfaction. The prospect of a dedicated program for complaint intake, tracking, investigation, and resolution can be a costly one, especially where the program is entirely manual. As the company grows, fintechs should look to automate their complaint management process as a way to optimize costs.

A documented complaint management program with little to no automation (e.g., single support email) should suffice for those fintechs in a closed beta testing/pilot program where complaint volumes should be nominal. However, once the company launches its product to the general public, that manual process will quickly become unmanageable as complaint volumes increase.

Developing an integrated process for complaint management should start with a technology solution that can streamline the process for complaint intake, classification, tracking, and response. Ticketing tools with customizable workflows can serve this purpose well, whether built in house or using a third-party service provider. In addition to organizing complaints in a centralized repository for review/response, ticketing tools can provide customizable reports used to complete trend analyses and identify systemic issues.

As detailed further below, fintechs can also consider wholly outsourcing its complaint management function to third-party service providers. While this can be appealing from a cost and efficiency perspective, fintechs should consider what impacts this may have on overall customer satisfaction and retention.

STAFFING

Consider Outsourcing

When building a compliance team, it can be difficult to gauge whether full-time hires will have the comprehensive expertise and/or bandwidth needed to manage the compliance function. In addition, full-time fintech hires are expensive in terms of onboarding/training, benefit costs, and demands for cash/equity compensation. A potentially cost-saving alternative fintechs should consider is business process outsourcing (BPO).

During the transitory period post-launch where compliance tasks can be voluminous, but difficult to estimate, fintechs should consider BPO in place of extensive full-time staff hires. BPOs firms can oftentimes be used effectively to manage costs and quickly operationalize key processes. However, to ensure overall integrity of the compliance function, the fintech must have sufficient oversight and monitoring of any out-sourced tasks, including adequate training of BPO staff on the fintech's specific compliance procedures, establishing key performance indicators, quality control of BPO work product, and requirement of strong information and data security measures at the BPO firm (such as ISO/SOC 2 certifications).

Staffing Models

As fintechs scale, their unique compliance staffing needs will come more into focus.

Once there is a solid grasp on volumes of the daily compliance tasks mentioned above, fintechs should implement staffing models to help measure the adequacy of current staffing levels and estimate future staffing needs based on business growth projections. At a rudimentary level, a staffing model can be based on the following:

Staffing Needs = (# of tasks per month X time needed to complete task) / Staff Bandwidth

Staffing models are not an exact science, but can provide a guiding light to help senior management think strategically about staffing. These models should be an ongoing exercise and when incorporated correctly, can ensure compliance staffing costs are continuously evaluated and optimized.

III. Conclusion

A poorly developed compliance function can lead to increased regulatory scrutiny, failed bank partnerships, costly fines/enforcement actions, bloated fraud losses, diminished reputation, and operational failures that impact the overall health of a fintech. Following the practical guidance provided here can put fintechs in a strong position financially and operationally - setting the program up for continued success in an otherwise turbulent period. Implementing these strategies can transform compliance from a cost center to a competitive edge for any fintech.

About the Authors

Chris Sidler
Partner, Advisory
csidler@fsvector.com
Washington, D.C.

Ethan Singleton
Principal, Advisory
esingleton@fsvector.com
New York City, NY

FS Vector is a strategic consulting firm for financial services clients in a rapidly evolving industry and complex regulatory environment. As trusted advisors, we seamlessly collaborate with clients to develop, launch, and mature fintech products and compliance programs. Our team's diverse expertise make us the go-to partner for a vast range of matters, such as exploring new market opportunities, licensing acquisition and maintenance, digital banking, independent assessments, interim and full-time resourcing, due diligence, and more. For more information visit www.fsvector.com or email us at info@fsvector.com.