



Fintechs and regulatory compliance

The risk management imperative

May 2018

CENTER for
**REGULATORY
STRATEGY**
AMERICAS

An emerging irony of the financial technology (fintech) industry is that the very companies which have disrupted the financial services industry may themselves experience disruption as a consequence of their own success – that is, as regulators increase their attention and expectations.

As reported in a [previous Deloitte point of view \(POV\)](#), domestic and foreign regulators continue to take notice of the financial products and services that fintechs offer and the way they operate. While acknowledging that fintechs have introduced technology which enables innovation in financial services, it appears that lines are being blurred between fintechs and other more traditional financial institutions that offer the same or similar type of products. This lends support to regulators who may seek to subject fintechs to some of the same regulations as other financial institutions.

US federal bank regulatory agencies (e.g., the Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), and the Office of Comptroller of the Currency (OCC)) do not have the authority to apply bank regulations to fintech firms. However, certain fintech firms may be subject to enforcement actions if, for example, they fall under the Bank Service Company Act's definition of service provider. And, as we

previously reported, the introduction of a possible special purpose charter for fintechs would provide the OCC with regulatory and enforcement authority over firms that opt to pursue this charter¹. Consistent with this interest, regulators continue to scrutinize banks' third-party service providers, including fintech firms.

To this end, the US Government Accountability Office (GAO) issued a report in 2017² analyzing the four key areas of fintech—mobile payments, marketplace lenders, digital wealth management platforms and financial advice, and distributed ledger technology—to assess:

1. Benefits, risks, and protections for users
2. Current regulatory oversight
3. Regulatory challenges
4. The steps taken by regulators in the US and non-US jurisdictions to encourage financial innovation.

The report sets forth several recommendations for federal agencies—including the FRB, FDIC, OCC, Consumer Financial Protection Bureau (CFPB), Securities and Exchange Commission (SEC), and others—related to:

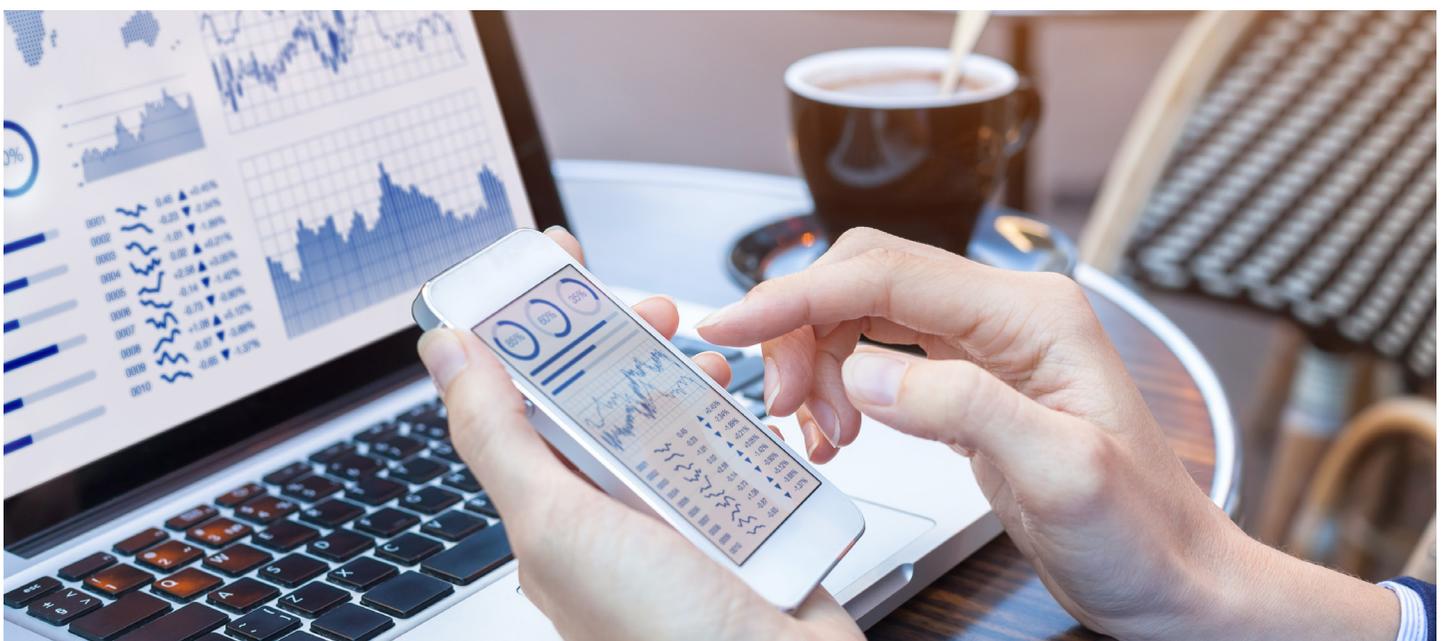
1. Improving interagency coordination with respect to fintech
2. Addressing concerns on financial account aggregation

3. Evaluating whether it would be “feasible and beneficial” to adopt regulatory approaches similar to those undertaken by regulators in other countries

The agencies agreed with the GAO's recommendations and said they would take responsive steps to implement them³.

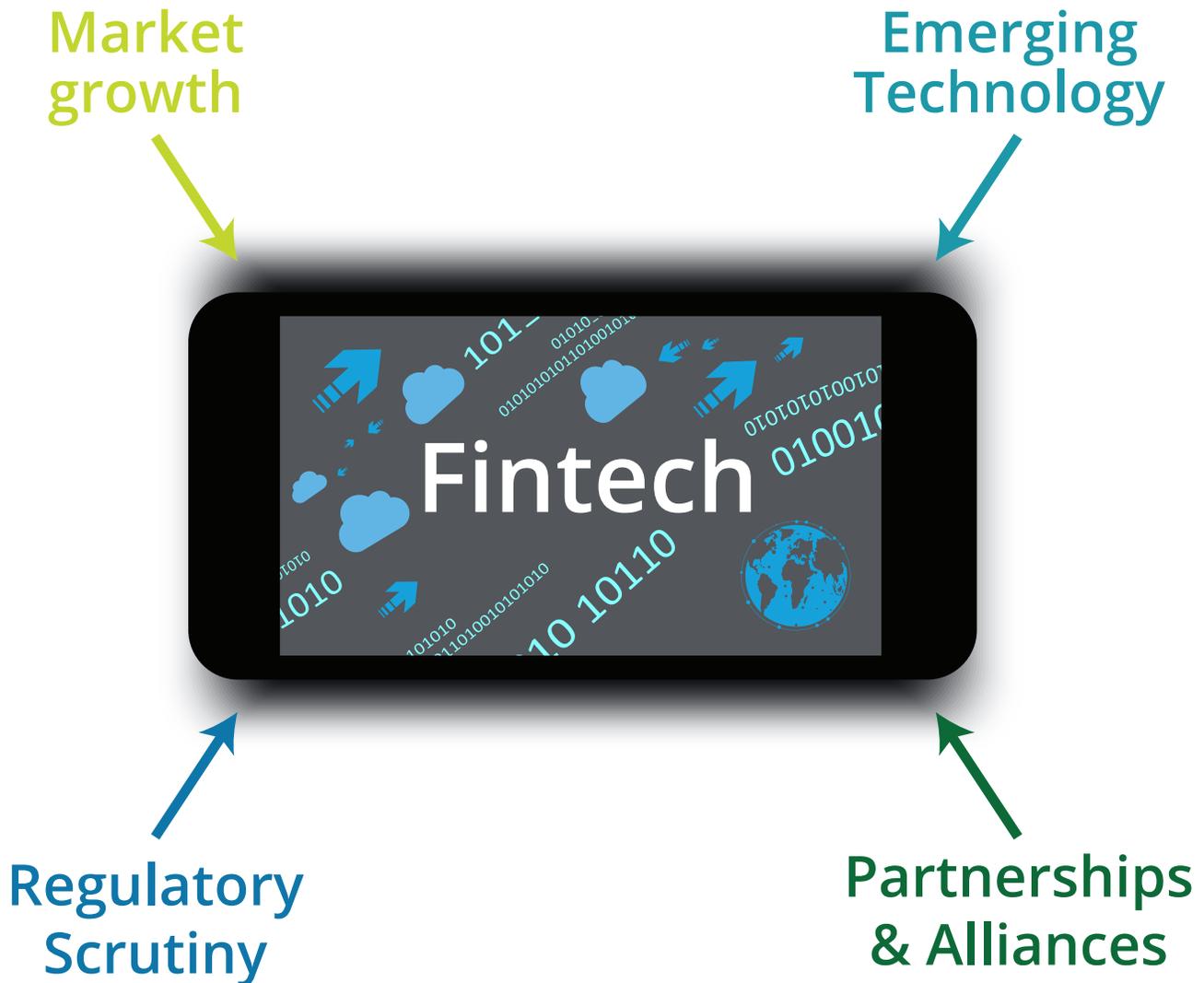
Growing exposure to the regulatory environment is creating, and will likely continue to create, potential risk management requirements for fintechs in many of the same areas as other financial services companies, including consumer protection, Bank Secrecy Act (BSA)/anti-money laundering (AML), privacy, and cybersecurity, among others. The ability of fintechs to proactively identify and address these risks through effective risk management programs may significantly impact their success and competitive edge going forward.

This second in a series of three POVs offers a high-level look at some common risks for fintechs in this changing regulatory environment, how risk management is both a growing imperative and an opportunity, and which principles promote effective risk management. The final POV in the series will describe a framework and associated elements of a fintech regulatory risk and compliance model. ▶



Some common risks for fintechs?

As the fintech sector has coalesced and expanded, several internal and external forces have contributed to making it both an exciting and challenging business environment



Market growth. Economic, social, demographic, and technological changes of the past decade provided fertile ground for fintechs. In particular, customers empowered by broadband and smartphones began demanding faster, easier, and more direct access to financial products and services. Fintechs responded with a combination of vibrant entrepreneurialism and technological and product innovation—fueled by abundant investment capital—that enabled them to scale and gain access to markets around the world.

Emerging technology. The aforementioned technological innovation, including the growing use of mobile, robotic process automation, cognitive technologies, and blockchain, has led to new business models, new product and service delivery channels, and creative approaches to attracting, interacting with, and gaining the loyalty of customers.

Partnerships and alliances. Initially engaged in competition among each other and with traditional financial institutions, fintechs have more recently begun collaborating with other financial

institutions through joint ventures, alliances, or acquisitions. Such arrangements are providing additional growth opportunities for fintechs while enabling more mature institutions to expand their traditional operations.

Regulatory scrutiny. Early on, fintechs were relatively unhindered by regulatory requirements that bound banks and other financial institutions. But as the sector matured and fintechs and traditional financial institutions began sharing each other's space, regulators have started articulating their expectations of fintechs.

Combined, these forces are creating an array of potential risk management requirements for fintechs, which can have impacts in four broad areas:



Operational

Incomplete, broken, or suboptimal processes can lead to customer service disruption and discontent, while processes ceded to a third party, whose services aren't transparent, can create undue risk.



Financial

Impeded processes can lead to costly remediation in the forms of regulatory sanctions making the consumer whole, legal fees, and potential loss of business and opportunity.



Regulatory

Non-compliance with regulatory requirements can lead to fines, sanctions, and increased oversight from regulators.



Reputational

Regulatory, operational, and financial risks can lead to the damage of a fintech's reputation, resulting in the loss of customers, diminished brand equity, and unwanted media reputation.

As these risks become more apparent and increase with the growth of a fintech company, existing risk management programs inclusive of compliance—if they exist—will likely need to be revisited or expanded. Notwithstanding that risk management is costly and often not measured in terms of return on investment (ROI), without it a fintech's ability to continue on its trajectory to generate revenues may become inhibited. Effective risk management can be a revenue enabler. The success of those programs in rapidly changing regulatory and business environments will likely become increasingly important, as they are already for traditional

financial services companies.

Principles of effective risk management

In light of the changing regulatory environment and risks associated with it, the importance of effective risk management is clear. Yet it also begs the question of where to begin if a company does not have some form of risk management program in place or if an existing program is rudimentary in scope and design.

As mentioned previously, the final POV in this series will describe a more detailed framework for risk management and its associated elements. But first, fintech executives and other stakeholders, such as private equity investors and outside counsel, may benefit from an understanding of the following basic principles of effective risk management:

Tone at the top. Effective risk management starts and ends with tone at the top. It is imperative for a company's board of directors and executive management to understand the organization's critical processes, internal controls, and mitigation plans and to spearhead the creation of an organizational structure and culture in which "risk appetite" is both understood and adhered to.

Vital to this effort is the creation of a board-directed risk committee, potentially led by a C-level executive with responsibility for

CRO should provide regular, formal reports to the board and senior management of the company, such as the CFO and internal audit leader. This reporting should summarize key indicators of risk such as performance metrics and risk trends.

Effective cascading of the tone from the top down through the operational levels of the organization, along with the risk management framework, requires attention to the following:

- Shifting the cultural mindset around risk
- Clearly defining governance structure roles and responsibilities
- Monitoring for performance requirements and adjusting compensation accordingly
- Establishing systems and processes for testing, tracking, and assessing progress

The CRO and others in the C-suite should assist them with understanding and executing their role in setting an effective and consistent tone at the top.

An end-to-end perspective with strong focus on "risk-based" actions.

With tone at the top established and a risk management organization in place, it is important to define and document a risk framework that aligns with the regulatory and operational risks identified through a formal enterprise risk assessment. Once

Effective risk management can be a revenue enabler.

enterprise-wide risk management activities. Some companies create a chief risk officer (CRO) role. Whatever the choice, it is important that this type of executive be independent of business responsibilities – that is, the executive must not report to or manage revenue-producing areas. The CRO should also have authority to act independently and have unmitigated board access.

It is then the board's responsibility to confirm that the CRO's duties are performed consistently and effectively. Moreover, the

framework is established and regulatory risk processes and programs are in place (e.g., Know Your Customer (KYC), AML/BSA), periodic testing should be performed for risk identification and control mitigation.

Effective incentives. With clear risk tolerances established and communicated throughout the organization by the board, management, and risk committee, employees at all levels should be empowered to step forward if they have risk-related concerns. These employees should



be appropriately recognized and rewarded to reinforce the tone at the top and encourage compliant behavior, including willingness of others to come forward if warranted.

Risk management baked into new products. As new products and services are developed across the organization, and as new relationships with outside parties are formed, all the dimensions of risk should be considered and incorporated. This embedding of risk management principles and mechanisms should extend to new product development approval and oversight processes, as well as the review and monitoring of customer-facing activities. The firm-wide risk strategy, along with critical processes and controls, should become integral to the day-to-day planning and operations of business units, all the way down to the individual decision-making level.

Accountability: Stakeholders across the organization, inclusive of revenue producing and non-revenue producing support staff, should be responsible for adhering to established risk tolerances. Systems and

controls can't be accountable. Instead, accountability should be shared among stakeholders for managing a broad view of risks that can impact the reputation of the company, beyond products or services.

A review process should be in place to assess the effectiveness of risk identification processes and promote accountability. Reviews should be conducted by the CRO or designated risk committee member, and they should include the new product committee or review board. Emphasis should be placed on the importance of assigning and monitoring accountability across the organization.

Enterprise-wide monitoring and testing of the business units should be reported at various levels within the organization through established management and board-level committees.

It's time for a closer look

Although fintechs aren't considered banks, their bank-like products continue to encroach on and disrupt the financial

services industry, whether in trading, lending, deposit taking, or other areas. These outcomes are likely to attract a growing level of scrutiny from regulators that are focused on repeatable, sustainable, and compliant operational performance for the financial services industry. The knock-on effect is that many fintech companies will likely need to focus on their own risk management capabilities to keep pace.

This is an important opportunity for fintechs, especially as they begin to confront a variety of challenges similar to those that traditional financial institutions have long faced. Beyond regulatory compliance and the protection of a fintech's operational, financial, and reputational integrity, an effective approach to risk management can help promote continuous operational improvement across the enterprise. Effectively instilled risk management principles—starting with tone at the top and driving down through the very core of the business—can help ease the disruption that fintechs themselves are likely to experience from increasing regulatory oversight.

Contact us

Peter Reynolds

Managing Director
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP

Tel: +1 212 313 1660

Email: pereynolds@deloitte.com

Gina Primeaux

Principal
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP

Tel: +1 714 436 7341

Email: gprimeaux@deloitte.com

Christopher Spoth

Executive Director, Center for Regulatory Strategy
Managing Director, Deloitte Risk and Financial Advisory
Deloitte & Touche LLP

Tel: + 1 571 243 7478

Email: cspoth@deloitte.com

Harish Dakshina

Senior Manager
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP

Tel: +1 404 388 2898

Email: hdakshina@deloitte.com

Amanda Williamson

Senior Manager
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP

Tel: +1 704 887 2069

Email: amawilliamson@deloitte.com

James D Simpson

Senior Manager
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP

Tel: +1 816 881 5197

Email: jsimpson@deloitte.com

Tara Wensel

Manager
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP

Tel: +1 347 224 4056

Email: tawensel@deloitte.com

Endnotes

1. "Fintechs and regulatory compliance: Understanding risks and rewards," October 2017, <https://www2.deloitte.com/us/en/pages/regulatory/articles/future-of-fintechs-risk-and-regulatory-compliance.html?nc=1>
2. "FINANCIAL TECHNOLOGY: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight, published March 22, 2018, <https://www.gao.gov/products/GAO-18-254>.



About Deloitte

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2018 Deloitte Development LLC. All rights reserved.