International Journal of Legal Expatiate Vol 1 (2021), Pg. 37-49 ISSN: 2583-7885(Online)
Published by Author Lens

NAVIGATING THE CHALLENGES OF FINTECH: BALANCING INNOVATION AND REGULATION FOR FINANCIAL INCLUSION AND DATA PRIVACY

- Roopali Shekhawat[1]

ABSTRACT:

Non-bank institutions' use of finance and technology to deliver monetary services, colloquially known as "fintech," has developed a stranglehold on the financial landscape. This article examines the intricacies of influence and repercussions for new products, processes, and services, as well as financial inclusion, in light of this evolution. The combination of Jan Dhan-Aadhaar-mobile phones creates an excellent setting for fintech to reach the "last mile." Despite its numerous advantages, there is a need for caution in areas such as privacy and data ownership. The primary goal of this research is to provide a legislative framework to protect the privacy and security of subscriber data in financial technology, because Fin-Tech apps and services contain sensitive information about their customers. This regulatory framework has a comprehensive set of criteria for securing FinTech services. In a fast-paced world of rapidly developing technology and related financial services, regulators must be vigilant to avoid impeding the success of this emerging sector.

Keywords: *Fintech, Data privacy, Banking regulation, electronic banking, cyber security.*

I. INTRODUCTION

"Technologically empowered Financial innovation that might give rise to new business models, apps or products with a related material effect on capital markets and the banking services" is "fintech," as defined by the Financial Stability Board."

Between 2015 and 2020, India had a tremendous increase in new fintech start-ups, particularly in the areas of digital payments, lending, and wealth management. India had the second-highest number of new fintech start-ups in the last three years after the United States, according to the MEDICI India FinTech Report 2020[2]. India currently has around 2,000 fintech firms. According to a recent report by the Boston Consulting Group, India's fintech business will be valued at $150-160 billion by 2025, with a $100 billion opportunity for value creation. The

[1] Assistant Professor, (CA); B.A.LL. B; LLM, Galgotias University.
[2] INDIA FINTECH REPORT 2020, MEDICI Available at: https://gomedici.com/research-categories/india-fintech-report-2020 Visited on 01.03.2022.

major enablers and role of government in the emergence and expansion of fintech start-ups, as well as significant fintech categories and a strategy for increasing fintech start-ups, are highlighted in this article. Various factors act as key enablers resulting in the success of fintech start-ups in India, including:

1. Capital availability and a thriving investment ecosystem;
2. India has a favourable demographic (more than 65 percent below the age of 35 years)
3. having a desire for cutting-edge technologies;
4. For the majority of the population (unbanked, rural areas, as well as small and mediu m-sized businesses), financial services penetration is low (SMEs)
5. Fintech efforts and regulatory forbearance by the government;
6. Access to the internet and mobile devices has increased.
7. Through the use of cloud-based services and India Stack, infrastructure and method to estimate have been reduced; and
8. Technological advancements

II. POLICY AND REGULATORY INITIATIVES FOR THE FINTECH INDUSTRY IN INDIA

Given the competitive nature of the fintech sector and its interaction with other industries, effective policy and regulation are important for the sector's growth and stability. With the implementation of demonetization, India saw a massive increase in cashless transactions. Unified Payments Interface (UPI), Jan Dhan Yojna, Startup India, Digital India Programme, Recognition of P2P lenders such as non-banking financial companies (NBCs), and National Common Mobility Card are some of the recent Indian government programmes aimed at fostering a favourable business climate for fintech companies (NCMC). The RBI announced its detailed framework for a Regulatory Sandbox (RS) for fintech products on R5 in 2019, including provisions for startup entry and exit, duration, and an indicative list of innovative products, additional services available, and technology that may be considered for testing under the RS.

"In 2019, the insurance regulator (IRDA) launched the IRDA1 Regulatory Sandbox to achieve a balance between the insurance sector's orderly growth and the protection of policyholder interests, while also supporting insurtech innovation. Similarly, SEBI, India's securities regulator, published a framework for RS in 2020, allowing firms registered with it to

experiment with fintech solutions. By and large, Indian regulatory agencies (including the RBI, SEBI, and IRDA) have taken a collaborative approach to the fintech sector, providing a larger framework and sandbox environment to foster responsible innovation. Additionally, fintech start-ups have benefited from the government's pro-startup policies and flexible regulatory environment.

III. FINTECH-SPECIFIC LEGISLATION AND REGULATORS ARE LACKING:

The Reserve Bank of India and the Securities and Exchange Board of India have yet to issue extensive and independent regulations for the fintech industry, which is still controlled by banking and securities legislation. Increased regulation might stifle fintech's key characteristic of innovation, as well as push up operational expenses. Regulatory coherence, on the other hand, will help the fintech sector thrive in the long run by increasing customer trust, which is a vital component in generating more financing. As with any other industry, as the fintech sector evolves and start-ups scale up, regulators will be more likely to scrutinize them.[3]

The regulator's main task is to create an environment that fosters innovation while balancing issues such as customer protection, data security, and privacy. Because of the rapid pace of innovation in the fintech sector, regulators have had to play catch-up and have knee-jerk reactions to some market activity, for example. The regulator's main task is to create an environment that fosters innovation while balancing issues such as customer protection, data security, and privacy. Because of the rapid pace of innovation in the fintech sector, regulation 10 has had to play catch-up and respond in a knee-jerk manner to some market activities, such as its stance on bitcoin, payment laws, and market share restriction by the NPCT.

Fintech firms enjoy a lot of power, despite legal restrictions being imposed on these institutions in India. Consequently, there are many concerns surrounding the continued dominance of these entities in the Indian market. Specifically, such concerns include the need to regulate them, their potential impact on innovation, competition, investor sentiments, and transparency.[4] Given that regulations may pose threats to some companies, it will be prudent to explore ways through the establishment of fintech specific laws. Many companies have already started

[3] Gai, K., Qiu, M., Sun, X., Zhao, H. (2017). Security and Privacy Issues: A Survey on FinTech. In: Qiu, M. (eds) Smart Computing and Communication. SmartCom 2016. Lecture Notes in Computer Science, vol 10135. Springer, Cham. https://doi.org/10.1007/978-3-319-52015-5_24

[4] Kang, J. Mobile payment in Fintech environment: trends, security challenges, and services. *Hum. Cent. Comput. Inf. Sci.* **8,** 32 (2018). https://doi.org/10.1186/s13673-018-0155-4

working with regulators like SEBI. However, regulating only all fintech entities would limit our ability to benefit from innovations in other sectors that do not fall within the domain of regulated industries.

IV. RELEVANCE OF AN INDEPENDENT REGULATORY FRAMEWORK FOR A NEW CATEGORY OF COMPANIES

The current Indian financial regulatory framework lacks a clear definition of what constitutes an "organization" and a "person" as prescribed in the Banking Regulation Act, 1949. Both terms are often used interchangeably and loosely, creating confusion for the public and limiting the ability of organizations to attract funds. As per economists, this is especially important when assessing risk exposure, particularly among investors. Despite the fact that banks and other regulated segments of the economy are exempted from taxation, they still play a key role in ensuring economic stability in countries worldwide. In addition, several global studies have established that there is very limited data available about how much bank and credit card debt actually flows between private credit instruments and consumers due to limitations of both quantitative and qualitative information access.[5] Furthermore, researchers indicate that most consumer financing activities happen behind closed doors. This means that the sources of capital flow out of organized finance by conventional channels but into the secondary market where they are traded or exchanged for cash. Thus, it is crucial to establish new categories of companies to align them with regulations that define who should have what types of ownership. By doing so, it will become easier to determine whether the government has enough resources to achieve its objectives, reduce the cost of funding, enhance efficiency, promote growth, and improve competitiveness. It is crucial to understand that the process of building and growing innovative organizations must start by considering how various regulations apply to them. The objective is to move away from the existing system that does not adequately reflect the capabilities and needs of those seeking opportunities in fintech.[6]

V. REGULATION AND COMPETITION

Regulation is one of the common ways through which competition in business can be improved. According to scholars, regulation provides the necessary platform through which

[5] Security challenges in the evolving fintech landscape: PWC https://www.pwc.in/assets/pdfs/consulting/cyber-security/banking/security-challenges-in-the-evolving-fintech-landscape.pdf
[6] Anand Kumar, Fintech regulations, financial stability, and data privacy: So, what is the path to go forward, The Economic Times, January 27, 2021.

competitors can learn more about each other and gain better understanding of their respective markets. Most of these competitors already know their respective industries well and can compete effectively thanks to regulation that brings clarity and certainty. Although regulatory systems are complex, they can allow people who want to succeed to prosper.[7] There arises a strong synergy between competition and regulation. In a world where technology remains at the core of business growth, competition is the best way to ensure that customers get value for money or are able to make informed decisions for themselves. In order to foster success, it is essential to address issues relating to regulation and competition.

VI. REGULATORY ISSUES WITH REGARD TO FINTECH: WHAT CAN BE CONSIDERED NORMAL?

As mentioned earlier, regulation is a fundamental tool for improving competition in business. Additionally, research indicates that it also helps to maintain trust and professionalism while protecting stakeholders from abuse and misconduct. While regulations that govern commercial businesses are meant to prevent unnecessary harm to clients and employees, they are equally applicable to financial services business. Unlike conventional corporations, financial service institutions cannot afford any disruption to the services provided. Hence, ensuring that they are safe and secure is critical. Financial professionals must carefully analyze regulations for the sake of promoting high standards in these fields. Therefore, many regulations could be considered normal given the nature of these two sectors. Nonetheless, there are no rules set in place that dictate how companies can operate – only things can change. Similarly, regulation does not stop anyone from making financial mistakes. Fintech firms must strive to avoid risks associated with the regulation of their products that might affect their reputation and lead to increased investments. Such risks are unavoidable because regulations are usually slow to develop, evolve, and be transparent. Consequently, regulating financial institutions must strive to innovate or else they will crumble under pressure.

VII. REGULATION TO AID INNOVATION

In an open innovation process, every aspect of the production chain is scrutinized to minimize risks. If a firm learns of risky practices, it must seek alternatives and conduct research.

[7] Gregor Dorfleitner, Lars Hornuf, Julia Kreppmeier, Promise Not Fulfilled: FinTech, Data Privacy, and the GDPR, University of oxford blog post. https://www.law.ox.ac.uk/business-law-blog/blog/2021/11/promise-not-fulfilled-fintech-data-privacy-and-gdpr

Nevertheless, it is difficult to create an environment that encourages an open innovation process. Since there is little data on how such processes take place, companies will tend to adopt outdated practices in the hope of meeting the regulatory requirements. Fintech firms, therefore, need to identify potential areas for improvement before implementing any changes.[8] They need to use real cases to guide decision-making. Regulators must ensure that they offer adequate support as they work towards developing solutions. Focusing on innovations is a vital component of boosting client satisfaction as it ensures continuous learning. The same applies to policy reforms. Regulators must encourage innovators to propose ideas while keeping others on hold, as opposed to focusing on problems, instead. These policies ought to focus on the overall goal of ensuring corporate sustainability rather than merely focusing on rules in regulations. On the basis of this, it is important to recognize that innovation, even though costly and challenging to accomplish, is vital to long-term economic growth.

VIII. THE RELATIONSHIP BETWEEN INVESTMENT AND CORPORATE GOVERNANCE

Corporate governance refers to the relationship between shareholders and management. Research demonstrates that most shareholder proposals tend to fail. Most companies believe that shareholder proposals represent an obstacle to the continued realization of dividends. At the same time, shareholders think that the proposal is designed to control their interests. Instead, they tend to favor an alternative course in order to receive a higher return on their investment. Some companies go ahead and offer dividends that are highly diluted. Others offer dividend payouts of zero or negative amounts. While this might seem appealing, it compromises the entire company's interest. Corporations must adopt measures that ensure that they adhere to the principles outlined by shareholders. Adequate management should help shareholders evaluate the appropriate dividend policies that could help boost their confidence. One way to protect shareholders is through auditing, which focuses on identifying areas of concern and identifying solutions to avoid those situations in future. Auditing is fundamental and requires more scrutiny when dealing with financial statements than other types of audits. As such, the audit department must assess the degree at which these statements meet certain quality requirements. It is also recommended that auditors review the internal controls used by a company. The organization must then provide feedback to shareholders on their performance.

[8] Barclay-Simpson, FinTech: Growth Versus Governance, https://www.bankingtech.com/files/2018/11/Barclay-Simpson-growth-versus-governance.pdf

Investors have the right to ask questions that will enable auditors to identify weaknesses in the corporation's internal controls and also point out mistakes in the statements.[9] Therefore, auditors must examine the management policies, control procedures, and the results of the auditor's audit. When auditors notice areas of concern, they must inform shareholders of the matters identified and suggest steps that they could take to rectify the situation. Investors must be encouraged to question management whenever possible, which will act as a corrective action in case of issues like noncompliance with the terms of engagement. Once a problem is found, the board must initiate an investigation into the matter and recommend remedial actions to senior executives. Finally, auditors are required to submit reports to shareholders containing recommendations that could eliminate deficiencies to the statements.

IX. RISK TO DATA SECURITY AND PRIVACY:

The unrestrained data flow has helped the fintech sector the most. Data breaches, third-party security threats, ransomware, application security threats, cloud-based security threats, and digital identity risks are the top issues facing the financial industry.[10]

The increasing demand for information by customers has led to an unregulated business world characterized by frequent theft of customer data and exposure in privacy threats, which affects businesses' growth and profitability. Many firms have invested heavily in technologies aimed at protecting their clients' data against cybercrime and other potential threats. Unfortunately, some of these efforts have not been effective enough and most firms still cannot guarantee security and privacy. It is apparent that this situation requires new approaches to safeguard against such threats while retaining a focus on operational efficiency.[11] It should be noted that increased digitalization has enabled many people and organizations to access different forms of electronic information. This has provided them with numerous opportunities for conducting business. However, it is important for companies to consider how they can protect their clientele's most sensitive information and ensure its safety and privacy. Therefore, it becomes pertinent to discuss several aspects of risk management in the context of digital environment.

[9] Luis Emilio Alvarez-Dionisi, Fintech Governance Challenges, Levels and Theories, ISACA Journal, Issue 2020, Vol 6.

[10] IDX, Data Privacy Concerns in Booming Fintech Industry, https://www.idx.us/knowledge-center/data-privacy-concerns-in-booming-fintech-industry

[11] Reserve Bank of India, Guidelines on Information security, Electronic Banking, Technology risk management, and cyber frauds, https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf

X. RISK MANAGEMENT APPROACH

In the wake of recent trends in digital environments, a variety of approaches to addressing the risks associated with digital information have emerged as viable solutions. For instance, one school of thought argues that the best way to address cyber threats is through proactive risk mitigation. The approach asserts that digital information is a major threat to all businesses because it presents challenges to decision-making processes and the ability to make informed decisions. Additionally, an array of technological advancements has allowed firms to adopt more advanced strategies for managing digital risks and protecting their clients' confidential information.[12]

One of the key advantages of leveraging predictive measures that are currently available in the technology field is to help reduce risk exposure to clients. According to studies carried out by, using machine learning to analyze historical data for a given domain enables firms to determine specific risks when making decisions related to such domains. Such approaches enable managers to identify factors that affect an organization's overall risk exposure and allow managers to mitigate those. A second advantage of implementing such innovative approaches is the possibility of determining the likelihood of certain activities being triggered when resources for handling the activity are limited. As such, it becomes possible to prevent unplanned costs from taking effect when resources like human capital or physical resources are unavailable. Furthermore, using such methods helps firms avoid losses by avoiding resource shortages. On the opposite side of the scale, a disadvantage of these risk-mitigation measures is the reliance on existing IT infrastructure, as well as the need for additional training and support to handle critical areas like regulatory compliance and maintenance. These two disadvantages are important in identifying new ways of tackling digital privacy threats.[13]

Another approach to mitigating digital risks involves focusing on control measures. Research conducted reveals a common trend among governments in securing cyberspace: empowering individuals with skills to deal with digital risk.[14] Governments recognize that people who want to safeguard digital assets from attacks have insufficient skills. One of them is law enforcement

[12] By Mr. Ashraf Khan, Majid Malaika, Central Bank Risk Management, Fintech and cyber Security, IMF Working Paper.
[13] Paolo Giudici, 'Fintech Risk Management: A Research Challenge for Artificial Intelligence in Finance' Front. Artif. Intell., 27 November 2018, https://doi.org/10.3389/frai.2018.00001
[14] Nicoletti, B. (2017), The Future of FinTech, Springer International Publishing.

agencies. However, there is no clear way forward because these entities do not have adequate manpower in these fields. Other countries like Japan and Germany develop private security firms that provide expert services to enterprises interested in safeguarding their digital secrets. Thus, by employing private security firms to offer protection in digital environments, governments can mitigate risks to their citizen privacy and reduce economic losses from the same. By doing so, governments establish policies and measures that assist firms comply with international rules and regulations, thereby ensuring their compliance with market standards.

The development of legal mechanisms to enforce adherence to laws on digital rights and protections, coupled with the proliferation of online platforms that are accessible to customers can also lead to enhanced digital safety for consumers, thereby improving the effectiveness of such programs. Organizations involved in e-commerce and social media marketing can benefit greatly from adopting a legal framework that encourages e-commerce and social media security initiatives for clients. At the same time, government systems can continue to enhance national privacy measures for citizens to safeguard themselves against risks that arise during these services.[15]

The above three approaches have demonstrated their value over the years. In addition, considering that many digital service providers have made huge contributions to the advancement of these practices, the latter are likely to remain relevant as the industry continues to grow and expand into new markets. Moreover, these emerging approaches have reduced the cost of compliance, especially where the majority of employees work from home. All these developments show why utilizing both private and public techniques is a good strategy to leverage to better serve your customers.[16]

XI. RISKS RELATED TO DIGITAL INFORMATION PROTECTION AND SAFETY

Recent reports[17] indicate that cybercrime cases increased to 17 million in the year 2020. They were 7% higher than those reported in 2019. The increase stems from numerous digital sources

[15] Artie W. Ng, Benny K.B. Kwok, Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator, Journal of Financial Regulation and Compliance ISSN: 1358-1988,13 November 2017
[16] Ng, A.W. and Tang, W. (2016), "Regulatory Risks and Strategic Controls in the Global Financial Centre of China", in Choi, J.J., Powers, M. and Zhang, X.T. (Eds), International Finance Review – The Political Economy of Chinese Finance, Emerald Publishing, Vol. 17, pp. 243-270.
[17] Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document, OECD, 2015, https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf

of insecurity including phishing networks, stealing passwords from online logins, malicious content and malware, as well as other incidents like hacking in 2014. Consequently, much effort needs to be put into strengthening existing cybersecurity frameworks, creating laws to protect computer-related crimes, providing education on cybercrime, building proper defenses for businesses, and enhancing awareness of appropriate and safe practices such as following all the steps indicated in the case. The US Department of Justice estimates that about 90% of Americans possess a smartphone. Thus, criminals have the opportunity to target innocent victims through devices that have similar features as smartphones, which have recently become popular targets.[18]

A lot of attention is now focused on reducing the risks faced by online businesses and digital services providers. However, many stakeholders still argue that internet security is too complex with far too many loopholes to manage. Therefore, it is imperative to address several concerns, such as data leakage, fraud, and cyber-terrorism, in order to ensure improved cybersecurity performance. Since hackers are always attempting to steal personal information from businesses through fake news programs, it cannot just be about restricting online sales for criminals but rather protecting consumers from harm caused by misinformation. Consequently, cybercrime statistics show that every dollar lost to cybercriminals goes to the federal government, which is responsible for compensation and restitution. Federal leaders estimate that about $60 billion in damages was incurred by cybercriminals due to their actions. Some of these losses come from reputational harm, although others stem from corporate losses, which include intellectual property infringement that leads to lawsuits and litigation charges. Another concern is the fact that many states have failed to prosecute offenders for crime committed in New York City after some of the biggest hacks occurred there. Several lawsuits have already been filed in 2017 in New York related to various incidents including the ones described above. These lawsuits claim that defendants like Amazon Prime, Google, Netflix and Facebook have contributed immensely to the rise in cybercrimes in the city. Despite the fact that these companies may have denied accusations through lawsuits, the evidence suggests otherwise. Hence, the problem remains severe to the extent that policymakers and lawyers in each state are debating whether to pursue criminal charges against these companies. Although lawsuits

[18] Artie W. Ng, Benny K.B. Kwok, Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator, Journal of Financial Regulation and Compliance, ISSN: 1358-1988

may not stop cyber-crime, they still add another layer of complexity to the issue, as they have shown how often defendants and victims fail to cooperate.[19]

In order to improve cybersecurity practices, lawmakers need to look at the root causes of insecurity and recommend practical ways to tackle them. Lawmakers should address weaknesses in the current system and propose reforms that will minimize losses. First, they need to fix gaps in funding, staffing, infrastructure and reporting. Second, lawmakers must promote data sharing and transparency with the aim of guaranteeing accountability for information disclosure. Finally, legislators could improve incentives by giving funds and improving penalties. Through the involvement of experts, politicians and stakeholders, such laws would see the light of day.

Fintech firms are increasingly playing a critical role in shaping our economy. While fintech firms face unique challenges in terms of regulation and competition, we see them evolving towards becoming vital components in the global economy. As such, it is important to assess how the tech industry can thrive in the future and what obstacles it poses to success. For instance, fintech firms are often reluctant to share their ideas, which is why regulators and lawmakers need to push the boundaries. Also, fintech is undergoing massive changes, yet the overall mission remains unchanged. Currently, large banks dominate the market, however, smaller players still have an opportunity to disrupt the status quo by offering alternative banking solutions.

Therefore, regulators and lawmakers need to change the prevailing perspective, where incumbents dictate policies and decisions that are favorable to their interests rather than serving societal needs. Instead, they should seek to understand individual aspirations and focus on providing fair opportunities that are based on fairness, truth and integrity. For example, it is important to note that fintech firms need to engage on a larger scale in order to generate competitive advantage. Given the changing nature of the tech industry, it is critical to collaborate with stakeholders to achieve success.

In the past decade, startups such as Uber, Spotify, Airbnb and Snapchat have made significant advances in the field of transportation, hospitality, retail, health care and telecommunications,

[19] Khakan Najaf, Md Imtiaz Mostafiz and Rabia Najaf, No Access Fintech firms and banks sustainability: Why cybersecurity risk matters, International Journal of Financial Engineering, Vol. 08, No. 02, 2150019 (2021) https://doi.org/10.1142/S2424786321500195

respectively. Their applications, coupled with innovation in networking technology create unparalleled opportunities for scaling businesses worldwide. Companies like Walmart and Mastercard have played crucial roles in accelerating the adoption of distributed computing systems. Nowadays, any small company or startup can tap the power of these innovations, as long as it provides an Internet connection. Nevertheless, since most of these firms require minimal initial investment, many investors are hesitant to give them direct funding.[20]

XII. CONCLUSION

In conclusion, corporate governance, in general, and corporate law, in particular, offer great opportunities for the development of innovative technologies to grow, expand, and thrive. Moreover, they are vital tools in aiding innovation and growth in the field. Indeed, they are central to promoting successful competition in modern business. Besides, the relationships between investors, management, and the board, they also facilitate greater involvement and communication in an effort to strengthen the foundations of a healthy society. Investing in a proper corporate law and management makes it possible for a corporation to function efficiently, attain greater returns, protect investors' rights, and make profits without compromising the welfare of shareholders. Although regulatory frameworks are complicated and need serious attention from experts, the importance of regulation in enhancing the performance of innovative companies cannot be overlooked.

To tackle the cyber threat and prevent hackers from gaining access to critical data, the fintech industry need a balanced approach to innovation. Unprepared governments around the world have been obliged to speed up legislative measures to protect citizens' data and rights as a result of the rapid digital revolution.

The Personal Data Protection Bill 2019 was submitted in the Lok Sabha to protect the interests of users, as recommended by the Sri-Krishna Committee, by making data localization necessary for all sensitive personal data (PDPB).

The business models of fintech start-ups rely heavily on outsourcing technical assistance and cloud services to low-cost, competitive providers. Start-ups will be unable to select the most cost-effective cloud service providers from a global supply pool due to data localisation criteria

[20] Jennifer Callen-Naviglia, Jason James, FINTECH, REGTECH AND THE IMPORTANCE OF CYBERSECURITY, Issues in Information Systems Volume 19, Issue 3, pp. 220-225, 2018, https://doi.org/10.48009/3_iis_2018_220-225

specified in the PDPB. Data localization would also necessitate product re-engineering in order to comply with complex requirements, raising both technological and operational expenses.