

# The Intersection of Fintech, Regtech, and Cybersecurity: Challenges and Opportunities

Dr. S. Rajalakshmi

Associate Professor

Head of the Department

Department of Criminal Law and Criminal Justice Administration

School of Excellence in Law,

The Tamil Nadu Dr Ambedkar Law University

**Abstract:- Financial institutions are facing increasing pressure to advance digitally due to consumer demand for more remote banking, faster response times, and the ease of online purchasing. Failure to do so could result in a loss of market dominance. To remain competitive, the banking sector has created fintech, which has led to the emergence of RegTech - products and services aimed at managing fintech. However, the potential threats of hacking, security breaches, and theft have made internet security a crucial aspect of the development and growth of fintech and RegTech. To address concerns about the impact of fintech on regulatory bodies, the ability of RegTech to keep up with fintech's growing demands, and the evolution of cybersecurity to provide adequate protection from financial threats, this research will examine how fintech, RegTech, and confidence contribute to effective cybersecurity through a review of relevant literature.**

**Keywords:-** FinTech, RegTech, Cybersecurity.

## I. PROLOGUE

Cybersecurity, FinTech, and RegTech have a close relationship in the finance sector. Through cutting-edge FinTech goods and services, technological advancements are revolutionising the US financial sector and causing a change in the governing environment. By reviewing pertinent literature, this research seeks to provide an overview of how FinTech, RegTech, and cybersecurity are related. The meaning of FinTech, its history, and an explanation of RegTech's function and advantages are just a few of the parts that make up this research paper. The research also emphasises the significance of cybersecurity and the adoption of FinTech and RegTech in India, as well as how these developments affect cybersecurity there.

## II. FINTECH: DEFINITION

The phrase "FinTech" has grown in prominence over the past few years and is now frequently used to refer to new technology in the financial sector. This covers both recently created goods or changing services, as well as internal technological developments within financial organisations. Digital currencies, online finance, and credit card services are a few examples of these ever-evolving goods and

services. To enhance their internal technological skills, financial institutions may also implement cloud-based systems or upgrade their outdated systems. Customers, investors, and businesses can now stay current with market trends, grow their market share, and provide services at cheap or no cost thanks to fintech. Future changes to the financial sector due to FinTech growth are anticipated.

According to Forbes (2018), the year 2018 was expected to bring several highly anticipated FinTech advancements. Major banks buying FinTech startups was one of the developments mentioned, along with the automation of financial decisions and actions through financial apps and autopay, the modernization of identification verification procedures in the financial sector, the automation of fraud and risk management procedures, the expansion of FinTech in B2B lending, and the enhancement of KYC (know your customer) products. The banking sector was anticipated to gain a lot from these developments, including better security, efficiency, and client experiences. In the years to come, it's likely that we will witness more developments in these fields as the Fintech sector continues to expand and change.

## III. FINTECH'S : EVOLUTION

The relationship between technology and finance has existed within the US monetary system for a very long time, despite the fact that the word FinTech has become more common in recent years. The financial sector has undergone major technical developments over the last century. For instance, the Fedwire Funds Service, which allowed for computerised money transactions between organizations, was introduced by the US Federal Reserve Banks in 1918. By creating the first credit card, the Diner's Club card revolutionised how people made transactions in 1949–1950. In 1969, Chemical Bank in Rockville Centre, New York, put the first automated teller machine (ATM), greatly simplifying the banking experience for customers. In 1971, the NASDAQ started to provide computerised trading and initial public offerings (IPOs). In 1995, Wells Fargo became the first bank to provide internet accounts, fundamentally altering how people handled their finances. The first mobile payment was made in 1997, and PayPal, which subsequently became a well-known digital payment network, was founded in 1998. In 2005, "banks without branches," also referred to

as "virtual banks," were launched, giving customers the option to conduct their banking online. An option to conventional money was made available in 2009 with the rise of the altcoin Bitcoin. The introduction of Apple Pay in 2014 sealed the deal by increasing the simplicity and ease of smartphone transactions. The financial sector has undergone a revolution thanks to these technical developments, which have increased the effectiveness, security, and accessibility of banking and payment systems for people all over the globe.

Since the global financial crisis of 2008, which had far-reaching effects across markets in Europe and Asia as well as the United States, there has been a rapid increase in investment in FinTech (Skan, Dickerson, and Masood, 2015; Ng and Kwok, 2017; Arner et al., 2017). Financial institutions have been compelled to reinvent or create new products and services to remain competitive and meet customer demands (Ng & Kwok, 2017). The development of technology within the US financial industry has led to a need to innovate within the regulatory and compliance frameworks (Arner, et al., 2017). The emergence of fintech has introduced technological advancements to an industry that was previously dominated by compliance and governmental oversight. However, the rise in popularity of digital currencies has raised concerns about current regulatory standards, and the efficacy of existing laws in controlling virtual currencies (Kirby, 2014). To address this, the State of New York introduced a revolutionary regulatory law called BitLicense in 2015, which could influence future efforts to regulate FinTech products and services (Callen-Naviglia, 2017; Hughes, 2014).

The financial sector's risk profile and susceptibility to cyber-attacks by malicious actors have grown with the adoption of technology and the increasing reliance on digital financial products and services. Pascu (2017) reported that data breaches increased from 19% to 24% between 2016 and 2017. As a result, research shows that "78% of financial institutions have increased their IT security budgets, up from 58% in 2016" (paragraph 4). With the rise of FinTech, security is becoming increasingly critical.

Will the development of FinTech make it more difficult for officials to perform their jobs? According to Kidd (2018), as innovation accelerates, advancements in FinTech could overwhelm regulators' ability to regulate the financial sector effectively. This could result in increased workloads that require regulators to work more quickly without sacrificing accuracy or effectiveness. FinTech experts believe that technological innovation is likely to outstrip regulatory capacity, according to Kidd. As a result, heavily regulated industries like finance may begin using regulation to stifle competition and protect profits and market share. RegTech is a response to this inadequate government oversight of FinTech development. The current questions are, what is RegTech, and what role will it play in the regulatory landscape? This shift in financial regulation raises concerns about regulators' ability to maintain accuracy, consistency, and effectiveness.

#### ➤ *RegTech: Meaning*

Magnuson (2018) argues that regulators are not keeping up with financial technology advancements, which requires a significant reconsideration of financial regulation in the age of technology-enabled finance. To regulate the fast-changing financial technology sector, RegTech needs to be utilized and put into practice, according to Arner et al. (2017). RegTech refers to the use of technology, particularly information technology, in regulatory monitoring, reporting, and compliance, as explained by Arner, Barberis, and Buckley (2017) on page 371. As FinTech continues to evolve and more complex regulatory compliance requirements are introduced, the evolution of RegTech also changes to keep up.

#### ➤ *RegTech's : function*

According to Arner et al. (2017) and Ng and Kwok (2017), regulatory requirements and expenses have increased since the 2008 financial crisis. Deloitte's 2018 financial regulatory outlook indicates that there will not be a complete rollback of the post-crisis regulatory framework. This presents a challenge for the expanding FinTech industry in terms of preserving risk management. As financial institutions continue to rely on outdated systems that cannot keep up with the increasing digital financial requirements, they are turning to RegTech solutions. The rise in compliance costs is driving financial institutions to adopt RegTech solutions to fulfill their regulatory obligations and meet customer demands. RegTech offers both immediate and long-term benefits.

#### ➤ *Benefits of Reg Tech*

Reg Tech, also known as regulatory technology, is a young discipline that uses technology to handle compliance issues that the finance sector faces. Reg Tech is becoming more popular in the business because of a number of advantages. Reg Tech options can greatly lower the cost of compliance in the near future. Reg Tech solutions automate many compliance duties, lowering the need for manual intervention. The conventional strategy to compliance entails employing sizable teams of compliance officers. Reg Tech solutions also provide scalable, lasting solutions that can change with the legal environment. Reg Tech solutions' sophisticated data gathering and analysis skills also give businesses insights into their operations and assist in identifying and managing risks. Another advantage of Reg Tech is the merging of risk and control, which enables businesses to rapidly identify and address possible hazards. Overall, Reg Tech solutions are assisting financial institutions in maintaining regulation compliance standards while concentrating on their primary company goals.

Reg Tech solutions offer a number of long-term advantages in addition to the short-term ones, which can have a major effect on the financial sector. The favourable client experience that Reg Tech products can provide is one such advantage. Reg Tech solutions can offer clients a faster and more effective service, enhancing their overall experience, by streamlining compliance processes and lowering the need for human involvement. Customers may

become more devoted and believe financial organisations more as a result of this. Increased market security can also be achieved with the help of Reg Tech products. Reg Tech solutions can aid in preventing financial offences like money laundering, which can shake up the financial system, by assuring compliance with regulations. Additionally, by promoting accountability and clarity in decision-making processes, Reg Tech solutions can enhance administration. By streamlining data gathering and analysis, Reg Tech solutions can also improve regulatory filing, assuring correct and prompt reporting. By doing this, financial institutions can better their partnerships with regulating agencies and prevent fines and penalties. Overall, Reg Tech solutions have long-term advantages that can benefit financial institutions by enhancing their operations, enhancing their connections to clients and authorities, and promoting a more secure financial system.

The shift in financial regulations towards technology-enabled finance raises concerns about the security of the financial sector and FinTech goods and services. The significance of cybersecurity and its role in the US economy are also growing. The importance and challenges of cybersecurity in the American market are discussed in the section on the importance of cybersecurity.

#### ➤ *Cybersecurity's importance*

According to Spidaleri and Kern (2014), the emergence of the Internet and information technology has brought about new possibilities for the global economy and humanity. However, this dependence on technology has also led to new vulnerabilities and increased cyberattacks from various groups such as hackers, criminals, terrorists, state players, and non-state actors. These cyberattacks have affected both governmental organizations and public/private businesses. Critical infrastructure in the United States, including the electric grid, telecommunications networks, and financial systems, are also susceptible to cyber threats. The motivations of cyber attackers are expected to increase as the world's dependence on information technology continues to grow rapidly.

The events of 9/11 and the Enron and WorldCom scandals resulted in the passing of the Sarbanes-Oxley Act, which led to increased federal and state regulations regarding information privacy and security. Additionally, computer networks now face unprecedented risks, making cybersecurity more crucial than ever before in 2017 and beyond. With the rapid growth of data networks, digital applications, and mobile devices, as well as the rise in cyberattacks, companies must maintain constant vigilance in securing sensitive data. (The University of Phoenix and the ISC2 Foundation, 2014).

In today's world, cybersecurity professionals' expertise and knowledge are essential to protect individuals' and businesses' online transactions. As companies and government agencies increasingly rely on information technology and information systems for data processing, storage, and transmission, adequate security measures are crucial to prevent data breaches. Business executives are now recognizing the importance of cybersecurity and

elevating it to a top priority (The University of Phoenix and the ISC2 Foundation, 2014). Several well-publicized cyberattacks, including Target, Home Depot, Neiman Marcus, JPMorgan Chase, and the Office of Personal Management, have highlighted the need for businesses to enhance their security measures (Harris, Perlroth, & Popper, 2014; Tobias, 2014; Scitutto, 2015). No company is immune to cybersecurity threats, and inadequate security measures can result in devastating outcomes.

The financial sector is particularly vulnerable to cyber attacks due to the digital evolution of finance, including the development of FinTech and RegTech. As a result, cybersecurity is crucial in this industry, and it has become a major concern for regulators and international institutions like the FSB and Basel Committee. Financial institutions themselves are also focusing more on cybersecurity as centralization and digitization continue. Additionally, cybersecurity should be a top priority for new FinTech start-ups, as they often handle large amounts of data and may not have a full understanding of security measures. While a lack of funds led to the development of safe deposit boxes and payment systems, the abundance of data in the digital age may not provide sufficient incentives for businesses to prioritize cybersecurity, which can harm consumers. Therefore, FinTech and RegTech are inextricably linked, and cybersecurity is a critical component of both. (Arner, et al, 2016; Dahlgren, 2015; The Board of the International, 2016).

#### ➤ *Fin Tech in India*

The use of financial technology or fintech has grown rapidly in India in recent years, as the country offers a huge market with its population of over 1.3 billion people. One of the main drivers behind fintech development in India is the government's efforts to promote financial inclusion and digital payments through initiatives such as Digital India, PMJDY, and BBPS. The introduction of UPI by NPCI, which allows for instant money transfers between bank accounts using a mobile device, has also been a significant advancement in the fintech sector in India. Indian fintech startups like Paytm, PhonePe, and Razorpay have seen substantial growth and investment in recent years, as more Indians adopt digital payments and financial services. The fintech sector in India is expected to expand significantly over the next few years, thanks to the country's expanding market, favorable regulatory environment, and growing startup ecosystem. India is rapidly becoming a fintech hub in Asia and around the world.

#### ➤ *Regtech in India*

The concept of Regtech, or regulatory technology, is relatively new in India and is aimed at assisting companies in adhering to the various regulatory requirements in a more efficient and effective manner. The regulatory environment in India is complex and subject to constant change, which is driving the development of Regtech. As companies expand, they must comply with more regulations, which can be both costly and time-consuming. Regtech solutions can help companies manage their compliance requirements more efficiently, thereby reducing costs and minimizing the risks

associated with non-compliance. Additionally, India's government is increasingly using technology to improve monitoring capabilities, and as a result, regulatory sandboxes have been created to provide a safe environment for companies to test new products and services. The demand for regtech solutions has increased due to government initiatives to promote financial inclusion and digitization, which have resulted in the need for banks to comply with KYC regulations. LegalEase Solutions, Compliance, and Quintegra Solutions are some of the top regtech companies in India. Although the sector is still in its early stages, it has great potential for growth, as there is a growing demand for technology solutions that can help companies manage their compliance duties more effectively and efficiently.

#### ➤ *Fintech, Regtech, and Cybersecurity in India*

In the rapidly developing nation of India, the fintech, regtech, and cybersecurity sectors have undergone substantial growth and evolution in recent years. Particularly, the fintech sector has witnessed significant expansion over the last decade, with several companies, such as Paytm, PhonePe, and Razorpay, achieving tremendous success. This growth can be attributed, in part, to the robust regulatory framework in place, including the digital payments guidelines established by the Reserve Bank of India (RBI), which have fostered a favorable environment for innovation and development. One of the most noteworthy advances in the fintech industry is the introduction of the Unified Payments Interface (UPI) by the National Payments Corporation of India (NPCI), which provides a secure and reliable platform for digital payments.

Similarly, the growth of the regtech sector in India has been substantial, as organizations increasingly need to manage their compliance obligations in response to the growing number of regulatory requirements in the financial services industry. In this context, several regtech firms have emerged in India, including LegalEase Solutions and Compliance, which provide compliance management and regulatory compliance services for the finance sector, respectively.

Moreover, India has witnessed a proliferation of cybersecurity companies, such as Lucideus and Sequaretek, which offer a range of services and solutions for managing cyber risks and safeguarding businesses against cyber attacks. Given the rapidly expanding market for security solutions and services in India, these companies are well-positioned to meet the growing demand for advanced cybersecurity measures.

Overall, the significant growth and development of the fintech, regtech, and cybersecurity sectors in India can be attributed to the robust regulatory structures in place and the increasing demand for innovative solutions in the financial services industry. As the industry continues to modernize and evolve, these sectors are poised to play an increasingly important role in shaping its direction and trajectory.

#### IV. CONCLUSION AND SUGGESTION

To summarize, the demand for innovative and convenient financial products and services will drive continued growth in the FinTech industry. However, it is crucial for regulators to maintain oversight to protect consumers and the economy from potential technological threats. This involves prioritizing RegTech and cybersecurity to ensure a secure and successful FinTech sector. As FinTech continues to evolve, these tools must also keep pace to ensure financial stability and consumer safety. Failure to adequately address any gaps in RegTech or cybersecurity in the Indian financial industry could have negative consequences for the country's economy.

Fintech, Regtech, and cybersecurity are areas that are constantly changing and need continuous invention and advancement to stay useful. To better their services and the user experience, fintech businesses should adopt new technologies like blockchain, artificial intelligence, and machine learning. Fintech firms can have a greater effect by improving underbanked and underserved groups' access to financial services and financial inclusion. Open banking can be used by fintech businesses to offer their clients more complete financial services and products. Advanced analytics and data analysis methods can be used by regtech businesses to find and reduce risks associated with regulatory compliance. Regtech firms should create solutions that are adaptable to the particular demands and specifications of various businesses and sectors. To better their solutions and increase their effect, regtech firms should work with other participants in the regulatory ecosystem, such as financial organizations, regulatory agencies, and policymakers. By utilising cutting-edge technologies like AI and machine learning, cybersecurity firms should improve their threat intelligence skills. To rapidly identify and react to cyber threats, cybersecurity firms should prioritise real-time surveillance. In order to prioritise security from the outset and incorporate cybersecurity into every facet of their products and services, cybersecurity businesses should create secure-by-design solutions. Overall, these recommendations can help increase the efficiency of the fintech, regtech, and cybersecurity sectors and guarantee their ongoing expansion and influence.

#### REFERENCES

- [1]. Arner, D., Barberis, J., Buckley, R. (2016). FinTech, RegTech and the Reconceptualization of Financial Regulation. *Northwestern Journal of International Law and Business*.
- [2]. Avery, C. & Fanger, G. (2014, Nov/Dec). Cybersecurity: The human factor. *FinTech Law Report*, 17(6), 1-14.
- [3]. Dahlgren, S. (2015). The importance of addressing cybersecurity risks in the financial sector, Speech at the OpRisk, North America Annual Conference, New York City.
- [4]. Dattani, I. (2016, June). Financial Services and Fintech- A review of the cyber security threats and implications.

- [https://www.researchgate.net/publication/304023925\\_Financial\\_Services\\_and\\_Fintech\\_-\\_A\\_review\\_of\\_the\\_Cyber\\_Security\\_threats\\_and\\_implications](https://www.researchgate.net/publication/304023925_Financial_Services_and_Fintech_-_A_review_of_the_Cyber_Security_threats_and_implications)
- [5]. FinTech Futures. (2018, March 5). Infographic: the incredible growth of fintech. <https://www.bankingtech.com/2018/03/infographic-the-incredible-growth-of-fintech/>
- [6]. Grant, G.H. & Grant, C.T. (2014, May). SEC cybersecurity disclosure guidance is quickly becoming a requirement. *The CPA Journal*, 69-71.
- [7]. India's RegTech Space: Opportunities and Challenges," a report by KPMG in India: <https://home.kpmg/content/dam/kpmg/in/pdf/2020/10/india-regtech-opportunities-and-challenges.pdf>
- [8]. "Regtech in India: A New Approach to Regulatory Compliance," an article by Deloitte India: <https://www2.deloitte.com/in/en/pages/finance/articles/regtech-india.html>
- [9]. "Regtech Startups Are Here to Streamline Compliance in India," an article by Analytics India Magazine: <https://analyticsindiamag.com/regtech-startups-are-here-to-streamline-compliance-in-india/>
- [10]. "The Rise of Fintech in India," an article by Harvard Business Review: <https://hbr.org/2020/05/the-rise-of-fintech-in-india>
- [11]. "India Fintech Report 2020," a report by MEDICI Global: <https://gomedici.com/india-fintech-report-2020/>
- [12]. Kidd, J. (2018). Fintech: Antidote to rent-seeking? *Chicago-Kent Law Review*, 93(165).
- [13]. Magnuson, W. (2018, May). Regulating Fintech. *Vanderbilt Law Review*, 71(1167).
- [14]. Ng, A.W. & Kwok, B.K.B. (2017). Emergence of Fintech and cybersecurity in a global financial centre. *Journal of Financial Regulation and Compliance*, 25(4), 422-434.
- [15]. Pascu, L. (2017, December 22). Financial services industry among top targets of cyberattacks. <https://securityboulevard.com/2017/12/financial-services-industry-among-top-targets-of-cyberattacks/>
- [16]. "Why Regtech Is the Next Big Thing in India's Financial Sector," an article by Entrepreneur India: <https://www.entrepreneur.com/article/363517>
- [17]. Sanicola, L. What is FinTech? From Huffpost.com: [https://www.huffingtonpost.com/entry/what-is-fintech\\_us\\_](https://www.huffingtonpost.com/entry/what-is-fintech_us_)
- [18]. Sciutto, J. OPM government data breach impacted 21.5 million. <http://www.cnn.com/politics/office-of-personnel-management-data-breach-20-million>