Emerging Technologies and Trends for Banking Supervision

By
Mr. Musa I. Jimoh,
Director, Payments System Management Department
Central Bank of Nigeria

13.0 Introduction

New technology has changed the foundations upon which the banking industry was built. The advent of the internet has led to significant changes in global business models and growth in e-commerce, online banking, etc. These technological transformations have led to disruptions in many sectors, banking included, and those that cannot keep up will lose their ability to compete. However, these disruptions are not all bad. Those who adapt their business models and find ways to use emerging technology to their advantage will thrive.

The changes and developments will be market-driven as banks respond to the shifting demands of financial service consumers. Thus, market forces will lead banks to deploy new technology to improve the quality, pricing, and convenience of products. The resulting innovation and competition would typically work in favour of the consumers. Today's consumers are different – they are technologically savvy, consume round-the-clock and on the go, are more informed, demand faster and better services, and due to smart mobile internet-based technology, have more access to goods and services worldwide. Access to goods and services via the internet translates to fewer physical interactions and more remote transactions. As a result, their expectations have evolved too -Businesses, banks included, are expected to provide services 24/7 to meet a very demanding customer base. The recent pandemic is proof of how a business that had been able to deliver services remotely prior to, and leading into, the pandemic was able to remain profitable – the global e-commerce share of total retail sales was at 7.4% in 2015, 13.6% in 2019 and rose significantly to 18% in 2020[i]. The growth has been forecast to increase by 8% between 2019 and 2024. Although the trend had shown a steady upward trajectory, there was a significant paradigm shift during the pandemic, which forced businesses to adapt quicker and sooner. The banking sector was no exception and needed to adapt to the trends, and investment in technology enabled them to stay on track.

13.1 Banks and the Management of the New Realities

Banks, globally, had recognised that their core infrastructure no longer consisted of multiple physical branches. Again, with the trend in the consumption and the arrival of smart mobile devices, digital banking has become a more effective way to extend banking services to its customers. This meant that establishing several physical bank branches was no longer effective, and the return on these physical assets made them less cost-effective than deploying digital access to banking services. For example, the total number of bank branches in the European Union reduced from 237,700 to 174,000 between 2008 and 2018[ii] – i.e., there was a steady decline in numbers resulting in the closure of an estimated 63,700 branches over a 10-year period.

On the other hand, investment in ICT infrastructure is increasing. Annual global IT spending was forecast to be 4.3 trillion USD in 2021, a 9.5% increase from 2020[iii] - Financial services firms are expected to spend 500 billion USD (12% of the total). IT investments will drive improvements in digital systems for financial services, and those banks who invest wisely in these emerging technologies will no doubt be able to compete better to retain or grow their market shares.

Also, as the services become more digital, banks need a completely different type of workforce and skills to manage their IT systems, as well as experts to manage emerging risks such as cybersecurity risks. Thus, one of the key areas that banks should expect to compete with one another, as well as with other Financial Service Providers, is security. Cybersecurity is a threat to all things digital, so there is an increasing need to ensure convenience for product end-users, as well as ensure full-proof customer authentication and verification processes. This is particularly crucial for Nigerian banks considering the "Know Your Customer" (KYC) obligations and responsibility to protect the system against criminal financial activities, including Money Laundering and Financing of Terrorism.

Banks today deploy Biometrics, Optical Character Recognition (OCR), cryptography, etc., as part of measures to secure their authentication and approval process. Nonetheless, there are still more opportunities to be harnessed from evolving technologies, including Big Data, Cloud Computing, Application Programme Interfaces (APIs), and Distributed Ledger Technology (DLT), to name a few, so banks should be encouraged to think creatively and innovate with its deployment of financial products and services. The landscape for financial services is changing fast, and the following models have become obvious:

- Digital Transformation by Incumbents
- The emergence of BigTechs/TechFins in the financial services space
- Open Banking and Open Finance
- Partnerships and Collaborations

13.2 Emerging technologies facilitating the New Paradigm

The following list is not exhaustive.

Internet of things (IoT)

This refers to the growing network of internet-enabled devices that have the capability to collect data about the physical world and transmit the same through the internet. These devices are collectively referred to as smart devices and include mobile devices, machinery, tools, etc., that can be embedded with software, sensors, processors, and other technology.

Data Analytics

Data analytics is the process of collecting, modeling, and analyzing information to extract insights for decision-making – this can either be post-mortem or forecasting analysis.

Artificial intelligence (AI)

This is a technology developed to mimic human intelligence with capabilities to perform tasks, identify patterns, learn and improve its capability based on the information it collects. It has also been suggested that AI gives machines the capability to think. More businesses are deploying this technology in targeted advertising.

Machine learning (ML)

This is a method of data analysis that automates analytical model building. It is a subset of Artificial Intelligence and is based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention. This is a useful tool for analysing customer patterns and detecting and mitigating fraud.

Cloud Computing

On-demand model for outsourcing and minimising upfront IT infrastructure costs. It enables subscribers to deploy applications and store/manage/access their data remotely. This technology has facilitated the entrance of smaller players in many fields by enabling businesses to scale and manage their infrastructural requirements at reduced costs.

Application Programming Interface (API)

An application programming interface, or API, is a functionality that enables companies to easily and safely share and exchange data with external third parties, including developers, business partners, regulatory agencies, other internal departments within their companies, etc. This technology has proved extremely useful in the drive to implement Open Banking in Nigeria. It also has the potential to open up the entire financial space as it is being implemented in Australia.

Distributed Ledger Technology and Digital Currencies

This is a technology protocol that has enabled the tokenisation of fiat currencies. These developments in ICT have led to the capability to deploy technology to facilitate operations in all sectors.

13.3 Emerging and Inherent Risks to Technology-Facilitated Operations

There are unique risks associated with the deployment of technology. Some of the inherent and emerging risks are as follows:

Third-Party Risk

Third-party risk includes service delivery issues as well as operational risks and their components, such as cybersecurity risks and data privacy breaches. An example is when a third-party vendor has downtime issues that impact a business negatively. Also, in a digital space, network connectivity makes businesses more vulnerable as any system connected to 3rd party networks can breach a bank's network when security is compromised – internally or remotely. Service Level Agreements and Data Protection requirements are often signed by businesses and their third-party service providers as part of their contracts. And the establishment of minimum IT protocols and standards across the industry helps to ensure secure connectivity between parties.

Operational Risk

There is a heightened risk of downtimes, third-party/outsourcing failures, resource challenges, and human errors as more businesses transition to digitalised service delivery. Some of the unique components of operational risk associated with digitalisation are:

Cybersecurity Risk

The risk of reputational and financial exposure or loss resulting from remote internet-facilitated attacks, data breaches, and other security incidents. These attacks can be sporadic or targeted, and businesses can be vulnerable to these attacks through their IT network, staff, and third-party interactions. In the payments ecosystem, for example, malware targeted at Point of Sale (POS), interbank funds transfer systems, and ATMs in Nigeria had been identified by intelligence

Data Protection and Privacy breaches

This is an incident that usually occurs in the event of a cyber-attack or security breach leading to theft, or leakage, of proprietary and confidential data.

Competition Risk

This is where the actions of competitors directly or indirectly impact a business. The impact can be positive or negative. Typically, negative impacts arise in a market where there are unhealthy competitive practices unchecked by appropriate supervision. Therefore, it is critical that healthy competition is encouraged through fair and equitable supervisory processes by industry Regulators.

Liquidity Risk

Liquidity risk measures the ability of a business to use its assets to meet short-term financial obligations. Prolonged exposure to liquidity risk could lead to the inability to meet short-term financial obligations, which could increase the risk of insolvency

Collateral is a tool used in the banking sector to mitigate liquidity issues and risk. The use of collateral ensures that banks do not default in settlement of their customer's transactions. However, instant or real-time payment has heightened the risk.

Risk of default/Collateral reconfiguration

With additional participants in the payments space, and rising transaction volumes and values, it is essential that the collateral of settlement banks is aligned with the risk their levels of transaction pose to the banking and payments system. Risk-based collateral management, including online real-time monitoring tools to visualise and analyse liquidity requirements during settlement cycles, would mitigate this risk effectively.

These and other risks must be anticipated, with relevant mitigants in place, to ensure the continued stability and security of the financial system. Therefore, Regulators and Supervisors must also innovate and adapt to remain effective and efficient. To do this, we must invest in technology – Technologies to aid and improve Supervisory functions already existing under the umbrella term SUPTECH[29] , i.e., Supervisory Technology. More and more supervisory authorities around the world are considering and deploying the use of this class of technology to support their supervisory functions.

13.4 The Role of the Regulator

The Central Bank has been proactive in creating an enabling environment through many initiatives and policies to support these developments in the Banking and Payments space. Policies and regulations are being released to not only facilitate the adoption of new technologies but to draw attention to risk and provide regulatory guidance on risk management

More recently, some of these Policies and initiatives include;

- Issuance of the Risk-Based Cyber-Security Framework and Guidelines for Deposit Money Banks and Payment Service Providers
- Issuance of the Nigeria Payments System Risk and Information Security Management Framework
- Issuance of the New Licence Categorisation for Nigeria Payments System
- Establishment of the Consumer Protection Department
- Establishment of the Payments System Management Department
- Issuance of the Framework for the Operations of the Regulatory Sandbox
- Issuance of the Regulatory Framework on Open Banking Operations in Nigeria
- Development of an Industry Security Operations Center
- Recognition of Payments Service Providers as Other Financial Institutions in BOFIA 2020 for proper supervision and oversight
- Implementation of the Global Standing Instruction
- Issuance of the Revised Mobile Money Regulatory Framework and Guidelines
- Issuance of the Revised Bank Verification Number and Watchlist Framework

Notwithstanding the efforts so far, there is more to be done. As supervisors and regulators, it is important to remember that we must not get in the way of market forces – our role is not to stifle innovation but to monitor emerging developments in order to ensure that prudential safety remains high, especially through periods of swift technological changes and shifts in consumption trends.

[29] SUPTECH uses include the automation and streamlining of administrative and operational procedures (including approval and communication processes), digitization of data and work tools, improvement of data analytics etc.

Also, we must supervise sector players fairly in order to maintain a level playing field across the market – this includes new entrants operating in unfamiliar and innovative ways.
There is a need for enhanced collaboration among regulators and supervisors across the financial system. Indeed, the lessons of the Global Financial Crises and the interconnectedness of markets should not be lost on us. Indeed, technology has heightened the possibility of a repeat.
Therefore, Supervisors, including the NDIC, are encouraged to continue to build competency, stay agile and consider the acquisition of relevant SUPTECH to facilitate and enhance its supervisory and oversight functions. While strengthening internal capabilities, we need to rejig the model of collaboration to become more proactive in responding to emerging risks as well as the existing risk that is being made more pronounced by the adoption of new technologies in the financial services space.

13.5 Conclusion

Technology is the future. Digital Transformation is inevitable. Consumers are driving change. Digitalisation of financial services is here. Risk is evolving. And Regulators, as well as regulatory approaches, should evolve. As clearly enunciated in the Payment Systems Vision 2025 of the Central Bank of Nigeria, the Bank is focused on strengthening the safety and reliability of our national payments infrastructure, as well as the regulatory frameworks that would encourage the development of the financial system, increase financial inclusion and promote the adoption of electronic payments.

All stakeholders, therefore, must re-evaluate and appreciate their roles in safeguarding the Nigerian financial system and ensuring its stability in line with the evolving landscape. Formal considerations should be made by Regulatory Authorities for the acquisition and deployment of relevant SUPTECH to improve the effectiveness and efficiency of the Supervisory function.

---

[i] Impact of COVID Pandemic on ecommerce – www.trade.gov
[ii] Number of Bank branches in Europe - www.statista.com
[iii] Overall IT spending worldwide – www.statistica.com