مصرف لبنان
BANQUE DU LIBAN

FinTech and Cyber Regulation:
Insights from Lebanon

Raed H. Charafeddine, First Vice-Governor, Banque Du Liban
Dr. Lâma Daher – Banque Du Liban

13th High-level Meeting for the Arab Region:
Global Banking Standards and Regulatory and Supervisory Priorities
Jointly organized by the Basel Committee on Banking Supervision (BCBS), Financial Stability Institute (FSI) and Arab Monetary Fund (AMF)

December 13th, 2017 | Abu Dhabi - United Arab Emirates

Table of Contents

I. Introduction

Over the past century, the financial sector has undergone multiple changes starting with the Fedwire (1918), Dinner's Club Credit cards (1950s), Telex (1966), ATM (1967), BACS and CHIPS (1968), SWIFT (1973), debit cards and CHAPS (1980s), contactless payment and PayPal P2P online transfers (2000), M-Pesa mobile money transfers (2007), Faster Payments Service (2008), SQUARE mobile payment solutions (2009), TransferWise P2P money transfers (2011), Google digital wallet (2011), Bitcoin virtual currency (2013), wearables and Internet of Things (2014), Fino PayTech payment bank (2015). FinTech landscape is evolving rapidly. Technologies made it easier for banks and financial institutions to provide financial services tailored to each customer. They are seen as a source of economic growth and progress .

In spite of these positive effects, threats have emerged. Cyber risk is on the top of the list. Banks and financial institutions are particularly targeted by cyber-attacks due to the criticality of their economic function and the nature and value of their assets. Both financial assets and non-financial assets (personal data, credit card numbers, etc.) held for the account of their customers could be targeted by cybercriminals. And these assets can be breached through different tactics: hacking, malware, social engineering like phishing, privileged credentials stealing, and others. Moreover, cyber risk could no more be considered a mere security risk as it increasingly embraces critical issues such as data protection, privacy, stakeholders consent on the usage of big data, as well as business continuity.

In Lebanon, the banking industry is known to be one of the cornerstones and drivers of the economic growth. It is also most concerned with the advancement of technologies and digitalization of services and processes. Hence, there is no doubt that this sector guided by Banque Du Liban (BDL) – the central bank of Lebanon, is reasonably the most developed in terms of preparedness, prevention, competencies, tools, equipment and governance in the matter of cybersecurity.

In the present paper, I will first recall briefly the expansion of FinTech, and the potential opportunities and risks it is bringing about to the industry. Second, I will address the issue of the rising cyber risks and their impact on financial stability. Then, I will present the initiatives to regulating FinTech as well as cyber risks in Lebanon.

II. FinTech: Opportunities and Risks

An Overview of FinTech

FinTech, also known as financial technology or financial cyber activities, refers to "technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services"[1]. It may also refer to start-ups, technology firms, or even legacy providers that aim at providing financial services by making use of software and modern technology[2].

FinTech can be classified into three product sectors that relate to core banking services:

(1) credit, deposit and capital-raising services: crowdfunding, lending marketplaces, mobile banks and credit scoring;
(2) payments, clearing and settlement services: retail services such as mobile wallets, peer-to-peer transfers and digital currencies; and wholesale services such as value transfer networks, foreign exchange wholesale and digital exchange platforms;
(3) Investment management services: high-frequency trading, copy-trading, e-trading and robo-advice.

FinTech relies on new technologies and advanced software tools that play a significant role in FinTech evolution[3].This supporting layer nowadays includes software-defined infrastructure; advanced application integration tools (Application Programming Interfaces – APIs); cloud computing (public/private cloud); cognitive computing and artificial intelligence technologies (big data analytics, machine learning tools, predictive modelling); distributed ledger technologies – DLT (blockchain and other distributed ledgers); internet of things and smart contracts; with higher level of security required namely for identity verification (encryption, electronic signature, biometric technology, crypto-hash algorithms for digital currencies "cryptocurency").

Opportunities of FinTech

Financial innovations are transforming the way conventional financial services providers interact with each other and with their customers, in terms of communication, data storage, delivery and processing, and access and use of financial services[4]. They attempt to fulfill customers' needs for reliable, seamless, ubiquitous and cheap financial services. But also sometimes they disintermediate the traditional banks and financial institutions from their customers through allowing direct access to financial services eliminating borders, distances and physical costs.

These opportunities are mainly perceived in the areas of microfinance, insurance, remittances, and crowdfunding[5]. For instance, according to a report by Capgemini Consulting (2016), the usage of smart contracts in retail banking could potentially save between USD 480 to USD 960 per loan, with an aggregate cost reduction for banks ranging between USD three to USD 11 billion a year. The report estimates also annual cost savings of USD 21 billion globally for the usage of smart contracts in personal car insurance[6].

In addition to that financial innovations bring about three main opportunities[1,2,7]:

(1) consumer experience: for financial services providers, this involves innovative use of data for marketing and risk management purposes; as for customers (individuals and MSMEs), this means increased access to and convenience of financial services, more customer-centered services and products, clearer disclosure, greater transparency, enhanced understanding and empowerment;

(2) efficiency: for financial services providers, this means improved and more efficient processes, better capital allocation, lower transaction costs, and stronger operational resilience; as for customers, they have better and more tailored products and services, more choices, faster services, mobility and lower prices;

(3) system resilience: greater depth, competition, decentralization and diversification, and bigger opportunity for partnerships between FinTech companies and established banks and financial institutions.

A recent report by the IFC (2017) exhibits in details the implications of derisking and the solutions raised by over 300 surveyed correspondent banking clients in 92 countries[8]. Among these solutions are financial technology with the potential to contribute to a reduction in compliance costs and an increase in risk assessment precision. Known as RegTechs, these are "innovative technologies that can help banks and financial institutions comply with regulatory requirements (reporting, financial crime, operational risk, consumer protection and data protection) and pursue regulatory objectives"[1]. RegTechs may reduce compliance costs[9] by using new technologies to automate manual processes (artificial intelligence), aggregate, share and store data (cloud computing, DLT); enhance security (cryptography); identify suspicious transactions, security analytics, big data) and facilitate regulator-bank interactions (APIs). Supervisors could also use SupTechs, i.e. to be able to identify and explore new technologies for internal supervisory purposes.

Risks of FinTech

Along with its attractive opportunities, FinTech encompass various risks[1]. The risks for consumers include inappropriate marketing practices[i], data privacy, data security, and discontinuity of banking services. The risks for banks and the financial system, the risks encompass strategic and profitability risks, increased interconnectedness between financial parties, high operational risk, third party/vendor management risks, compliance risk including failure to protect consumers and data protection regulation, money laundering and terrorism financing, liquidity risk and volatility of bank funding sources. In addition to these, cyber risks constitute one of the common risk factors for both consumers and providers.

FinTech from governments' perspective is increasingly perceived as a catalyst for financial inclusion and is welcome to scale up in the digital finance sector. Other regulatory bodies such as the Financial Stability Board (FSB) argue that FinTechs may cause serious micro- and macro-risks on financial stability if they do not intersect with regulatory frameworks. In that perspective, there is a need to develop both RegTech and SupTech in order to detect systemic risks and reduce the cost of reporting.

The Size of FinTech

The FinTech industry is based on top technology and talent. It is fast growing and relatively well funded. FinTechs are customer-centered, nimble, and agile. With the adoption of smartphones, empowered by digital stores, they offer unlimited options of cost-effective and efficient solutions. Also, with less human friction, convenient and speedy services, FinTechs are being enabled to scale-up faster, differentiate to gain a market share, fill the vacuum where brick and mortar are not there, and compete with incumbents. Their acceptance has been accelerated by the damaged reputation of the banking and financial industry from the global financial crisis. According to a recent survey report by the World Economic Forum (2017), FinTechs have changed how financial services are structured, provisioned and consumed, but have not yet successfully established themselves as dominant players[10].

Globally, FinTech is evolving rapidly. Its growth can be measured using venture capital (VC) investment in FinTech companies. According to a recent study by KPMG (2017), the volume of global venture investment reached USD 13.6 billion across 840 deals in 2016, compared to USD 13.8 billion for 653 deals in 2015, and USD 0.8 billion for 199 deals in 2010[11]. The KPMG (2017) report states that besides the investment made by VC funds, many of which

[i] Convenience, speed, and low cost digital solutions with misleading marketing for financial products with higher returns can affect users' behavior and judgment, and many may fall victim of shadow digital banking activities.

are backed by financial institutions, banks and other institutional investors are also making large direct investments in FinTech companies.

In 2016, according to a global survey by the Basel Committee on Banking Supervision[1], the category that includes payments, clearing and settlement services had the highest number of FinTech services providers, followed by the category that includes credit, deposit and capital-raising services. Within the payments, clearing and settlement category, retail payment services firms represented the majority of FinTech firms identified, as compared with wholesale payment services providers.

Regionally, the Middle East and North Africa (MENA) region is following the global trend. According to a report by Wamda and PayFort (2017), during the last ten years MENA FinTech startups raised more than USD 100 million in funding[12], and analysts expect it to double by 2020. The number of disclosed investment deals doubled from five in 2013 to ten in 2016 according to the same report. The number of FinTech startups totaled 105 in 2015, which is greater than the current number of education, energy and healthcare startups, and is expected to reach 250 by 2020. Like the global trends, the majority of FinTech startups provide payment solution, or money lending and capital raising activities.

Locally, according to a recent survey by Arabnet (2016), 54% of overall bank account holders in Lebanon are adopters of digital banking (online banking, mobile banking, or both), including 10% using online banking only and 6% using mobile banking only[13]. According to PayFort (2017), Lebanon ranks second most advanced FinTech startup ecosystem in the region, hosting 14% of the region's FinTech startups in 2015 after UAE (30%). Lebanon is also the fourth most served market by FinTech companies with 27% of MENA FinTech startups serving the Lebanese market in 2016 after Jordan (39%), Egypt (34%) and Saudi Arabia (29%)[12].

III. Cyber Risk: A Growing Systemic Risk

An Overview of Cybersecurity

Cybersecurity threats can emerge from many different sources. The most common are: (1) criminal organizations seeking financial gain; (2) disgruntled employees seeking revenge or motivated by financial gain; (3) accidental breaches due to human error, failure to follow internal procedures or ineffective internal procedures; (4) exposure due to control failures in external services providers (outsourcing) who have access to the firms' systems; (5) competitor firms seeking to steal intellectual property or trade secrets; (6) hostile nation-states seeking to undermine a rival state's economy; and (7) ideological groups seeking to damage the financial system[14].

As information technology grows, so do the capabilities of cyber criminals. These criminals have a wide range of tools to execute cyber-attacks, many of which are easily obtainable and relatively inexpensive to procure. In addition, they know that there is a low likelihood of being detected or prosecuted and many attack strategies can be executed cheaply. Therefore the risk-reward trade-off for cybercrime is very attractive. Cybercrimes encompass data theft, malware, hacking, and disruption of IT and business services (denial of service). It also include traditional crime, such as bank heists, fraud, forgery, theft, industrial espionage and ransom. The consequences of a cyber-attack at an institution's level range from financial losses, penalties for non-compliance to regulations, damaging reputation of the bank and its public image, losses of customers, and losses of opportunities. Recent cyber-attacks include the 2016 cyber theft of USD 81 million from the Bangladesh Bank, the WannaCry ransomware attack of 250,000 computer systems in 150 countries, and the Equifax hack of up to 143 million individuals' personal information[15].

The top five challenges of cybersecurity according to a survey by PWC (2017) are: (1) the assessment of security protocols and standards of third party vendors; (2) complex technologies; (3) ability to protect personally identifiable customer information; (4) the need for clear regulatory guidance; and (5) employee training[16]. According to Momentum Partners (2017) and TUVRheinland (2015), three key topics are expected to increasingly attract the attention of cybersecurity companies[17,18]. These are data privacy[ii], cloud security[iii] and the internet of things[iv] (IoT).

Cybersecurity and Financial Stability

In an attempt to prevent global financial crises to reoccur, global regulatory reforms such as Basel III were designed to improve the ability of banks and financial institutions to absorb shocks and improve balance sheet governance and risk management while enhancing transparency[19]. These reforms focus only on regulating financial risks mainly capital adequacy and liquidity, and seek out less technology and cyber security risks. This may be because the volume of losses from these risks is not yet critical. Furthermore, most financial institutions still consider cyber risk under operational risk-external fraud,

[ii] The EU General Data Protection Regulation (GDPR) is driving growth in software-based privacy solutions with capabilities such as artificial intelligence, machine learning, automation, identity intelligence and big data.

[iii] As more organizations and consumers migrate to cloud-based services and infrastructures at external cloud providers, there is a growing need to secure cloud services and endpoints. Consequently, global cloud security market is expected to increase from USD 5.9 billion in 2017 to USD 9 billion in 2020.

[iv] By 2020, an estimated 50 billion devices will connect the 8 billion people worldwide to their cars, homes, communities, medical information and work (Accenture's 2017 Global Distribution & Marketing Consumer Study). As more devices are connected via the internet, the society as a whole is increasingly vulnerable to cyber-attacks on control and infrastructure systems.

according to a recent survey by Oliver Wyman (2017) reporting that 82% of the surveyed institutions quantified cyber risk as part of operational risks, while 9% as a standalone risk and 9% haven't quantified it at all[20].

However, the same survey brings about interesting findings, namely that 67% of leading financial institutions worldwide have dedicated cyber risk management strategies, and that 73% of these institutions have purchased cyber risk insurance. Accordingly, as the consequences of cybercrimes are becoming more costly at all levels, the task of cybersecurity is expanding and a shift in responsibility is expected to take place from the IT department to the compliance department[21]. The importance of cyber defence is not less than compliance to AML, CTF and tax evasion regulations, as well as international financial standards (Basel III, IFRS, etc.). Two main characteristics of cybercrimes raise them among the prominent sources of systemic risk. First, there is the development of interdependencies across financial intermediaries due to accelerated dematerialization of financial intermediation and increased automation in financial activities, especially clearing and payment activities. Second, there is the potential loss of trust from the general public in electronic and digital activities that could be caused by a failure to protect their assets and data.

As attacks have become more sophisticated, regulators are raising their level of scrutiny, and global cybersecurity and privacy legislation is changing. They are taking regulatory and supervisory steps to facilitate cyber risk mitigation by regulated financial services providers, and effective response to and/or recovery from cyber-attacks[22].

The Size of Cybersecurity

Globally, two out of three people experienced a tech support scam in the previous 12 months according to a global survey conducted by the Microsoft Digital Crimes Unit and Ipsos (2016)[23]. Around 91% of attacks by sophisticated cybercriminals start through spear phishing emails[24]. A report by Cybersecurity Ventures[25] (2017) states that ransomware damages are up to 15 times in the past two years. The report predicts that a business will fall victim to a ransomware attack every 14 seconds by 2019, increasing from every 40 seconds in 2017.

A report by Momentum Partners[26] (2017) shows that cybersecurity startups raised USD 17.6 billion across 1,428 deals since 2010. Another report by Cybersecurity Ventures[24] (2017) states that the global cybersecurity market was worth USD 3.5 billion in 2004 and is expected to reach more than USD 120 billion in 2017. It predicts global spending on cybersecurity products and services to exceed one trillion USD cumulatively over the next five years, from 2017 to 2021.

From the perspective of the banking and financial services industry[27], its is reported that this industry faces the greatest economic risk related to cybersecurity[28], and that financial services firms are hit by cybersecurity incidents 300 times more frequently than firms in other industries[29]. For instance, J.P. Morgan Chase & Co. revealed that it will double its annual cybersecurity budget in 2015; it has effectively increased from USD250 million in 2014 to USD500 million in 2015[30]. Bank of America declared it has an unlimited budget when it comes to combating cybercrime[31].

Also according to some industry experts cited by the Palo Alto Networks Research Center (2016), by 2019, the demand for cybersecurity professionals is projected to grow to approximately 6 million globally[32]. The cybersecurity unemployment rate will remain at 0%, whereas the shortage of trained professionals is expected to be 25% or 1.5 million jobs unfilled by 2019. Furthermore, this shortage is expected to reach 3.5 million by 2021 according to a report by Cybersecurity Ventures (2017)[25].

Cybersecurity in BDL

In Lebanon, some banks reported spending around 10% of their IT department's budget on cybersecurity measures, including a larger dedicated staff and more advanced technological tools acquired and utilized[33]. The tipping point after which cybersecurity became a top priority of local banks, according to the same source, was the discovery of the so-called Gauss malware. According to a report by Kaspersky Lab[34], this was the first publicly known nation-state sponsored banking Trojan. Gauss malware was the cyberespionage toolkit designed to steal sensitive data from banks, namely credentials required to access online banking accounts, has infected 1,600 computers of banks in Lebanon as of the end of July 2012. During this period, BDL sent awareness messages to Lebanese banks providing them several tips on how to detect and remediate Gauss malware, and how to prevent its re-occurrence.

In 2016, the Financial Intelligence Unit of Lebanon, known as Special Investigation Commission (SIC) reported[35] an exponential rise in the number of cases of embezzlement of private funds due to cybercrimes. It stated an increase from four declared local cases in 2013, to 44 in 2014, then 80 in 2015, to reach 123 in 2016. Thus, the embezzlement of private funds is ranked first among the types of predicate offence representing 32.8% of the total number of received cases in 2016. It states that since 2016 banks are being less targeted by cybercriminals compared with other types of companies, and the overall piracy cases growth rate, year-on-year, decreased from 525% on 2013-2014, to 66% on 2014-2015, to 51% on 2015-2016. For instance, the number of email phishing cases reported by local banks dropped from 78 in 2016 to 32 cases in the last nine months of 2017, whereas the number of cases of email

phishing attacking individuals increased from 47 to 90 cases over the same period[36].

IV. Regulating FinTech in Lebanon

In Lebanon, as well as globally, FinTech represents relatively a small portion of the global banking services market. However, the pace of adoption of financial technology is faster as new generations digital natives are growing up with advanced technology proficiency and capabilities. Acknowledging the important role of FinTech as an enabler for financial inclusion[2], BDL has taken various measures to enable the responsible development of this sector in parallel to the measures taken by the government.

Enabling Environment

According to the Office of the Minister of State for Administrative Reform (OMSAR)[37], Lebanon was the first Arab state to draft a bill on both electronic evidence and electronic signature. In the year 2000, the Council of Ministers approved a bill aiming at amending certain provisions of the Civil Procedure Code related to evidence. The bill was thereafter transmitted to parliament by decree[v] but hasn't been yet approved by Parliament.

1. Support ecosystem: Today, the Lebanese infrastructure includes also tech parks (Beirut Digital District, Lebanon Science and Technology Park), clusters (Beirut Creative Cluster, Lebanon Softshore), events and competitions (Arabnet, Start-up Weekend, Wamda), platforms (Bader, Asdaa, Entrepreneurs Lebanon), co-working spaces (961 co-working, ServCorp), funds and awards (Maurice Fadel, Faro), mentor organizations (Injaz, TEC, Mowgli), and training and capacity building hubs (Chamber of Commerce, Darwaza Center).
2. Incubators and accelerators: As of 2017, there were eight incubators/accelerators (BIAT, Berytech, UK Lebanon Tech Hub, Flat 6 Labs, AltCity, Speed BDD, Smart ESA, and South BIC)[38]. A significant portion of the startups and SMEs in Lebanon trained and/or funded by these accelerators are in the field of financial services.
3. Fiscal incentives: Lebanese tax rates are among the lowest globally. To further encourage innovation, the Investment Development Authority of Lebanon[39] (IDAL) offers tax breaks for up to 10 years, as well as other incentives to local and foreign companies operating in the ICT sector meeting specific requirements.
4. Partnership between banks and FinTechs: Lebanese banks have started embracing innovation either by implementing new in-house financial innovations or through investing in local FinTech startups. In fact, banks that have invested in their technology offerings either through partnering

[v] Decree no. 3553/2000

with a FinTech company or internal technology innovations will be in a position to be most competitive; they can leverage more and better data to answer customer demands, maximize marketing efforts, easily integrate new services and be able to satisfy the regulatory requirements.

5. Highly skilled labor: In 2016, Lebanon ranked 19th worldwide for the quality of its higher educational system, while it occupies the 6th place globally for the quality of its math and science education (Global Competitiveness Report 2015-2016). According to IDAL[39] (2017), around 2,000 university graduates specialized in ICT-related activities join the sector every year, and around 1,500 graduates specialize in Finance and business.
6. Competitive labor cost: The Lebanese workforce is relatively less expensive than the GCC countries, Europe and the USA, with the average wage of a software engineer nearly 37% lower than in GCC and 50% lower than those in developed countries (Payscale, 2016).

BDL as a key actor in the enabling environment

BDL is playing a significant role in enabling FinTech environment with the latest technology standards by applying the following strategical actions:

1. Equity financing: In 2013, BDL issued a regulation[vi] through which Lebanese banks were encouraged to dedicate up to 3% of their shareholders' equity, up to 10% of which can be invested in a single company, to equity investments into startups, incubators, accelerators, and VC funds operating in the technology sector in Lebanon. In 2016, the banks' participation limit was raised to 4% or about USD 650 million, and this trend is expected to continue in the coming years. Each of these investments are 75% guaranteed by the central bank in exchange for 50% of any profits. As of end of December 2017, the central bank has approved investments of USD 368, USD 203 million of which have been executed, and another USD 132 million are awaiting approval[vii]. Since the inception of this circular, the Lebanese Tech sector has grown 8% a year, creating 9,000 jobs, and is expected to reach a target of 25,000 jobs by 2025[40]. In 2017, there were six VC firms in Lebanon and many regional VCs which have backed various local FinTech companies.
2. Innovation hub: Since 2013, BDL funds and hosts an annual international innovation hub on knowledge economy and technological innovation. In 2016, the BDL Accelerate[41] forum attracted more than 20,000 attendees, 100 speakers from 50 countries including Steve Wozniak (co-founder of Apple) and Tony Fadell (father of the iPod and founder of Nest), 100 startups from 40 countries, and one of the largest hackathons in the world.

[vi] BDL Circular no.331/2013

[vii] Lebanon's GDP was estimated at USD 40.06 billion in 2013, and 49.5 in 2016 (World Bank).

3. IT roadmap for short, mid and long term[42]: BDL has put in place a strategic and innovative roadmap that covers all IT projects including digital transformation and cybersecurity, and that is updated on yearly basis, in order to follow the latest threat landscape and business and technology evolution. This roadmap will facilitate the financial ecosystem to adopt the latest FinTech technology, with the highest level of security and availability. Accordingly, BDL has introduced new intelligent payment controls and compliance solutions to enhance the fraud detection rate and reduce compliance and credit risks. On the other hand, BDL, as a service provider for the Lebanese National Payment System, is maintaining high level of quality assurance in order to guarantee the business continuity and high resiliency for the whole Lebanese banking sector (an example is BDL's participation in SWIFT COLD-START Exercise with the banking sector to ensure business continuity in case of global SWIFT outage).
4. Cybersecurity memos and policies: BDL plays a key role in continuously providing IT security policies and recommendations to banks, for protecting their business environments, especially with the move to the digital transformation. One of the latest memo on which BDL and the Banking Control Commission of Lebanon (BCCL) are working on, is the e-banking security memo that covers the assessment and management of the risks related to the electronic online banking and payment systems, the best defense strategy with a multi-layered security approach, the multi-factor authentication techniques, the security awareness program, as well as the necessary business continuity and incident management procedures.
5. Regional conferences and events: BDL organizes annual information technology forums in financial industry and invites the big technology alliances and providers in the world in order to boost and enable the transformation of banking industry towards the latest FinTech innovations (Blockchain), digital transformation and advanced cybersecurity, and advanced payment controls in order to reduce credit and compliance risks.
6. International awards and certifications: BDL IT projects and operations are continuously achieved and maintained as per the latest system, network, application, and security best practices and standards. One of the latest certification examples is the "Tier III certification of design documents for the Banque du Liban – Primary Data Center" provided by the International Uptime Institute Professional Services to BDL, that recognizes the BDL's Primary Data Center design as compliant to the latest IT Data Center Standards and though supporting any planned work on the site infrastructure without disrupting operations.

Globally, the new European Union recently issued a payments service directive PSD2 that made it easier for third parties such as FinTech companies and multinational technology companies (such as AliPay and Apple) to enter the payments market and increase competition and innovation further[43].

Some central banks have gone further, such as the Bank of England, whose Governor Mark Carney[44,45] set out the following new opportunities to enable the FinTech transformation and modernize the UK's 20-year old RTGS System: (1) widening access to central bank money to non-bank payment services providers; (2) being open to providing access to central bank money to new forms of wholesale securities settlement; (3) exploring the use of DLT in our core activities; (4) partnering with FinTech companies on projects of relevance to our mission; and (5) calibrating our regulatory approach to FinTech developments. They are also working to ensure that the right soft and hard infrastructures are in place to allow innovation to thrive while keeping the system safe[46].

Similar to the UK, some other countries have implemented various initiatives to guide FinTech companies understand the regulatory framework, while allowing regulators and supervisors interact with FinTech and understand better the risks and benefits from the new technologies, products and services. The following initiatives are developed by their regulator and tailored to their own jurisdiction:

(1) Innovation hub: a place to meet and exchange ideas (Australia, Belgium, ECB, France, Germany, Italy, Hong Kong, Japan, Korea, Luxembourg, Netherlands, Singapore, Switzerland and UK);
(2) Accelerator: a boot-camp for start-ups, culminating in a pitch presentation (Australia, France, Singapore and UK);
(3) Regulatory Sandbox: a controlled testing environment with tailored policy options (Australia, Hong Kong, Korea, Netherlands, Singapore, Switzerland and UK).

Future Steps

1. FinTech roundtables: BDL is planning other forms of interactions such as roundtable with local FinTech companies. The FinTech roundtable will allow (1) to map the FinTech providers in the country; (2) assess whether the offered FinTech services constitute traditional banking activities by another name and thus should be regulated as such; (3) to understand the new technologies and the new cyber activities, and their potential incentives and risks for customers, existing regulated financial services providers, and the domestic system; (4) to assess the extent to which customer privacy and data security are protected, among other concerns.
2. Central bank-issued digital currency (CBDC): BDL is currently assessing the potential of having its own digital currency that will be used as an additional payment tool. BDL considers that establishing protective measures is an introduction and prerequisite to this step. Also extensive research will be conducted to research and assess all aspects of the CBDC. One of the aspects would be the technology to use: the distributed ledger technology or another technology.

3. Regulatory sandbox: BDL is looking into the possibility of establishing a regulatory sandbox, and researching other innovative approaches tailored to the local needs and regulatory landscape[viii]. BDL will contribute in organizing the FinTech environment in Lebanon, knowing that BDL will play the role of certificate authority for banks and financial institutions to provide keys and certificates to secure all electronic transactions. In addition, BDL has strategy to moderate and guide the Lebanese financial sector with the latest recommended security controls in order to protect the FinTech ecosystem from all the current cyber threats.

V. Regulating Cyber Risk in Lebanon

Despite the lack of proper legislation in Lebanon, the country witnessed some improvement in the field of electronic commerce, whereby BDL has secured a proper legislative environment while controlling the cost of such transactions and guaranteeing the protection of customers engaging in electronic banking operations.

Enabling Environment

1. National cybersecurity infrastructure: In 2012, the Presidency of the Council of Ministers formed a National Cyber Security committee[ix] to develop a national and common strategy for the protection of the Lebanese governmental websites with shared responsibility among the different stakeholders. BDL is part of this committee, which has commissioned OMSAR to produce a set of security policy guidelines to be adopted and implemented in all public agencies. The guidelines were published in 2015[47].
2. On-going law on electronic transactions and personal data: BDL is actively contributing in defining this law that will mainly regulate the electronic signature in Lebanon, guide for the establishment of a centralized Lebanese certification authority, and provide the best strategy for the protection of personal data.

BDL as a key actor in the enabling environment

1. Regulation: As early as the year 2000, BDL issued a circular[x] to define electronic financial and banking operations and restrict these transactions to institutions registered with BDL in order to enhance and improve electronic money transfer operations in addition to transactions done

[viii] A FinTech sandbox is a testing environment, contained within a regulatory authority, that allows reducing barriers to test innovative financial products and services, while at the same time ensuring that adequate safeguards are in place to mitigate risks and protect consumers.

[ix] Decision no. 32/2012

[x] BDL Circular no. 69/2000

through ATMs. In 2001, BDL issued another circular[xi] to regulate the control of financial and banking operations, including electronic transfers, electronic banking and operations carried out electronically, for fighting money laundering and terrorist financing. In 2005, a new circular[xii] regulating electronic money transfers was issued.

2. Protective regulation: In 2017, BDL issued a circular[xiii] to regulate protective measures against electronic and cybercrimes. These measures include the requirement of regulated banks and financial institutions to (1) assess potential electronic crime risks; (2) always be abreast of the latest developments in the field of IT security; (3) allocate funds to set up information technology security systems; (4) buy cyber-insurance against electronic crime risks; (5) create a specific taskforce for protection from electronic crimes; (6) prepare incident reporting and response plans, recovery and business continuity plans, immediate intervention plans, and other cybercrime protection plans; (7) carry out awareness campaigns to educate staff and clients about how to protect themselves from e-crimes including not using emails for money transfers; (8) exchange information pertaining to electronic crimes with concerned internal and external entities; and (9) be vigilant and cautious when commissioning third-party services providers for tasks relating to IT systems.

   In terms of technical measures, that circular requires from regulated banks and financial institutions to: (1) implement multi-factor authentication using at least two methods of authentication from independent categories of credentials to verify the external users' identity to access the system and restrict unauthorized access; (2) use a safe coding technique for vital databases to prevent their loss and data leakage; (3) apply strict rules to the filtering of inbound emails; (4) harden and secure all devices at the disposal of employees for external use; (5) carry out tests to identify weaknesses in the network that make it vulnerable to potential hacking; (6) monitor the network traffic, the database, and employees with major access to the IT system in order to detect unusual or illicit activities. Furthermore, regulated banks and financial institutions must also abide by BDL's guidelines to protection from email crimes, which was issued last year in collaboration with the Association of Banks and the Internal Security Forces. Regulated banks and financial institutions must also set up specific internal rules to deal with money transfer requests received through electronic means such as emails and electronic banking. The contracts signed with customers should include specific clauses that identify means other than emails to contact clients, such as phone calls to verify that the money transfer requests received electronically are authentic.

3. Banning the use of decentralized crypto-currencies: As early as 2013, BDL warned[xiv] against purchasing and holding bitcoin and other virtual currencies. BDL states that these consist of commodities and not a currencies, which should be based on concepts and principles necessary

[xi] BDL Circular no. 83/2001
[xii] BDL Circular no. 99/2005
[xiii] BDL Circular no. 144/2017
[xiv] BDL Annoucement no.900/2013

for trusting a currency. Cryptocurrencies lack a fundamental value, and consequently their value increase and decrease very fast. Money is a store of value and one of its fundamental characteristics is related to price stability. This is the reason why crypto-currencies cannot be mistaken for ordinary national currencies which are under the control of central banks.

4. Awareness: In 2016, SIC organized, for the third consecutive year, in collaboration with the Internal Security Forces (ISF), a forum on cybercrimes to raise further awareness on the subject. In 2016, SIC and ISF also organized a press conference to raise awareness on Cybercrime matters. In October 2017, BDL and the World Union of Arab Bankers (WUAB) have organized the annual information technology forum on "Digital Transformation and Cybersecurity", where the latest innovative cybersecurity topics have been discussed and challenged between BDL security experts and international security leading companies and key actors in Lebanese and Middle East banks. Furthermore, BDL has put in place a non-stop security awareness campaign for all BDL employees, covering several security sessions during the year, highlighting the latest IT security topics and controls (advanced cybersecurity attacks, social engineering and preventive behaviors, Internet and email security, and computing security).
5. Guidance: BDL issued a guide and a pamphlet on cybercrime prevention jointly with SIC and the ISF[48].
6. Transparency: SIC publishes statistics and selected cases on cybercrime in its annual reports.
7. Upgrade the capabilities of supervisory and regulatory staff: BDL and SIC employees regularly attend local and international seminars, workshops, conferences and training courses on financial crimes, including cybercrimes.
8. Technical collaboration: Regular Anti-cybercrime steering group meetings between BDL and SIC.
9. Information exchange: BDL and SIC exchange with local and international sources data, indicators and trends on cybercrimes.
10. Local cooperation: BDL is cooperating with other countries' Financial Intelligence Units (FIUs), data protection authorities, conduct authorities and other regulators on cyber defence. In 2016, an Anti-cybercrime steering group from BDL, SIC and ISF was formed, and meet on a regular basis.
11. International cooperation: SIC has signed MOUs with 36 FIUs, the latest being with the FIUs of China, Poland and Bangladesh.

Future Steps

1. Legal protection: Adopting a domestic law and dedicated enforceable legal powers to investigate and prosecute cybercriminals in Lebanon. Also, given the borderless nature of cyber risk, encouraging the establishment of a more comprehensive legal international framework such as a treaty to empower authorities to bring cyber criminals to justice.

2. Governance: Encouraging a more strategic and specific focus by boards of regulated financial service providers to invest in cybersecurity infrastructure systems and procedures, strengthen oversight over cybersecurity risks, and be mindful that cyber risks are properly understood at all levels within the institution.
3. Assessment and quantification: Mandating third-party companies with expertise and certification in cybersecurity to make internal, external and overall security assessment and quantification.
4. Intra-sector collaboration: Encouraging collaboration between cybersecurity officers of Lebanese banks and the creation of a Lebanese Financial Computer Emergency Response Team (CERT). Sharing the security incidents and attack experience between the Lebanese banks when being targeted or hit by cyber-threats, sharing and discussing the latest threat landscape and the related cyber defense programs, are essential for unifying and developing an efficient and common security remediation plan that will ensure reactivity and even proactivity in the cyber-attack defense strategy.
5. Inter-sector cooperation: Encouraging cooperation with telecommunications companies and internet service providers to ensure that cybercriminals do not take advantage of external vulnerabilities to penetrate the security parameter.

Globally, several international initiatives attempted to set a common cybersecurity framework (Word Economic Forum, G7, BIS). Yet only the European Union effected advanced measures in the area of cybersecurity. These measures include:

- *setting strategies (EU Cybersecurity Strategy 2013, European Agenda on Security 2015-2020; Digital Single Market Strategy 2015; Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry 2016);*
- *issuing legislations (Directive on Network and Information Security; Legislative actions to fight cybercrime);*
- *building networks and organizations (EU Agency for Network and Information Security; the EU Computer Emergency Response Team; The Europe's Cybercrime Centre);*
- *allocating funding for research and innovation and infrastructures;*
- *investing in international cooperations (OECD, OSCE, UN).*

VI. Conclusion

Innovation and technology are not only infiltrating the financial industry, they have become a characterizing aspect of every industry. All stakeholders need to wisely embrace the opportunities of new technologies and to seek to understand and proactively manage their inconveniencies. One of the latter is the increasing dependency on computers, IT systems and technology networks, which, in turn, can sometimes get infiltrated by cybercriminals.

Banks and financial institutions have the largest responsibility in managing cyber risks. Regulators and supervisors have also a critical role to play in advancing robust oversight of cybersecurity risks and disseminating best practices. For that, national regulators and supervisors should continue to deliver guidance to the industry and help raising awareness and educating stakeholders on cybersecurity issues.

And given the borderless nature of cybercrimes, their rapid evolution and complexity, collaboration at the national level between financial services providers, regulators, and the government, should be complemented with an international collaboration to better detect cyber risks, share knowledge and experience, and develop innovative strong and forceful responses to prevent and manage these risks.

On a final note, as we, in the region, face similar risks and are typically being the targets of the same threats, our key recommendation is to create a regional team to collaborate on this issue and elaborate the best security strategy in the region for combatting and defeating the targeted standard, zero day, advanced persistent threats or any sophisticated attacks. We trust that well coordinated actions will have broader and stronger impact on financial stability, financial inclusion and economic sustainable growth in our countries.

References

[1] Basel Committee on Banking Supervision (2017). Sound Practices: Implications of FinTech developments for banks and bank supervisors, Consultative Document, August, 2017.

[2] Charafeddine, R. and L. Daher (2017). Financial Inclusion : Challenges and Opportunities – The Case of Lebanon, prepared for the 2017 AFI Global Policy Forum, Sharm El Sheikh, September 15, 2017.

[3] IMF (2017). FinTech and financial services : initial considerations, IMF Staff Discussion Note, June 2017.

[4] Bank for International Settlements (2017). The BIS 87th Annual Report, 2016/17.

[5] Bank for International Settlements (2017). Financial systems and the real economy, BIS Papers, No.91, BNM-BIS conference on Financial systems and the real economy, Kuala Lumpur, October 16–18, 2016.

[6] Capgemini Consulting (2016). Smart Contracts in Financial Services: Getting from the hype to reality.

[7] Financial Stability Board (2017). Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention, June 27, 2017.

[8] Starnes, S., Kurdyla, M., Prakash, A., Volk, Ariane, and S. Wang (2017). De-Risking and Other Challenges in the Emerging Market Financial Sector: Findings from IFC's Survey on Correspondent Banking, IFC, September, 2017.

[9] IMF (2017). FinTech and financial services : initial considerations, IMF Staff Discussion Note, June 2017.

[10] World Economic Forum (2017). Beyond FinTech: A Pragmatic Assessment Of Disruptive Potential In Financial Services, prepared in collaboration with Deloitte, August 2017.

[11] KPMG International (2017). The pulse of FinTech : Global Analysis of Investment in FinTech, Q4 2016, data provided by Pitchbook updated February 2017.

[12] Wamda and PayFort (2017). State of FinTech in MENA : Unbundling the financial services industry.

[13] Arabnet (2016). Digital Banking Adoption in MENA 2016, in partnership with OMD.

[14] Roux, C. (2015). Cybersecurity and cyber risk, speech by the Deputy Governor of the Central Bank of Ireland to the Society of Actuaries in Ireland Risk Management Conference, Dublin, September 30, 2015.

[15] See : https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8; http://www.bbc.com/news/technology-39913630; https://www.ft.com/content/2394ee58-9997-11e7-b83c-9588e51488a0.

[16] PWC (2017). Global State of Information Security Survey 2017 US Financial services respondents.

[17] Momentum Partners (2017). Cybersecuirty Market Review – Q2 2017. Available at: http://momentum.partners/docs/Quarterly/Cybersecurity_Market_Review_Q2_2017.pdf.

[18] Tüv Rheinland (2015). Cyber Security Trends 2015. Whitepaper. Available at: https://www.tuv.com/media/germany/isec/flyer_2/Cybersecurity_Trends_2015-E_.pdf.

[19] Basel Committee on Banking Supervision (2017). Basel III : Finalising post-crisis reforms, Bank for International Settlments, December, 2017.

[20] Oliver Wyman (2017). Financial Technology and Cyber-risk regulation – Staying on top of things.

[21] Deloitte and Thomson Reuters (2017). Financial Crime in the Middle East and North Africa 2017 – The Need for Forward Planning.

[22] Financial Stability Board (2017). FSB publishes stocktake on cybersecurity regulatory and supervisory practices, Press release, No.38, October 13, 2017.

[23] Microsoft Digital Crimes Unit and Ipsos (2016) . Tech Scams Public Report. Available at: https://mscorpmedia.azureedge.net/mscorpmedia/2016/10/Tech-Scams-Public-Report.pdf.

[24] See: https://www.mimecast.com/solutions/email-security/spear-phishing/.

[25] See: https://cybersecurityventures.com/cybersecurity-market-report/.

[26] See: http://momentum.partners/docs/Quarterly/Cybersecurity_Market_Review_Q2_2017.pdf.

[27] See: https://www.forbes.com/sites/stevemorgan/2016/01/30/why-j-p-morgan-chase-co-is-spending-a-half-billion-dollars-on-cybersecurity/#649be5925991.

[28] See: https://www2.deloitte.com/global/en/pages/financial-services/articles/2015-banking-outlook.html.

[29] See: https://www.infosecurity-magazine.com/news/banks-hit-300-times-more-attacks/.

[30] See: http://investor.shareholder.com/jpmorganchase/secfiling.cfm?filingID=19617-15-367.

[31] See: https://www.forbes.com/sites/stevemorgan/2016/01/27/bank-of-americas-unlimited-cybersecurity-budget-sums-up-spending-plans-in-a-war-against-hackers/#3dc1de4a264c.

[32] See: https://researchcenter.paloaltonetworks.com/2016/06/cybersecurity-more-threats-but-also-more-opportunities/.

[33] Schellen, T. (2017). Cyber(in)securities: Fresh thinking needed to protect the banking system, Executive Magazine, March 15, 2017. Available at : http://www.executive-magazine.com/cybersecurity/cyberinsecurities.

[34] Kaspersky Lab (2012). Gauss : Abnormal Distribution, Kaspersky Lab Global Research and Analysis Team, August, 2012. Available at : https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/kaspersky-lab-gauss.pdf.

[35] Special Investigation Commission of Lebanon (2016). Annual Report 2016.

[36] See : www.iktissadevents.com/events/ACCF/3.

[37] OMSAR (2002). The E-Government Strategy for Lebanon.

[38] IDAL (2017). Incubators/Accelerators in Lebanon 2017.

[39] IDAL (2017). FinTech Sector in Lebanon : Factsheet.

[40] See: https://www.ft.com/content/cff284b0-c0bd-11e7-b8a3-38a6e068f464.

[41] See: http://bdlaccelerate.com/2016/.

[42] BDL IT Department. IT Roadmap (2017).

[43] Rohde, Lars (2017). The future of money and banking, speech by the Governor of the Danmarks Nationalbank (Central Bank of Denamrk) at Aarhus Symposium, November 3, 2017.

[44] Carney, M. (2016). Enabling the FinTech transformation : Revolution, Restoration or Reformation?, speech by the Governor of the central bank of England at Lord Mayor's Banquet for Bankers and Merchants of the City of London, London, June 17, 2016.

[45] Hauser, A. (2017). The Bank of England's FinTech Accelerator : what have we done and what have we learned ?, speech of the Executive Director of Banking, Payments and Financial Resilience at the Bank of England at the meeting for FinTech contacts of the Bank of England's Agency for the South East and East Anglia, Cambridge, October 6, 2017.

[46] Carney, M. (2017). Building the infrastructure to realise FinTech's promise, speech by the Governor of the Bank of England at the International FinTech Conference, Old Billingsgate, April 12, 2017.

[47] OMSAR (2015). Lebanese National Cyber Security Policy Guidelines.

[48] See (in Arabic): https://sic.gov.lb/report/Cybercrime%20Guide.pdf and https://sic.gov.lb/report/Cybercrime%20quick%20reference.pdf.