Financial Law Review

No. 23 (3)/2021

UNIVERSITY OF GDAŃSK • MASARYK UNIVERSITY • PAVEL JOZEF ŠAFÁRIK UNIVERSITY • UNIVERSITY OF VORONEZH
http://www.ejournals.eu/FLR

WAEL SAGHIR*

THE ONLINE AGE: THE SHIFT FROM TRADITIONAL BANKING TO ONLINE BANKING IN THE UK AND ITS EFFECT ON APPLIED REGULATIONS

Abstract

As businesses are actively incorporating technology as means of cost reduction and service provision, financial institutions have lately been one of the most active institutions in utilising information technology (IT) to their advantage.

Although technology presented financial institutions with many opportunities and opened the door for a new hybrid sector to be formed, this came with its share of disadvantages one of which revolves around cyber security. Combined with the complex nature of products and services offered online through non-traditional financial institutions, this meant that adjusting the regulatory framework governing such products, services and institutions has now become a must.

Since the current regulatory framework applicable on online banking does not differ much from that applied on bricks-and-mortar ones especially in terms of money laundering and deposit protection schemes, this paper recommends a hybrid, tech-centred, regulatory framework that is specifically designed to cater for financial institutions in order to offer users of these platforms higher levels of protection and suggests the creation of a joint regulatory and supervisory body that oversees and regulates activities of FinTechs. Such change should take into consideration the higher risk factor

* PhD., Lead for the International Trade, Investment and Corporate Governance Think Tank programme and Junior Fellow at Global Research Network. An International Consultant, Consulting Professor and an expert in international business and financial law with particular interest in foreign investment, governance, sustainability and technology. Member at Society of Legal Scholars, London Court of International Arbitration and Swiss Arbitration Association under 40.
Contact email: wael.s@grn.global, ORCID: https://orcid.org/0000-0002-6684-974X.

associated with online banking and the nature of service provision. The paper in its unique approach aims to inspire and influence change to further enhance customer protection and service provision of online banks.

Key words: Banking Regulation, Online Banking, FinTech.

JEL Classification: G28

1. Introduction

With many corporations looking at the internet as a way of reducing their expenses, and creating better exposure for their products and services, financial institutions have been increasingly active in adopting information technology [IT] as a means of providing better services to their existing customers and, at the same time, reaching a larger customer base.

Due to increased competition over, and demand for, financial services, traditional retail banks have embraced technology and allocated portions of their annual budgets to IT and mobile development [FCA 2014: 4], while other institutions have considered the internet as their primary, and only, interface for their services. Such online providers are referred to as FinTechs. These developments have, in particular, saved operating costs by reducing the need for traditional "bricks-and-mortar" market outlets.

However, these developments have also come with a major downside, as the provision of online services has exposed both financial institutions and customers to an assortment of threats centering on cyber security. This, and the lack of physical presence of FinTech institutions, requires a better understanding of the nature of the laws and regulations that govern the provision of financial services online, particularly as these services raise not only purely financial regulatory questions that are shared with traditional "bricks-and-mortar" institutions but also questions that are driven and dependent on IT. There is a resulting, and growing, need for a better tailored regulatory framework that governs IT based customer services and how FinTechs offer their financial services online.

FinTechs have a higher risk exposure compared to those of traditional banks. Such exposure is centered mostly around the risk of cyber-attacks, as was the case recently with HSBC Bank in Malta which was targeted by a group of hackers in 2018 [Vella 2019].

2. Online Banking v. Traditional Banking

The history of banks dates back more than 700 years with the earliest establishments being founded in Venice under the name of the "Chamber of Loans" [Hildreth 2001: 5].

The Chamber was entrusted with safeguarding merchants' money and was sometimes engaged in buying and selling bills of exchange [Hildreth 2001: 5].

These establishments continued to evolve leading to private bankers providing modern day banking activities. Private bankers managed money affairs on behalf of individuals and countries and received money on deposits [Hildreth 2001: 10]. Additionally, they bought and sold bills of exchange and coins [Hildreth 2001: 10].

This sector is renowned for embracing technology to offer their services and as such, it is important to understand the transition from traditional banking to online banking and how the two differ.

2.1. Traditional banking

According to the Oxford Dictionary, a bank is a "financial establishment that uses money deposited by customers for investment, pays it out when required, makes loans at interest, and exchanges currency" [Oxford Dictionary]. It is therefore understood that banks are institutions that grant credit and receive deposits that are invested into loans. These institutions make profit through charging interest on loans they grant.

Today, commercial banks accept deposits for safekeeping, provide loans and issue payment options such as debit and credit cards [BoE Online]. Investment banks on the other hand mainly trade with shares, foreign currency and other commodities in financial markets [Banking Act 2009, Financial Services and Markets Act 2000 Order 2001].

Banks have been constantly embracing advances in IT. For example, they pioneered telephone banking services, and, after the introduction of the internet, banks began to provide range of services online through internet banking, providing traditional banking services electronically via the internet [Gkoutzinis 2006: 8].

Utilisation of the internet to provide day-to-day banking services could perhaps be regarded the cornerstone of today's online banking and the rise of FinTechs.

2.2. Online banking

As the internet became more accessible through mobile phones and with the introduction of mobile applications, banks and other financial institutions saw in this medium an opportunity to further provide their services to their customers and be more accessible. Such accessibility is currently known as Mobile Banking. All these means of service provision may be referred to as Home Banking since customers may gain access remotely to the services they require [Gkoutzinis 2006: 8].

Internet, or online banking, allows customers to access their accounts virtually, make transactions including money transfer, bill payments, check deposits and allows customers to apply for loans and for credit cards and allows them to request bank statements [Natwest Online, HSBC Online, Lloyd's Bank Online, FCA 2014: 4].

Moreover, many financial institutions are utilising technology to reduce transaction costs and to offer a range of products and services to different customers without having a physical presence that requires the customer to visit a physical outlet [Gupta 2013: 3]. They saw in technology a medium of which would allow them to reach new and wider markets and even larger access to capital [Gkoutzinis 2006: 15]. Such institutions are known as FinTechs and they are defined as "computer programs and other technology used to support or enable banking and financial services" [Oxford Dictionary].

Generally, FinTechs provide peer-to-peer lending, online payments, foreign exchange services, digital wallets, e-money and automated investment advice among other products and services [Deloitte 2018: 4, Ofcom and PSR 2014: 51-62]. They could also provide mobile investing services and issue cryptocurrencies.

It is noted that banks with physical presence like HSBC, Lloyd's and Natwest to name a few, were among the financial institutions embracing mobile banking. However, competition from online banks has been recently increasing with banks like Monzo and Monese providing banking services to customers purely online. These online banks have a competitive edge over traditional banks given the lack of physical presence where online banks are able to offer better interest rates to customers than traditional banks [Durisin 2013].

2.3. Criticism of online banking

Although technology is helping customers conduct their banking with greater ease, these banks are not, however, shielded from criticism especially when technology fails both customers and financial institutions. These criticisms take two major directions. The first is centred around the adequacy of the technology the bank uses and the second centres around the delivery of the service to customers of specific age groups.

Reliance on cyber banking methods has caused occasional outages to provision of online banking services. For example, the Royal Bank of Scotland [RBS] admitted to outages caused, as the bank's CEO reported, to changes in the technology used by the bank [Reuters Online].

Another common criticism of online banking is that it does not provide the same level of reassurance as brick-and-mortar banks, especially for elderly customers, who may also feel uneasy using the small screens of mobile devices for online banking [Georgieva 2018, 4].

3. The regulatory framework governing the banking sector

The financial sector went through numerous changes in how it is regulated. From deregulation to being actively regulated, this sector's regulatory framework and supervisory authority received major shakeups in the wake of the financial crisis in 2008.

What is noted, however, is that the regulatory framework governing this sector has not been actively following up advances in technology and resulting changes in the provision of services. From here, it is important to understand the regulatory framework applicable on this sector and to examine how FinTechs and online banks are regulated before examining the challenges facing online banks.

3.1. How the banking sector is governed

In general, banks in the United Kingdom are subjected to specific regulations and their activities are regulated by the Bank of England (BoE), the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA), which is also responsible for overseeing banks (BoE Online).

Banks are expected to be in conformity with the Financial Services Markets Act of 2000 [FSM], the Banking Act of 2009, the Banking Reform Act of 2013, Bank of England and Financial Services Act 2016, the Payment Services Regulations 2017, the Consumer Credit Act 1974 the PRA Rulebook, the FCA's Handbook and the Payment Services Regulations 2017. Additionally, the UK banking sector is regulated by EU regulations like the EU Benchmark Regulation (BMR) No. 2016/1011.

As innovation gained pace during the last decade, investors began to optimise their services and to fully utilise the internet for their benefit. Financial institutions expanded their service base and offered products and services online resulting in a serious of regulatory challenges. Nevertheless, financial services offered online were still subjected to the same regulations covering brick-and-mortar institutions.

3.2. The framework applied to online banks and fintechs

UK regulators are catching up through the use of what is currently referred to as Regulatory Sandboxes. Sandboxes are specifically created environments that allow businesses to test their innovations and are neither protected within a specific regulatory framework nor supervised by any agency [Thew 2018, Deloitte 2018: 6, FCA Online]. The UK's approach in this respect is regarded as a principles-based approach to regulation where regulations are focused more on outcomes which allows for more flexibility in delivering services [Hill 2018: 310].

Nevertheless, the mere fact that these Sandboxes are testing grounds does not mean innovators should be granted absolute freedom without supervision or minimum standards to adhere by. Perhaps this is why the FCA's principles-based approach was criticised for not prescribing certain minimum standards [World Economic Forum 2016: 14]. In essence, these Sandboxes are assumed to help start-ups understand how they are expected to comply with applied financial regulations [Thew 2017]. They are not, however comprehensive regulations that apply specifically to online financial institutions. This is especially true since these Sandboxes are considered as training grounds for innovators who are expected to provide their products and services in conformity with regulations generally applied to brick-and-mortar institutions.

Upon closer inspection, it is noted that online banks are partially regulated by the FCA [FCA 2014: 6]. Furthermore, certain financial activities in which online banks and other online financial institutions may be involved in is subject to different regulations. For instance, money transfer through online platforms is regulated by the Payment System Regulator (PSR), which, in turn, is a subsidiary of the FCA [Payment Services Regulations 2017, FCA Online, FCA Consultation Paper 2014: 7]. Moreover, the PSR also regulates issuers of electronic money which, according to the UK's Electronic Money Regulations of 2011, refers to electronically and magnetically stored monetary value as represented by a claim on the electronic money issuer which is issued upon receiving funds for the purpose of making a payment; and is accepted by a party other than the electronic money issuer [Electronic Money Regulations 2011]. Online financial institutions are additionally required to adhere by the Data Protection Act 2018.

This is especially true since many FinTechs, like Revolut for instance [Revolut Online], began to trade and provide their services to customers while awaiting to be awarded their full licence by the FCA. This means that, even though they are still regulated by the FCA, customers' deposits are not yet covered by the Financial Services Compensation Scheme.

3.3. Challenges facing online banks

In general, one of the main concerns in the financial sector is the issue of money laundering and as such, this matter has been subject to increased regulations. Certainly, with the continuous rapid growth of online banking and the FinTech sector, this creates its own challenges particularly in the sphere of cyber security where organised crime groups are using unregulated cryptocurrency exchange to hide the source of their illegal money especially since these technologies do not store information about account holders. This matter requires special attention especially since FinTechs voiced their concern regarding the effectiveness of current regulatory framework for combatting financial crime [The Economist 2019; 3]. The issue of digital money laundering is especially apparent in what is referred to as transaction laundering where launderers use details of an authorized merchant's payment credentials to process payments for unknown products. In terms of FinTechs and challenger banks, these institutions could be infiltrated by criminal organisations through mule accounts which are accounts created using stolen identities or it could even be genuine accounts whose owners allowed criminal organisations to use them to hide their illicit source of funding and digitally cleanse their money.

Given the complexities of regulations governing financial institutions and especially FinTechs, the need to constantly monitor regulatory changes and compliance equally has increased. This, in turn, has resulted in a new form of start-ups focused on monitoring these changes known as Regulatory Technology or, RegTech [Hill 2018: 312]. RegTech is concerned with the creation of applications and programmes to monitor and enforce compliance [UNSGSA, CCAF 2019: 8].

Given the constant changing nature of technology and the complexities of financial products and services that are equally evolving at a fast rate, it is important that financial products and services offered online have their own regulatory framework and supervisory body to ensure the minimum proper protection of customers' information and property. Such a framework would apply to any institution offering its services online.

As there is no specified regulatory framework applicable to online banks, some provisions applicable on brick-and-mortar banks still apply to online banks creating confusion for FinTechs and online banks, making understanding what governs their activities more challenging. As such, it is important to have a unified regulatory framework that specifically governs online mobile banking and FinTechs.

Looking deeper into online banks, one can notice major risks that online banks are exposed to more than traditional banks such as fraud, identity theft and data breach [Bouveret

2018: 13-15]. Such threats to customers' identity and property can be considered as cyber risk. In general, online banks are more prone to cyber risk than physical banks. This is possibly true given the fact that financial institutions are, in general, dependent on highly interconnected networks [Bouveret 2018: 11]. What is notable, however, is that even traditional banks, nowadays, are exposed to cyber risk given that customers' data are stored virtually.

Banks, in general, have been subject to many cyber-attacks resulting in huge monetary losses and in access to customers' information. For example, earlier in 2019, Metro bank was targeted by hackers who emptied customers' accounts through targeting verification codes sent to customers via SMS [Bernal 2019].

Cyber-attacks targeting banks do not only result in financial or data loss, they could also result in business disruption and suspension of services due to technological challenges [Bouveret 2018: 12]. For instance, Monzo, the online bank, encountered difficulties in providing its service due a technical issue [Griffen 2019]. Customers reported their inability to make payments using cards provided by the bank while others suffered from having their accounts completely "disappearing" [Griffen 2019].

As it has been recorded in a study by Ofcom, one of the main contributors to the slow growth of online payments was security and privacy concerns which form part of the cyber risk. The study found that around "One in three non-users in the UK stated they were concerned about privacy and control of their personal data (33%)" [Ofcom 2014: 59].

Given that online banks and traditional banks offer similar products and services, regulators did not introduce newly designed regulations to govern online banking rather they opted to apply regulations governing the traditional banking sector.

4. The way forward in regulating online banking

It is just as important for regulators to understand the technical nature of mobile and online banking as they understand the financial and legal aspects of it. This will result in designing a more comprehensive customer-protection oriented regulatory framework especially since regulators are expected to be up to date with the changing environment of the sector and to be quick in responding to the technological changes and innovation in the sector [Abrams, Taylor 2003: 4].

4.1. A new regulatory framework

Regulations should take into consideration the fact that online financial services providers are exposed to higher risk and as such their capital requirement and compensation schemes should equally be different. This means FinTechs' required regulatory capital should be more than the 8% held by traditional banks and their contribution, or annual levy, to the compensation scheme should be higher than traditional banks. This also means that regulations governing institutions utilising a hybrid of brick-and-mortar and online product and service provision should be different than those offering their products and services purely online.

In essence, banks that utilise both brick-and-mortar and online provision of service, in matters other than the capital requirement and compensation schemes, should primarily be governed by the current regulatory framework and to the special framework applied on FinTechs.

Moreover, as there is currently a movement heading towards special regulations governing FinTechs, it is of importance that regulators keep in mind technical issues related to data storage and provision of service where regulators are expected to design a minimum technical standard for provision of online banking services that financial institutions are expected to follow. Additionally, they are expected to specify the minimum standard of data protection these institutions are required to hold especially in terms of cyber security standards.

Leaving such matters unregulated or leaving them for the discretion of financial institutions through means of self-regulation may be a double-edged sword where it could arguably lead to a crisis in the sector [Kaminsky, Schmukler 2003: 2].

Regulating FinTechs does not necessarily entail burdening the creativity and service-offering of the sector nor does it mean creating caps on the profit margins investors are keen on making, rather, it means giving the sector minimum standards within which innovators and investors are required to work within. This will arguably encourage and incentivise investors to compete in providing their products and services, by exceeding the minimum cited threshold by the regulator [Crisanto, Prenio 2017: 4].

However, regulating the sector does not mean neglecting self-regulation where the latter is expected to achieve conformity with the former especially since innovation in the sector is manifesting itself at an increased pace in which it would present regulators with a difficult task in following or anticipating these changes. Self-regulation is particularly important given that it remains an integral part of the UK's start-up environment with over than 90% of digital lenders voluntarily joined the Peer-To-Peer Finance Association [P2PFA] [World Economic Forum 2016: 23]. As such, it would be wise for regulators to capitalise on this self-initiative and use it to their advantage.

4.2. A joint supervisory authority

A further recommendation is separating the FinTech sectors' supervision into different parts, each supervised by a specialist agency, given the complexity of the environment in which the products and services are offered. For example, supervising online banking should be entrusted to a specialist agency which is different from that entrusted with supervising the issuance of, and trade with, cryptocurrencies. This is exemplified by the regulatory environment implemented in Chile where the insurance and banking sectors are supervised by different agencies [Abrams, Taylor 2003: 4].

Regulators mainly need to consider how financial innovation interacts with regulatory objectives [UNSGSA, CCAF 2019: 14]. They also need to assess the limit of cyber risk associated with FinTechs, operational and data risks, product risk, cross-border regulatory risks and governance and disclosure risks [FSB 2017: 2-3].

Additionally, as FinTech has a multifaceted nature where it encompasses the provision of financial products and services through mainly utilising information technology, the regulatory framework that governs this sector needs to meet the varied nature of this sector [Crisanto, Prenio 2017: 5].

Regulating and overseeing FinTechs should be jointly made by the financial regulator and the communications regulator since the latter is entrusted with regulating mobile applications and airwaves. This does not necessarily mean having different regulatory bodies working independently, rather, both regulators should join forces and form a single regulator overseen by both agencies. This is particularly necessary since the communications regulator in the UK, Ofcom, has stated that it might have the capacity to regulate certain aspects of FinTech's services [Ofcom, PSR 2014: 9] and since financial regulators are not technology experts in most cases [UNSGSA, CCAF 2019: 15].

Although the FCA is collaborating with the Innovation Hub on matters related to regulatory changes [UNSGSA, CCAF 2019: 20], it is, however, still necessary that the FCA joins forces with Ofcom in setting up a joint regulatory force that regulates and jointly supervises the proper implementation of suggested new regulations.

5. Concluding remarks

As the IT sector is continuously developing, so too is the financial sector, where institutions are increasingly offering their services either partially or fully online. Banks, in particular, have been increasingly involved in innovation within the FinTech sector and this, in turn, has resulted in an increased number of risks for customers.

Due to increased innovation in the FinTech sector, the UK has set up specialised offices that advise on regulatory changes in the field and has introduced Regulatory Sandboxes to allow innovators to test their products and services first-hand without increased red tape. These movements have been mainly directed at the FinTech sector at large without taking into consideration the different risks associated with each type of financial service provided and without taking into consideration proper knowledge of the technology behind provision of products and services or proper cyber risk allocation. This is especially true since, as it stands, online banks are still subjected to prior authorisation from the PRA and are regulated by both the FCA and the PRA.

Although regulation governing brick-and-mortar banks could be applied to online banks, this doesn't mean that they would be effective. There is a need to have knowledgeable regulators who understand the nature of financial products and services and, at the same time, the nature of the technology used to offer such products and services. This can be effectively achieved in the UK if the FCA, BoE and Ofcom were to join forces and create a single supervisory and regulatory body that regulates and oversees the regulation of FinTech sector in general. Additionally, this new regulatory body would have sub-committees each in charge of a different aspects of the FinTech sector. For example, one can oversee online banks while the other could be in charge of online insurance.

Such a structure will help in creating more enhanced regulatory framework within which FinTechs could operate, ensure a higher level of customer protection and would reduce the risk of a financial crises caused by this emerging sector.

References

A new regulatory framework for payment systems in the UK, Financial Conduct Authority Payment System Regulators, Consultation Paper PSR CP14/1, November 2014.
Available at:
https://www.fca.org.uk/publication/other/psr-cp14-1-cp-a-new-regulatory-framework-for-payment-systems-in-the-uk.pdf, accessed: 31st July 2019

Abrams, R. K. and Taylor, M., Issues in the Unification of Financial Sector Supervision, IMF Working Papers December 2003.

Bernal, N.: Metro Bank Hit by Cyber Attack Used to Empty Customer Accounts, 1st February 2019 (The Daily Telegraph Online)
Available at:
https://www.telegraph.co.uk/technology/2019/02/01/metro-bank-hit-cyber-attack-used-empty-customer-accounts/, accessed: 29th July 2019

Bouveret, A.: Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, IMF Working Papers WP/18/143 (2018).

Crisanto, J.C., Prenio, J.: FSI Insights on policy implementation No 2: Regulatory Approaches to Enhance Banks' Cyber-Security Frameworks, Bank for International Settlements 2017

Durisin, M.: Here's Why Online Banks Are Better Than Traditional Banks', 6th May 2013, Business Insider Online
Available at:
https://www.businessinsider.com/online-bank-vs-traditional-banks-2013-5, accessed: 29th July 2019

Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandbox and RegTech, FinTech Working Group of the United Nations

Financial Stability Implications from FinTech: Supervisory and Regulatory Issues Raised by FinTech that Merit Authorities Attention, Financial Stability Board, June 2017
Available at: https://www.fsb.org/wp-content/uploads/R270617.pdf, accessed: 30th July 2019

FinTech: Regulatory Challenges and Financial Crime Exposure, Deloitte, Issue 11/2018
Available at:
https://www2.deloitte.com/content/dam/Deloitte/de/Documents/finance/Deloitte_FinTech.pdf, accessed: 28th July 2019.

Georgieva L.: Digital Inclusion and the Elderly: The Case of Online Banking (2018).
Available at: http://lrec-conf.org/workshops/lrec2018/W14/pdf/2_W14.pdf, accessed: 1st March 2020

Griffen, A.: Monzo Down: Cards Stop Working as App-Powered Bank Hit by Technical Problems 29 July 2019th (The Independent Online).
Available at:
https://www.independent.co.uk/life-style/gadgets-and-tech/news/monzo-down-not-working-card-payments-broken-fail-transactions-a9025326.html, accessed: 29th July 2019

Gkoutzinis, A., Internet Banking and the Law in Europe: Regulation, Financial Integration and Electronic Commerce, Cambridge: Cambridge University Press, 2006

Gupta, S.: The Mobile Banking and Payment Revolution, The European Financial Review (February-March 2013)
Available at:
https://www.hbs.edu/faculty/Publication%20Files/The%20Mobile%20Banking%20and%20Payment%20Revolution1_b37fc319-e15f-46c8-b2f9-c0d4c8327285.pdf, accessed: 31st July 2019

Hildreth, R., The History of Banks: To Which Is Added, a Demonstration of the Advantages and Necessity of Free Competition In the Business of Banking, Kitchener: Batoche Books, 2001

Hill, J.: Fintech and the Remaking of Financial Institutions, Cambridge: Elsevier Academic Press, 2018

Innovation in UK Consumer Electronic Payments: A Collaborative Study by Ofcom and the Payment Systems Regulator', Ofcom and PSR, 13th November 2014.
Available at:
https://www.psr.org.uk/sites/default/files/media/PDF/ofcom-psr-joint-study.pdf, accessed: 31st July 2019.

Kaminsky, G. L., Schmukler, S. L.: Short-Run, Long-Run Gain: The Effects of Financial Liberalization, National Bureau of Economic Research, June 2003. NBER Working Paper Series, Working Paper 9787
Available at: https://www.nber.org/papers/w9787, accessed: 30th July 2019
Mobile Banking and Payments Thematic Review, Financial Conduct Authority (FCA), September 2014
Available at:
https://www.fca.org.uk/publication/thematic-reviews/tr14-15.pdf, accessed: 29th July 2019
On the Frontline: FinTechs vs Money Laundering, 4th June 2019 (The Economist White Paper).
Available at:
https://eiuperspectives.economist.com/sites/default/files/money-laundering-exposed-fintech-wp-uk_1.pdf, accessed: 1st of January 2020
Rummney E., White L.: MPs criticise RBS and Barclays for online banking outages, 21st September 2018 (Reuters Online)
Available at:
https://uk.reuters.com/article/uk-natwest-outages/mps-criticise-rbs-and-barclays-for-online-banking-outages-idUKKCN1M10NN, accessed: 1st March 2020
The Complex Regulatory Landscape for FinTech An Uncertain Future for Small and Medium-Sized Enterprise Lending, World Economic Forum White Paper, 2016
Thew, O.: What is a Regulatory Sandbox?, BBVA Online, 20th November 2017
Available at:
https://www.bbva.com/en/what-is-regulatory-sandbox/, accessed: 27th July 2019
Thew, O.: UK Leads Global FinTech Regulation: Sandboxes and FinTech Bridges Drive Innovation, OMFIF Online, 25th April 2018
Available at:
https://www.omfif.org/analysis/commentary/2018/april/uk-leads-global-fintech-regulation/, accessed: 27th July 2019
Vella, M.: HSBC warned of BOV hackers last year, 11th March 2019 (MaltaToday Online)
Available at:
https://www.maltatoday.com.mt/news/national/93525/hsbc_warned_of_bov_hackers_last_year#.XTzP2i2ZOuU, accessed: 27th July 2017

Legal Acts

United Kingdom's Banking Act 2009
Available at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945165/SRR_CoP_December_2020.pdf, accessed: 21st of April 2020
United Kingdom's Electronic Money Regulations of 2011
Available at: https://www.fca.org.uk/publication/archive/emoney-approach.pdf, accessed: 1st March 2020
United Kingdom's Financial Services and Markets Act 2000
Available at: https://www.legislation.gov.uk/ukpga/2000/8/contents, accessed: 21st of April 2020
United Kingdom's Payment Services Regulations of 2017
Available at: https://www.legislation.gov.uk/uksi/2017/752/pdfs/uksi_20170752_en.pdf, accessed: 1st March 2020

Other Official Documents

Action Plan for Anti-Money Laundering and Counter-Terrorist Finance, HM Treasury, April 2016.
Available at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/517992/6-2118-Action_Plan_for_Anti-Money_Laundering__web_.pdf, accessed: 1st March 2020
International Communications Market Report, Ofcom, Research Document (11 December 2014)
Available at:

https://www.ofcom.org.uk/__data/assets/pdf_file/0030/26796/icmr_2014.pdf, accessed: 31st of July 2019

Secretary-General's Special Advocate for Inclusive Finance for Development (UNSGSA) and Cambridge Centre for Alternative Finance (CCAF), (2019).
Available at:
https://www.unsgsa.org/files/2915/5016/4448/Early_Lessons_on_Regulatory_Innovations_to_Enable_Inclusive_FinTech.pdf> accessed: 31st July 2019

Ring-Fencing Information Policy Paper, HM Treasury, 24 March 2017
Available at: https://www.gov.uk/government/publications/ring-fencing-information/ring-fencing-information, accessed: 1st of March 2020

Internet Resources

Financial Conduct Authority
Available at:
https://www.gov.uk/government/organisations/financial-conduct-authority, accessed: 1st March 2020

Internet Banking, Lloyd's Bank Online
Available at:
https://www.lloydsbank.com/online-banking/benefits-online-banking.asp?WT.ac=NavBarTop/Navigation/SNOBB1012, accessed: 28th July 2019

'Is Money Safe?', Revolut Online
Available at: https://www.revolut.com/help/more/security/is-my-money-safe, accessed: 24th December 2019

Mobile Banking, HSBC Online
Available at: https://www.hsbc.co.uk/ways-to-bank/mobile/, accessed: 28th of July 2019

'Payment Services Regulations and Electronic Money Regulations', (Financial Conduct Authority Online), published 22 November 2015 and Updated 13 January 2018
Available at:
https://www.fca.org.uk/firms/payment-services-regulations-e-money-regulations> accessed: 31st July 2019

Supervision (Bank of England Online)
Available at:
https://www.bankofengland.co.uk/prudential-regulation/supervision, accessed: 29th July 2019

'Regulatory sandbox' (Financial Conduct Authority Online, first published 11 May 2015 and updated 29 April 2019)
Available at:
https://www.fca.org.uk/firms/regulatory-sandbox, accessed: 31st July 2019

The Oxford Dictionary Online
Available at: https://www.lexico.com/en/definition/bank#h69849199471760, accessed: 28th July 2019

Ways to Bank: Online Banking, Natwest Online
Available at:
https://personal.natwest.com/personal/ways-to-bank/online-banking.html#discolb, accessed: 28th July 2019

'What do Banks do?', Bank of England Online
Available at:
https://www.bankofengland.co.uk/knowledgebank/what-do-banks-do, accessed: 28th July 2018

'Which firms does the PRA regulate?' (Bank of England Online)
Available at:
https://www.bankofengland.co.uk/prudential-regulation/authorisations/which-firms-does-the-pra-regulate, accessed: 29th of July 2019