Regulating virtual banks: towards a technology-centric regulatory approach

Article

Published Version

REGULATING VIRTUAL BANKS: TOWARDS A TECHNOLOGY-CENTRIC REGULATORY APPROACH

Dr. Law Sau Wai *

ABSTRACT

*This article examines the legal aspects of virtual banking as a fintech ("**Financial Technology**") platform. It emphasizes the need for a thorough review of the regulatory framework governing virtual banking, focusing on its organizational structure, business scope, and operational model. The article argues that the current technology-neutral regulations are inadequate in addressing the long-term effects of technology in the banking sector. Therefore, it proposes a technology-centric framework specifically designed for virtual banking, which would govern the use of devices, software, and online dispute resolution channels. This framework would enable both banks and regulators to regain control over technology implementation, effectively managing virtual banking risks and challenges while ensuring regulatory oversight and accountability. The article is based on extensive legal analysis conducted internationally, with a focus on the Asia region where virtual banking licenses are prevalent, and incorporates insights from interviews with virtual bank executives. The article aims to provide a comprehensive overview of the distinctive features of virtual banking and its regulatory landscape, and to identify the need for a tailored framework that safeguards the integrity and security of virtual banking operations.*

Keywords: Virtual Banking, Bank Digitalization, Financial Technology, Cyber Law.

TABLE OF CONTENTS

* *Dr. Law Sau Wai serves as a Lecturer (Assistant Professor) specializing in Corporate and Commercial Law, at University of Reading, United Kingdom.*

I. REGULATING TECHNOLOGY IN BANKING

The rapid advancement of financial technology has paved the way for virtual banking, a digital-only platform that offers a wide array of financial services to customers. While virtual banking presents numerous benefits, including increased accessibility and convenience, it also brings forth a pressing issue: the absence of specific laws and regulations governing its operations. This article reviews the current virtual banking regulations, considers the challenges posed by the current technology-neutral regulatory landscape, and distinguishes the need for technology-centric regulation and promises for the overall structure of such a framework.

The international landscape of virtual banking is rapidly evolving, and policymakers, regulators, and practitioners rely on valuable resources from organizations such as the Bank for International Settlements ("**BIS**") to navigate this complex domain. The BIS, through its various committees and publications, provides comprehensive insights into the regulation and governance of virtual banking.

One focus is on fintech financing, which encompasses digital banks and fintech platforms. The BIS's Financial Stability Institute ("**FSI**") has published a paper called "Regulating Fintech financing: digital banks and fintech platform" that delves into the regulatory aspects of fintech financing.[1] This paper explores new technology-enabled business models related to deposit-taking, credit intermediation, and capital-raising. It covers topics such as digital banking-specific licensing frameworks, initiatives to facilitate market entry, fintech balance sheet lending, and crowdfunding. It covers five major areas: data privacy; money laundering; cyberattacks; customer protection; and investor confidence. Whilst it is acknowledged that the delivery of the banking services of digital bank

[1] Johannes Ehrentraud et al., *Regulating Fintech Financing: Digital Banks and Fintech Platforms,* BIS (Aug. 27, 2020) https://www.bis.org/fsi/publ/insights27.pdf.

is over the internet, which is clearly different from traditional banks,[2] the issues arising from the delivery channel have not been investigated in depth.

Another crucial aspect is cryptocurrencies. The Basel Institute on Governance has produced a working paper, "Regulating cryptocurrencies: challenges and considerations", that explores the legal and regulatory dimensions of cryptocurrencies.[3] This publication provides insights into government policies, enforcement actions, and case studies related to crypto assets. As virtual currencies gain prominence, understanding the legal and regulatory challenges presented is vital for policymakers and regulators seeking to strike a balance between innovation and consumer protection. Yet, the very purpose of cryptocurrencies is to avoid centralized governance from banks or regulators; it is very difficult to enforce issues on fraud, money laundering, and other illicit practices when the legal nature of cryptocurrency remains undetermined in most jurisdictions.[4]

The Basel Committee on Banking Supervision ("**BCBS**"), as the primary global standard setter for prudential regulation, plays a pivotal role in shaping the international landscape of virtual banking. The BCBS's publications cover a wide range of topics relevant to banking supervision. These include capital adequacy, accounting standards, cross-border issues, core principles for effective banking supervision, credit risk, market risk, money laundering, operational risk, and transparency and disclosure. Notable publications include Basel III, which addresses capital adequacy, market risk, and liquidity, providing a comprehensive regulatory framework for banks. Additionally, the BIS's Committee on Payments and Market Infrastructures ("**CPMI**") focuses on ensuring the safety and efficiency of payment and market infrastructures. Their publications cover principles for financial market infrastructures, payment systems, securities settlement, and retail payment instruments. By establishing robust frameworks for payment systems and market infrastructures, the CPMI contributes to the stability and resilience of the virtual banking ecosystem. The Committee on the

---

[2] *Id.* at 9-10.

[3] Federico Paesano, Regulating Cryptocurrencies: Challenges and Considerations (Basel Inst. on Gov., Working Paper 28, 2019), https://baselgovernance.org/sites/default/files/2019-06/190628%20Working%20Paper%20Cryptocurrency%20Regulations.pdf.

[4] Bejan, C.A. et al., *Considerations About the Regulatory Framework of Cryptocurrency,* 159 (IE 2023).

Global Financial System ("**CGFS**"), another BIS committee, assesses global financial market stability and structural underpinnings. Their publications explore various aspects of international banking, financial crises, risk management, market liquidity, and more. By examining the systemic risks associated with virtual banking and analyzing the structural foundations of global financial markets, the CGFS provides valuable insights for policymakers and regulators. Lastly, the Irving Fisher Committee on Central Bank Statistics ("**IFC**") promotes discussions on statistical issues relevant to central banks. By strengthening the relationship between data compilers and users, the IFC enhances the quality and availability of statistical information crucial for understanding the international financial system. Whilst they are all applicable to virtual banking, none of them directly addresses the presence of virtual banking platforms.

The international landscape of virtual banking is complex and dynamic due to its mobility. Organizations like the BIS, through its committees and publications, offer invaluable resources covering the products and services that could apply to virtual banks. By leveraging these insights, stakeholders can navigate the evolving landscape of virtual banking, ensuring both innovation and stability in this rapidly changing sector. However, these efforts fail to question the current regulatory practice of using the established regulations that cover traditional banks and applying them to virtual banks. The regulation of the digital platform itself is not explicitly governed.

This article investigates the regulation of virtual banking platforms. Asia has emerged as a prominent region with a higher number of virtual banking licenses compared to the Western counterparts. This allows us to identify the distinct features of virtual banking regulation through licensing only. This article is a result of an extensive comparative study, evidenced with focus group findings between March 2021 and October 2022 conducted with retail banking clients, senior executive, investors and bank executives of virtual banks. These interviews provided valuable insights into the distinct regulatory challenges and opportunities specific to virtual banks operating in Asia. By combining the expert perspectives with a rigorous analysis of the regulatory landscape, this paper aims to provide an Asia-specific overview of the regulatory framework of virtual banking and contributes to the scholarly understanding of the evolving

virtual banking regulatory landscape. It also advocates for a new regulatory technology-centric framework that should be adopted in this digital era.

II. CURRENT REGULATORY LANDSCAPE OF VIRTUAL BANKING

Terms such as virtual banks, digital banks, challenger banks, or internet banks are used interchangeably in different jurisdictions. They usually provide virtual-only core banking services like deposit-taking, payments, lending and investments. When delivering hitherto conventional banking services, providing better value propositions, or enriching customers' experiences when interfacing online with banking services, the use of powerful and innovative technical solutions like AI, blockchain, IoT, data analytics enable virtual banks to operate without needing to have physical bank branches and need fewer resources, thereby providing cost savings that can be passed on to consumers.[5]

However, the convergence of innovative technology and banking may give rise to new risks in virtual banks. For example, the adaptation of Application Programming Interfaces ("**APIs**"), which involve collaborations with third parties in hosting systems on virtual private clouds, could trigger privacy data issues when managing customers' personal data. Further, the deployment of cloud technology outside of the jurisdiction of the main operation may contribute to cross-border data transfer issues. Engagement with third parties may also enhance exposures to cyberattacks and cybercrimes.[6]Reliance on third party devices and software in delivering these platforms should not be ignored as banks would have no control over any malfunctioning of third-party devices and software.[7]

Considering these new kinds of risks arising from collaborative activities with third parties, closer cross-border cooperation with other major fintech hubs across the world could be helpful for addressing associated operating risks linked to virtual-only banking activities. However, virtual banks licenses may not

[5] Peter Yeoh, *An International Regulatory Perspective of Digital Banks*, 41(6) BUS. L. REV. 205, 213 (2020).
[6] *Id.*
[7] Law, S., *Promoting Financial Inclusion Through the Launch of Virtual Banks? Empirical Insights from Hong Kong Banking Customers,* 37(11) J. I. B. L. R. 429, 439 (2022).

facilitate collaboration between banks and other non-banking entities. One example is DBS Singapore, which sets up subsidiaries to run all its virtual-only operations to segregate them from its main operations.[8] Increasingly, virtual banks emerge as partnerships between big tech platforms with a huge clientele base and conventional banks.[9]

Therefore, regulatory authorities generally keep close vigilance over virtual banking activities but might overlook the impact on the wider financial system arising from collaboration with non-banking third parties not regulated under the existing regulatory regime. The use of emerging technologies to disrupt conventional banking activities may also bring unforeseen operational risks, as well as linkages to nefarious activities like money laundering, tax evasion, and the transactions of illegal products. Thus, virtual banks are regulated similar to that of conventional banks and are subject to expensive banking regulatory compliances after a license is granted.[10] Yet, not all jurisdictions have virtual banking licenses. Whilst most jurisdictions, such as United Kingdom, United States, China, and the European Union apply established banking laws and regulations to virtual banks,[11]those that grant licenses to virtual banks under a specific regulatory framework are mostly, if not all, in Asia *(Table 1)*

Table 1: Regulation of virtual banking in selected jurisdictions

Specific Virtual Banking Licensing and Regulatory framework	Virtual Banking regulated under general regulatory framework
Hong Kong, Chinese Taipei, Korea, Singapore, Malaysia, the Philippines, Pakistan	Argentina, Australia, Brazil, Canada, China, Dominica, European Union, Japan, Indonesia, New Zealand, Nigeria, Russia, South Africa, United Kingdom, United States

[8] DBS, *Driving Digital Transformation Through Partnerships,* DBS BANK (May 2020) https://www.dbs.com.sg/corporate/insights/driving-digital-transformation-through-partnerships.

[9] Yeoh, *supra* note 5.

[10] Bank for International Settlements, *supra* note 1 at 12.

[11] *Id.* para 1, para 16. *See also,* Alliance for Financial Inclusion, *Policy Framework on the Regulation, Licensing and Supervision of Digital Banks*, AFS (Nov. 23, 2021) https://www.afi-global.org/wp-content/uploads/2021/11/DFSWG-framework_FINAL.pdf.

Source: *Alliance for Financial Inclusion*[12]

Notable financial centers like Hong Kong and Singapore have designed special licensing regimesthrough licensing requirements, together with the use of established regulations, unlike those in Anglo-Saxon/European economies that rely on the use or adaptations of established laws and regulations. Further, Asian jurisdictions that are particularly active in the deployment of exponential technologies in financial services take the position that virtual-only banks should obtain an additional license for non-traditional banks. The rationale that non-financial institutions, such as big tech platforms, could become majority shareholders of virtual banks and participate in the core aspects of banking activities, and hence bank regulators should review their capacities before allowing entry.[13]However, this explanation may not justify why established laws and regulations could not serve the same purpose when covering virtual-only banking platforms, and it does not provide a rationale for mandating the need for an additional license.

III.THE THREE DISTINCT FEATURES OF A VIRTUAL BANK LICENSE

The original initiative to license virtual banking was to ease the entry barriers for market participants.[14]There are three specific requirements that are distinctly applicable to a virtual banking license, which relates to ownership and control, business scope and operational model.

A. ORGANIZATIONAL STRUCTURE– OWNERSHIP

A virtual bank incorporated in Hong Kong should be majority owned by a bank or financial institution, or through a holding company incorporated in Hong Kong, that is also subject to capital adequacy. A similar requirement exists in Singapore where, for a DFB, the company must be controlled by Singaporeans and headquartered in Singapore. Foreign businesses can apply for

[12] *Id.* at 14.
[13] Yeoh, *supra* note 5.
[14] Deloitte, *Development of Digital Banking License Framework in Asia Pacific*, DELOITTE (Dec. 27, 2019) https://www2.deloitte.com/content/dam/Deloitte/my/Documents/risk/my-risk-regulatory-requirements-digital-banks.pdf.

this license, provided they form a joint venture with a Singapore company and the joint venture complies with the headquarters and control requirements. DWB licenses are opened to all businesses. In Malaysia, licensees will be assessed on whether it is in the national interest. Although there is no requirement of ownership there is a preference that controlling equity interest resides with Malaysians. In South Korea, a non-financial company can own up to 34% of an internet-only bank whilst in Taiwan the amount can be up to 60%, but at least one of the founders needs to be a bank or financial holding company with a shareholding of 25% or above.[15]Ownership appears to be crucial because virtual banks are usually new ventures subject to higher risk, therefore support from those with a track record and who can act as parent company is crucial.[16] There has been no analysis or explanation about why majority control in terms of nationality has been a requirement but it could be related to both moral and legal commitment to the region.[17] In reality, the FinTech companies are still the major owners of virtual banks.[18]

Virtual banks in Hong Kong require board members and senior management staff to have the requisite knowledge and experiences for discharging their duties (but not specifically in financial technology) and having material outsourcing approved by the HKMA in compliance with the principles. The *Philippines* requires at least one member of the board and one senior management officer to have a minimum of three years of experience and knowledge in operating a business in the field of technology and e-commerce; whilst Taiwan requires at least one member of the board to have more than five years of experience in financial technology, e-commerce or telecommunication business.

It should be noted that what is not governed is cross-border operations and collaboration with fintech companies, which are non-bank institutions not subject to the regulatory requirements. The mobile nature of virtual banks means they are more prone to cross-border risk, and extensive collaboration will force

---

[15] Bank for International Settlements, *supra* note 1 at para 11, para 13.

[16] HKMA, *Authorization of Virtual Banks*, HKMA (May 5, 2000) https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/guide-authorization/Chapter-9.pdf.

[17] Monetary Authority of Singapore, *Digital Bank Licence*, MAS (2019) https://www.mas.gov.sg/regulation/Banking/digital-bank-licence.

[18] Sally Chen et al., *Virtual Banking and Beyond*, BIS (Jan. 27, 2022) https://www.bis.org/publ/bppdf/bispap120.pdf.

virtual banks to have a higher regulatory burden when collaborating with fintech companies.

B. BUSINESS SCOPE

There is limited business scope for virtual banks. In Hong Kong, virtual banks "normally target" retail banking clients and SMEs.[19] Although there is no explicit prohibition of the client segment who can be targeted, the product range is limited; for example, out of eight virtual banks in Hong Kong, only two offer business accounts. The product range is also limited to simple loan services, credit cards, debit cards, insurance, and foreign exchange.[20]The minimum capital requirement for a virtual bank in Hong Kong is HK$300 million.

In Singapore, DFBs have a phase-in arrangement where there is no time requirement but rather a minimum paid-up capital requirement from S$15 million (restricted DFB). The restricted DFB licensee has to comply with an aggregate deposit cap of SGD 50 million deposits from a limited scope of depositors, be covered by a deposit insurance scheme, and observed capital and liquidity rules similar to local banks. At the stage, the licensees will be restricted to simple credit and investment products, have no more than two banking operations in overseas markets, have no minimum account balance and fall below fees, comply with unsecured credit rules, and have no access to automated teller machines ("**ATMs**") or cash deposit machines (commonly regarded as CDMs) networks, other than the offering of cashback services. To migrate to DFB status, the applicant must have a minimum paid-up capital of SGD 1.5 billion, but will not be restricted by a deposit cap, and can operate as a fully functioning bank.[21]The key requirements for a DWB license include a minimum paid-up capital of SGD 100 million and compliance to capital and liquidity rules similar to existing wholesale banks. In addition, a DWB will not be able to take Singapore dollar deposits from individuals of less than SGD250,000, but is free

---

[19] Hong Kong Monetary Authority, *Digital Banks,* HKMA (2024) https://www.hkma.gov.hk/eng/key-functions/banking/banking-regulatory-and-supervisory-regime/virtual-banks/.

[20] Hong Kong Monetary Authority, *supra* note 23.

[21] Monetary Authority of Singapore, *Monetary Authority of Singapore Eligibility Criteria and Requirements for Digital Banks*, MAS (2023) https://www.mas.gov.sg/-/media/Digital-Bank-Licence/Eligibility-Criteria-and-Requirements-for-Digital-Banks.pdf.

to open and maintain deposit accounts for MSEs and corporates. There is a similar requirement in Malaysia, with the amount of paid up capital stated at different phases withRM100million at the foundational phase, reaching RM300 million (S$99 million) at the end of the fifth year. Notably, there is no explicit restriction of the scope of their products or services and hence their scope is mainly restricted by their business strategy and targeted segment.[22]

The minimum capital requirement for a virtual bank in Taiwan is NT$10 billion, which is the same as required for setting up a conventional commercial bank. The minimum capitalization of virtual banks in the Philippines should be P1.0 billion (50% lower than that for a commercial bank). Any individual (either foreign or local) or non-bank corporation may each own or control up to forty percent only of the voting stock of a virtual bank.

The phenomenon under consideration pertains to the emergence of small-scale banks in the market that exclusively offers digital services. These banks adopt client onboarding procedures that deviate from those employed by traditional banks, resulting in a limited geographical scope of client outreach. Specifically, virtual banks can only target individuals with internet access, as their services are exclusively accessible through online platforms. However, the virtual banks lack the ability to control internet availability for potential clients. This predicament engenders uncertainty regarding the source of clients and the potential of innovative strategies to attract new assets. Consequently, virtual banks are characterized by modest dimensions and a restricted range of products. An additional concern pertains to technology risk, which currently lacks a dedicated category within capital requirements. Although virtual banks may allocate provisions to address technology-related risks, the realization of such risks cannot be resolved solely through liquidity or capital measures. This is due to the inherent uncertainty surrounding the reliance of banks on third-party devices and software.

C. OPERATIONAL MODEL

There are operational restrictions on virtual banks. In Hong Kong, there is an explicit requirement for a virtual bank to operate without any physical branches, but it must have a physical office in Hong Kong. It must maintain an explicit objective to promote financial inclusion and hence cannot impose a minimum

[22] Bank for International Settlements, *supra* note 25 at 14, table 2.

deposit requirement. In Singapore, on top of the no minimum deposit balance, the limitation of physical access to clients has been made explicit by prohibiting access to ATMs or cash deposit machines. Both DFB and DWB licensees can only have one physical place of business for conducting activities within the proposed business scope.[23]The operation of virtual banks is in practice more restrictive than the regulatory requirements; the key challenges for regulators have been reported to be to ensure no regulatory compromises despite convenience, as well as issues around data governance[24] Yet, arguably these issues are equally applicable to non-conventional banks. Nonetheless, a physical branch or office may be necessary for potential customers who need help in onboarding and for existing customers who need special attention under certain circumstances, e.g., when making complaints, or gaining access to cash when digital networks are down.[25] In Malaysia and Singapore, virtual bank applicants are required to demonstrate during the application process their ability to serve customer needs and reach underserved and hard-to-reach market segments. In other jurisdictions, there is a more general expectation for virtual banks to help promote financial inclusion.[26] In the Philippines, a virtual banking license applicant must provide a detailed review and assessment of the supporting information technology systems and infrastructure vis-a-vis the digital banking business model which is performed by a competent independent third-party IT expert.

Regulatory sandboxes are currently offered by more than 70 countries as a means for virtual banks to test innovative products and services within a controlled environment. This initiative presents virtual banks with unique opportunities to experiment with and refine their offerings, thereby facilitating progress within the virtual banking sector. It is important to note that sandboxes are not exclusively available to virtual banks, as traditional banks may have distinct operational models that may not align with sandbox participation. The

[23] Monetary Authority of Singapore, *supra* note 28 at 3–4.
[24] Bank for International Settlements, *supra* note 1 at para 13.
[25] Alliance for Financial Inclusion, *Policy Framework on the Regulation, Licensing and Supervision of Digital Banks,* AFI (Nov. 23, 2021) https://www.afi-global.org/wp-content/uploads/2021/11/DFSWG-framework_FINAL.pdf.
[26] *Id.*

existence of sandboxes emphasizes the necessity of consumer education and awareness. Users must be adequately informed about the functioning of the virtual banking platform and be equipped with the knowledge required to navigate and operate the platform effectively. Unlike physical banks, where human staff members are available to assist clients with their inquiries, virtual banks necessitate that clients take full responsibility for mastering the operation of the platform. Consequently, consumer education becomes imperative to ensure that users are well-versed in utilizing the virtual bank's services and know how to respond in the event of any operational issues or deviations from expected functionality.

These three features have important implications that lead to unveil the insufficiency of purely adopting existing regulatory requirement.

First, is that these requirements are explicit in the eyes of clients without the need for any further enquiries, indicating that the regulatory requirements might have direct impacts on the services clients receive and these impacts have been incorporated into the licensing requirements without the need to write them down.

Second, is their focus on the technology requirements, made through imposing the mandate of financial inclusion. In the Basel Report listing the technology related licensing requirements of digital banks, [27] there are four major requirements, relating to a fitness and propriety test, track record in technology, third-party assessment of IT systems, and financial inclusion. Except for Taiwan, all countries listed have a mandate of financial inclusion, therefore virtual banks are destined to advance technology in the banking industry.

Third, there is no subsequent indication of how to improve the technology literacy of clients, contrary to traditional banking where financial literacy is a key mandate; for example in Hong Kong there is a need to treat retail customers fairly. [28] Although the regulatory requirements are largely the same as in conventional banking, these notable added requirements make it critical to acknowledge that virtual banking could be a separate segment of its own as it operates a brand new channel to provide banking services and products. Largely,

---

[27] Bank for International Settlements, *supra* note 1 at para 13, table 2.
[28] HKMA, *Treat the Customer Fairly Charter*, HKMA (Oct. 14, 2020) https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/consumer-corner/TCF_Charter.pdf.

clear objectives from the regulators incorporated in the licensing requirements integrated into the regulatory regime makes the regulatory requirements of virtual banks tighter than those of non-virtual banks. This could create a possible loophole for non-virtual banks to not be subject to these requirements, even though they could equally build the same technology-centric platform for their clients.

IV. TOWARDS A TECHNOLOGY-CENTRIC REGULATORY APPROACH FOR VIRTUAL BANK

The absence of specific virtual banking laws and regulations poses significant challenges for the industry and regulators. To address this, comprehensive virtual banking regulations should be established to create a level playing field, ensure fair competition, and protect consumers across the banking landscape. Such regulations should cover licensing requirements, prudential standards, consumer protection measures, risk management guidelines, and data privacy and cybersecurity provisions. The existing gap between virtual banking and traditional banking regulation comes from technology as a medium of delivery of service. A technology-centric regulatory approach should bridge this gap to cater for the paradigm shift from a physical mode to an online-only mode, while maintaining the trust and confidence clients have built through human touch and a physical presence.[29]

A comprehensive focus group study was conducted between October 2021 and March 2022, involving interviews with a total of 64 individuals. The aim of the study was to explore and gather insights into the perceptions and experiences of individuals regarding the utilization of virtual banking services. Additionally, in order to gain expert perspectives on regulatory frameworks, four industry experts were interviewed. The experts included the Chief Risk Officer of a virtual bank in Hong Kong, an investor of a virtual bank in Taiwan, and a senior executive from a virtual bank. Through the analysis of the focus group discussions and the insights provided by the experts, several key themes emerged. These themes shed light on the regulatory landscapes surrounding virtual

[29] Law S.W., *Banking Made Easy: The New Theory of Digital Financial Inclusion from a Users' Perspective*, 4(4) INT. J. ELECT. BAN. 336-380 (2024).

banking and their implications for the industry. By synthesizing the perspectives of the expert opinions, the following noteworthy themes have been identified:

A. The Absence of Virtual Banking Specific Laws and Regulations

The absence of a dedicated legal and regulation framework designed for virtual banking presents a challenge. There is an apparent regulatory gap under the technology-neutral regulatory approach as existing laws may not fully capture the complexities and challenges of this evolving sector. One obvious gap is the absence of physical space for clients as a contingency in case the virtual platform fails to operate. This presents a competitive disadvantage to the virtual bank as its access to clients is limited to internet users, and they have no control over who will have access to the internet. Another gap is that there is no clear guidance to which existing regulations should be followed. Some are obviously out of place as they have been designated for physical branches. Participants also observed that the client onboarding requirements is different among different virtual and conventional banks:[30]

"It is unfair that we are subjected to the same set of regulations because our mode of operation is entirely different. The fact that we operate solely in the virtual realm is both a blessing and a curse. It limits our avenues for business expansion as we cannot control who will go to the internet."[31]

"Sometimes, I find it challenging to meet certain regulatory requirements that seem to be designed specifically for traditional banks. For instance, I question whether it is necessary for us to ensure that the ramp leading to our branch has the correct slope to ensure accessibility and financial inclusion. Or should these requirements also apply to our office, which is not open to our clients?"[32]

Without specific virtual banking laws and regulations, there is a lack of clarity and guidance for industry participants and regulators alike. This gap creates uncertainty regarding compliance requirements, consumer protection, risk management, data privacy, and cybersecurity. Moreover, it leaves room for potential regulatory arbitrage, where virtual banks may exploit regulatory

[30] *See*, focus group with Participant 24 (Oct 2021), Participant 43 (March 2022), Participant 59 (March 2022).
[31] Interview with Chief Risk Officer (March 2022).
[32] Interview with an executive of a virtual bank (March 2022).

loopholes or operate in a less regulated environment compared to their traditional counterparts.

B. Ensuring Fairness: Bridging the Gap between Virtual and Conventional Banking

While virtual banking operates in a digital space, it is important to recognize that conventional banks also have a virtual presence through online banking platforms. It would be unfair and impractical to solely focus on regulating virtual banks without considering the virtual operations of traditional banks. Both types of banks face similar challenges in the digital realm, such as cybersecurity threats, data protection, and customer authentication. Therefore, regulations should aim to create a level playing field, ensuring fair competition and consumer protection across the entire banking landscape, irrespective of whether the services are delivered virtually or through physical branches:

"Virtual banks operate exclusively in a virtual environment, whereas traditional banks have the capability to operate both physically and virtually. This imbalance creates an unfavorable situation for virtual banks, as traditional banks can easily control the number of physical branches to achieve cost savings. The notion that virtual banks inherently possess cost advantages is, in fact, misleading."[33]

"I think the government should have more regulations to emphasize the issues of cyber security, protections on personal information and other transaction records. Because virtual bank services have no physical back up, virtual bank is more vulnerable to cybersecurity risk, we need more protection from the law and regulation in this aspect."[34]

Therefore, a perception that virtual banks have lower costs to operate may be a misnomer because they would have to invest more to secure the trust and confidence of clients to make a virtual-only platform is as convenient as a traditional bank. In fact, Participant 37 rightly observed that in Hong Kong, whilst digital payments are not as common, virtual banks need to rely on a

[33] Interview with a virtual bank investor (March 2022).
[34] Interview, *supra* note 39.

traditional bank's ATM machine for clients to withdraw their cash. This means that they must open a traditional bank account anyway. The presence of the virtual bank might not be as beneficial when the geographical divergence is not as influential in other countries. There seems to be a repeated effort to issue a virtual bank license and impose restrictions on them.

C. THE NEED FOR VIRTUAL BANKING REGULATIONS

To address the regulatory gap and ensure fairness, there is a pressing need to establish virtual banking regulations. These regulations should encompass various aspects, including licensing requirements, prudential standards, consumer protection measures, risk management guidelines, data privacy provisions, and cybersecurity protocols specific to virtual banking:

1. *Licensing Requirements*

Clear and transparent criteria should be established for granting licenses to virtual banks, ensuring that only qualified and reputable entities enter the market. On top of the usual factors such as capital adequacy, management expertise, and operational capabilities, technological resilience should be thoroughly examined to ensure that the risk of over-reliance on third-party devices is properly mitigated. Necessitating a specific license for a virtual bank is current practice but this does not explain why it is essential and it is unclear how it differs from a non-virtual bank license. I propose that the reasons why a virtual bank needs a specific license include ownership and control, business scope and operational model (part IV), which ensure non-bank corporate owners have the capacity and commitment to run a banking business as they are likely to provide the technology that virtual banks need. These owners do not solely operate a virtual bank and therefore their commitment must be examined.

2. *Prudential Standards*

Virtual banks should be subject to prudential standards that ensure the stability and soundness of their operations. The usual standards of capital adequacy and liquidity requirements are still important but virtual banks face technology risk rather than the usual credit and market risk. However, there should be a more forward-thinking approach to not just prevent the occurrence of risk events driven by the market, but also the risks arising from technology turbulence, such as how virtual banks can maintain services in an event of a

cyber-attack or electricity shut down. Virtual banks are particularly vulnerable to external attacks. Therefore, there is an added meaning of prudential standards.

3. *Consumer Protection Measures*

Regulations should prioritize consumer protection by mandating the transparent disclosure of terms and conditions, fair treatment of customers, online mechanisms for resolving disputes, as well as the need fora contingency plan for business continuity. Virtual banks should be required to implement robust customer authentication processes and safeguards to protect customer data and privacy. Training should be provided to clients to equip them with data and technology literacy. Also, a dispute resolution mechanism is a critical issue as customers would be forced to raise their disputes through "typing", and it can become more difficult for clients to collect evidence of disputes as all statements are presented online. Specific measures should be taken to ensure customers are aware of how to escalate their complaints given the change of communication methods – for example, the change from face-to-face communications to the use of a chatbot.

4. *Risk Management Guidelines*

Virtual banks should be equipped with comprehensive risk management guidelines that address technological risks, cyber threats, operational vulnerabilities, and business continuity planning. These guidelines should also encompass anti-money laundering and counter-terrorism financing measures. The focus is no longer on capital adequacy because a virtual bank can could easily be disrupted due to issues with their supplier's technology. An analogy is a power company providing electricity to banks, with the requirement from a government to provide back-up power in case of disruption. Such requirements become very difficult when the technology supplier is not governed in the same jurisdiction – global collective efforts become essential.

5. *Data Privacy and Cybersecurity*

Regulations must carefully address the specific data privacy and cybersecurity risks associated with virtual banking. Virtual banks should be required to implement robust data protection measures, encryption protocols, intrusion

detection systems, and incident response plans to safeguard customer information and prevent unauthorized access. The real risk is associated with difficulties in enforcement because of cross-jurisdictional issues, which equally call for collective efforts to be made to ensure that common standards and enforcement mechanisms are applied globally.

The findings from the focus group study and expert interviews provide valuable insights into the perceptions and experiences of individuals regarding virtual banking and shed light on the regulatory landscapes in this domain. The identified themes of the regulatory landscape specific to virtual banking are the backbone of building trust and confidence for a virtual-only platform, as disrupted by the transformative potential of virtual banking, the criticality of effective risk management practices, and the significance of collaboration and partnerships:

"Why bother with a virtual-only bank? Because the banking industry as a whole is transitioning towards virtual operations, and it is foreseeable that eventually all banks will become virtual banks. It is only logical that all banks should be subject to the same regulatory requirements, as virtual banks currently face similar business restrictions. Ensuring a level playing field in terms of regulatory compliance is essential for fair competition and the overall development of the banking sector."[35]

Nevertheless, many of the aforementioned attributes are common to both virtual and traditional banks. The key issue lies in the lack of recourse when errors occur, which applies to both types of institutions. Consequently, comparable regulatory frameworks are also applicable to traditional banks, as previously discussed. The primary distinction arises from the virtual-only nature of neobanks (otherwise known as digital-only banks), where a physical presence is either prohibited or not required. Thus, a more comprehensive examination of the licensing framework is necessary.

Consider a scenario in which a traditional bank experiences a computer system malfunction. In such cases, clients have the option to visit a physical branch and inquire about their transactions. Banks typically maintain physical

[35] Interview, *supra* note 38.

branches to accommodate these clients. However, in the case of virtual banks, where can clients turn to for assistance? The risk arises when all traditional banks transition to a virtual-only model, as the situation would be disastrous if there is no specific resolution process in place to address issues arising from reliance on third-party software and devices. It is commonly predicted that virtual banking will become the norm, as all banks ultimately aim to establish a virtual or virtual-only presence, enabling broader client outreach at minimal costs. To maintain the trust and confidence that have traditionally been fostered through physical presence, regulators should adopt a forward-looking approach and undergo reform to account for the technology-driven elements inherent in this banking channel.

V. WHAT IS NEXT?

The rapid proliferation of online financial services and activities has heightened the importance of the underlying internet infrastructure for the stability and functioning of the financial system. As Arner, Buckley, and Zetzsche (2018) observe, the growing digitalization of finance has rendered the accessibility and reliability of critical financial websites and online platforms a key operational and systemic risk consideration for regulators.[36] This dynamic necessitates a more coordinated approach to governing the availability of internet and website domains used for core financial functions.

Financial authorities should seek to establish a regulatory partnership with internet governance bodies and domain name registrars, as advocated by Dempsey (2020).[37] Such a partnership could involve setting guidelines for the prioritization and protection of domains vital to financial stability, as well as streamlined procedures for resolving outages or ownership disputes that could disrupt financial activities. Collaborated efforts of this nature, drawing on the technical expertise of internet organizations and the regulatory purview of financial authorities, will be essential for mitigating the operational and systemic

[36] Arner, D. et al., *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, 37(3) NORTHWESTERN J. INT'L L. & BUS. 371-413 (2018).
[37] Dempsey, J., *Stabilizing the Internet's Domain Name and Addressing System: An International Public-Private Partnership Approach*, 21(1) GEORGETOWN J. INT'L AFF. 92-101 (2020).

risks posed by potential failures or disruptions to critical online financial infrastructure.

By taking a proactive role in this domain, policymakers can help fortify the resilience of the digital financial ecosystem. Establishing this type of regulatory partnership should be a priority for financial regulators in the years ahead.