William Ting, Esq.[1]
emergingtechlaw.org
8000 Hong Kong Place
Dulles, VA 20189
United States
[redacted]

October 12, 2017

Bank for International Settlements ("BIS")
Basel Committee on Banking Supervision ("Committee")
Postfach
CH-4002 Basel
(+4161) 2808080
email@bis.org

Re: Sound Practices: Implications of fintech developments for banks and bank supervisors ("Consultative Document")

Dear Committee,

Part I: Setting the Overarching Philosophy: How Will Banks Adapt to Expectations of Speed & Convenience?

This is not the first time that the banking industry is facing change. As the Consultative Document points out, there have been times when other emerging technologies like automated teller machines (ATMs), videotex, electronic payments, and online banking have created challenges for the global banking industry which has adapted fairly well to the age of the internet. But the industry faces new challenges brought about by new technologies that enable the real-time transfer of assets.

[1] Since 2004 advisor to TSMC Ltd., the world's 45th most valuable company listed on the New York Stock Exchange, with US$194+ Billion market capitalisation (as of October 6, 2017), and Director of Emerging Technologies & Special Projects at www.IIPCC.org a non-governmental organization working with the United Nation's World Intellectual Property Organization, APEC and PBEC to establish global IP best practices and standards. Member of the Chamber of Digital Commerce based in Washington D.C., which is the world's leading trade association representing the digital asset and blockchain industry. This comment letter has been submitted in my individual capacity and does not reflect the views and opinions of the above entities.

Whereas the age of the internet created instantaneous communications (with emails sent and received in a matter of nano-seconds), the current enabling technologies (like permission-less distributed ledgers and faster computer processing and mobile internet connectivity speeds) create the opportunity to allow consumers to make instantaneous transfers of assets. The financial industry celebrated a key-milestone on September 5, 2017, when it successfully implemented a shortened settlement cycle (two business days or T+2) for most securities transactions, pursuant to amendments to Rule 15c6-1 that the U.S. Securities & Exchange Commission adopted earlier this year. However, from the consumers' perspective, such a move to shorten settlement cycles to 2 days seems incomprehensible when all internet communications occurring online are done instantaneously. Further the processing time to clear wire transfers (which can take up to 2-3 days) also seems incongruent with the reality of fast online communications.

In order to address any growing challenge, it is wise to set the overarching philosophy through which to view the problems to come. Like all things in life, there needs to be a constant, a North Star that provides general direction for any human endeavor. Therefore, to set the primary philosophical consideration as the foundation for the study on fintech's impact on banking and bank supervision, regard must be had to the ever growing consumer demand for speed and convenience in financial transactions.

There are three important groups that make up the cast of characters in our discussion on the impact of fintech on banking. First, there are the fintech firms who are smaller, technology-enabled new entrants ("Fintech Firms"). Second there are "BigTech" firms defined (in Box 2, page 16 of its Consultative Document) as "large globally active technology firms with a relative advantage in digital technology" (such as Google, Amazon, Facebook, Apple, Baidu, Alibaba and Tencent, the examples listed). Lastly legacy banks ("Legacy Banks") consists of the world's traditional banking institutions. Each of these firms has been trying to find innovative business models to cater to such growing consumer expectations. In doing so, the tempo, speed and convenience of financial transactions will keep increasing (some say exponentially) into the future. For example, consumers' expectations for convenience are driving increased demand for online, mobile and digital currency payment systems which are set to overtake credit and debit cards as the most popular ways to pay in e-commerce worldwide by 2019 according to the United Nations.

Recently Commissioner Brian Quintenzhe of the U.S. Commodity Futures Trading Commission delivered a keynote address on the effects of fintech on financial regulation at the Symphony Innovate 2017 Conference and noted that:

> "we see a world that moves faster, at lower cost, more transparently, and with greater efficiency….[n]ew technologies and innovations can also be accompanied by new risks. While speed in trading can have significant benefits, it can also trigger events that undermine market stability."

So the primary question for banks and their supervisors becomes this: how can banks and banking regulators manage increasing consumers' demand for speed and convenience? If responsible innovation needs to be balanced against traditional banking prudential safeguards (as the Committee stated in its Recommendation #1 on page 6 of its Consultative Document), then how can banking regulators condition and shape such expectations?

Part II of this comment letter sets forth ten additional observations that have not been addressed in the Consultative Document as follows:

#1) Importance of Fintech Intellectual Property Protection
#2) Enforcement of IP Rights = Disruptive Force in Global Banking Economy
#3) Imperative to Create Standard-Essential Patents Framework for the Banking Industry
#4) Regulators & Industry Need to Promote More Interoperability of Fintech Projects
#5) Risks Inherent in Regulatory Sandboxes
#6) Risks Inherent in Enabling Technologies to Affect Banking
#7) Virtual Fiat Currency To Disrupt Fractional Reserve Banking/Lending
#8) Accounting Standards Lacking for Digital Assets
#9) Prudential Standards for Fintech Mergers & Acquisitions
#10) Qualitative-driven Prudential Safeguards

These new technology, accounting, financial and legal-driven observations will influence to a significant extent how banks and their regulators balance responsible innovation against traditional banking prudential safeguards during fintech's ever increasing effect on global banking and its supervision.

Part II: Ten New Observations & Recommendations

#1) Importance of FinTech Intellectual Property Protection

As the Committee noted in Part II.A. of its Consultative Document, the term "fintech" means "*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." (emphasis added). The importance of technology, innovation and novelty clearly stand in a

preeminent position within the very meaning of "fintech" because without 21st century "tech", the "fin" of finance would be left back in the 20th century. For this reason, the Executive Chairman of Alibaba Jack Ma coined the term "techfin" giving prominence to technology over finance. To underscore the importance of technology, Mr. Ma's company Alibaba on October 11, 2017 announced its plan to invest more than US$15 billion over three years in a global research and development project to include fintech as one of its ambitious R&D programs.

If "tech" plays a prominent part of the very definition of "fintech" then the protection of technology and its intellectual property ("IP") logically must be incorporated as one of the key practices of banking in the fintech era. The problem is most (if not the majority of) professionals in the fintech and banking industries do not appreciate the role and importance of intellectual property rights and protection. This will create critical vulnerabilities within the global banking system in the future (as discussed in Part II.2 of this comment letter).

Innovation without IP is Charity

A noted fintech industry veteran once said that "innovation without protection is philanthropy." Not many banking and fintech leaders understand that intellectual property is perhaps the only source of competitive advantage that their firms have in the fight for future market shares.

Consumers prefer speed and convenience of online banking transactions. Companies who are able to meet that preference will win market shares. To win market shares, companies need to develop key innovative technologies that would allow them to improve their relationships with their respective customers. Developing innovative fintech services requires significant expenditures of time and money. If such investments are not protected under relevant intellectual property laws, then the firm's shareholders (and ultimately the general investing public) loses out as its competitors take the resulting know-how and adapt it for their own use. To demonstrate the extent of shortcomings in this often neglected area for example, not a single event of the many dozens hosted at leading jurisdiction's Fintech Week to be held on October 23 & 24, 2017 even remotely discusses the role of intellectual property protection (trade secrets, patents or software copyrights) in fintech. Legacy Banks and Fintech Firms are doing their shareholders a gross dis-service by not focusing debate and discussion in this area. (BigTech firms in general appreciate the importance of IP much better due to their experience with patent litigations to be discussed below.)

Rise in Fintech Patents Worldwide

Not all players are asleep at the proverbial wheel however. The smart ones like Goldman Sachs, Bank of America, Visa and Mastercard are hard at work filing and obtaining key patents in the race to build competitive IP portfolios. Global fintech patents filings have jumped by a whopping 49 per cent in the past five years, reaching 9,545 in 2016 which was a drastic spike compared to 2015. Unsurprisingly, the United States had the most fintech patents filings with 4,523 in 2016. This was twice as many filings as China, the country with the second highest number of patents followed by South Korea. The other countries with the highest number of patent filings in 2016 were Australia, Japan, Singapore, UK, Russia, Canada and Germany at rank 10.

In 2017 so far, the number of cryptocurrency and blockchain-related patent applications being submitted and published in the U.S. has nearly doubled.

The effect of having IP protections over fintech innovations grants market dominance to lucrative banking fields of business. For example just in the field of mobile payments alone, worldwide annual transactions volume is expected to cross US$ 1 trillion in 2020 from US$ 500 billion in 2015. To help enable European players to capture a piece of this growing market, in November 2016, the European Payments Council rolled-out the SEPA Instant Credit Transfer scheme to spearhead adoption of instant mobile payments and transactions worldwide and provide shape to an unstructured and incomplete mobile payments legal framework. But the lack of patents and trade secrets over fintech mobile payment innovations will hurt most players in this lucrative field. This is because only a handful of fintech players concentrated in OECD countries own the majority of mobile patents issued worldwide. For example, both Visa and Mastercard stride over this field as giants with over 300 worldwide patented inventions each. Bank of America follows with over 260 worldwide patented inventions. Paypal (145), Samsung (86), Qualcomm (64), Google (54), Apple (45) and IBM (44) are some of the other key mobile payments patents holders.

Other business sectors in fintech tell the same story. For example, Goldman Sachs received its first U.S. fintech-related patent entitled "Cryptographic currency for securities settlement" to process foreign exchange transactions using distributed ledger technology.

There are legal issues surrounding whether blockchain technology is even patentable under U.S. law. This is because of the questions posed in the seminal 2014 Supreme Court case of *Alice Corp. v. CLS Bank International*, (573 U.S.___, 134 S. Ct. 2347) over whether or not an abstract idea is eligible for patent protection when it "merely

requires generic computer implementation" or "attempt[s] to limit the use of [the idea] to a particular technological environment." I will address these issues in my blog more closely so as not to burden this comment letter with too much technical legalism. But the consensus is that it is much better to have a patent over fintech innovations than not given the valuable stakes in this field.

Alternative IP Protection: Trade Secrets

Despite the legal question of whether blockchain technologies may be patented under U.S. law, most intellectual property is protected under the doctrine of "trade secrets". Trade secrets are managed as part of a firm's overall IP portfolio which may consists of patents, trademarks and copyrights. But be mindful that the vast majority of a firm's IP portfolio could consist of trade secrets because trade secrets do not expire (unlike patents for example) so long as certain continuing legal requirements are met. Therefore trade secrets form an indispensable part of any firm's IP strategy. For example, it has been publicly disclosed that roughly 90% of the intellectual property rights of one of the world's leading semiconductor companies are protected as trade secrets.

The patent filings described above merely reflect the state of the patent market for fintech related innovations like blockchain and mobile payments. They do not even include the patent filings for cloud computing, big data and AI which will be crucial enabling technologies for fintech related inventions. Whether or not any bank or fintech institution may be "adopted or actively considered as a means of enhancing banks' current products, services and operations" (in the Committee's words) depends significantly on whether such institution owns or can license at a reasonable cost efficient rate relevant IP rights in these fields.

Concentration of Fintech Market Shares in Handful of Players

The Consultative Document describes five likely scenarios (that may blend into each other) affecting the future of banking in the era of fintech ranging from a legacy bank better adapting to technologies to the fully "disintermediated bank". Yet this comment letter proposes a sixth likely scenario: the rise of the "dominating IP entities or DIPEs."

As discussed above, intellectual property rights provide key competitive advantages in all areas of commerce. Banking is no exception. This is why we have seen the big players like Goldman Sachs, Bank of America, Visa and Mastercard racing to build globally competitive IP portfolios. These handful of players are also concentrated in OECD countries. Ironically, even though blockchain technology is built upon a decentralized premise, the future business of blockchain will be concentrated in a relatively small club

of players that either own or are able to license key fintech IP rights which they can exploit and monetize at their own terms vis-a-vis other fintech players.

Given the preeminent role that technology will play in "fintech", the market will see a new development or scenario rising. If IP rights will be the ultimate differentiator in the future fintech era, it is highly likely that the fintech market (just like the search engine, smart phones, server, chip design and social media markets) will become extremely concentrated with "dominating IP entities" or DIPEs playing significant roles in creating, shaping and controlling the destiny of this growing market regardless of what they are actually called, whether as a Fintech Firm, BigTech or Legacy Bank. The future fintech field will not be a level playing field and those firms racing to become DIPEs will be disproportionately influential. The next observation explains the rise of DIPEs and how will they influence the general fintech market?

#2) Enforcement of IP Rights = Disruptive Force in Global Banking Economy

In the last decade, international lawsuits related to IP rights of smart phones and WIFI connectivity rocked the hi-tech world. We all saw the media headlines for the famous "smart phone war" between Apple and Samsung (the last dying shots of which are still being fired this day over the amount of damages awardable for design patent violations). Not many outside the hi-tech world appreciate the potentially disruptive effects of international patent litigations on a party's business. Patent litigations demand a lot of time and resources to manage well. Companies that lose their competitive advantages risk going bankrupt or forfeiting tremendous market shares. In this high stakes game, executives of parties involved in IP disputes are distracted by the many vicissitudes of international litigations. Worse, in some jurisdictions like the U.S., quasi-administrative bodies like the U.S. International Trade Commission has the power to prohibit completely the importation of goods that violate domestic patent rights. The grant of an injunction to stop all import of any product that violate a U.S. patent right is a formidable weapon that can literally put any going concern out of business.

In general, the banking and financial communities have remained relatively unaffected by disruptive patent litigations of the last decade. One of the reasons is that the financial incentives were not as strong to launch wide-spread patent litigations in the banking and finance industries since the technologies at stake were not as valuable as those underlying modern smart phones. But this will change to the detriment of fintech players and the global banking system as more banks incorporate more emerging technologies into their operations.

How IP Fights Will Endanger Banking Stability

Key emerging technologies like blockchain are increasingly being protected as intellectual property rights such as patents and trade secrets. See discussion in Part II.1 above. The Consultative Document describes the many ways in which traditional banks and "neo-banks" have been trying to incorporate emerging technologies (like AI, big data and blockchain) into their operations to remain competitive in light of the challenges of the fintech era. Yet many of these emerging technologies are increasingly being protected as the intellectual property rights of dominating IP entities who are likely to see such wide adoption of technologies as violative of their respective IP rights.

There are many reasons why firms launch IP lawsuits such as securing market shares, undercutting competition and receiving a steady stream of licensing revenues. All of these reasons will justify dominating IP entities to launch IP protection lawsuits of the kind unseen since the smart phone wars either: (1) against each other (as a turf battle); or (2) against other entities which lack strong IP portfolios (as potential targets to extract lucrative royalty payments) as discussed below. The financial incentives are very attractive and conditions for doing so extremely ripe.

Apple and Samsung (two dominant IP entities) engaged in the smart phone war as a way to stop the other from becoming the world's dominant smart phone maker. Businesses routinely file IP lawsuits to undercut the commercial plans and aspirations of their key competitors. These lawsuits are typically filed against two relatively equal contestants. Apple and Samsung were both large established tech companies, they were the two biggest boys on the proverbial block and soon fought a key battle to establish each other's dominance. Most high-stakes patent disputes involve dominating entities. For example, Qualcomm and Apple are now both engaged in another fight: the battle over wireless modems.

Many of these lawsuits however also involve so-called "NPEs" or non-practicing entities that hold relatively strong IP portfolios which they have bought or licensed. NPEs then leverage their IP portfolios to sue other companies with the aim of forcing defendants to enter into settlement agreements that licenses the underlying technologies at lucrative royalty rates. There has been a lot of literature written about NPEs and their effects in the patent space. In fact, the companies that filed the most patent lawsuits in the U.S. in 2016 were NPEs. Some see them as locusts or "trolls" preying on innovation. Some see them as champions of personal inventors who are often at the mercy of large multinational companies.

IP lawsuits also are launched against businesses with weak or non-existent IP portfolios with disastrous results. Their shareholders will lose out when their invested company pays licensing royalties, becomes enjoined from doing business in a particular jurisdiction or loses an entire product/service line as violative of third party's IP rights. Many Fintech Firms and Legacy Banks simply do not have the experience, know-how or background to design a competitive IP portfolio to ward off patent litigations.

Gathering Fintech IP Wars

Churchill gave one of his history books on the Second World War the title "The Gathering Storm". In the fintech era, the storm clouds for the coming fintech patents wars are gathering fast. Since most Fintech Firms operate without any regard for the need to protect their respective trade secrets and completely forgo the filing of any patents to protect their inventions, Fintech Firms will be the most vulnerable in the coming IP wars. The dangers and pitfalls of how Fintech Firms unwittingly lose their trade secrets is analyzed here. Since most Fintech Firms are under-capitalized compared to Legacy Banks and BigTech players, they are more likely to settle any IP lawsuits at very unfavorable terms rather than expend funding on long drawn-out litigations. This is because patent litigations require a disproportionate amount of time, attention, money and internal resources to defend. Most Fintech Firms will be crushed by such onerous litigation-related burdens.

Legacy Banks make excellent lawsuit defendants because of their perceived "deep pockets" especially when the deposits of most banks in the world are insured by their respective national authorities. They are literally cash-rich "piggy" banks in the eyes of seasoned patent litigators and NPEs. In the fintech space the stage is also being set for a showdown amongst the dominant IP entities as they begin to jockey for market shares. It would also be a matter of time before the U.S. BigTech titans clash with their counterparts in China in the fintech era given the value of markets, technologies and incentives at stake.

One condition distinguishes the coming fintech patent wars from the old smart phones or WIFI connectivity wars: banks are inherently connected to the macro-economy of their respective home countries and together act as the keepers of global financial stability. If the activities of banks become disrupted in IP lawsuits, the knock-on effects on the general economy will be costly for society.

Dangers of IP Lawsuits Versus Banks

Banks are intricately connected to the national economies of which they are a part. This is because banks act as intermediaries working with their respective central banks to control the money supply of their respective home economies via fractional reserve lending. Banks are also particularly vulnerable to systemic risks. Banks are also subject to much more regulatory scrutiny than BigTech or Fintech Firms. For example, financial regulators maintain a list of the world's systemically important banks as a way to keep track which banks are most likely to take down the rest of the world's financial system if they were to go under.

As discussed above, IP lawsuits in the hi-tech industries are disruptive. In the fintech space, IP lawsuits will be several orders of magnitude more disruptive. This comment letter focuses primarily on patent enforcement actions arising in the U.S. because federal patents rank among the world's most valuable IP rights and patent litigations in the U.S. are potentially the most disruptive. Patent litigations will be challenging for fintech players for two major reasons.

First, Fintech Firms and Legacy Banks are relatively inexperienced in dealing with or managing IP litigations and lack basic awareness of IP protection and management. This makes it easier for their business to be interrupted by unscrupulous plaintiffs who are positioned to exploit such vulnerabilities. Second, the business of fintech like traditional banking and finance is extremely time sensitive. Being unable to conduct trading operations in the open market even for a few minutes is costly in terms of lost revenue. Given the time sensitive nature of fintech operations, defendants will be more vulnerable to time-consuming IP litigations which can run up to 2 to 3 years without counting time for the appellate process. As such, fintech defendants will be more susceptible towards settling on unfavorable terms that compromise shareholders' interests. BigTech firms, especially those operating in the U.S. understand the significance of IP protection and the pitfalls of patents & trade secrets litigations because they have either been defendants or plaintiffs themselves in lawsuits launched in the hi-tech space in which they operate. BigTech like Apple, Samsung and Google are old hats to the patent litigation game having themselves shaped some of the key judicial opinions in this area.

Court actions are only the beginning. Another popular tool to enforce patents arises in Section 337 of the U.S. Tariff Act of 1930 in the U.S. International Trade Commission ("ITC"). Section 337 allows IP owners to seek redress for unfair practices in import trade that threaten to injure or in fact do injure a U.S. domestic industry. Future cases will need to test the argument whether a financial product designed overseas in violation of a U.S. patent right that is sold in the U.S. will grant jurisdiction to the ITC.

Experienced IP plaintiffs know the value of injunctions in extracting favorable settlements. For example, NPEs are experienced in asking for injunctions from the ITC as settlement leverage. If they go after a large bank with global operations, NPEs can potentially obtain an injunction from the ITC to prevent defendant bank from using any technology violative of their patents in the U.S. which is the world's key financial center and currency. If this happens and the underlying technology enjoined covers vital banking activities like deposit taking, commercial lending, settlements of accounts, remittances or trade finance, then such banking activities will come to a stand-still within the enjoined jurisdiction causing massive disruptions to banking transactions and counter-parties obligations. Since banks operating within one jurisdiction are interdependent on other banks worldwide, a well-positioned injunction or IP lawsuit (by a NPE or dominating IP entity) may undermine not only national macro-economics, but also international financial stability in a way unlike any patent litigations against a smart phone maker. This uncertainty is compounded by the fact that patent litigations often have an international dimension as ancillary lawsuits are filed in multiple jurisdictions worldwide. If a fintech patent plaintiff manages to obtain preliminary or permanent injunctions against one or several Legacy Banks in multiple jurisdictions each enjoining a core banking activity that they perform therein, then the systemic disruptive knock-on effects will be multiplied.

The problem is compounded by new "post-grant" PTAB proceedings enacted in the U.S. American Invents Act in 2011 that allows any third party to challenge the validity of a patent issued by the U.S. Patent & Trademark Office. These proceedings are controversial because they have the potential of invalidating patents after their issuance and creates much room for "gamesmanship". Most pharmaceutical companies do not favor their use. Most hi-tech companies however favor them. Conceivably, a patent issued in the U.S. may become invalidated in one of these proceedings to the consternations of the fintech patent holder. Patent litigation is an area fraught with perils. The dynamic nuanced interplay among patent litigation proceedings, ancillary anti-competition actions, International Trade Commission hearings and post-grant PTAB proceedings present a trap for the unprepared fintech player, to be sprung upon them by seasoned NPEs or dominating IP entities. The world's best IP law firms are compensated millions just to advise their clients on how to navigate the relationship of all these different types of proceedings that can sink an unsuspecting fintech player's business prospects. To the uninitiated, the stakes are simply too high not to receive the wise counsel of experienced IP attorneys in this regard.

Scenario #6: Rise of Dominating IP Entities

As a sixth likely scenario, the future impact of fintech on banking will be increased IP lawsuits being launched by NPEs and dominating IP entities attempting to monetize their IP portfolios or undercut their respective competition. Patents allow their owners to enjoy a limited window of monopoly in which they are incentivized to enforce against third parties. Given the current lack of awareness of the importance of IP protection of fintech innovations, the risk of systemic IP litigations is extremely high. When Legacy Banks are involved in high-stakes fintech IP lawsuits, both national and global financial systems will be in danger of being disrupted if their operations are enjoined by a legal injunction issued to stop their infringement of a third party IP right. Fintech Firms simply lack the experiences and financial resources to defend against sustained IP litigations filed by seasoned NPEs and DIPEs. One of the ways to manage such risk is to fashion a framework whereby important patents are required to be licensed at fair and reasonable rates. This leads us to the next observation.

#3) Imperative to Create Standard-Essential Patents Framework for the Banking Industry

Some fintech related patents can be very important or essential to setting the standards of future banking activities. If a company owns such a patent, then it will be in an extremely favorable commercial position. But other third parties will not be so lucky. This is because such patent will be extremely valuable to third parties who need it to conduct their own operations given its standards-essential nature. If there are no safeguards on how and to what extent the patent owner may behave in its effort to monetize its standards-essential patent, then third parties will be vulnerable to abusive monetization efforts.

The Committee is advised to explore ways to work with industry setting bodies like the IEEE to create a framework that serves two important mediating functions: (1) which fintech patents ought to be classified as "standards-essential"; and (2) whether to define "fair, reasonable and nondiscriminatory" or "FRAND" terms on which standards-essential patents may be licensed to third parties so as to prevent market abuse.

How Standard Setting Works

Standards-setting bodies like the IEEE hold periodic meetings to identify certain patent claims which may be essential for the use of standards in various industries like semiconductor manufacturing, WLAN connectivity or 3G or 4G/LTE connectivity. If they identify any patent claims that they deem are essential for the implementation of a

certain standard, they will ask the owner of such patent claim whether it will voluntarily commit to license such patent claim on FRAND terms to third parties. A patent claim is deemed "standard-essential" under IEEE if it covers a technology required by the applicable standard and there are no commercially or technically feasible non-infringing alternatives (ie. there is no workaround). The owner of a standard-essential patent claim may choose not to voluntarily commit its claim to the standard. If the owner prefers not to, the IEEE or standards setting body will try to identify alternative technologies to use for the applicable standard.

The IEEE prefers not to define too specifically what FRAND terms should be. (See its definition on "reasonable rate" on page 16 of its Bylaws.) This is because it is impossible to anticipate the scope and nature of such terms when a standard is deployed in the future. Usually, the parties are able to commercially negotiate such terms. But there are times when the courts will need to intervene. (See here, here and here.)

The incentives in standard-essential patents are structured in such a way as to balance the interests of innovators who use the technology in their products and the interests of the owners of such patents who needs to recoup costs of research and development. The licensor will receive fair compensation for its standards-essential patent claim. The licensee will enjoy a lower market entry barrier which will enable them to adapt more quickly to competition. In turn the general industry benefits because many innovators will be using the same standards that will generate more consumer choice at competitive prices. For example, in the mobile technology area, innovators are creating numerous products and services using an industry standard (such as 4G/LTE) to make communications faster and cheaper for consumers.

Fintech Needs Standards

As applied in the fintech area, the BIS is encouraged to contact standards-setting boards like the IEEE to help them to identify which fintech related patent claims will be essential to setting certain standards in core banking activities. The BIS needs to share its expertise relating to modern banking and prudential safeguards while technical standards-setting bodies like the IEEE can contribute its technical expertise towards a joint endeavor to maintain the stability of banking in light of emerging technologies. The way forward will be a multi-disciplinary approach to manage the effects of fintech on banking and its regulation. One of the best ways to do so is to help standards-setting bodes establish standards on fintech related banking and identify which patent claims ought to be incorporated into these standards.

Setting standards is important for two reasons. First, it will dampen the disruptive of effects of IP litigations as discussed above by encouraging the rise of industry-supported standards. Second, setting standards will help promote the interoperability of various fintech related projects currently under development, which leads to the next observation.

#4) Regulators & Industry Need to Promote More Interoperability of Fintech Projects

Finance and banking is premised on the need for uniform standards upon which core banking activities may be transacted. Uniform standards also facilitate prudential regulation of the banking sector as the resources of regulators need not be expended on understanding and keeping track of multiple competing standards. For example, there is one standard (and not multiple ones) for conducting most international money and security transfers: the SWIFT system standardized under ISO 15022 and ISO 20022.

The problem with fintech-related banking technologies being developed now is that there are too many of them being designed and tested without a clear understanding on how these systems will interoperate with other systems used by third parties. For example, Commerzbank, KfW Banking and MEAG are testing the sale of securities on a distributed ledger platform ("DLS") using an extension of R3's Corda platform. How will this project interoperate with Goldman Sachs' new patent granted on a system for settling securities trades using a built-in cryptocurrency?

There are also multiple systems being developed for cross-border payments. Barclays, JPMorgan Chase, Goldman Sachs and Bank of China, are testing DLS to increase the efficiency and security of forex settlements and ultimately replace SWIFT. How will this affect the interoperability with the research being done by Canada's largest bank the Royal Bank of Canada in testing blockchain technology for cross-border payments? All of these different DLT systems and adoption cycles from major banks will lead to interoperability problems that will not be beneficial to stable banking.

#5) Risks Inherent in Regulatory Sandboxes

There is a trend towards the adoption of various "sandboxes" by regulators to test the actual workings of various fintech innovations against traditional prudential safeguards, market stability and effects on consumers. For example, regulators from the following jurisdictions have adopted some form of sandboxes: Hong Kong, Singapore, the United Kingdom, Malaysia, Indonesia, Australia and Thailand. Sandboxes also allow regulators a chance to see how a particular fintech innovation interacts with real-world factors. But

there is a relative lack of analysis in the media on the risks inherent in regulatory sandboxes.

First, the process for applying for permission to conduct fintech activities in a regulatory sandbox appears to be subjective and balanced against Fintech Firms in favor of Legacy Banks.

Second, there has been no discussion on the extent to which other bank regulators would accord "safe harbor" status to a sandbox being hosted by another bank regulator. Would the statements and actions taken with respect to a particular fintech innovation being tested in a sandbox bind or have "preclusive effect" on other bank regulators? If not, then the beneficial effects of sandboxes would be severely limited if there is no system of mutual recognition amongst bank regulators. The most highly likely result is that bank regulators would only view the actions taken by another bank regulator with respect to a sandboxed fintech innovation as "non-binding" or persuasive.

Regulator sandboxes raise other issues which if not address would present significant risks in their continued viability and relevance:

- what is the mechanism to apply for a sandbox? is it informal process or formal process?
- to what extent is the application review process transparent and free from vested interests?
- is there a right of appeal if an applicant's sandbox application is refused?
- how will the length of time for experimentation and scale of testing be determined?
- who decides if further extensions may be granted or whether the experiment is a success or failure? are there any right of appeal on these decisions?
- what is the legal effect of a successful or failed sandbox testing? will it bind other bank regulators? will a failed sandbox testing from one jurisdiction preclude the applicant from applying to another regulator?
- what is the effect of a successful sandbox testing in a future enforcement action launched by the regulator (who tested the innovation)? will there be legal preclusive effect to estop such regulator from bringing a later enforcement action if such regulator approved the sandbox testing?
- what is the effect of a successful sandbox testing in a future enforcement action launched by a third party regulator (who was not involved in the initial testing of the innovation)?
- can a successful sandbox testing be used as a mitigating factor in a future related enforcement action?
- will other regulators approve or grant safe haven status to innovations approved in a sandbox hosted by another regulator?

- will rulings made by a regulator with respect to a particular sandbox be deemed as legal precedent binding against that same regulator or a third party regulator?

#6) Risks Inherent in Enabling Technologies to Affect Banking

Most of the world's leading financial institutions are exploring ways on how to incorporate enabling technologies like AI, cloud computing and blockchain (a form of DLT) into traditional banking practices. They are doing so in order to offer consumers faster and convenient methods to conduct banking and financial transactions. However each of these enabling technologies has their own risks and pitfalls. If adopted into banking practices, these risks and pitfalls (if not mitigated) will carry over into the banking sector as well. The banking sector is a critical infrastructure in almost all economies and significantly affects the level of domestic systemic economic risks. If the risks inherent in enabling technologies are carried over into the banking sector, their potential for disrupting the overall economy will increase exponentially.

AI Risks: Bias & Ethical Vacuum

Two major pitfalls plague current AI technologies: programmer bias and ethics.

AI is powered by machine learning algorithms. But these algorithms can be very biased. This summer a group of researchers, together with the American Civil Liberties Union, launched an effort to identify and highlight algorithmic bias. AI systems are now use to make important decisions such as analyzing credit worthiness for credit card applications, loans and financial assistance. Studies have shown that algorithms are susceptible to bias. This creates the risks that certain minority groups and people from certain genders, sexual orientations and ethnicity may unfairly be rejected to obtain access to basic financial and banking services. This problem is compounded by the fact that most financial institutions use mathematical models in a very un-transparent manner. If the bias lurking inside the algorithms is not addressed, such bias could have negative social consequences, especially for less affluent countries, neighborhood and ethnic groups or minorities. One of the perceived benefits of fintech is its potential to broaden financial inclusion. But it will be very ironic if fintech's use of AI perpetuates prejudicial stereotypes and impedes financial inclusion instead.

AI & Financial Ethics

The business of banking and finance is subject to various ethical safeguards. Some of the world's leading banking institutions subject their professionals to stringent code of ethics. For example, see here and here. Further, financial advisors regulated by the U.S.

SEC are bound by the fiduciary standard which requires them to act in their clients' best interests. Someone who is a "Certified Financial Planner" must also adhere to these same ethical standards.

If banks and human financial advisors are subject to ethics, then why not the systems of AI which they employ to enable fintech innovations, especially financial "robo-advisors"? Many financial firms are making the move to using more "robo-advisors" to penetrate the retail investment market. This raises the question whether it is appropriate in light of traditional prudential safeguards to require robo-advisors to comply with a particular code of ethics, much in the same way their human counterparts are so subject?

There are many forms of systemic risks that fintech presents to the banking industry. Much has been focused on documenting the potential disruptions that are tangible in form such as ineffective money laundering safeguards and lack of interoperable standards. However, enabling technologies like AI systems ungoverned by ethics present a much more invidious threat: casting doubt on the credibility of the banking and financial sector. After the 2008 financial crisis which many blamed on poor banking ethics, the world's financial systems suffered from a lack of public trust which delayed recovery and almost disassembled the banking system. If the world's currencies are now founded on "faith" and "credit" then it is all the more important to prevent the public from losing faith in the credibility of the world's banking system.

Cloud Computing Risks

Data localization issues have been increasingly influencing the general development of cloud computing which will also affect the growth of banking activities in the fintech era. (See in general for this discussion: *Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?, John Selby, Oxford International Journal of Law and Information Technology*, 2017, 00, 1–20).

There are two kinds of data localization. Many governments like Russia have passed laws that require global internet firms to store local client data on servers physically located within the domestic borders of the relevant government. This is known as "localized data hosting". The other type is known as "localized data routing" which requires internet service providers to route data packets required by local Internet users across networks located only in that jurisdiction. Both forms of data localization threatens to undercut innovations in Big Data and would render the use of the general Internet slower and less convenient.

Data localization seeks to control the flow of data. This harms the Internet which assumes the free-flow of data. The business of banking and finance also assumes the free flow of capital. Indeed one of the tenets of the European Union is founded on the free flow of capital. But if cloud computing will be incorporated into fintech banking practices, then there is the risk that the banking transactions (which will be supported by cloud computing) will also be subject to national data localization laws. This will render financial transactions slower and less convenient just as these laws undermine the experience of Internet users. National bank regulators should focus on ensuring that the creditworthiness, competence and experience of a banking institution meet global standards and not where and how data is stored.

Blockchain Risks: Hacking the World's Computer

One of the co-creators of the Ethereum (one of the enabling platforms of blockchain and smart contracts) stated that Ethereum is essentially the world's computer. Ethereum uses its blockchain to record "state" transitions in a very big distributed computer. So users who runs Ethereum on their computer is participating in the global workings of the Ethereum Virtual Machine (EVM). This nature of Ethereum, one of the key enabling technologies being used by banks and financial firms worldwide to build smart contract systems, has enormous implications for cybersecurity.

The co-founder of Airbnb Mr. Haseeb Qureshi recently wrote about the pitfalls of blockchain. His warning is important and therefore warrants quoting in full:

> "In blockchain, code is intrinsically unrevertible. Once you deploy a bad smart contract, anyone is free to attack it as long and hard as they can, and there's no way to take it back if they get to it first. Unless you build intelligent security mechanisms into your contracts, if there's a bug or successful attack, there's no way to shut your servers and x the mistake. Being on Ethereum by definition means everyone owns your server…. A common saying in cybersecurity is "attack is always easier than defense." Blockchain sharply multiplies this imbalance. It's far easier to attack because you have access to the code of every contract, know how much money is in it, and can take as long as you want to try to attack it. And once your attack is successful, you can potentially steal all of the money in the contract."

To illustrate his warning, Mr. Qureshi documented a cryptocurrency wallet heist that was partly foiled by the online good guys or "whitehats" in July 2017. The good guys detected the attempted heist (after the hacker had stolen US$31 million in ethers) and wrote a code to hack the remaining wallet before the hacker could do so:

> "[t]o prevent the hacker from robbing any more banks, the white-hats wrote software to rob all of the remaining banks in the world. Once the money was safely stolen, they began the process of returning the funds to their respective account holders. The people who had their money saved by this heroic feat are now in the process of retrieving their funds."

Mr. Qureshi pointed out that this incident does not reveal problems in Ethereum or in smart contracts in general because the attack vector was created by a developer error in a particular contract. But Mr. Qureshi advised that the blockchain "ecosystem is young and immature… [i]t's going to take a lot of work to develop the training and discipline to treat smart contracts the way that banks treat their ATM software."

The vast majority of the world's banks are exploring ways to incorporate blockchain into their operations. For example, according to a survey of 200 global banks published by the IBM Institute for Business Value and The Economist Intelligence Unit, 15 percent of banks expect to introduce full-scale commercial blockchain solutions in 2017, with others to follow suit – bringing the total to 65 percent of banks by 2020. As the above case study shows, the decentralized nature of blockchain complicates efforts to manage cybersecurity risks. This is because malware or malicious coding in public blockchains are not amenable to computer "patches" or updates to be fixed. If cybersecurity risks are not managed well in blockchain technology which is being increasingly adopted by global banks, the world's banking system may be significantly disrupted if hackers figure ways to exploit attack vectors and remain hidden in the decentralized nature of blockchain.

In light of the risk of faulty developer codes (particularly third party software libraries) which blockchain platforms incorporates, the banking industry and its regulators need to pay particular attention on two key factors: (1) whether hacking penetrations of public blockchain smart contracts can be detected in real-time; and (2) whether banks would have the requisite technical skills and experience to counter such attacks in real-time as the attacks are happening (as in the case study provided above).

#7) Virtual Fiat Currency To Disrupt Fractional Reserve Banking/Lending

Recently the Managing Director of the International Monetary Fund Christine Lagarde warned that cryptocurrencies "can replace national monies, conventional financial intermediation and…puts a question mark on the fractional banking model we know today." She noted that cryptocurrencies "allow for peer-to-peer transactions without central clearinghouses, without central banks." (Emphasis in the original.) Although she was discussing about cryptocurrencies in general, her remarks could equally apply to virtual fiat currencies issued by national governments. They are identical to fiat currencies

used currently except that they exist in virtual form and they do not necessarily need to be issued via a blockchain or DLS.

Some of the world's largest economies are either testing or plans to issue virtual fiat currencies. China will test its virtual renminbi in Shenzhen before rolling the system out country-wide. China is not alone. Russia also announced its goal of launching a virtual ruble, the launch of which is only a matter of time. The U.S. Federal Reserve, the Bank of England, Sweden and Singapore are all exploring ways to issue their respective national digital fiat currency. In another article I have explained the benefits of virtual fiat currencies that attract governments to issue them. For example, economists at the Bank of England have concluded that issuing a digital fiat currency "could permanently boost GDP by as much as 3 percent due to reductions in real interest rates, distortionary taxes, and transaction costs, while also increasing economic stability."

Here the comment letter discusses how virtual fiat currencies will significantly alter the current model of fractional reserve lending.

The modern banking system depends upon the interplay between national central banks and their respective domestic private banks based upon fractional reserve lending. Through this model that uses private banks as intermediaries, central banks attempt to influence the money supply in response to prevailing economic conditions. During recessionary times, central banks in general seek to expand the money supply and vice versa during inflationary times. However the problem with this model is that private banks are risk adverse and often halt lending during recessionary times.

For example, in October 1, 2008 during the last financial crisis, the Libor rate shot to its all time high to 6.9% because all of the world's banks failed to trust each other to justify lending at lower interest rates. The U.S. Federal Reserve and policy-makers were frustrated to see that at a time when money supply expansion was needed to stem the crisis, cash was not flowing to places that needed it. The rise in Libor slowed the U.S. economy at the worst possible time.

The inability of central banks like the U.S. Federal Reserve to directly control the money supply in response to changing macro-economic conditions has been one of the persistent problems with the fractional reserve lending system. If central banks are able to issue digital fiat currencies that can flow through new channels (other than via legacy banks), central banks will be in a better position to control monetary supply and respond more quickly and effectively to the demands of changing economic situations.

According to the Bank of England, central banks currently already issue digital fiat currencies to banks and not to everyone. This is because bank reserves are electronic, and they are used as a final means of settlement between banks. Effectively they are the banks' digital currency. Commercial banks now also issue their own respective digital currency to anyone or entity with a deposit account from a particular bank. According to the Bank of England again, the majority of the money in circulation issued by commercial banks plus the money issued by central banks exist in the form as digital currencies. Excluding transactions in notes, coins and paper checks, all global payments are now made using digital currency.

Therefore, it will not be technically difficult to find ways to issue digital fiat currencies on a national level if banks and central banks are already effectively doing so now. The issuance of digital fiat currencies will create novel ways to influence the money supply (as noted by the Managing Director of the IMF) which needs to be explored by policy-makers.

#8) Accounting Standards Lacking for Digital Assets

Currently there are no generally accepted accounting standards that applies to the measurement of digital assets like cryptocurrencies. If blockchain and other DLT will be incorporated into traditional banking practices, then the critical issue becomes formulating the applicable accounting standards to protect consumers and shareholders' interests. Regulators would also need a binding set of accounting standards to make sense of the digital transactions undertaken by regulated banks so as to comprehend the nature and seriousness of the underlying risks that they entail.

In a June 8, 2017 comment letter to the U.S. Financial Accounting Standards Board ("FASB"), the Chamber of Digital Commerce (the world's largest trade association representing the blockchain industry based in Washington D.C.) requested that FASB add to its agenda a project to address the accounting for digital currencies. Specifically the Chamber asked FASB to address "the recognition (and derecognition), measurement (initial and subsequent), presentation and disclosure for digital currencies".

The Chamber identified four different ways to account for digital currencies under current U.S. GAAP:

- ASC 305, Cash and Cash Equivalents;
- ASC 825, Financial Instruments;
- ASC 350, Intangibles – Goodwill and Other; or
- ASC 330, Inventory.

However, after an exhaustive analysis of the relevance of each of the above methods, the Chamber noted that FASB should develop a new project group to formulate a new standard "to provide guidance that best represents the economic characteristics of digital currencies."

This comment letter recommends that the BIS work in close association with global accounting setting bodies like FASB to produce generally accepted accounting standards for digital assets.

#9) Prudential Standards for Fintech Mergers & Acquisitions

With increasing market entrants into fintech and competition for market shares, experts expect a wave of mergers and acquisitions activities to follow. M&A activities help bring about market efficiencies and consumers' benefit. However, if not managed well, certain M&As may disrupt the banking market for three reasons.

First, Legacy Banks have a very different corporate culture from BigTech and Fintech Firms. This will likely undermine how M&A entities integrate into each other's operations and daily workings. If integration cannot occur seamlessly, then consumers' interest will likely be negatively affected.

Second, firewalls need to be placed so as to segregate traditional banking activities of a Legacy Bank acquired in a M&A deal. It is expected that some BigTech firms will likely buy traditional banks to better develop banking capabilities. The reverse is also true as the market has seen traditional banks form partnerships with Fintech Firms. Fintech Firms and BigTech are not experienced in traditional banking practices. If they are permitted to acquire traditional banks, prudential safeguards require a thorough review of the likely impact or disruption to the banking operations of the ensuing corporate structure and on the overall banking economy. One of the ways to ensure consumers' protection is to require the use of firewalls to segregate traditional banking activities from novel fintech-driven activities pending the successful integration of the two different activities and corporate cultures.

Third, bank regulators need to work with anti-competition regulators to assess the potential monopolistic effects on the general economy of a potential M&A deal. This is because most BigTech firms are very well capitalized and rank as some of the world's most dominant companies in their field of commercial expertise. Some of the Legacy Banks also rank amongst the world's most valuable companies and have extensive roots in the banking system. If a BigTech firm merges with or acquires the substantial assets of

a Legacy Bank (or vice versa), the market may potentially see a dramatic effect in the ensuing combination. It is recommended that bank regulators formulate M&A guidelines that help balance prudential concerns with market efficiencies.

#10) Qualitative-driven Prudential Safeguards

Technology-driven Banking License Requirements

Banks are required to meet quantitative (like fixed capital reserve ratios) and qualitative requirements in order to receive and maintain their banking license or charter established by the relevant regulator. This comment letter recommends that additional technology-driven qualitative prudential safeguards be included in bank licensing requirements.

These new requirements help balance consumers' protection against innovation. For example, licensing requirements should be introduced that are designed to help fintech service providers (whether they are Legacy Banks, Fintech Firms or BigTech) protect their intellectual property ("IP") rights and ensure their continued validity. It is in the interest of both fintech service providers, their investors and consumers to ensure that its IP rights are managed effectively. Otherwise, the service provider would lose its capital, investors would lose their investment and consumers would lose their confidence in the banking sector.

Therefore, IP rights (and not solely reserve ratio requirements) will be determinative of the financial success of any fintech entity. As such, the BIS should consider incorporating five new technology-driven qualitative bank license requirements (explained below).

a) Technology & IP Due Diligence Licensing Requirement

It is near impossible to ask a fintech entity to guarantee that its patent rights do not infringe on any third party rights because questions of infringement are almost always resolved through litigation and settlement. Instead, this requirement mandates the licensee to show to the satisfaction of its regulator that it has complied with all applicable procedural requirements and best practices relevant to the development, invention and commercialisation of its technologies and intellectual property rights (collectively, "Tech-IPs"). The disclosure provided would be publicly available to allow investors and consumers to gauge the scope, nature and perceived quality of the licensee's Tech-IPs.

Specifically, the licensee should make binding representations and warranties as to the following non-exhaustive items:

- list of its issued patents, provisional patents, trademarks, service marks and copyrighted materials with issuing authority;
- whether its issued patents have been substantively reviewed for patentability by the relevant patent office by examining all relevant prior arts, subject matter eligibility, novelty and obviousness;
- whether the export of relevant technologies, data and software complies with applicable export control laws and cross border data privacy laws;
- whether it has duly paid all of its IP maintenance fees (such as annual patent fees) and complied with any upkeep requirements to keep its IP rights valid;
- whether any of its IP rights are or will likely be the subject of any controversy or litigation;
- whether it has protected its IP rights by using confidentiality and invention assignment agreements with current and former employees, founders, owners, consultants and relevant third parties) and whether there are any material exceptions therefrom (such as co-ownership rights retained by such persons);
- whether the licensee possesses and develops any trade secrets (if so, the applicant should list the steps it has taken to preserve their secrecy);
- whether the licensee has received any notice designating its patents as standard-essential and therefore requiring it to license them on a fair and reasonable basis;
- whether the licensee has received any notice requesting it to license standard essential patents;
- a description of the technologies which the licensee owns or has the right to use and their importance to its revenue-generating ability;
- the significance of its Tech-IPs on its bottom line going forward;
- a description of the licensee's licensing transactions involving its Tech-IPs;
- whether the licensee has granted any indemnities to third parties with respect to its Tech-IPs; and
- any liens or encumbrances on its Tech-IPs.

b) Trade Secret Registration Licensing Requirement

One of the most difficult issues for IP owners is providing evidence of its authorship over its trade secrets. By nature, trade secrets must be kept reasonably secret so any publicly disclosed information about its authorship, invention and contents may risk stripping the IP of its trade secret protection. Unlike patents where a central authority issues a publicly accessible document showing authorship and claims, no central authority issues any documentation proving the authorship of trade secrets.

Recently there have been a number of private and public service providers that offer digital fingerprinting systems that would time-stamp a document containing the trade secret with a hash code to help prove its authorship. Licensees should be cautioned to select trade secret registration registrars who are not subject to any conflict of interests or perceived to be biased.

Banking regulators should require regulated entities with trade secrets to register them with a reputable digital registrar, especially one using appropriate cybersecurity controls to ensure that the registration system is being patched and monitored for vulnerabilities on a real-time basis. Such a registration requirement helps protect the value of the licensee's trade secrets (and therefore shareholders' value) in case they become the subject of a controversy.

c) IP Friendly Work Place Certification Licensing Requirement

Many fintech startups and even Legacy Banks work in very open office environments in which persons not bound by any terms and conditions on confidentiality can overhear, see or have physical access to the Tech-IPs of the unsuspecting startup. If this happens, both corporate and shareholders' values are lost.

Bank regulators should require that licensees have all of their work place areas (such as research & development centers and employee cubicle spaces) certified as being Tech-IP friendly, with a further requirement that such certification be renewed at least annually.

The certifying body can be a professional services entity (like an international law firm, auditor, or accounting body) or a non-governmental organization who will examine the following non-exhaustive items:

- whether the glass walls of the licensee's offices or meeting rooms are enabled to be "fogged-up" at the command of the user to keep prying eyes out;
- whether tight printers and office keys access controls exist;
- whether their internet access router, office LAN, critical infrastructure systems (like its manufacturing sites) are duly secured by appropriate cybersecurity control systems;
- whether its employees present in its commons or pantry areas are able to be over-heard chatting by outsiders;
- whether its employees use open WIFI networks maintained by an outsider; and
- whether outsiders have physical access to employees' laptops, storage devices or physical copies of key work products.

d) Chief IP Officer Certification Licensing Requirement

Many fintech entities have a chief financial officer, a chief information security officer or a chief legal & compliance officer. But not many have a chief IP officer who would be responsible for managing, maintaining, training and monetizing the licensee's Tech-IP affairs along with relevant stakeholders. We are already living in an age of tech-driven businesses. It would be irresponsible from a corporate governance perspective not to have an internal chief officer fluent in today and tomorrow's technological and IP trends.

This new licensing requirement has two parts. First, all licensees must appoint a Chief IP Officer to sit on its board of directors and/or its committee(s) as an executive member to lead discussion of any significant Tech-IP matters, business plans, opportunities and risks. If the Chief IP Officer is fired by the issuer or resigns, the issuer must publicly disclose such fact and the reasons therefor to the markets (much like the disclosure in stock exchanges which takes place when an independent auditor is fired or resigns) to allow investors and consumers a chance to gauge the significance of such change. Second, the Chief IP Officer must possess the relevant technical and scientific background, experience and know-how to perform such role. He or she must possess relevant industry certification(s) that must be renewed.

e) Cybersecurity Safeguard Licensing Requirement

It goes without saying that fintech entities are living in an age of rampant cybersecurity attacks. The list of Legacy Banks, Fintech Firms and BigTech who have suffered cyber hacking is growing every quarter. As shown earlier, cyberattacks against blockchains are especially dangerous and more potentially disruptive because there is no viable technological way at the moment to stop a hack on a blockchain other than to beat the hackers real-time in a race to empty out the value stored before the bad guys do so. This is why bank regulators should impose a qualitative licensing requirement mandating that regulated entities appoint at least one independent director with cybersecurity background, knowledge or know-how.

This requirement helps ensures that the board members of regulating banking entities would have the requisite guidance to be able to ask management the right questions about cybersecurity affecting fintech and banking operations. Asking the right questions on cybersecurity sets the best "tone from the top" to push timely and effective cybersecurity controls throughout the regulated entity. Many times, the major stumbling block towards adequate cybersecurity protocols is the regulated's board of directors unfortunately, especially those sitting on the boards of traditional banks. This is natural because most board members come from non-IT or technology backgrounds. Most have probably been

born significantly before the dawning of the "digital age". As such they would not be in the best position to ask management the right questions, absent some independent expert assisting them on the board.

This cybersecurity licensing requirement has three parts.

First, the regulated entity must appoint an independent director with cybersecurity background, knowledge or know-how. Since cybersecurity is a dynamic field (with new attack vectors every month), banking regulators must be flexible in setting the requisite minimum requirements. Setting the requirement too high would make it difficult for the issuer to find and hire an independent director who can meet such standards (considering that there is already a global shortage of qualified cybersecurity professionals). There are several major certification bodies for cybersecurity and infosec, such as CISSP (which is held for example by the current Senior Advisor to the Chairman of the U.S. SEC for Cybersecurity Policy) and GIAC whose certifications banking regulators can consider recognising for purposes of this licensing requirement.

Second, the regulated entity should be permitted to hire an independent cybersecurity advisor to its board of directors if it is unable to retain an independent director satisfying this requirement on a timely or cost-effective basis. Such a regulated entity would need to disclose publicly such fact and undertake to continue to find such a director diligently.

Thirdly, the regulated entity is required to appoint either its Chief Technology Officer or Chief Information Security Officer (or both) to its board of directors as an executive (non-independent) member to assist the board on related matters and provide the internal clout needed for him or her to implement company-wide cybersecurity related controls. This also ensures that the regulated entity's technical IT teams maintain a line of communications directly to the board room to ensure quick cyber incident response actions. The better that an issuer manages its cybersecurity risks, the better its corporate assets and shareholders' value can be safeguarded.

Part III: Conclusion

The near-instant speed of assets transfers (whether in the form of land title deeds, insurance claims, currency or securities) in the future will bring convenience to consumers who are becoming increasingly demanding of shortening transaction times and barriers to a speedy conclusion of their contemplated transaction. Yet such expectations for increased speed and convenience create new issues for prudent banking business and regulation as discussed above.

Seen in this light, the key issue for banks and their regulators will be managing the challenges of near-instantaneous assets transfers against ever increasing consumers' expectations for ever faster speed and easier convenience in conducting banking transactions worldwide.

There are two ways to face the challenges presented by fintech on banking and its regulation: either cut standards which would create a "race to the bottom" mentality or balance the need for innovative products and services that improves the speed and convenience of financial transactions with prudential governance principles, robust consumer' protection and sound risk management.

I welcome the opportunity to speak or work on these issues further with the BIS or any interested regulator worldwide. Please feel free to email me at wt@emergingtechlaw.org

Thank you.

respectfully submitted,

By: /s/ William Ting
William Ting

Copied also to below recipients:

- Board of Governors of the U.S. Federal Reserve System (by email)
International Training and Assistance for Bank Supervisors
BSRInternationalTraining@frb.gov

- The People's Bank of China (by email)
webbox@pbc.gov.cn

- The Central Bank of the Russian Federation (by email)
media@cbr.ru

- Bank of England (by email)
Fintech Accelerator
FinTech@bankofengland.co.uk

- Bank of Japan (by email)

Fintech Center
post.fintech@boj.or.jp

- Monetary Authority of Singapore (by email)

Financial Technology & Innovation Group
fintech_office@mas.gov.sg

- European Central Bank (by email)

info@ecb.europa.eu

- Hong Kong Monetary Authority (by email)

Fintech Facilitation Office
fintech@hkma.gov.hk

- International Monetary Fund (IMF) (by email)

Legislative Affairs
publicaffairs@imf.org

- The U.S. Office of Comptroller of the Currency (by email)

specialpurposecharter@occ.treas.gov

- The Deutsche Bundesbank (by email)

info@bundesbank.de

- The U.S. Commodity Futures Trading Commission, LabCFTC (by email)

LabCFTC@cftc.gov.

- Bank of Canada (by email)

info@bankofcanada.ca

- IEEE.org, Standards Activities (by email)

stds-info@ieee.org

- New York State, Department of Financial Services (by email)

licensing@dfs.ny.gov

- The World Bank (by email)

research@worldbank.org